UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

WELLINGTON DA SILVA GOMES

A ESSÊNCIA DO CONCEITO DE CONFIANÇA PARA A PRESERVAÇÃO DIGITAL:

uma análise nas publicações técnicas do Conselho Nacional de Arquivos

João Pessoa
2024

WELLINGTON DA SILVA GOMES

A ESSÊNCIA DO CONCEITO DE CONFIANÇA PARA A PRESERVAÇÃO DIGITAL:

uma análise nas publicações técnicas do Conselho Nacional de Arquivos

Tese apresentada ao Programa de Pós-Graduação em Ciência da Informação da Universidade Federal da Paraíba como requisito à obtenção do grau de Doutor em Ciência da Informação.

Área de concentração: Informação, Conhecimento e Socieade.

Linha de Pesquisa: Ética, Gestão e Políticas de Informação.

Orientador: Prof. Dr. Edivanio Duarte de Souza.

João Pessoa

2024

Catalogação na publicação
Seção de Catalogação e Classificação

G633e Gomes, Wellington da Silva.
A essência do conceito de confiança para a preservação digital : uma análise nas publicações técnicas do Conselho Nacional de Arquivos / Wellington da Silva Gomes. - João Pessoa, 2024.
359 f. : il.

Orientação: Edivanio Duarte de Souza.
Tese (Doutorado) - UFPB/CCSA.

1. Conceito. 2. Confiança. 3. Conceito de confiança. 4. Conselho Nacional de Arquivos. 5. Preservação digital. 6. Publicações técnicas I. Souza, Edivanio Duarte de. II. Título.

UFPB/BC CDU 161.1(043)

Elaborado por WALQUELINE DA SILVA ARAUJO - CRB-15/514

WELLINGTON DA SILVA GOMES

A ESSÊNCIA DO CONCEITO DE CONFIANÇA PARA A PRESERVAÇÃO DIGITAL:

uma análise nas publicações técnicas do Conselho Nacional de Arquivos

Tese apresentada ao Programa de Pós-Graduação em Ciência da Informação da Universidade Federal da Paraíba, como pré-requisito parcial para obtenção do título de Doutor em Ciência da Informação, em 28 de março de 2024.

BANCA DE DEFESA

_____

Prof. Dr. Edivanio Duarte de Souza – PPGCI/UFPB (Orientador/Presidente)

_____

Profa. Dra. Edna Gomes Pinheiro - PPGCI/UFPB (Titular interno)

_____

Prof. Dr. Gustavo Henrique de Araujo Freire - PPGCI/UFPB (Titular interno)

_____

Prof. Dr. Daniel Flores – ICHCA/UFAL (Titular externo)

_____

Profa. Dra. Thais Helen do Nascimento Santos – PPGCI/UFPE (Titular externo)

_____

Profa. Dra. Maria Cristina Vieira de Freitas – FLUC/UC (Titular externo)

_____

Profa. Dra. Alzira Karla Araújo da Silva – PPGCI/UFPB (Suplente interno)

_____

Profa. Dra. Manuela Eugênio Maia – PPGDARQ/UEPB (Suplente externo)

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

ATA DE DEFESA DE TESE

Defesa nº 102

Ata da Sessão Pública de Defesa de Tese do(a) Doutorando(a) **WELLINGTON DA SILVA GOMES** como requisito para obtenção do grau de Doutor(a) em Ciência da Informação, Área de Concentração em Informação, Conhecimento e Sociedade e com Linha de pesquisa em Ética, Gestão e Políticas da Informação.

Aos vinte e oito dias do mês de março de dois mil e vinte e quatro (28/03/2024), às quinze horas, no formato híbrido (Presencial/remoto), na Sala virtual do Google Meet (meet.google.com/jby-ijgn-vni), reuniu-se a banca examinadora designada pelo Colegiado do Programa de Pós-Graduação em Ciência da Informação para avaliar o(a) candidato(a) ao Grau de Doutor(a) em Ciência da Informação na Área de Concentração Informação, Conhecimento e Sociedade, o(a) doutorando(a) **WELLINGTON DA SILVA GOMES.** A banca examinadora foi composta pelos (as) professores(as): Dr. Edivanio Duarte de Souza – PPGCI/UFPB (Presidente/Orientador), Dra. Edna Gomes Pinheiro – PPGCI/UFPB (Examinadora interna), Dr. Gustavo Henrique de Araújo Freire – PPGCI/UFPB (Examinador interno), Dra. Thais Helen do Nascimento Santos – UFPE (Examinadora externa), Dr. Daniel Flores – UFSM (Examinador externo), Dra. Maria Cristina Vieira de Freitas – UC (Examinadora externa), Dra. Alzira Karla Araújo da Silva –PPGCI/UFPB (Suplente Interna) e Dra. Manuela Eugênio Maia – UEPB (Suplente Externa). Dando início aos trabalhos, o(a) Professor(a) Dr(a). Edivanio Duarte de Souza, Presidente(a) da Banca Examinadora, explicou aos presentes a finalidade da sessão e passou a palavra ao(à) discente para que fizesse oralmente a apresentação do trabalho de tese intitulado: "**O conceito de confiança para a preservação digital: uma análise nas publicações técnicas do Conselho Nacional de Arquivos".** Após a apresentação, o(a) doutorando(a) foi arguido(a) na forma regimental pelos examinadores. Respondidas todas as arguições, o(a) Professor(a) Dr.(a). Edivanio Duarte de Souza, Presidente(a) da Banca Examinadora, acatou todas as observações da banca e procedeu para o julgamento do trabalho, concluindo por atribuir-lhe o conceito:

(x) Aprovado ( ) Insuficiente ( ) Reprovado.

Observações da Banca:
A Banca Examinadora recomendou a publicação da tese, no todo ou em partes, bem como a indicação a premiações.

Proclamados os resultados e encerrados os trabalhos, eu, Professor(a) Dr.(a) Edivanio Duarte de Souza, Presidente da Banca Examinadora, lavrei a presente ata que segue assinada por mim pelos(as) participantes da banca, juntamente com os pareceres de avaliação da tese e da defesa de tese do(a) doutorando(a), devidamente assinados por seus respectivos avaliadores e em formato digital.

João Pessoa, 28 de março de 2024.

Documento assinado digitalmente
gov.br
EDIVANIO DUARTE DE SOUZA
Data: 30/03/2024 17:42:36-0300
Verifique em https://validar.iti.gov.br

Dr. Edivanio Duarte de Souza
Presidente/ Orientador (a) – PPGCI/UFPB

Documento assinado digitalmente
gov.br
EDNA GOMES PINHEIRO
Data: 01/04/2024 10:48:54-0300
Verifique em https://validar.iti.gov.br

Dra. Edna Gomes Pinheiro
Examinador (a) Interno (a) – PPGCI/UFPB

Documento assinado digitalmente
gov.br
GUSTAVO HENRIQUE DE ARAUJO FREIRE
Data: 30/03/2024 18:36:55-0300
Verifique em https://validar.iti.gov.br

Dr. Gustavo Henrique de Araújo Freire
Examinador(a) Interno(a) – PPGCI/UFPB

Documento assinado digitalmente
gov.br
THAIS HELEN DO NASCIMENTO SANTOS
Data: 04/04/2024 20:38:37-0300
Verifique em https://validar.iti.gov.br

Dra. Thais Helen do Nascimento Santos
Examinador (a) Externo (a) – UFPE

Documento assinado digitalmente
gov.br
DANIEL FLORES
Data: 02/04/2024 09:24:58-0300
Verifique em https://validar.iti.gov.br

Dr. Daniel Flores
Examinador (a) Externo (a) – UFSM

Assinado por: **Maria Cristina Vieira de Freitas**
Num. de Identificação: 31211703
Data: 2024.04.08 15:25:32 +0100

Dra. Maria Cristina Vieira de Freitas
Examinador(a) Externo (a) – UC

Documento assinado digitalmente
gov.br
MANUELA EUGENIO MAIA
Data: 30/03/2024 19:26:11-0300
Verifique em https://validar.iti.gov.br

Dra. Alzira Karla Araújo da Silva
Suplente Interno(a) –PPGCI/UFPB

Dra. Manuela Eugênio Maia
Suplente Externo (a) – UEPB

Documento assinado digitalmente
gov.br
WELLINGTON DA SILVA GOMES
Data: 04/04/2024 21:45:25-0300
Verifique em https://validar.iti.gov.br

Wellington da Silva Gomes
Doutorando(a)

AGRADECIMENTOS

Primeiro, à minha mãe, cujo amor e apoio incondicional foram a minha força motriz durante esta jornada. Sua fé em mim nunca vacilou, mesmo nos momentos mais desafiadores.

Aos meus filhos e super companheiros felinos, Theodoro Gomes Perrayon e Bartholomeu Gomes Perrayon, agradeço por serem uma fonte constante de conforto e de alegria. Vocês trouxeram um toque de leveza aos meus dias mais estressantes.

A todos os meus amigos, agradeço por estarem sempre ao meu lado, em especial a Marcelo Dias Perrayon, por cada risada compartilhada, cada palavra de encorajamento, cada momento juntos e cada madrugada de conversas, contribuindo para reforçar a minha determinação, mesmo nos dias mais turbulentos.

À minha orientadora, Professora Marynice de Medeiros Matos Autran, agradeço por sua orientação incansável e por acreditar em mim e no meu trabalho. Sua sabedoria e sua paciência foram fundamentais para o meu crescimento acadêmico.

Ao meu orientador, Professor Edivanio Duarte de Souza, agradeço pelo investimento em mim e em minha formação. Sua perspicácia e seu conhecimento são essenciais para a conclusão desta tese.

Agradeço a todos que fizeram parte desta tese, direta ou indiretamente; a esses os meus mais sinceros obrigado.

RESUMO

Vivemos num mundo onde a obsolescência tecnológica está cada vez mais vigente, aferindo a vida útil da informação no ambiente digital. Tal problemática tem causado adversidades aos documentos, podendo torná-los inelegíveis, e, consequentemente, inacessíveis; sendo necessário apropriar-se dos preceitos de preservação para garantir a longevidade desses insumos. Quando se trata do espaço digital, o ato de confiar pode ser representado, entre outros fatores, pela preservação digital. Ademais, há uma escassez de publicações brasileiras sobre o conceito de confiança, tanto no campo da Ciência da Informação, quanto no da Arquivologia. Em nossos escritos, o significado de confiança está espelhado nos documentos das Publicações Técnicas do Conselho Nacional de Arquivos. Esses registros trazem diretrizes e recomendações de boas práticas, projetando elementos e critérios que caracterizam a autenticidade documental. Dessa forma, o objetivo deste estudo foi analisar o conceito de confiança nas Publicações Técnicas do Conselho Nacional de Arquivos de preservação digital. Para alcançar este fim, foram estabelecidos os seguintes objetivos específicos: compreender o conceito de confiança na perspectiva da Filosofia e da Sociologia para assim analisar os aspectos de confiança das Publicações Técnicas citadas; examinar, nessas Publicações, os elementos de confiança; relacionar o conceito de confiança aos elementos de confiança identificados nas Publicações Técnicas de preservação digital; apresentar que essas Diretrizes, no âmbito da preservação digital, trazem garantia de confiança à informação e ao documento de arquivo. Metodologicamente, esta pesquisa foi de natureza teórica, qualitativa, documental e descritiva, como forma de pormenorizar o significado do conceito de confiança e relacioná-lo às Publicações em questão. Em relação ao método, foi empregada a Teoria do Conceito de Dahlberg e o paradigma indiciário como base interpretativa, buscando compreender a essência do conceito de confiança numa óptica sociológico-filosófica. Para isso, foram analisados os elementos de confiança de cada Publicação Técnica, concatenando-os aos postulados do nosso Referencial Teórico acerca do conceito de confiança. Como resultado, ficou constatado que os elementos de confiança: enunciados, características e definições nas Publicações citadas estão intimamente ligados ao conceito de confiança em sua essência, ou seja, suas definições, enunciados e características mais longíquas. Logo, compreender a confiança em sentido substancial foi uma questão necessária para comprovar que as diretrizes e as recomendações de preservação digital do Conselho Nacional de Arquivos trazem garantia de confiança à informação, e, consequentemente, ao documento de arquivo.

Palavras-chave: conceito; confiança; conceito de confiança; Conselho Nacional de Arquivos; preservação digital; publicações técnicas.

ABSTRACT

We live in a world where technological obsolescence is increasingly prevalent, measuring the useful life of information in the digital environment. This problem has caused adversity to documents, potentially making them ineligible and, consequently, inaccessible; It is necessary to adopt preservation precepts to guarantee the longevity of these inputs. When it comes to the digital space, the act of trust can be represented, among other factors, by digital preservation. Furthermore, there is a scarcity of Brazilian publications on the concept of trust, both in the field of Information Science and Archival Science. In our writings, the meaning of trust is mirrored in the documents in the Technical Publications of the National Archives Council. These records provide guidelines and recommendations for good practices, projecting elements and criteria that characterize documentary authenticity. Therefore, the objective of this study was to analyze the concept of trust in the Technical Publications of the National Council of Digital Preservation Archives. To achieve this end, the following specific objectives were established: understand the concept of trust from the perspective of Philosophy and Sociology in order to analyze the trust aspects of the aforementioned Technical Publications; examine, in these Publications, the elements of trust; relate the concept of trust to the elements of trust identified in Technical Publications on digital preservation; present that these Guidelines, within the scope of digital preservation, bring a guarantee of trust to information and archival documents. Methodologically, this research was theoretical, qualitative, documentary and descriptive in nature, as a way of detailing the meaning of the concept of trust and relating it to the Publications in question. Regarding the method, Dahlberg's Concept Theory and the evidentiary paradigm were used as an interpretative basis, seeking to understand the essence of the concept of trust from a sociological-philosophical perspective. To this end, the trust elements of each Technical Publication were analyzed, linking them to the postulates of our Theoretical Framework regarding the concept of trust. As a result, it was found that the elements of trust: statements, characteristics and definitions in the cited Publications are closely linked to the concept of trust in its essence, that is, its more distant definitions, statements and characteristics. Therefore, understanding trust in a substantial sense was a necessary issue to prove that the guidelines and recommendations for digital preservation from the National Archives Council bring a guarantee of trust to the information, and, consequently, to the archival document.

Keywords: concept; trust; concept of trust; National Archives Council; digital preservation; technical publications.

LISTA DE FIGURAS

Figura 1 – Triângulo do conceito 36
Figura 2 – Guarda-chuva da proteção documental 78
Figura 3 – Cadeia de custódia de documentos arquivísticos analógicos 89
Figura 4 – Cadeia de Custódia Digital Arquivística 92
Figura 5 – Ambientes informatizados para gestão, preservação e acesso 93
Figura 6 – Interoperabilidade do Sigad com o RDC-Arq 97
Figura 7 – Cenário de uso no ciclo de vida total dos documentos de um RDC-Arq em interação com um Sigad 99
Figura 8 – Uso do RDC-Arq na fase permanente dos documentos 100
Figura 9 – Uso simultâneo de armazenamento em sistema de *storage* e de RDC-Arq 100
Figura 10 – Interoperabilidade entre sistema de négocio-Sigad-RDC-Arq 101
Figura 11 – Sistema de negócio, com requisitos do Sigad, interopera com RDC-Arq 102
Figura 12 – Os papéis de administrador de preservação e de TI em uma plataforma de preservação 103
Figura 13 – Exemplos de sistemas de comunicação 117
Figura 14 – Exemplo de sistemas 119
Figura 15 – Elementos da Teoria Geral dos Sistemas na Preservação Digital Sistêmica 126
Figura 16 – A Fábrica Inteligente da Indústria 4.0 135
Figura 17 – Integração da cadeia de valores 135
Figura 18 – Os nove pilares da Indústria 4.0 137
Figura 19 – 6 Vs do *Big Data* 138
Figura 20 – Digitalização x digitalização com digitalização com digitização 143
Figura 21 – Cinco domínios da TD 144
Figura 22 – Do Governo Eletrônico ao Governo Digital 155
Figura 23 – 10 passos para a TD 156
Figura 24 – Seis diretrizes da EGD 2020-2023 157
Figura 25 – Indicadores da EGD 2020-2023 159
Figura 26 – Ferramentas da TD 162
Figura 27 – Modelo lógico da E-Digital 164

Figura 28 – Matriz da organização e da relação dos eixos temáticos 165
Figura 29 – Eixos da Transformação Digital 166
Figura 30 – Marcos mais recentes da TD na Paraíba 169
Figura 31 – Quatro eixos da do Programa Justiça 4.0 170
Figura 32 – Estrutura intelectual do InterPARES 2 208
Figura 33 – Estudos gerais e de caso do InterPARES 2 212
Figura 34 – Forma documental e suas características essenciais 235
Figura 35 – Continuação dos conjuntos de “Requisitos A” do Apêndice A 243
Figura 36 – Conjunto de Requisitos de Base 244
Figura 37 – Tabela com os elementos a serem cumpridos por um Sigad nos Requisitos Funcionais e Não Funcionais 272
Figura 38 – Ficha com o preenchimento dos metadados na seção de Metadados do e-ARQ Brasil 2022 273
Figura 39 – Diagrama de organização dos documentos 274
Figura 40 – Organização do esquema de metadados do e-ARQ Brasil 2022 277
Figura 41 – Entidades funcionais do modelo OAIS 284
Figura 42 – Informação a partir dos dados 285
Figura 43 – Conceitos e relacionamentos do pacote de informação 286
Figura 44 – Fluxo de auditoria e de certificação 292

LISTA DE QUADROS

Quadro 1 – Elementos dos conceitos de confiança extraídos das Publicações Técnicas do Conarq sobre preservação digital 37
Quadro 2 – Síntese dos elementos do conceito de confiança 37
Quadro 3 – Síntese dos conceitos e das definições de confiança extraídos das Publicações Técnicas do Conarq sobre preservação digital 38
Quadro 4 – Características da confiança 59
Quadro 5 – Os dez pontos do conceito de confiança de Guiddens 66
Quadro 6 – Fases da TD 142
Quadro 7 – Princípios e diretrizes da Lei nº. 14.129/2021 167
Quadro 8 – Domínios do InterPARES 1 181
Quadro 9 – Estrutural intelectual da Relatório da Força-tarefa de Estratégia 205
Quadro 10 – Elementos do conceito de confiança extraídos da Carta para a Preservação do Patrimônio Arquivístico Digital 228
Quadro 11 – Recursos de Preservação do Projeto Interpares 1 e 2 229
Quadro 12 – Elementos do conceito de confiança extraídos das Diretrizes do Produtor 240
Quadro 13 – Elementos do conceito de confiança extraídos das Diretrizes do Preservador 252
Quadro 14 – Elementos do conceito de confiança extraídos da Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais 256
Quadro 15 – Características dos documentos arquivísticos à luz do e-ARQ Brasil - versão 2 263
Quadro 16 – Elementos do conceito de confiança extraídos do e-ARQ Brasil - versão 2 278
Quadro 17 – Requisitos para um repositório digital confiável 289
Quadro 18 – Elementos do conceito de confiança extraídos das Diretrizes para a Implementação de Repositórios Arquivísticos Digitais Confiáveis – RDC-Arq - versão 2 294
Quadro 19 – Síntese dos conceitos e definições de confiança extraídos das seis Publicações Técnicas do Conarq de preservação digital 297

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AIP	Pacote de Informação de Arquivo
AMP 2.0	*Accelerating US Advanced Manufacturing*
AMP	*Advanced Manufacturing Partnership*
ANPD	Autoridade Nacional de Proteção de Dados
BDR	*Business-Driven Recordkeeping*
BDTD	Biblioteca Digital Brasileira de Teses e Dissertações
BPC	Benefício de Prestação Continuada
Brapci	Base de Dados em Ciência da Informação
CCD	Código de Classificação de Documentos
CCDA	Cadeia de Custódia Digital Arquivística
CCSDS	*Consultative Committee for Space Data Systems*
CDESS	Conselho de Desenvolvimento Econômico Social Sustentável
CE	Comissão Europeia
Cege	Comitê Executivo de Governo Eletrônico
CEN	Comitê Europeu de Normalização
CGG	Comitê Gestor de Governança
CIA	Conselho Internacional de Arquivos
CJF	Conselho da Justiça Federal
CNI	Confederação Nacional da Indústria
CNJ	Conselho Nacional de Justiça
Conarq	Conselho Nacional de Arquivos
CoP	*Chain of Preservation*
CPA/RLG	Comissão de Preservação e Acesso/Grupo de Pesquisa de Bibliotecas
CPS	Sistemas Ciberfísicos
CSTJ	Conselho Superior da Justiça do Trabalho
CTDE	Câmara Técnica de Documentos Eletrônicos
Cura	Alianças de Pesquisa Comunidade-Universidade
DataJud	Base Nacional de Dados do Poder Judiciário
DIP	Pacotes de Informação e Disseminação
DLT	*Distributed Ledger Technology*
DoD	Departamento de Defesa

EAD	Descrição arquivística codificada
ECM	*Enterprise Content Management*
E-Digital	A Estratégia Brasileira para a Transformação Digital
EGD	Estratégia de Governo Digital
e-Gov	Governo Eletrônico
EGTI	Estratégia Geral de Tecnologia da Informação
Enap	Escola Nacional de Administração Pública
e-PMG	Grupo de Trabalho de Padrão de Metadados do Governo Eletrônico
GED	Sistemas de Gerenciamento Eletrônico
Gigo	*Garbage-in, Garbage-out*
GTTI	Grupo de Trabalho em Tecnologia da Informação
IA	Inteligência Artificial
ICPSR	O Consórcio Interuniversitário para Pesquisa Política e Social
IDEF (0)	Definição de Integração para Modelagem de Função
IES	Instituições de Ensino Superior
IGI	Índice Global de Inovação
InterPARES	*International Research on Permanent Authentic Record in Eletronic Systems*
IoT	*Internet of Things*
ISAAR (CPF)	Norma Internacional de Registro de Autoridade Arquivística para Entidades Coletivas, Pessoas e Famílias
ISAD(G)	Norma Geral Internacional de Descrição Arquivística
ISDF	Norma Internacional para Descrição de Funções
ISDIAH	Norma Internacional para Descrição de Instituições com Acervo Arquivístico
ISO	Organização Internacional para Padronização
KAMS	*Korea Advanced Manufacturing System*
Lavid	Laboratório de Aplicações de Vídeo Digital
LGPD	Lei Geral de Proteção de Dados
Libras	Língua Brasileira de Sinais
Madras	Padrão de Metadados, Descrição Arquivística de Documentos e Sistema de Análise
MAT	*Multilingual Archival Terminology*

MCP	Modelo da Cadeia de Preservação
MEC	Ministério da Educação
METS	Padrão de codificação e transmissão de metadados
MGDN	Modelo de Gerenciamento das Diretrizes de Negócio na Gestão de Documentos
MGI	Ministério da Gestão e da Inovação em Serviços Públicos
Modelo OAIS	*Reference Model for an Open Archival*
MoReq	Modelo de Requisitos para a Gestão de Arquivos Eletrônicos
MoreqJus	Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário
Nara	*National Archives and Records Administration*
Nobrade	Norma Brasileira de Descrição Arquivística
OAI-PMH	Protocolo para coleta de metadatos
OCLC	*Online Computer Library Center*
ODS	Objetivos de Desenvolvimento Sustentável
OMPI	Organização Mundial da Propriedade Intelectual
ONU	Organização das Nações Unidas
PCD	Plano de Classificação de Documentos
PDPJ-Br	Plataforma Digital do Poder Judiciário Brasileiro
PDS	Preservação Digital Sistêmica
PJE	Processo Judicial Eletrônico
PNUD	Programa das Nações Unidas para o Desenvolvimento
Premis	*Preservation Metadata: Implementation Strategies*
Proname	Programa Nacional de Gestão Documental e Memória do Poder Judiciário
RDC-Arq	Repositórios Arquivísticos Digitais Confiáveis
RLG	*Research Libraries Group*
SAAI	Modelo de referência para um Sistema Aberto de Arquivamento de Informação
Saesp	Sistema de Arquivos do Estado de São Paulo
Siespj	Sistema de Estatística do Poder Judiciário
Sigad	Sistema Informatizado de Gestão Arquivística de Documentos
Sigepe	Sistema de Gestão de Pessoas do Poder Executivo Federal
Sinapses	Plataforma nacional de armazenamento, treinamento supervisionado,

	controle de versionamento, distribuição e auditoria dos modelos de Inteligência Artificial
Sinar	Sistema Nacional de Arquivos
SinDigital	Sistema Nacional para a Transformação Digital
SIP	Pacote de Submissão de Informação
SISP	Sistema de Administração dos Recursos de Tecnologia da Informação
Soge	Sistema da Ouvidoria Geral do Estado
SSHRC-CURA	Conselho de Pesquisa em Ciências Sociais e Humanas das Alianças de Pesquisas Comunidade-Universidade do Canadá
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TCU	Tribunal de Contas da União
TD	Transformação Digital
TDICs	Tecnologias Digitais da Informação e da Comunicação
Team	*Theoretical Elaborations into Archival Management*
TEDGI	Coleta de Dados de Elemento de Modelo
TGS	Teoria Geral dos Sistemas
TI	Tecnologia da Informação
TIC	Tecnologias da Informação e da Comunicação
TJPB	Tribunal de Justiça da Paraíba
TJRO	Tribunal de Justiça de Rondônia
Trac	*Trustworthy Repository Audit and Certification: Criteria and Checklist*
TSE	Tribunal Superior Eleitoral
TTDD	Tabela de Temporalidade de Destinação de Documentos
UBC	University of British Columbia
UBC-DoD	Universidade de British Columbia e Departamento de Defesa dos EUA
UFPB	Universidade Federal da Paraíba
UM	Modelo Unificado
Unesco	Organização das Nações Unidas para a Educação, a Ciência e a Cultura
Unicamp	Universidade Estadual de Campinas

SUMÁRIO

1 INTRODUÇÃO 18
2 PERCURSO METODOLÓGICO 28
2.1 O MÉTODO UTILIZADO 31
2.2 A TEORIA DO CONCEITO DE DAHLBERG 32
3 O CONCEITO DE CONFIANÇA 39
3.1 AS PERSPECTIVAS VIGENTES DO CONCEITO DE CONFIANÇA 52
3.2 A CONFIANÇA COMO PRINCÍPIO 72
4 PRESERVAÇÃO DIGITAL: HISTÓRICO 77
4.1 CONCEITOS BASILARES DA PRESERVAÇÃO DIGITAL 81
4.2 A TRILHA PARA A PRESERVAÇÃO DIGITAL SISTÊMICA 84
4.2.1 Cadeia de Custódia Arquivística (ininterrupta) 88
4.2.2 Cadeia de Custódia Digital Arquivística 90
4.2.3 A Preservação Digital Sistêmica 95
5 A TEORIA DE SISTEMAS COMO FUNDAMENTO DA PRESERVAÇÃO DIGITAL 108
5.1 BASES DA TEORIA DE SISTEMAS NA COMPREENSÃO DA REALIDADE 109
5.2 PARÂMETROS DA TEORIA GERAL DE SISTEMAS NA PRESERVAÇÃO DIGITAL SISTÊMICA 113
6 A QUARTA REVOLUÇÃO, A INDÚSTRIA 4.0 E A TRANSFORMAÇÃO DIGITAL: QUE TEM EM COMUM? 128
6.1 A INDÚSTRIA 4.0 134
6.2 TRANSFORMAÇÃO DIGITAL: TECNOLOGIAS EMERGENTES, DISRUPTIVAS E SUSTENTADAS 140
6.3 TRANSFORMAÇÃO DIGITAL NO BRASIL A PARTIR DA ÓPTICA GOVERNAMENTAL 152
6.3.1 A Estratégia Brasileira para a Transformação Digital 161
6.3.2 O Programa Justiça 4.0 169
7 O PROJETO INTERPARES: OS PRIMEIROS ESTUDOS DE REFERÊNCIA CONCEITUAL E METODOLÓGICA À PRESERVAÇÃO DIGITAL 178
7.1 O PROJETO INTERPARES 1 180

7.1.1 Relatório da Força-tarefa de Autenticidade 182
7.1.2 Relatório da Força-tarefa de Avaliação 190
7.1.3 Relatório da Força-tarefa de Preservação 197
7.1.4 Relatório da Força-tarefa de Estratégia 203
7.2 O PROJETO INTERPARES 2: A EXPERIÊNCIA INTERATIVA E DINÂMICA 207
7.3 O PROJETO INTERPARES 3: PRESERVAÇÃO EM ORGANIZAÇÃO DE PEQUENO E MÉDIO PORTE 217
7.4 O PROJETO INTERPARES 4 (CONFIANÇA E CONFIABILIDADE) 221
8 DESCRIÇÃO DAS PUBLICAÇÕES TÉCNICAS DE PRESERVAÇÃO DIGITAL DO CONSELHO NACIONAL DE ARQUIVOS 225
8.1 CARTA PARA A PRESERVAÇÃO DO PATRIMÔNIO PÚBLICO ARQUIVÍSTICO DIGITAL 226
8.2 DIRETRIZES DO PRODUTOR. A ELABORAÇÃO E A MANUTENÇÃO DE MATERIAIS DIGITAIS: DIRETRIZES PARA INDIVÍDUOS 229
8.3 DIRETRIZES DO PRESERVADOR. A PRESERVAÇÃO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS: DIRETRIZES PARA ORGANIZAÇÃO 241
8.4 DIRETRIZES PARA A PRESUNÇÃO DE AUTENTICIDADE DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS 253
8.5 MODELO DE REQUISITOS PARA SISTEMAS INFORMATIZADOS DE GESTÃO ARQUIVÍSTICA DE DOCUMENTOS – E-ARQ BRASIL 257
8.6 DIRETRIZES PARA A IMPLEMENTAÇÃO DE REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS – RDC-ARQ 280
9 RESULTADOS E DISCUSSÃO 296
10 CONSIDERAÇÕES FINAIS 312
REFERÊNCIAS 320
APÊNDICE A – PUBLICAÇÕES TÉCNICAS DO CONARQ SOBRE PRESERVAÇÃO DIGITAL 339
APÊNDICE B – SÍNTESE DOS ELEMENTOS DO CONCEITO DE CONFIANÇA 340

1 INTRODUÇÃO

Com a emergência das Tecnologias Digitais da Informação e da Comunicação (TDIC), a análise sobre esses insumos passaram a ter uma óptica diferenciada pelas áreas científicas, causando modificações na realidade humana, sobretudo, direcionadas à dinamização do conhecimento.

Nessa época do Pós-Segunda Guerra e da Guerra Fria ficou nítido o avanço das tecnologias em vários setores e os resultados desses acontecimentos foram procedentes do desenvolvimento técnico-econômico, sendo um dos pontos centrais para a aproximação das diversas áreas do saber (Castells, 1999). Freire e Freire (2009) corroboram com isso ao considerar que a ciência em sua contemporaneidade tornou-se a principal forma de conhecimento, fundando a base para que tecnologias digitais transformassem os meios de produção e por isso deve ser vista como uma estrutura que atende às necessidades de organização da sociedade, seja entre seu sistema de comunicação, econômico ou tecnológico.

Quanto às TDIC, direcionam-se aos recursos associados ao meio digital e às pessoas, por meio de arquétipos, de dispositivos, de equipamentos e de programas, visando facilitar a comunicação de seus integrantes na otimização e na difusão da informação. Sobre esse entendimento, há, prioritariamente, o uso do computador e da *Internet* como instrumentos essenciais, dicotomizando-as das Tecnologias da Informação e da Comunicação (TIC), que não utilizam o ambiente digital de maneira exclusiva.

No contexto das Ciências Sociais Aplicadas, as TDIC contribuíram não só para o progresso, mas também à sua visibilidade frente às áreas já consolidadas. A Arquivologia e a Ciência da Informação, analogamente, fazem-se presentes neste sentido, uma vez que apreenderam métodos, técnicas e teorias à assimilação dos seus estudos.

Hodiernamente, vive-se imerso no mundo *Web*, onde existe a necessidade de transição dos registros convencionais para o ambiente digital, pois, com subsídio dos *hardware* e dos *software*, vêm possibilitando de forma cada vez mais confiável a interação com as pessoas. Porém, do ponto de vista técnico surgem lacunas, substancialmente em termos da obsolescência tecnológica. Esses problemas podem levar à ilegibilidade de informações, à impossibilidade de acesso e, consequentemente, ao desaparecimento dos objetos digitais, sendo necessário apropriar-se dos preceitos da preservação para garantir a autenticidade e a certificação de confiabilidade a longo prazo. Essas mudanças alteram também os métodos aplicados aos arquivos, exigindo a ampliação do conhecimento de seus profissionais para a utilização de ferramentas na realização de atividades laborais com duas finalidades: assegurar

a autenticidade da informação e facultar acesso. Assim, torna-se imprescindível identificar e compreender quais são os elementos de confiança direcionados aos registros digitais, no intuito de perceber a urgência de preservá-los às gerações futuras.

No escopo da Arquivologia, o ato de confiar pode ser representado pela Gestão de Documentos, que engloba, entre outros mecanismos, o controle e a orientação dada aos documentos de arquivo, desde antes de sua gênese; pelo próprio documento de arquivo e as suas características, tornando-o diferente dos demais tipos de registros; pela Diplomática, na identificação da veracidade do documento, por meio da análise de seus elementos internos e externos, além do contexto que esteja inserido; e para esta pesquisa, especificamente, pela preservação digital, tendo como objetivo a proteção e a manutenção do documento por um processo sistêmico, que atravessa a criação, a transmissão e o acesso (numa cadeia que precisa ser ininterrupta) pelo tempo que for necessário.[1]

Compreender o conceito de confiança requer uma observação nuançada de como ele se põe em outras áreas. Sua dinâmica é estudada pela Filosofia, pelo Direito, pela Psicologia e pela Sociologia, entre outras areás, e nos mais diversos sistemas sociais. Seu princípio advém das vontades entre as partes como um contrato que, em tese, beneficiaram-nos. Tais partes podem ser representadas por indivíduos, por sistemas de informação, por regras, por normas, entre outros elementos em que haja uma súmula entre os envolvidos.

A confiança, no sentido mais amplo de fé nas próprias expectativas, é um fato básico da vida social. Claro, em muitas situações, o ser humano pode, em certos aspectos, decidir se concede confiança ou não. Mas fato é que a base das relações provém da possibilidade de confiar, que é uma característica natural do mundo e parte dos limites dentro dos quais se vive cotidianamente, embora não seja um componente intencional, portanto, variável da experiência (Luhmann, 1996, tradução nossa).

Em um viés jurídico, na teoria da confiança, a vontade declarada só prevalece em caso de conflito com a vontade real; somente substitui a vontade inexistente quando o destinatário tiver suscitado um grau elevado de confiança e levando em consideração as circunstâncias objetivas do caso, tenha acreditado na normalidade da declaração, atuando com fundamento na crença legítima (Ráo, 1994). No realce dessa afirmação, a teoria da confiança suscita a ideia de crença como uma referência de acordo e de resolução de conflito, atuando como ponto de mediação entre os envolvidos, ou seja, ela traz o entendimento que serve para

[1] O fato é que a confiança na área da Arquivologia não se esgota nas temáticas do parágrafo exposto; contudo, na perspectiva desta tese, compreende-se que semelhantes temas compõem-se como os principais elementos que trazem o *status* do que significa confiar.

abrandar divergências. Confiar pressupõe bem mais a boa vontade do outro que simplesmente crer que sua palavra é verdadeira.

Ketzer (2015) reitera a confiança como uma relação que envolve obrigações e direitos. Quando se confia, reconhece-se a competência e a autoridade do falante; é responsabilidade do ouvinte realizar este reconhecimento. Caso o falante não cumpra o que se espera dele, há uma atitude de ressentimento por parte do ouvinte. Confiar é o tipo de laço social que pode ser um indicador de sucesso nas relações interpessoais.

A autora acrescenta que a confiança possui duas dimensões: uma normativa e uma descritiva, denominada fiar-se *(rely).* Confiança (*trust*) é a camada mais profunda e origina-se das relações interpessoais, pressupondo entrega e boa vontade por parte dos envolvidos em uma relação em que o sujeito espera sinceridade e reciprocidade, mas, se isso não acontece, a sensação é de traição; já fiar-se (*rely*) é mais "simples", caracteriza-se pela relação que o sujeito estabelece com o mundo e com as coisas dele. Quando a fiabilidade (*reliability*) não se efetiva no mundo, a sensação que se tem é apenas de desapontamento (Ketzer, 2015).

Ketzer (2015) destaca dicotomias entre essas duas formas de confiar. A (1) confiança *(trust)* é um tipo de relação interpessoal estabelecida entre seres humanos; pressupõe boa vontade das partes e envolve a promessa daquele que é confiado em corresponder à confiança que lhe foi depositada, refletindo uma relação explícita. Se esse tipo de confiança se rompe, a sensação é de traição, entretanto isso não compromete a relação com o mundo, se não com aquela pessoa que rompeu a relação. A (2) fiabilidade *(reliability)* torna possível a instituição da moralidade na sociedade, na tentativa de eliminar os riscos de algo, por meio de reflexão racional; é o que confere *status* de evidência a alguma coisa.

Fiar-se *(rely)* é o tipo de relação que torna a moralidade possível, uma vez que possibilita relações sociais básicas, como a sinceridade e o cumprimento de regras de convívio. As pessoas, em geral, por exemplo, não estão mentindo quando dão informações, não vão violar os corpos quando saem às ruas, e assim por diante, porque fiam-se no funcionamento do mundo. Percebe-se que essas duas referências podem ser afinadas, visto que se vive sobre condutas no mundo real, as quais envolvem acreditar nas pessoas, de forma direta ou indireta, e que elas vão cumprir seus acordos.

Vale destacar que o conceito de confiança na Ciência da Informação e, principalmente, na Arquivologia possui um espaço ainda incipiente, quando direcionado a uma perspectiva teórica. Então, falar em preservação digital, neste domínio, na época presente, é saltar os muros das suas conhecidas "estratégias", ligadas à preservação física, lógica e intelectual que envolvem o cuidado básico com a migração da informação e do suporte para questões de

políticas mais ativas como o financiamento e a escolha de padrões, de normas, de definição de metadados e de infraestrutura técnica, compreendo o documento num processo sistemático, em o todo seu ciclo.

Assim, quando se pensa em gerenciamento, isto é, em criação, em armazenamento, em controle, em proteção, em difusão e em acesso, recorre-se à ideia de que a preservação necessita de tecnologias e de esquemas robustos para gerar confiança ao documento. Na Arquivologia, esses dispositivos, para fins desta tese, podem ser representados pelas Publicações Técnicas do Conselho Nacional de Arquivos (Conarq) com foco na preservação digital, as quais trazem recomendações importantes que descrevem condutas para que tecnologias arquivísticas sejam consideradas confiáveis a longo prazo.

Fia-se que a preservação digital possui forte influência das TDIC por estar localizada no seio do ambiente digital e por compreender procedimentos que demandam *knowhow* de profissionais especializados, como aqueles que possibilitam a criação e a utilização de diretrizes, de *hardware* e de *software* específicos.

Direcionando esse pressuposto aos documentos de arquivo, a preservação sem a assistência do conhecimento e das técnicas arquivísticas deteria lacunas, sobretudo, porque tal objeto possui particularidades de gerenciamento e precisa resguardar suas características, isto inclui, obrigatoriamente, as três idades documentais, corrente, intermediária e permanente, seja por um processo de transformação digital ou para os documentos nato-digitais. Representada, pioneiramente, com objetivos arquivísticos, a preservação digital apareceu nos estudos do Conselho Internacional de Arquivos (CIA), já nos idos de 1960 (Arellano, 2008).

Na atualidade, nos cenários nacional e internacional, são os órgãos, são as universidades e suas produções, que dão vazão a este entendimento sobre confiança relacionada à informação. Internacionalmente, como um dos principais representantes das pesquisas sobre preservação digital para os arquivos, têm-se o CIA e o projeto *International Research on Permanent Authentic Record in Eletronic Systems* (InterPARES); e no Brasil, o Conarq.

Ademais, por trás dos grupos de estudos e das agências políticas que criam condutas de/para confiança, encontra-se um segmento maior a ser refletido, isto faz pensar em torno de um campo mais abrangente do que significa confiança e de como ela se relaciona com a Arquivologia. Contudo, por meio das fontes de informações e dos veículos científicos, percebe-se a escassez de pesquisas sobre semelhante conceito na literatura nacional da Ciência da Informação e da Arquivologia. Contudo, identifica-se uma maior ênfase dada ao significado de confiança quando posta à égide das Publicações Técnicas do Conarq e pelos

estudos que envolvem os repositórios digitais e as estratégias de preservação.

A observação desta pesquisa foi direcionada ao conceito de confiança, subsidiada pelo Método Indicários e, sobretudo, pela Teoria do Conceito de Dahlberg (1978), a fim de compreender como esse fenômeno se manifesta nas Publicações Técnicas do Conarq de preservação digital. Tal conceito torna-se importante a partir do momento em que se reputa o foco da preservação digital como um recurso de confiança à informação.

Desde que a humanidade foi capaz de pensar e de externar sua fala, empregou palavras para designar as coisas e assim decodificar pensamentos formulados sobre si mesmo; e, por meio dessa forma verbal, é que se fizeram entender pelos seus semelhantes (Dalhberg, 1978). Assim, graças à comunicação houve o progresso das sociedades, fato que possibilitou a interação humana como todo o mundo. Dahlberg (1978) reforça que esse processo de crescimento há de perdurar enquanto o homem existir sobre a terra e utilizar a linguagem como expressão de seus pensamentos.

Criar conceitos pode se equiparar a um conjunto de fragmentos que serve para reunir partes e representar uma totalidade. Essa formação se concebe por meio da compilação de enunciados a respeito de um determinado objeto, o qual se pode dar o nome de palavras ou de vocábulos, também conhecidos por signos ou símbolos linguísticos. Em síntese, todo enunciado sobre um objeto contém elementos do respectivo conceito e esses elementos são chamados de características ou atributos predicáveis. O nome dado a este processo é análise do conceito.

A confiança é abordada a partir de variadas perspectivas; é um conceito indispensável quando se pensa o ser humano vivendo em sociedade e interagindo com outros sujeitos, o que auxilia a pensar na política e a na cooperação social como um mecanismo de redução de complexidade. Porém, permanece longe de possuir um único enunciado e, por isso, buscam-se, em outras áreas, elementos que tragam um entendimento mais sólido do que significa confiar para associá-lo às Publicações Técnicas do Conarq de preservação digital.

Tradicionalmente, muitos filósofos buscaram auxílio na Filosofia Moral para resolver questões epistemológicas; na Filosofia Moderna, John Locke trabalhou com noções como ética da crença e de responsabilidade em crer (Ketzer, 2015). Posteriormente, Luhmann (1996) também utilizou enunciados semelhantes para reduzir a complexidade dos sistemas sociais. Este último, além de outros autores contemporâneos, endereçam-se a este estudo, uma vez que o concede uma visão holística e dinâmica do cenário presente, sobretudo, ao objeto de análise desta pesquisa.

A partir do que foi dito, lançam-se as seguintes questões: qual o significado de

confiança nas Publicações Técnicas do Conarq com foco na preservação digital? Quais foram os recursos ou os elementos utilizados nessas Diretrizes que serviram para nos fazer compreender o conceito de confiança?

Com efeito, em toda sua história, a informação e a comunicação desempenharam papel de suma importância nas relações entre os indivíduos, principalmente, quando postas à interpessoalidade. Nessa linha, foi por meio dos documentos que uma lente diferenciada pôde ser atribuída aos sistemas sociais, caso em que torna tais dispositivos, eixo central à desburocratização das ações humanas, no intuito de legitimar e de garantir os direitos de seus atos.

Capurro e Hjørland (2007) compeendem que a informação não deve ser considerada como um elemento estático, muito menos conceituada de maneira isolada, mas fundamentada a partir de ideias já conhecidas, isto é, sem um contexto ela não tem significado. Le Coadic (1996) complementa: a informação, *per si*, é cheia de sentidos em um suporte espaço-temporal, considerando um sistema de signos de linguagem que associa um significante a um significado. Sumariamente, essas afirmações denotam que a acepção desse insumo deve estar contextualizada. Então, mantê-las, sem que sejam modificadas, é um dos maiores desafios dos custodiadores. Fator que, às vezes, incomodam os arquivistas por não terem formatos normalizados, um programa de políticas, impedindo a razão da conservação para longa duração dos documentos (Delmas, 2010).

Outrossim, não atentar para a preservação é pôr em risco a continuação do conhecimento humano. Alguns métodos contribuem para esse feito, os quais se situam por intermédio de práticas cotidianas, tendo como objetivo conservar e garantir proteção à informação (Ferreira, 2006). É, a partir desse entendimento, que são analisadas as seguintes Publicações Técnicas do Conarq de preservação digital: as Diretrizes para a implementação de Repositórios Arquivísticos Digitais Confiáveis – RDC-Arq (Brasil, 2023a); as Diretrizes do Produtor (Brasil, 2013a); As Diretrizes do Preservador (Brasil, 2013b); as Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais (Brasil, 2012); o Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos – e-ARQ Brasil (Brasil, 2022); e a carta para a preservação do patrimônio arquivístico digital (Brasil, 2005a).

Em âmbito nacional, as citadas Diretrizes arquivísticas certificam, apresentam e representam elementos de confiança à informação e aos documentos (de arquivo). E, para se compreender semelhantes nuances, debruça-se em um estudo com perspectiva interdisciplinar, dando importância à Filosofia e à Sociologia sob o prisma do conceito de

confiança para o contexto da Arquivologia.

No sentido de apreender e de testificar o que foi exposto, lança-se a hipótese de trabalho de que, *na Arquivologia, é a preservação digital por meio de suas Publicações Técnicas do Conarq, que concede o caráter de confianca à informação e ao documento (de arquivo) digital.*

Nessa perspectiva, esta pesquisa visa analisar o conceito de confiança nas Publicações Técnicas do Conarq de preservação digital. E, para tanto, busca, especificamente:

- compreender o conceito de confiança na perspectiva da Filosofia e da Sociologia, para, assim, analisar os aspectos de confiança das Publicações Técnicas do Conarq de preservação digital;
- examinar, nessas Publicações, os elementos de confiança;
- relacionar o conceito de confiança aos elementos de confiança identificados nas Publicações Técnicas do Conarq de preservação digital;
- certificar se essas Diretrizes, no âmbito da preservação digital, trazem garantia de confiança à informação e ao documento (de arquivo).

É certo que o progresso tecnológico digital imerso nos documentos traz reflexões acerca de um cenário diferente imposto pela tradição analógica. A buca pela compeensão deste atual contexto remete a um cuidado maior pela instabilidade do mundo digital, imprescindível situação que deve fazer os arquivistas se atentarem à etapa que antecede à gênese documental.

Consoante Schmidt (2012), a existência dos arquivos é um dos princípios básicos à comprovação de fatos, de evidências, de transações, da democracia, da transparência, da preservação dos direitos humanos e da construção da memória; motivos que demandam que suas especificidades sejam garantidas. A autora acresce: falar sobre essas especificidades no campo dos arquivos é voltar à verdade arquivística, que fundamenta a área e tem como objeto o documento de arquivo, em que informações de “fora” e de “dentro”, podem ser requeridas nas mais diversas situações, as quais advém o atributo científico para o campo dos arquivos.

Georgete Medleg Rodrigues em entrevista à Schmidt (2012), ao definir o objeto científico na área dos arquivos, ressalta não haver diferença entre a informação arquivística e o documento arquivístico. Com efeito, quando se fala nesse tipo documento, refere-se ao suporte e ao conteúdo que nele há, porém ambos, tanto o suporte como o conteúdo, formam informação. Então, ao definir informação arquivística, ela a entende como um suporte aliado a um conteúdo, dentro de um contexto de produção; é sempre a junção desses dois em um contexto de produção. Não se pretende discutir o objeto científico da Arquivologia aqui, mas

enfatizar que o tipo de informação tratada pela área é peculiar às demais.

A motivação pela escolha temática desta pesquisa é existente desde os primórdios de nossa graduação, pois por ser um assunto inserido no contexto das tecnologias digitais, aliada ao cuidado e à proteção documental, fez aguçar interesse. Nossa construção acadêmica circundou produções nesse tema, ou associado. Dessa forma, no mestrado, o interesse se intensificou e a dissertação foi construída no entorno da preservação digital, sendo mote à sua continuação nesta tese.

No âmbito da Arquivologia, justifica-se por envolver aportes teórico-práticos relacionados à preservação digital sob a óptica das Publicações Técnicas do Conarq, que trazem boas práticas relacionadas à confiança, à proteção e ao cuidado no gerenciamento de todo o ciclo documental. E, complementarmente, na redoma interdisciplinar, torna-se importante, uma vez que permite utilizar-se do conceito de confiança numa perspectiva sócio-filosófica atrelada às diretrizes citadas do Conarq. O que envolve um entendimento mais acentuado sobre a informação/documento na preservação digital, atrelada à noção de **tempo,** transmitindo a ideia de longo prazo à perpetuação dos registros; de **risco,** no intuito de reduzir a complexidade causada pelos elementos centrífugos que desertam os documentos a uma instabilidade; de **liberdade**, num fluxo orgânico e contínuo de acesso à informação, levando a cabo, a importância de uma cadeia de custódia ininterrupta para os arquivos; e de (**in)segurança** ((des)confiança), atentando para as potencialidades da preservação ativa e passiva como mecanismo de confiança aos documentos.

Para o contributo social, intenciona-se expor um estudo parcamente explorado no campo dos arquivos como forma de legitimar e de reforçar que o conceito de confiança está estritamente relacionado à área, sobretudo, quando representado pela preservação digital. Isto posto, ansia-se alcançar os diversos profissionais, acadêmicos ou não, neste escrito, assim também o público em geral, no sentido de difundir uma temática mais que necessária nos tempos atuais.

Esta tese está organizada em 10 seções e subseções, além das Referências e dos Apêndices. A seção 1, que é *Introdutória*, situou e destrinchou este trabalho no tempo-espaço, expondo problemática, tese, objetivos e justificativa de forma integrada, tendo como objeto de estudo o conceito de confiança e as Publicações Técnicas do Conarq de preservação digital.

A subseção 2, *Percurso Metodológico*, mostrou os tipos de pesquisa, na qual destacou-se sua natureza descritiva, teórica e documental, além da aplicação do método indiciário e da Teoria do Conceito de Dahlberg em suas subseções. Tais métodos foram necessários para se entender e explicar como o fenômeno do conceito de confiança manifestava-se nas

Publicações Técnicas do Conarq de preservação digital. Como subsídio para essa interpretação, empregou-se uma visão sociológico-filosófica acerca do conceito citado.

A seção 3, *O Conceito de Confiança*, divididiu-se em duas subseções, e abarcou um referencial teórico não apenas do conceito, mas também de definições de confiança sob a óptica de vários autores, em uma perspectiva mais clássica e outra vigente. No que tange à parte do *Princípio de Confiança*, sua concepção basiou-se no escritos do Direito.

A seção 4, *Preservação Digital: histórico*, trouxe a perspectiva histórica da preservação digital passiva, e duas subseções, a primeira acerca de *Seus Conceitos Basilares* e a segunda, *A Trilha para a Preservação Digital Sistêmica*. Esta última contemplou ainda algumas subseções, como: *Cadeia de Custódia Arquivística (ininterrupta), a Cadeia de Custódia Digital Arquivística e a Preservação Digital Sistêmica* propriamente dita. A composição desta seção mostrou que para um gerenciamento confiável de todo o ciclo de vida dos documentos de arquivo faz-se necessário a utilização sistemas informatizados, subsidiados por normas e que cada seção é um crescente complementar.

Para compreender melhor a seção 4, tornou-se preciso abarcar a Teoria de Sistemas como fundamento à Preservação Digital na seção 5, a qual serviu de aporte a um esclarecimento acerca dos elementos que compõem a Preservação Digital Sistêmica, intitulada: *A Teoria dos Sistema como fundamento da Preservação Digital.*

A seção 6 evidenciou *A Quarta Revolução Industrial, a Indústria 4.0 e a Transformação Digital* e seus pontos em comum. Para expor esses pormenores, criou-se 3 subseções, *A Indústrica 4.0; Tranformação Digital: tecnologia emergentes, disruptivas e sustentadas; e a Tranformação Digital no Brasil a partir da óptica governamental*. Esta, ramificada em mais duas subseções, *A Estratégia Brasileira para a Tranformação Digital*, que englobou o Poder executivo; e *O Programa Justiça 4.0*, que abarcou o Poder Judiciário. Destacou-se também, o percurso da Transformação Digital (TD) pelo governo do Estado da Paraíba, em João Pessoa.

A seção 7 tratou do *Projeto InterPARES* como um dos grupos pioneiros e internacionais de estudo de referência conceitual e metodológica ligado à Preservação Digital. Os seus subcapítulos enfocaram as quatro fases do Projeto, O InterPares 1, 2, 3 e 4. Nossa intenção em trazer o InterPARES nesta tese deu-se no intuito de realçar a sua importância para o campo da Arquivologia e do documento digital, e também devido à escassez de publicação na literatura nacional, já que muitos de seus estudos não são encontrados em português brasileiro.

A seção 8 descreveu as *Seis Publicações Técnicas do Conarq de Preservação Digital*

analisadas neste estudo, e no final de cada diretriz, quadros foram criados para expor os elementos de confiança extraídos dessas normativas. São elas: *A Carta para a Preservação do Patrimônio Público Arquivístico Digital, as Diretrizes do Produtor e do Preservador, as Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais, o Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivísticas de Documentos – e-ARQ Brasil e as Diretrizes para a Implementação de Repositórios Arquivísticos Confiáveis –RDC-Arq.*

A seção 9 trouxe os *Resultados e Discussão*. A sua síntese aglomerou em um quadro os conceitos de confiança das seis Publicações Técnicas do Conarq de perservação digital, compilando-os aos conceitos de confiança do nosso Referencial Teórico. Assim, fez-se o aporte entre esses dois objetos, a fim de depreender tal conceito nas Publicações em questão de um modo descritivo.

A seção 10, *Considerações Finais*, foi composta pelas conclusões da pesquisa, em que trouxemos algumas sugestões para futuros estudos, enfatizando o papel da preservação digital para a confiança da informação e do documento de arquivo. Após, têm-se as *Referências* utilizadas neste texto e, por fim, o *Apêndice A*, referenciando as Publicações Técnicas de preservação digital do Conarq utilizadas como *corpus* desta tese, e o *Apêndice B*, que sintetizou os elementos do conceito de confiança do nosso Referencial Teórico em forma de quadro.

2 PERCURSO METODOLÓGICO

Ao pesquisar sobre o conceito de confiança em direção à Arquivologia e à Ciência da Informação, percebe-se uma incipiência de publicações científicas. Ao tomar como referência, por exemplo, a análise dos registros na Biblioteca Digital Brasileira de Teses e de Dissertações (BDTD), que dá acesso a mais 898.982 mil documentos, com 656.162 mil dissertações, 242.820 mil teses e 139 instituições, recupera-se um resultado de 30 trabalhos, e apenas 15 enfocam o tema.

Na Base de Dados em Ciência da Informação (Brapci), maior sistema de indexação de registros digitais no Brasil, contando com uma gama de mais de 57.875 mil registros (86.05% artigos), 18.267 mil autores, 100 revistas, 20 livros e seis Anais de eventos; apenas um artigo foi encontrado num quantitativo de 30 trabalhos. Vale salientar que a Brapci envolve revistas de diversas áreas, a saber, Arquivologia, Biblioteconomia, História, Museologia, Administração, Direito, Ciências Humanas, Comunicação, Tecnologia, Saúde, e também em âmbito internacional (Portugal, Colômbia, Espanha, Argentina, Costa Rica e Cuba.

Nas métricas do "Google Acadêmico", encontram-se 243 veículos científicos, de vários idiomas e países. Nessa base de dados, direciona-se a revistas e a periódicos nas áreas do Direitos, da Filosofia, da Sociologia, da Psicologia e do *Marketing*, que serviram de base para esta pesquisa.

Esses e outros indicadores são interessantes para mostrar o quanto se faz necessário investir na temática da confiança para os arquivos, sobretudo, no ambiente digital, porquanto muito se fala em confiança, mas pouco se sabe acerca dela e de sua essência na área deste estudo. Além disso, na Ciência da Informação e na Arquivologia, identifica-se que as questões relacionadas à "confiança" estão estritamente entrecruzadas à preservação digital e suas nuanças, na qual o destaque põe-se a assuntos sobre repositórios digitais, como também sobre recomendações de boas práticas ao gerenciamento da informação a longo prazo e para os arquivos permanentes, representados por diretrizes e por normas.

A título ilustrativo dessas normativas, tem-se as Publicações Técnicas do Conarq em âmbito nacional, aqui estudadas, e, no contexto internacional, a ISO 16363:2012, o *Reference Model for an Open Archival (*modelo OAIS) (ISO 14721:2003) e a *Trustworthy Repository Audit and Certification: Criteria and Checklist* (Trac), entre outras, as quais não serão nossos objetos.

Esta pesquisa tem como objeto compilar o conceito de confiança junto às Publicações Técnicas de preservação digital do Conarq. Para isso, escolheu-se seis documentos

normativos que versaram sobre o escopo da preservação. O reflexo do que significa confiança aos documentos arquivísticos digitais são direcionados ao que a Câmara Técnica de Documentos Eletrônicos (CTDE) produziu. Parte das exigências encontradas nessas Publicações do Conarq são recomendações de boas práticas aos materiais digitais. Dessa forma, fez-se necessário compreender a essência da confiança, por meio de teorias e aplicá-las as tais Publicações, no intuito de dirimir os aspectos de tecnicidade que as normativas trazem.

O termo confiança nessas diretivas, muitas vezes, parecem ser empregados de forma muito generalista, e não definidos com substância, mas atrelados a instrumentos ou a ferramentas. Por exemplo, repositórios para serem confiáveis precisam de requisitos para compô-los; e Sistema Informatizado de Gestão Arquivística de Documentos (Sigad) possuem diversas funcionalidades para serem considerados confiáveis. Porém, a confiança não é explicada essencialmente, mas atrelada a peças e a elementos que justapostos significam confiança. Por isso, surge a inquietação em fazer um aporte mais filosófico e sociológico para compreender o que de fato significa confiança e como ela entrecruza-se a essas normativas.

Neste trabalho foram analisados seis documentos, versando a preservação digital. Assim, foram examinados elementos, tais como categorias, termos, conceitos e definições, considerados como referência ao conceito de confiança em uma perspectiva teórica. Tal análise foi feita a partir do referencial sobre o conceito de confiança. Eis as Publicações Técnicas de preservação digital do Conarq são:

1. **Carta para a preservação do patrimônio arquivístico digital[2]:** esta Carta para a Preservação do Patrimônio Digital da Organização das Nações Unidas à Educação, à Ciência e à Cultura (Unesco) manifesta a necessidade de os Estados-membros, incluindo o Brasil, estabelecerem políticas e ações para proteger o patrimônio digital.
2. **Diretrizes do Produtor[3]:** estas diretrizes foram desenvolvidas para pessoas que produzem materiais digitais no curso de suas atividades profissionais e pessoais, com o objetivo de elaborar e de manter registros, a fim de assegurar sua preservação pelo tempo que seja necessário. Tal documento ajudará a assegurar o acesso aos documentos que merecem ser preservados por um longo período em um repositório arquivístico, quando estes forem entregues aos cuidados de uma entidade arquivística confiável.

[2] Disponível em: Carta para a Preservação do Patrimônio Arquivístico Digital.
[3] Disponível em: conarq_diretrizes_produtor_preservador_resolucao_38.pdf (www.gov.br), Tanto “As Diretrizes do produtor” quanto as "Diretrizes do Preservador” encontram-se em um único documento.

3. **Diretrizes do Preservador:** enfoca o elo de preservação da cadeia de preservação e estão organizadas de acordo com a sequência de atividades apresentadas no modelo da Cadeia de Preservação do InterPARES, que mostra os vários passos sequenciais para a produção, a manutenção e a preservação de documentos autênticos. Estas diretrizes foram elaboradas de forma a responder às necessidades de preservação de organizações ou de programas cujos documentos arquivísticos têm que ser guardados e consultados durante longos períodos, bem como as necessidades das instituições arquivísticas responsáveis pela preservação a longo prazo de documentos arquivísticos de terceiros e pela continuidade de sua acessibilidade ao público-alvo.
4. **Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais[4]:** a presunção de autenticidade dos documentos arquivísticos sempre fez parte do processo tradicional de avaliação desses documentos e é fortemente apoiada na análise de sua forma e de seu conteúdo, que nos documentos não digitais estão inextricavelmente ligados ao suporte, isto é, forma, conteúdo e suporte são inseparáveis. Além disso, essa presunção baseia-se na confirmação da existência de uma cadeia de custódia ininterrupta, desde o momento da produção do documento até a sua transferência para a instituição arquivística responsável pela sua preservação no longo prazo.
5. **Modelo de requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos – e-ARQ Brasil - versão 2[5]:** é uma especificação de requisitos a serem cumpridos pela organização produtora/recebedora de documentos, pelo sistema de gestão arquivística e pelos próprios documentos, a fim de garantir sua confiabilidade e autenticidade, assim como sua acessibilidade. Além disso, o e-ARQ Brasil pode ser usado para orientar a identificação de documentos arquivísticos digitais, estabelecendo requisitos mínimos para um Sigad, independentemente da plataforma tecnológica em que for desenvolvido e/ ou implantado.
6. **Diretrizes para a implementação de Repositórios Arquivísticos Digitais Confiáveis - RDC-Arq - versão 2:** estas diretrizes têm por objetivo orientar os órgãos e as entidades integrantes do Sinar quanto à indicação de parâmetros e de

[4] Disponível em: DIRETRIZES PARA A PRESUNÇÃO DE AUTENTICIDADE DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS.
[5] Disponível em: EARQV205MAI2022.pdf (www.gov.br).

> requisitos para repositórios arquivísticos digitais confiáveis, de forma a garantir a autenticidade, a confidencialidade, a disponibilidade, o acesso e a preservação, tendo em vista a necessidade de manutenção dos acervos por longos períodos ou, até mesmo, permanentemente.

Todos esses documentos, na seara dos arquivos, possuem elementos e particularidades caracterizantes do que se pode chamar de confiança aos registros arquivísticos; são eles quem ditam as recomendações, as diretrizes e os instrumentos que trazem segurança e preservação à informação.

Essas teorias, metodologias e modelos específicos possuem o fito de possibilitar um acesso contínuo aos documentos, subsidiado pelas prática arquivísticas, por meio de fatores característicos como da autenticidade, pois sem ferramentas tecnológicas adequadas à preservação de documentos digitais não seria possível. Nesse sentido, a Arquivologia é umas das áreas pioneiras a se preocupar com a longevidade dos documentos, fator importante para perpetuar a história, a memória e garantir direitos aos cidadãos. A preservação digital na Arquivologia é, portanto, um objeto de estudo que propõe padrões, normas, políticas, critérios e procedimentos fundamentais e de planejamento a longo prazo.

2.1 O MÉTODO UTILIZADO

A natureza deste trabalho foi teórica (Gil, 2008). Desse modo, possui objetivo descritivo, uma vez que se pormenoriza o objeto estudado, mostrando suas relações, que envolveu o uso de uma observação sistemática, especialmente a partir da díade interpretação-explicação. Tal descrição foi feita após a leitura de bibliografias e de documentos acerca do conceito confiança, bem como das Publicações Técnicas do Conarq de preservação digital.

Para Deslandes (2002) e Gomes (2002), o objeto das Ciências Sociais é histórico, e isto significa dizer que a sociedade existe e se mostra num determinado espaço organizado de forma particular e diferente de outras, logo, possui essência qualitativa. Nesta abordagem qualitativa, foi utilizado o método indiciário como base analítica-interpretativa. Essa ação reflexiva torna-se fundamental para contextualizar os sinais de fenômenos, no sentido de elucidar fatos através da compreensão de um determinado contexto, sendo assim, uma forma de experiência, e, ao mesmo tempo, de análise gramatical.

É importante elucidar que, no final do século XIX, começou-se a se formar nas Ciências Humanas um paradigma chamado indiciário, porém, suas raízes são bem mais antigas. O que caracteriza esse saber é a capacidade de, a partir de dados aparentemente

“negligenciáveis”, remontar a uma realidade complexa não experimentável. Em rigor, seu surgimento remonta aos primeiros humanos e está relacionado ao próprio desenvolvimento da narração – o caçador teria sido o primeiro a narrar uma história, pois era o único capaz de ler, nas pistas mudas (se não imperceptíveis) deixadas pela presa, uma série coerente de eventos (Ginzburg, 1989).

O caçador utilizava-se do paradigma indiciário como um modelo venatório para afirmar que alguém passou por ali. Ginzburg (1989) percebeu a utilização de dois personagens importantes em sua teoria: Sherlock Holmes como representante da arte da detecção e Freud para o desenvolvimento da Psicanálise. Nesses casos, Ginzburg (1989) relata: pistas talvez infinitesimais permitem captar uma realidade mais profunda, de outra forma inatingível. Pistas, mais precisamente, sintomas (no caso de Freud) e indícios (no caso de Sherlock Holmes). Sinteticamente, o método indiciário ou divinatório significa formas de saber que podem revelar passado-presente-futuro.

No domínio desta pesquisa, tal paradigma trabalha descobrindo nas fontes e nos documentos dados além daqueles que pretendiam revelar, informações que, para a sociedade que produziu o documento, pode ser tido apenas como um fato posto, mas quando analisadas e desconstruídas podem revelar um sistema ainda não conhecido. Assim, enquanto Ginzburg (1989) enxerga esses vestígios como o fio de Ariadne, tal qual aquele que fez com que Teseu não se perdesse dentro do labirinto do minotauro, busca-se compreender o sentido do conceito de confiança nas diretrizes de preservação digital, no âmbito da Arquivologia sob uma perspectiva sociológico-filosófica, por intermédio dos sintomas deixados em cada objeto estudado.

A pesquisa com seus indícios incorpora uma multiplicidade consciente de enxergar as diversas possibilidades das variáveis pesquisadas, ou seja, buscando entrelaçar-se ao sentido interpretativo da hermenêutica (Ginzburg, 1989), pois consiste em investigar algo pautado em pistas e observação, que neste caso envolve os aspectos conceituais da confiança nas normativas mencionadas. Com efeito, registros de jornais, de periódicos e de livros servem como fontes bases para a investigação histórica. Tais registros, muitas vezes, servem como pistas ou indícios que podem apontar um caminho para onde conduzir nossas pesquisas.

Conforme Ginzburg (1989) e Kincheloe e Berry (2007), o paradigma indiciário caracteriza-se como conjunto de princípios e de procedimentos que contém a proposta de um método heurístico centrado no detalhe, nos dados marginais, nos resíduos tomados enquanto pistas, indícios, sinais, vestígios ou sintomas. Para os autores, documentos oficiais, relatórios, decretos leis, fontes secundárias e voluntárias, ou seja, as fontes investigadas pelo pesquisador

podem revelar muito mais do que o testemunho tomado apenas como um dado.

Ao utilizar-se deste método, procura-se ter uma estratégia de compreensão do fenômeno na resolução de um problema. Nesse sentido, esta pesquisa tem sua peculiaridade interpretativa e compreensivista que permite concatenar a relação entre o conceito de confiança em seus postulados teóricos e os das diretrizes de preservação digital.

Quanto aos procedimentos técnicos está classificada como bibliográfica e documental, pelo motivo das Publicações Técnicas do Conarq serem registros documentais, ou seja, informação registrada em suporte. Segundo Prodanov e Freitas (2013), a pesquisa documental requer a análise de textos já publicados, que se baseiam em materiais que não receberam ainda um tratamento analítico ou que podem ser reelaborados de acordo com os objetivos da pesquisa.

Tomando como referências estes procedimentos, para complementar o método indiciário, acostamo-lo na análise do conceito da Teoria do Conceito de Dahlberg com objetivo de compreender o significado, bem como as nuances do conceito de confiança.

2.2 A TEORIA DO CONCEITO DE DAHLBERG

As linguagens são utilizadas para a comunicação dia a dia e estão condicionadas a um tempo-espaço. Dessa forma, esse instrumento constitui a capacidade de designar objetos. Assim, elas são empregadas nas necessidades básicas cotidianas, e, quando isto ocorre, denominam-se de linguagens naturais. Além delas, há também as linguagens especiais, artificiais ou formalizadas, que são aquelas inseridas em uma área do conhecimento, como, por exemplo, a linguagem científica.

Por meio da linguagem natural torna-se possível relacionar diversos objetos, sejam eles individuais ou gerais (expressos por conceitos individuais ou gerais) e elaborar enunciados (descrição do objeto); cada enunciado representa um elemento ou uma parte do conceito.

Esses objetos individuais podem ser representados por coisas, fenômenos, processos, acontecimentos e atributos e são únicos, diferente dos demais, uma unidade inconfundível, expressos por conceitos individuais. Por exemplo, com o objeto individual “a preservação digital”, formulam-se os seguintes enunciados: 1) conjunto de ferramentas tecnológicas para migrar informação de um suporte antigo para um subsequente; 2) área de estudo da Arquivologia que se encarrega de proteger a informação e o suporte; 3) estratégias de proteção aos documentos digitais. A soma desses enunciados formam o conceito de

preservação digital.

Os objetos gerais, por sua vez, são formados por conceitos genéricos, tais como as verdades, as crenças, os sentimentos e a confiança. Em relação ao objeto geral “os sentimentos”, consegue-se formular os seguintes enunciados: 1) são sentidos por pessoas; 2) que estão fazendo um acordo; 3) que podem acarretar uma finalidade; 3) podem ser bilateral; 4) durante um determinado tempo. Sobre “a confiança”, tem-se os seguintes enunciados: 1) pode ser um sentimento ou uma virtude; 2) pode ser a crença em algo ou em alguma coisa; 3) está relacionada à cooperação entre pessoas. Laconicamente, a soma total dos enunciados sobre “preservação digital", sobre “os sentimentos” e sobre “a confiança” fornecem e/ou criam os seus conceitos. Cada enunciado faz referência a elementos do conceito. Ou seja, o conceito é constituído de elementos que se articulam numa unidade estruturada.

Em relação às linguagens especializadas, deve-se atentar para que os conceitos sejam definidos com toda precisão, que é o caso desta pesquisa. Sendo assim, a formação dos conceitos se dá pela compilação de enunciados de um determinado objeto, por meio de um instrumento: a palavra ou qualquer signo que traduz essa reunião de enunciados. **A partir disso, pode-se definir o conceito como a compilação de enunciados acerca de um objeto, fixado por um símbolo linguístico** (Dahlberg, 1978, grifo nosso).

Dessa forma, todo enunciado sobre objetos contém um elemento do respectivo conceito, que juntados são chamados de “características dos conceitos” ou “atributos” das coisas; esse processo também designa-se de análise de conceitos (Dahlberg, 1978).

Quando uma característica é muito geral, convém chamá-la de “categoria”, que é o conceito em sua mais ampla extensão ou hierarquia. Exemplo: a confiança (categoria/característica geral) é um sentimento de cooperação; a cooperação é uma atitude positiva; uma atitude positiva serve para trazer benefícios aos indivíduos. Caso um conceito não tenha nome, por meio da síntese de suas características, torna-se possível formulá-lo.

As características de um conceito para Dahlberg (1978) podem ser (1) essenciais: encontradas em todos os referentes relacionados a um conceito; (2) acidentais: identificadas em alguns dos referentes relacionados a um conceito, mas não sendo inerente a ele; e (3) individualizantes: encontradas em um único referente. Por exemplo, as características essenciais que tornam um documento de arquivo como tal e confiável são: unicidade, integridade, identidade, autenticidade, imparcialidade, inter-relação, fidedignidade (confiabilidade) e organicidade. Fazer uso desse documento é uma característica acidental, pois ele pode ou não ser usado. Ser criado no ambiente digital ou analógico pode ser uma característica individualizante.

A Teoria do Conceito de Dahlberg serve para estabelecer princípios para a identificação e para o entendimento dos conceitos, criando diretrizes teóricas com o fito de ser um modelo analítico idealizado para elucidar a natureza e a estrutura dos conceitos (Dahlberg, 1978).

As funções das características dos conceitos servem para classificá-los, defini-los e formar seus nomes. Então, sempre que diferentes conceitos possuem características idênticas existem relações entre eles. Por exemplo, se considerar os conceitos cooperação, mutualidade, trabalho em conjunto, existe uma característica comum, que no domínio deste estudo é a confiança entre pessoas, ou seja, esses objetos relacionam-se e formam um conceito mais amplo.

Tais relações também são representadas por hierárquicas. Ou seja, se dois conceitos são comparados e possuem características em comum, entre eles se estabelece a relação hierárquica ou relação de gênero e espécie. Assim, pode-se falar de conceitos mais amplos, genéricos ou superiores, ou mais restritos, inferiores ou específicos. Ao falar em confiança como termo mais amplo, as suas características são os termos inferiores e mais específicos: sentimento e crença, por exemplo. Há também a relação de oposição entre conceitos, como confiança-desconfiança, crédulo-incrédulo.

Há outros tipos de relação, conforme Dahlberg (1978), mas aqui interessa os mencionados no parágrafo acima. O conceito também possui intensão e extensão. Quando se fala em intensão do conceito, define-se-à como a soma total das suas características. Exemplo: a intenção do conceito “confiança” é: virtude/sentimento; – sentido por pessoas; – independente do gênero. Já a extensão do conceito é definida pela soma total dos conceitos mais específicos. Também pode ser entendida pela soma dos conceitos para os quais a intensão é verdadeira, aqueles possuem características em comum.

Vale destacar, que os conceitos também são compostos por definições, que são pressupostos constituídos de elementos necessários na construção de sistemas científicos. Essa importância é evidenciada também quando se tem em vista a comunicação internacional do conhecimento. Nesse horizonte, segundo Dahlberg (1978), a função da definição é estabelecer uma “equação de sentido”; de um lado (à esquerda) se encontra aquilo que deve ser definido [o *definiendum*] e do outro (à direita) aquilo pelo qual alguma coisa é definida [o *definiens*]. A definição é, de certo modo, uma limitação, ou seja, uma colocação de limites. Definição é, portanto, a delimitação ou fixação do conteúdo de um conceito (intensão, conjunto de características ou atributos). Exemplo: [*definiendum*] confiança = [o *definiens*] **df** crença que algo acontecerá positivamente.

Contudo, só os conceitos gerais necessitam de definições, pois eles têm que ser bem distinguidos dos demais, a fim de que apareçam com clareza nos objetos que se referem. Os conceitos individuais têm seus objetos bem determinados em virtude da presença das formas do tempo e do espaço, e por ser de mais fácil entendimento, pois são únicos.

A definição pode ser nominal, que fixa o sentido de uma palavra. O mesmo exemplo pode ser usado: confiança = df crença que algo acontecerá positivamente. Já a definição real delimita a intensão de conceito (soma total de suas características), distinguindo-o de outros com as mesmas características no *definiens*. É apresentar o conhecimento de um objeto. Exemplo: preservação digital = **df** proteção a documentos digitais (ou área da Arquivologia que estuda estratégias para longevidade da informação). As duas formas de definição agem, muitas vezes, conjuntamente. Há casos que não se consegue distingui-las muito bem.

Partindo dos pressupostos acima, Dahlberg (2009) enfatiza que a criação de um conceito pode ser representada por uma tríade, em que há um **referente** (objeto a ser conceitualizado); **as características do objeto** (enunciados "verdadeiros" [ou predicações] a respeito do referente); **e a forma verbal** (termo/nome/palavra/código) que representa o conceito e é o elemento comunicativo de seu conteúdo, conforme a Figura 1.

Figura 1 – Triângulo do conceito

Fonte: Maculam e Lima (2017, p. 73) adaptado de Dahlberg (1978).

O referente pode ser representado pelo universo de itens constituído de ideias, de objetos, de fatos, de leis, de propriedades, de ações, em que é possível selecionar um determinado item de referência, sobre o qual podem ser feitas afirmações que o caracterizem naquele contexto, em um acordo estabelecido entre os membros de uma dada comunidade, que, por sua vez, são sintetizadas na forma verbal por meio de um termo ou nome que será aplicado e comunicado no universo dos discursos, seja pela forma verbal ou escrita. Um conceito é gerado por predicações necessárias sobre um referente, que pode ser um objeto, uma atividade, uma propriedade, uma dimensão ou uma combinação dos mesmos, isto é,

podem ser os elementos de qualquer assunto.

A partir desse entendimento, procedimentalmente, foram sistematizados quadros para sintetizar o conceito de confiança nas Publicações Técnicas do Conarq de preservação digital, que, como descrito acima, compreendem seis normativas, e no Referencial Teórico sobre o conceito de confiança. Assim, extraíram-se e aplicaram-se os elementos da Teoria de Dahlberg, a fim de fazer relações entre o conceito de confiança do Referencial Teórico em questão e as Publicações Técnicas supracitadas.

Quadro 1 – Elementos dos conceitos de confiança extraídos das Publicações Técnicas do Conarq sobre preservação digital

Conceitos	**Definições**
Gestão Arquivística de Documentos	Tem o objetivo de garantir a produção e a manutenção de documentos fidedignos, autênticos, acessíveis, compreensíveis e preservável.

Fonte: Elaborado pelo autor (2024).

Após a descrição de cada uma das Diretrizes, quadros foram confeccionados sumarizando os conceitos e as definições que fazessem aporte ao entendimento sobre o conceito de confiança, de acordo de Referencial Teórico já destacado. Ou seja, para a extração dos conceitos e das definições das Diretrizes, foi necessário compreender as ideias dos autores acerca da confiança e, a partir disso, retirar os conceitos e as definições que se afinassem ao conceito de confiança, conforme exemplo do Quadro 1.

Quadro 2 – Síntese dos elementos do conceito de confiança

Autores	**Enunciados sobre o conceito de confiança**	**Conceitos de confiança**	**Características dos conceitos de confiança**
Confúcio (1996)	*1) Dá-se por meio das relações entre pessoas.* *2) É um princípio ou uma virtude.* *3) Pressupõe integridade, confiabilidade e fidelidade.* *4) Tem como antítese a desconfiança.*	*A confiança está afinada às relações pessoais na sociedade, traduzida em princípios e virtudes para um bom governo. Estes podem ser representados pela integridade, pela confiabilidade e pela fidelidade, significando conservar e preservar suas características originais, isto é, a confiança na relação entre indivíduos ou entre indivíduos e objeto de forma abstrata ou concreta. O filósofo mencionou a desconfiança como um sentimento desvirtuoso da boa conduta humana.*	*Relação/princípio/virtude/integridade/confiabilidade/fidelidade/desconfiança/conservar/preservar*

Fonte: Elaborado pelo autor (2024).

Em relação ao Referencial Teórico adotado sobre o conceito de confiança, sintetizou-se em um quadro a concepção dos seus autores, no intuito de auxiliar na análise dos resultados e discussão (Apêndice B). Assim, para precisar ainda mais a compreensão sobre o conceito de confiança, uma apuração foi feita no Quadro 1, utilizando o Quadro 2, e, por isso, o Quadro 3, incluiu apenas os conceitos que tivessem relaçao direta com o conceito de confiança.

Quadro 3 – Síntese dos conceitos e das definições de confiança extraídos das Publicações Técnicas do Conarq sobre preservação digital

Conceitos	**Definições**	**Normas em que os conceitos foram encontrados**
Acessibilidade	A acessibilidade é uma categoria que engloba o elemento "Recepção" e "Saída". Nesse sentido, acessibilidade, dá-se pelo acesso aos documentos, por meio de *software* e de *hardware*, além de formatos de arquivos, que garantam a facilidade de acesso a longo prazo. Um desses elementos é a interoperabilidade que facilita o acesso, permitindo a troca de informações entre sistemas diferentes, devendo levar em consideração a responsabilidade e competência técnica e profissional do preservador na cadeia de preservação.	• Diretrizes do Produtor (Brasil, 2013b). • Diretrizes do Preservador (Brasil, 2013a).

Fonte: elaborado pelo autor (2024).

O Quadro 3 contemplou conceitos que possuíam relação direta com o Referencial Teórico citado. Isso serviu para discutirmos as análises de forma mais assertiva, retirando elementos das Publicações Técnicas do Conarq de preservação digital, que não tinham afinação ao conceito de confiança precisamente.

3 O CONCEITO DE CONFIANÇA

Remete-se, incialmente, a alvorada da questão da confiança ao pensador chinês Confúcio, vivente entre aproximadamente os anos de 552 a 479 a.C. Sua filosofia baseia-se na moralidade pessoal e governamental, cujos princípios estão alinhados a uma boa conduta de vida, isto é, à ética, à lealdade, à veneração aos ancestrais, ao respeito com os idosos, à justiça.

O pensador possui uma das mais importantes filosofias do Oriente, e teria sido um dos primeiros a realçar o valor da confiança nas relações interpessoais e na condução de um governo. Propôs uma doutrina na qual seria possível viver em harmonia, mediante à adoção de um conjunto de comportamentos e preceitos morais (Belchior, 2015).

O confucionismo é uma sistemática de ideias e de idiossincrasias advindas da China antiga, desenvolvido a partir do que mais tarde ficou conhecido como as "cem escolas de pensamento"[6], apregoando que todas as pessoas nascem naturalmente boas e por meio de alguns fatores poderiam atingir a harmonia e o equilíbrio na sociedade. A escola de Confúcio tinha uma gama de princípios/virtudes essenciais, entre elas:

- *Ren* (humanidade e altruísmo) denota o bom sentimento que um ser humano experimenta ao ser altruísta. É a essência humana que se manifesta como compaixão, podendo ser traduzida como "benevolência", "bondade" e "humanidade".
- *Li* (rito), para a tradição chinesa antiga, são sistemas de normas ritualística que determinam como uma pessoa deve agir na vida cotidiana. Significa "bons costumes" e "regras morais".
- *Zhi* (sabedoria ou conhecimento) é a capacidade de ver o que é certo e justo.
- *Xin* (integridade), também é atrelado à confiabilidade, à fidelidade e à confiança nas relações pessoais e sociais. *Xin*, sob a óptica da preservação e da segurança da informação, significa armazenar e disponibilizar informações confiáveis, ou seja, autênticas, dispostas em formato compatível com o de utilização.
- *Zhing* (fidelidade) significa quem ou o que conserva, mantém ou preserva suas características originais. Fidelidade implica confiança e vice-versa, e essa relação aplica-se entre dois ou mais indivíduos ou a um sujeito e um objeto de forma

[6] Surgiu durante o período dos "Anais das Primaveras e Outonos", uma crônica atribuída a Confúcio. Foi uma era de grande expansão intelectual na China, e também de muitas batalhas sangrentas. Ficou também conhecida como a Era de Ouro da filosofia chinesa, uma vez que as ideias dos intelectuais à época eram discutidas livremente.

abstrata ou concreta.

- *Yi* (justiça e retidão) dá-se pela disposição moral para fazer o bem em um sentido de honradez.

> O pensador oriental sugeriu, no que ficou registrado na tradição chinesa como um diálogo entre o mestre e o seu discípulo, que alimentos, **confiança** e armas seriam os ingredientes essenciais a um bom governo. Alimentos para manter os cidadãos satisfeitos e tranquilos e cercear qualquer tumulto com gênese na fome; **confiança**, no caso da comida escassa, para que os cidadãos continuassem a acreditar que os seus líderes estavam a procurar resolver o problema; armar para o caso de nenhuma das duas condições anteriores resultar. Encontra-se na mensagem confucionista uma clara apologia da reciprocidade e da ética nas relações interpessoais, sendo a confiança no plano individual e político um recurso fundamental para uma vida harmoniosa e pacífica (Belchior, 2015, p. 23, grifo nosso).

Entre as obras mais conhecidas de Confúcio está o livro "O *Lun Yu"*, ou "Os Analectos", ou ainda "Os Diálogos de Confúcio", sendo uma compilação de textos feita entre os anos 475 e 221 a.C., que sintetiza a doutrina do pensador chinês com seus discípulos, por meio de discursos. Nos Analectos, são abordadas virtudes e ensinamentos morais que circundam a prática de comportamentos como a "benevolência", considerada a qualidade mais importante que um homem pode ter. Para citar mais, a "sabedoria" ou a "inteligência"; a "reverência" que não é estabelecida em função do medo, mas oriunda da consciência da responsabilidade em promover o bem-estar da sociedade (Confúcio, 1996).

Ao procurar os princípios norteadores desta pesquisa, a "confiança" e a "integridade" nessa obra, encontra-se cinco vezes a menção sobre o primeiro termo e 15 vezes acerca do segundo. Em relação à confiança "O *Lun Yu*" enfatiza os seguintes diálogos entre Confúcio e seus discípulos:

> Tseng Tzu disse, 'Cada dia eu me examino sob três aspectos: se sou ou não leal àqueles em nome dos quais estou agindo; se sou ou não de **confiança** quando lido com meus amigos; se pratico ou não o que prego.'. Confúcio disse, 'Ao chefiar um Estado de mil carruagens, respeite o cargo que ocupa e seja de **confiança**, economize no uso dos recursos e ame o povo, e empregue o povo quando for conveniente.' (Confúcio, 1996, p. 3, grifo nosso).

> Confúcio disse, 'Em casa, os jovens devem se comportar como lealdade filial, e fora, no mundo, com amor fraternal. Eles devem ser prudentes e de **confiança**. Eles devem amar todas as pessoas e ficarem próximos aos benevolentes, tendo feito isto, sua força restante deve ser usada no aprendizado da literatura.' (Confúcio, 1996, p. 4, grifo nosso).

> Confúcio disse, 'Dispense a comida. A morte sempre tem existido desde o começo dos tempos, mas sem **confiança**, o povo não pode estabelecer a sua posição.' (Confúcio, 1996, p. 140, grifo nosso).

> Confúcio disse, 'Sem antecipar indevidamente o engano, sem suspeitar **desconfiança**, mas porém sendo capaz de experimentá-los, um homem não é virtuoso.' (Confúcio, 1996, p. 184, grifo nosso).

> Tzu Hsia disse, ‘O homem de bem deve ganhar a **confiança** do povo antes de empregar os seus serviços. Sem **confiança**, o povo consideraria o seu emprego como exploração. O homem de bem deve ganhar a **confiança** do seu senhor antes de recomendar melhorias. Sem **confiança**, o senhor consideraria as suas recomendações como desprezativas.’ (Confúcio, 1996, p. 241, grifo nosso).

Os diálogos mencionados acima, sobretudo, colocam a confiança como um mecanismo primordial para as relações humanas. Confúcio preocupava-se veementemente com uma conduta de retidão da sociedade e para isso acontecer ele descrevia virtudes, realçadas pelo melhor modo de viver, segundo seus preceitos. O confucionismo possui entusiastas até os dias de hoje.

No Ocidente, entre os muitos assuntos abordados por Aristóteles (322-384 a.C.), a ética, a política, a lógica, a física, a metafísica, a poética e a retórica deram sustentabilidade ao seu pensamento. Como discípulo de Platão, endossava a ideia de que o conhecimento tem seu início nos sentidos, podendo evoluir para a racionalidade.

Sobre política (Estado), o filósofo grego pregava que os seres humanos são determinados pela natureza a viver em sociedade, sendo tal condição o que nos diferencia dos outros animais. Em complemento a essa concepção, o desenvolvimento da lógica aristotélica contribuiu demasiadamente para o conhecimento científico, trazendo a noção de um instrumento para o “correto pensar”. Assim também, foi na seara da ética (relação humana) que o pensador legitimou o objetivo da vida humana atrelado à felicidade e ao bem estar, virtudes estas alcançadas pelo ato de confiar nas pessoas (Aristóteles, 1991).

Com variadas obras, destaca-se que a questão da confiança em Aristóteles pode ser representada pelos registros da “Ética a Nicômaco”. A confiança, neste sentido, apregoa a relação humana com ela mesma e com a natureza.

> Como diz o provérbio, os homens não podem conhecer-se mutuamente enquanto não houverem “provado sal juntos”; e tampouco podem aceitar um ao outro como amigos enquanto cada um não parecer estimável ao outro e este não depositar **confiança** nele. Os que não tardam a mostrar mutuamente sinais de amizade desejam ser amigos, mas não o são a menos que ambos sejam estimáveis e o saibam; porque o desejo da amizade pode surgir depressa, mas a amizade não (Aristóteles, livro VIII, 1991, p. 3, grifo nosso).

Isto posto, no pensamento aristotélico, a virtude moral é o mecanismo que diz respeito às paixões e às ações, nas quais existem excessos, carências e um meio-termo. Por exemplo, tanto o medo como a confiança, o apetite, a ira, a compaixão, e, geralmente, o prazer e a dor, podem ser sentidos em demasia ou em grau insuficiente; e, tanto num caso como no outro, isso é um mal. Senti-los numa ocasião, numa referência a objetos e como pessoas apropriadas pelo motivo e da maneira conveniente, nisso consiste o meio-termo e a excelência

característicos da virtude (Aristóteles, 1991).

Em relação aos sentimentos de medo e de confiança, a coragem é o meio-termo; o covarde é, por isso, um homem dado ao desespero, pois teme todas as coisas. Já o bravo possui a disposição contrária, pois a confiança é a marca característica de um natural esperançoso (Aristóteles, 1991).

A influência de Aristóteles sobre o desenvolvimento da Filosofia do Ocidente é notada até hodierno; que instigou, especialmente, a Filosofia Cristã de São Tomás de Aquino na Idade Média. Com efeito, entre os anos de 354-430, Santo Agostinho, também conhecido como Agostinho de Hipona, foi uma das mais importantes figuras responsável pela concepção do pensamento cristão medieval e da filosofia patrística (começada por volta do século V), nomeada assim por ter sido desenvolvida por padres e teólogos da igreja cristã, os quais eram chamados de “pais da igreja”. Sua finalidade era defender o cristianismo e refutar o paganismo.

Os estudos de Agostinho foram influenciados pelo “idealismo” de Platão e pelo “maniqueísmo” (mas não permaneceu totalmente nele), segundo o qual o mundo seria regido pelas forças do bem (Deus) e do mal (Diabo) (concepções de base platônica), bem como pelo “neoplatonismo” de Plotino (Santo Agostinho, 2017) .

O filósofo e teólogo reforçou o conceito de “pecado original”, de “cidade espiritual de Deus” e de “livre-arbítrio”, este último, dependendo do caminho escolhido, causaria o afastamento do bem, pois a origem do mal estaria no livre-arbítrio. Defendia também a “predestinação divina”, associada à salvação dos homens pela graça divina e o “providencialismo”, em que a ocorrência das coisas é permissão de Deus.

Acreditava que a fé era o caminho para a verdade (a palavra de Deus) e a razão servia para provar/validar essas verdades. Logo, os dois pensamentos cooperavam-se: a razão auxiliando na busca da fé, que por sua vez, não poderia ser atingida sem o pensamento racional.

Com uma vasta obra, ainda assim, seu acreditar na questão da confiança está direcionado a Cristo, e, consequentemente, a tudo que compõe a virtude do que significa ser bom e do bem. No livro “Confissões”, sua autobiografia, Santo Agostinho relatou sua vida antes de cristão até sua conversão.

> Contudo, refletindo e comparando sempre mais o que os filósofos haviam teorizado acerca do mundo material e de toda a natureza sensível, cada vez mais me capacitava de que eram muito mais prováveis as doutrinas destes que as dos maniqueus. Por isso, duvidando de tudo e flutuando por entre as doutrinas, à maneira dos acadêmicos, como os julga a opinião geral, resolvi abandonar os maniqueus, julgando que enquanto tivesse em dúvida não devia permanecer em uma seita à qual eu já antepunha alguns filósofos. Recusava-me, contudo, terminantemente, a confiar-lhes a cura das enfermidades de minha alma, por ser-lhes desconhecido o nome salutar de Cristo (Santo Agostinho, 2017, p. 45).

Assim, o cristianismo está centralizado nas considerações do que é o verdadeiro caminho confiável, do modo de vida mais idôneo e reto. Santo Agostinho (2017, p. 46) realçou: "como estava certo de que me concederias o que faltava – pois lhe havias prometido a graça total – respondeu-me, com muita calma e com o coração cheio de confiança, que esperava em Cristo que, antes de sair desta vida, me havia de ver católico fiel", pois lança-te com confiança, que ele te receberá e te curará.

> Trevas deploráveis me envolvem, que me escondem minhas faculdades reais; por isso, quando meu espírito indaga a respeito de suas forças, bem sabe que não pode confiar em si mesmo, por seu íntimo permanecer muitas vezes insondável, até que a experiência lho manifeste. Ninguém, pois se deve ter seguro nesta vida, que é tentação perpétua. Pois. Como podemos nos tornar melhores, não aconteça de nos tornar piores. Nossa única esperança, nossa única confiança, nossa firme promessa é tua misericórdia. (Santo Agostinho, 2007, p 107).

Sua autobiografia não foi completa, datou do início dos anos 400, bem antes de sua morte. A filosofia agostiniana influenciou outro grande pensador, São Tomás de Aquino (1225-1274), notável padre italiano, intitulado Doutor da Igreja Católica e "príncipe da escolástica", igualmente a Santo Agostinho (Campos, 2016).

A Filosofia Medieval pregava que suas doutrinas deveriam ser ensinadas e ficou dividida em duas fases: a patrística e a escolástica (século IX-XVI), esta, que advinda do termo escola, foi o período no qual as primeiras universidades instituíram-se na Europa. Concebida como uma corrente filosófica, e também como um método de pensamento crítico dialético que unia fé e razão, reverberou nas áreas do conhecimento à época.

Como representante principal dessa última fase, Tomás de Aquino baseou-se, principalmente, nas ideias aristotélicas, corroborando que o objetivo da vida humana era a felicidade e para alcançá-la tornava-se necessário buscar o "justo-meio", a "prudência" e o "conhecimento prático" capaz de conduzir o indivíduo no caminho virtuoso para o bem. Reafirmou a lógica grega de Aristóteles como premissa reflexiva sobre o "ser", a fim de provar a "existência de Deus", da "alma humana" e da "imortalidade" e para justificar a fé a partir da razão.

Defendeu a religião cristã das "heresias" e em sua obra "As cinco provas da existência

de Deus", demonstrou tal existência pela razão, no que ficou conhecida como "vias" (Campos, 2016): 1. via do movimento – tudo se move e por isso deve existir uma causa, provocada, pioneiramente, por Deus, Criador de todas as coisas; 2. via da causa eficiente – tudo possui uma causa, sendo Deus o primeiro causador; 3. via do contingente e do necessário – as coisas existem por serem necessárias. Há algumas coisas que são acidentais, os "contingentes". Caso elas existam, obedecem a um propósito. Logo, existe algo superior que ordenou todo o universo para que todas as coisas pudessem existir, e, este ser é Deus; 4. via dos graus e da perfeição – para cada coisa que existe no mundo há graus diferentes de perfeição. E o ser mais perfeito é Deus, do qual derivam todas as criaturas; 5. via do governo das coisas ou da finalidade – tudo possui um fim, mas nem todas as coisas entendem sua finalidade. Deus é o fim de todas as coisas; é a inteligência maior para tudo que existe; foi Ele quem ordenou todas as coisas do universo.

Aquino (2001) acreditava que, para o conhecimento de qualquer verdade, o indivíduo necessitava da ajuda divina e que o intelecto era movido pelo agir de Deus. Na "Suma Teológica", o filósofo italiano apresentou relações entre Ciência, razão, Filosofia, fé, teologia, mística etc., isto é, o saber humano, a tradição cristã, a ética pessoal e social, a contemplação e união com Deus; tendo sempre como objetivo maior de se alcançar a realização plena do ser humano e da sociedade. Encontra-se diante de um novo pensamento filosófico cristão privilegiando também a vontade humana.

Conforme Aquino (2001), a palavra confiança significa "*fidúcia*" do latim, que vem de "*fides"*, fé; e a fé significa crer em alguma coisa ou em alguém, mesmo sem vê-los. Ora, a confiança é própria da esperança, definindo-se, principalmente, pelo fato de se acreditar nas palavras de alguém e, por isso, chama-se a confiança de esperança que se nutre, fundada num determinado fato.

Essa ideia de confiança como esperança é corroborada em diversos trechos da "Suma". Para Aquino (2001), segundo parece, a esperança é o mesmo que confiança; de onde vem dizer que quem espera confia, quase querendo identificar as duas expressões – confiar e esperar. A confiança, como a fé, pertence à potência cognitiva. Logo, também a esperança.

A esperança pressupõe o amor e o desejo da coisa esperada; ou, melhor dizendo, a confiança concerne à certeza da fé e a magnanimidade à grandeza da coisa esperada. O objeto próprio da magnanimidade é a esperança num bem difícil. Portanto, como a confiança robustece a esperança, por provocar uma reflexão, levando-se a opinar com segurança, que se conseguirá um determinado bem, resulta que a confiança faz parte da magnanimidade (Aquino, 2001).

Percebe-se que a esperança não é outra coisa senão a confiança. Ora, a esperança não pertence à coragem, mas antes, é uma virtude especial. Ademais, a confiança não deve ser considerada parte da coragem, uma vez que ela ensina a resistir aos perigos. Ora, a magnificência e a confiança não têm, por natureza, nenhuma relação com o perigo. Logo, não são convenientemente consideradas partes da coragem (Aquino, 2001).

Em contraponto, a confiança é oposta ao temor, pois não temer é antes próprio da coragem. Logo, também a confiança mais pertence à coragem que à magnanimidade (Aquino, 2001). Em outro trecho, o pensador italiano expõe a característica da escolástica, atrelando a confiança em Deus à fé e à razão.

> Mas temos confiança, e ansiosos queremos mais ausentar-nos do corpo, e estar presentes ao Senhor. Por onde é manifesto, que essas almas, separadas dos corpos, andam por visão, contemplando a essência de Deus, na qual consiste a verdadeira beatitude. – E isto mesmo também se demonstra pela razão. Pois o intelecto, para a sua operação, só precisa do corpo por causa dos fantasmas, nos quais descobre a verdade inteligível, como na primeira parte se disse. Ora, como também já se demonstrou nessa mesma parte, a divina essência não pode ser vista pelos fantasmas (Aquino, 2001, p. 956).

Conforme Rotenberg (2022), o uso da palavra "*trust*" na fala comum é datado do século XIII, em inglês medieval; provavelmente, sua origem é escandinava, sendo similar a *traust* (confiança) em norueguês antigo; e similar a *treowe* (fiel) em inglês antigo.

O termo confiança, quando inserido no contexto religioso, vem de muito antes. Pode-se encontrar “a confiança em Deus”, por exemplo, no novo e no antigo testamento, assim também no Alcorão. Hodiernamente, a confiança no uso religioso pode ser demonstrada na expressão “*In God We Trust*” (confiamos em Deus) – lema oficial dos Estados Unidos da América (EUA), aparecendo em muitas das notas de dólares (Rotenberg, 2022).

Mesmo que não tenha recebido tal nomenclatura, a confiança sempre esteve vigente na humanidade, pressupondo, sua existência, pela possibilidade da falta dela. É justo dizer que a corrupção e a falta de confiabilidade têm estado presentes durante todo o curso da história – Maquiavel atestou isso (Rotenberg, 2022) quando dizia:

> O desdém de uns e a desconfiança dos outros impedem qualquer cooperação proveitosa. Por isso um príncipe que não entenda de milícia, além de outras infelicidades já mencionadas, tende a não ser estimado por seus soldados nem poder fiar-se neles. Como consequência, ao regente de um principado cumpre dedicar-se com afinco aos misteres da guerra, sobretudo em tempos de paz (Machiavelli, 2019, p. 89).

Nicolau Maquiavel (1469-1527) foi um dos pioneiros no pensamento político moderno; apoiava os ideais republicanos e renascentistas, marcando o fim da Idade Média e a alvorada da Idade Moderna. “O Príncipe”, seu livro, causou uma revolução sobre política,

pautando-se em princípios morais e éticos. Estudou conceitos baseados na união da teoria e da prática; no empirismo e no método indutivo e na natureza humana (Machiavelli, 2019).

A frase “os fins justificam os meios” foi atribuída a Maquiavel, porém, não proferida pelo filósofo. **Essa paráfrase significa que qualquer método seria aceitável para se alcançar um objetivo importante.**

Para Machiavelli (2019), um príncipe deve ser lento no crer e no agir, não se alarmar por si mesmo e proceder de forma equilibrada, com prudência e humanidade, buscando evitar que a excessiva confiança o torne incauto e a demasiada desconfiança o faça intolerável.

> Isso, contudo, não deve impedir que um tal príncipe seja cauteloso no formar as suas opiniões e traduzi-las em atos, e que não se alarme sozinho, levado pela própria imaginação. Incumbe-lhe proceder sem excessos, para que a demasiada confiança não o tome imprudente e a demasiada desconfiança intolerável. Daqui nasce uma questão: é melhor ser amado ou temido? Na minha opinião, conviria ser ambas as coisas. Dada, porém, a dificuldade de preencher alguém esse duplo requisito, o mais vantajoso é ser temido (Machiavelli, 2019, p. 100).

A concepção de Maquiavel acerca da confiança denota a firmeza de um líder, de um governante, ou, como ele mesmo chamava, de “um príncipe”, em que o Estado detinha todo o poder e mérito para praticar suas ações desde que direcionada ao bem-estar dos cidadãos, dicotomizando da doutrina cristão medieval.

> [...] ao deitar a mão a um Estado, deve o conquistador refletir nas ofensas que precisa de fazer; e fazê-las todas de uma vez para não ter de renová-las todos os dias e poder, não as renovando, tranquilizar os cidadãos, bem como, beneficiando-os, ganhá-los para a sua causa. Quem por timidez ou maus conselhos procede de maneira diferente, parece estar sempre de espada em punho e nunca poderá ter confiança nos seus súditos, já que estes, a seu turno, pela força mesma das contínuas e sempre recentes injúrias, igualmente nenhuma poderão ter confiança nos seus súditos, já que estes, a seu turno, pela força mesma das contínuas e sempre recentes injúrias, igualmente nenhuma poderão ter nele (Machiavelli, 2019, p. 61).

No seio do pensamento filosófico moderno como se conhece atualmente, René Descartes (1596-1650) foi um estudioso francês da corrente do racionalismo e, especialmente, da Matemática. Criou o método cartesiano com a geometria analítica e com o sistema de coordenada (plano cartesiano) que serviu de alicerce para o desenvolvimento da ciência à época. Este, fundamentou-se em quatro etapas: a) verificar – observar se aquilo que se pretende estudar é real; b) analisar – desmembrar o objeto a ser conhecido em partes simples de serem compreendidas; c) sintetizar – reagrupar os conhecimentos obtidos em um todo verdadeiro e essencial; d) enumerar – definir e concluir todo o conhecimento que pode ser extraído do objeto estudado.

Não aderiu à escolástica, atribuindo que seus ensinamentos não conduziam a nenhuma verdade indiscutível, e corroborou que era a Matemática demonstradora daquilo que afirmava.

Em consequência, rompeu com a filosofia aristotélica, propondo uma ciência unitária e universal, lançando as bases do método científico moderno.

A filosofia de Descarte englobou as vias da verdade absoluta e incontestável; jamais se deveria acreditar no "falso". A ciência para ele deveria ser prática e não especulativa e para atingi-la desenvolveu o "método da dúvida", consistindo em questionar todas as ideias e teorias preexistentes; e só assim alcançaria o conhecimento verdadeiro: algo seguro e indubitável (Descartes, 2001).

Descarte corroborou que a única verdade possível era sua capacidade de duvidar. Para a verdade absoluta, o filósofo expôs quatro regras para se chegar ao conhecimento: 1. nada é verdadeiro até ser reconhecido como tal; 2. os problemas precisam ser analisados e resolvidos sistematicamente; 3. as considerações devem partir do mais simples para o mais complexo; 4. o processo deve ser revisto do começo ao fim para que nada importante seja omitido (Descartes, 2001).

> Mas não recearei dizer que julgo ter tido muita felicidade de me haver encontrado, a partir da juventude, em determinados caminhos, que me levaram a considerações e máximas, das quais formei um método, pelo qual me parece que eu consiga aumentar de forma gradativa meu conhecimento, e de elevá-lo, pouco a pouco, ao mais alto nível, a que a mediocridade de meu espírito e a breve duração de minha vida lhe permitam alcançar. Pois já colhi dele tais frutos que, apesar de no juízo que faço de mim próprio eu procure inclinar-me mais para o lado da desconfiança do que para o da presunção, e que, observando com um olhar de filósofo as variadas ações e empreendimentos de todos os homens, não exista quase nenhum que não me pareça fútil e inútil, não deixo de lograr extraordinária satisfação do progresso que creio já ter feito na procura da verdade e de conceber tais esperanças para o futuro que, se entre as ocupações dos homens puramente homens existe alguma que seja solidamente boa e importante, atrevo-me a acreditar que é aquela que escolhi. (Descartes, 2001, p. 6-7).

Dessa forma, a dita verdade absoluta sintetiza o "eu penso", a partir da qual conclui sua própria existência, encerrando uma de suas mais famosas teorias: "penso, logo existo"; frase disposta em uma de suas obras mais notáveis – "Discurso do Método". Essa obra é um tratado do matemático (1637) envolvendo o princípio da dúvida como método para o conhecimento (dúvida metódica) que lançou as bases do racionalismo. Buscou algo concreto que servisse de alicerce para o conhecimento, duvidando de tudo que existe até se deparar com uma certeza fundamental, o cogito: penso-existo.

Nesse sentido, fica assimilativo compreender a questão da confiança no pensamento de Descarte, o qual está direcionado ao método e, consequentemente, à busca da verdade e do conhecimento como chave resolutiva das coisas para se gerar e ter confiança.

> Depois que o conhecimento de Deus e da alma nos tenha dado a certeza dessa regra, é muito fácil compreender que os sonhos que imaginamos quando dormimos não devem, de forma alguma, levar-nos a duvidar da verdade dos pensamentos que nos ocorrem quando despertos. Pois, se sucedesse que, mesmo dormindo, tivéssemos alguma ideia muito distinta, como, por exemplo, que um geômetra criasse qualquer nova demonstração, o sono deste não a impediria de ser verdadeira. E, quanto ao equívoco mais recorrente de nossos sonhos, que consiste em nos representarem vários objetos tal como fazem nossos sentidos exteriores, não importa que ele nos dê a oportunidade de desconfiar da verdade de tais idéias, porque estas também podem nos enganar repetidas vezes, sem que estejamos dormindo, como ocorre quando os que têm icterícia veem tudo da cor amarela, ou quando os astros ou outros corpos extremamente distantes de nós se nos afiguram muito menores do que são (Descarte, 2001, p. 45).

Para John Locke (1632–1704), o ser humano é uma tábula rasa, uma folha em branco, que vai sendo preenchido por suas experiências de vida. E essa experiência torna-se a base para o conhecimento. Por essa teoria, o filósofo foi considerado empirista. Conhecido como um dos "patronos do liberalismo moderno", definiu que o direito à propriedade, à vida e à liberdade são naturais dos seres humanos.

Sua filosofia dizia: pessoas que vivem em comunidade possuem experiências compartilhadas, as quais são fontes de disputas que poderiam ser resolvidas por um terceiro elemento: o juiz (Locke, 2012). Esse agente regulador, garantidor da liberdade e dos direitos fundamentais, sobretudo, o direito à propriedade privada é o Estado, em que os indivíduos seguem um "contrato social". Semelhante teoria pertence a uma corrente de pensamento chamada "contratualismo" e pregava que pessoas deveriam ser livres e iguais, representando o abandono da liberdade natural para a liberdade civil sob à égide das leis do Estado. O viver de acordo com as leis da natureza, em um estado pré-social (estado de natureza), não se baseia no contratualismo.

Em consequência disso, também foi responsável pelo desenvolvimento da teoria das leis e do surgimento do Estado. A principal concepção filosófica de Locke era a afirmativa de que todo conhecimento provinha das experiências, tanto de origem externa, nas sensações, quanto interna, por meio das reflexões. Isto é, antes de o sujeito perceber qualquer coisa, a mente deveria ser pensada como uma folha de papel em branco. Contudo, após ele começar a perceber tudo à sua volta, surgem as "ideias sensoriais simples".

Tais sensações são executadas pelo conhecimento, pelo pensamento, pela dúvida e pela crença, no sentido de confiar/acreditar. Locke (2012) chamou isso de reflexão. Assim, a mente não seria apenas um receptáculo inerte, mas o processamento de sensações formadoras da personalidade do sujeito.

Não obstante, a política para o filósofo inglês cunhava ideais de liberdade intelectual e de tolerância, criticando também a teoria do direito divino dos reis, por exemplo. Em

complemento, dizia que a soberania não deveria residir no Estado, mas na população. Pois, para assegurar um Estado de direito, os representantes do povo deveriam promulgar as leis e o rei ou o governo executá-las e, assim, apresentou a teoria de divisão de poderes, propondo o equilíbrio entre o rei e o parlamento.

John Locke publicou algumas obras e entre um de seus destaque está o "Ensaio acerca do Entendimento Humano" de 1689. As características do significado de "confiar" ou "ter confiança" nessa obra estão afinadas às noções de ética da crença e de responsabilidade em crer e, precipuamente, na verdade, em que o ser humano era uma tábula rasa, folha em branco, e obtinha conhecimento durante seu percurso de vida, podendo, a partir daí, ter confiança em alguém ou em algo.

> Quanto mais considerarmos e compreendermos verdade e razão por nós mesmos, mais conhecimento real e verdadeiro teremos. A flutuação das opiniões de outros homens em nosso cérebro não nos torna mais sábios, mesmo que elas sejam verdadeiras. A ciência de outro homem é, em nós, opinião, se assentimos a venerada reputação sem usarmos, como ela, nossa própria razão, para entender as verdades que apresenta. Aristóteles foi certamente um homem de conhecimento; mas não era reputado por abraçar às cegas e expor como certa a opinião alheia. Se adotar princípios alheios sem examiná-los não é o que fez de Aristóteles um filósofo, é de supor que ninguém se torna filósofo nessa via. Em se tratando de ciências, cada um só tem o que realmente conhece e compreende: aquilo em que crê, e que aceita em base de confiança, não passa de migalhas: boas para o dono, nada acrescentam à provisão de quem as recolhe. Essa riqueza é como dinheiro falso: ouro nas mãos de quem empresta, pó nas de quem usa (Locke, 2012, p. 92).

Para Locke (2012), aqueles que falam em princípios práticos e não dizem quais seriam eles, como seria justo esperar de quem sustenta essa opinião, tem-se motivos para desconfiar de seu conhecimento e de sua sagacidade.

Foi também no começo da Idade Moderna que a palavra *trust* (confiança) adquiriu *status* de conceito em teoria política e Locke foi o autor que mais se notabilizou por conferir a esta palavra um verdadeiro sentido político.

No que confere à confiança, Locke a utiliza, no "Segundo Tratado sobre o Governo Civil", em um sentido estritamente político, como um elemento crucial de seu argumento contra o patriarcalismo político (Feres Júnior; Eisenberg, 2006). O filósofo começa por analisar a

> confiança pessoal em seu contexto mais próprio: a família. A intenção é mostrar que a confiança dos filhos na autoridade paterna se justifica pela proximidade dos laços afetivos que unem a família. De maneira similar, sustenta Locke, as primeiras comunidades eram formadas por laços de amizade e parentesco, e, consequentemente, esse tipo de confiança de origem pessoal foi estendido aos seus líderes. Tanto no caso da família como no das pequenas sociedades primitivas, a confiança depositada no chefe pressupõe tacitamente que este olhe pelo bem comum (Feres Júnior; Eisenberg, 2006, p. 467).

Então, para a resolução desse problema, John Locke propôs um contrato social em que as pessoas depositariam sua confiança no mandatário, mas com limitações. Assim, a palavra *trust* passa a ser usada num sentido diferente. Não se trata da confiança "irracional" direcionada ao patriarca, mas sim de uma confiança "racional" balizada na manutenção do bem comum. A necessidade de condicionar a confiança ao respeito à vida, à liberdade e à propriedade dos cidadãos é tão veemente que, sempre ao usar a palavra *trust* no texto, Locke (1994) em seguida reafirma as condições que limitam seu exercício.

Assim, o pensador tentou redefinir *trust* no sentido de mitigar o forte conteúdo de confiança pessoal associado a ela. Nesse esforço, Locke chamou seu novo tipo de confiança política de *fiduciary trust* (na forma latina *fides/fiducia*), a fim de reforçar o aspecto semântico contratual e, assim, distingui-lo do aspecto pessoal do uso comum de *trust* (Feres Júnior; Eisenberg, 2006; Locke, 1994). Em síntese, no início da Idade Moderna, Locke tentou

> associar significados à *trust* que já faziam parte do campo semântico de *fides* há mais de 15 séculos, isso é porque os dois termos não eram semanticamente equivalentes. A noção de *trust* parece estar fortemente ligada à ideia de confiança pessoal, enquanto *fides* sugeria, até para falantes do inglês, um tipo de confiança ligada a relações contratuais e comerciais. É interessante notar que nas línguas neolatinas, com a exceção do italiano, um prefixo "con-" foi adicionado ao radical de *fides*, o que reforça ainda mais o caráter de reciprocidade contratual do termo (Júnior; Eisenberg, 2006, p. 467-468, grifo nosso).

Outro filósofo moderno buscou criar uma revolução do conhecimento, sobretudo, influenciado pelo "Iluminismo". Immanuel Kant (1724-1804) uniu concepções racionalistas de Descarte e empiristas de Locke, a fim de criar uma compreensão sobre a razão e os "limites" do conhecimento humano. Essa nova teoria foi o "idealismo transcendental" e, como um produto geral de seu pensamento, fundou o "criticismo", estabelecendo uma crítica revisionista da Filosofia. Duas concepções incumbidas de delimitar os limites do conhecimento humano e entendê-lo. Kant (2001) mencionou que somente era possível conhecer aquilo que se pode intuir, ou seja, ver, ouvir; de fato experienciar as coisas.

O idealismo transcendental kantiano trouxe vários conceitos, em que o conhecimento poderia ser obtido com base na percepção do que ele chamou de "coisa em si ", ou "objeto". Esse processo ocorre pelo que o filósofo chamou de "intuição", sendo a racionalidade, por meio das faculdades mentais, fornecedora do conhecimento ao ser humano (Kant, 2001)

Na sua obra "Resposta à pergunta: o que é o Iluminismo", de 1784, difundiu a possibilidade do humano seguir sua própria razão, dotando-o da saída da "menoridade", sendo a covardia e a preguiça os fatores de permanência nesse estado. Para ele, a razão coordena as

sensações que são matérias-primas para o conhecimento e para a moral. “A crítica da Razão Pura” (1781) é conhecida como um dos grandes marcos de suas obras. Nesse livro, o filósofo desenvolveu a noção de argumento transcendental para mostrar verdades sobre o mundo “como ele é em si”, no qual os sujeitos são forçados a perceber e a pensar acerca do mundo de certas formas. Por exemplo, que cada evento estará causalmente conectado a outros, que aparições no espaço e no tempo obedecem a leis da Geometria, da Aritmética, da Física, entre outras áreas (Kant, 2001).

> Porque será então que ainda aqui não se encontrou o caminho seguro da ciência? Acaso será ele impossível? De onde provém que a natureza pôs na nossa razão o impulso incansável de procurar esse caminho como um dos seus mais importantes desígnios? Mais ainda: quão poucos motivos teremos para confiar na nossa razão se, num dos pontos mais importantes do nosso desejo de saber, não só nos abandona como nos ludibria com miragens, acabando por nos enganar! Ou talvez até hoje nos tenhamos apenas enganado no caminho; de que indícios nos poderemos servir para esperar, em novas investigações, sermos melhor sucedidos do que os outros que nos precederam (Kant, 2001, p. 45).

Além disso, formulou as bases de sua filosofia moral. O que funda a ação humana e o que é dado ao sujeito fazer, constituem assim, um tratado sobre a moral humana. Discutiu os princípios da ação moral enquanto forma de separá-la de uma fundamentação religiosa.

> A palavra fé, em tais casos, do ponto de vista objetivo é uma expressão da modéstia, mas ao mesmo tempo e do ponto de vista subjetivo, da firmeza da confiança. Se, neste caso, ao considerar algo verdadeiro, puramente teórico, quiser dar o nome de hipótese que fosse justificado aceitar, comprometer-me-ia, deste modo, a possuir da natureza de uma causa do mundo e de um outro mundo um conceito mais perfeito do que aquele que posso realmente mostrar. Com efeito, para admitir algo apenas como hipótese sou obrigado pelo menos a conhecer suficientemente as suas propriedades para não ter necessidade de imaginar o seu conceito, mas apenas a existência. Mas a palavra fé diz respeito unicamente à direção que me é dada por uma ideia e à influência subjetiva que exerce sobre o desenvolvimento dos atos da minha razão e que me confirma (Kant, 2001, p. 665).

Para o pensador, a razão era suficientemente capaz de resolver as questões relativas à moralidade, sem precisar do apelo à superstição ou a elementos sobrenaturais. Nisso, desenvolve o “imperativo categórico”, uma fórmula racional para a resolução de questões morais, sendo uma “lei” moral interior baseada na razão humana, não possuindo relação com autoridade do Estado ou religiosa (Kant, 2001). Entende-se que a confiança em Kant dá-se por meio da razão, uma vez que para se perceber o mundo como ele é, torna-se necessária a crítica para delimitar o conhecimento humano e resolver as questões relativas à moralidade.

Conforme Feres Júnior e Eisenberg (2006), até o século XVI, o termo confiança foi utilizado sem metáforas, referindo-se à relação entre amigos, parentes, pessoas conhecidas e a Deus. Ainda no mesmo século, “*trust”* passou a ser usado para significar “comprar em

confiança", ou melhor, comprar fiado, a crédito. Nesse período, o termo foi compartilhado pela terminologia jurídica como uma relação em que uma pessoa é a tutora de bens de outras.

> As palavras disponíveis nas principais línguas neolatinas que melhor traduzem a noção de *trust* são, em sua maioria, derivadas do termo latino *fides*: confiança em português, *confianza* em espanhol, *confiance* em francês, e *fiducia* em italiano. Contudo, os significados atribuídos ao termo *fides* em latim parecem não corresponder exatamente ao conteúdo semântico de *trust* em inglês. Uma vez que não nos é possível aqui proceder a uma análise pormenorizada dos termos de cada língua, vamos direto à língua fonte (Feres Júnior; Eisenberg, 2006, p. 465).

Nesta pesquisa, a confiança foi tratada de forma generalizada, com várias visões e teorias, levando em consideração conceitos advindos de áreas distintas e de autores distintos. No "*Cambridge Dictionary*"[7], a palavra confiança (*trust/confidence),* sinônimo de "fé", significa crença na honestidade de alguém. Já "*trust"*[8] (confiar/crer), por suave, denota acreditar que alguém é bom e honesto e não vai prejudicá-lo, ou que algo é seguro e confiável.

No "*Online Latin Dictionary*", o termo *fiducia*[9] significa confiança, fé e coragem. Já "fido"[10] confiar ou ter confiança em alguém. Nos registro do *"Dictionary Merriam-Webster", trust* é sinônimo de *confidence* (confiança), *care* (cuidado), *custody* (custódia) e *trustworthiness* (confiabilidade), definido como a crença de que alguém ou algo é confiável, bom, efetivo.

O Dicionário Brasileiro de Terminologia Arquivística e o Dicionário de Terminologia Arquivística de Camargo e Bellotto (1996) não mencionam o termo. Santos (2001), no "Dicionário Jurídico Brasileiro", diz que confiança é a segurança íntima com que se procede; sinônimo de crédito e de fé. Para o "Dicionário de Sociologia" aparece apenas o termo "confiabilidade", sendo o grau em que um instrumento de medida fornece os mesmos resultados a cada vez que é usado, isto é, aquilo que se mede não muda (Johnson, 1997).

Complementando, Filgueiras (2007) atenua que articular dialeticamente *confidence* com *trust* significa refletir o modo como as instituições políticas podem realizar a proteção das pessoas, visando diferentes imperativos éticos.

3.1 AS PERSPECTIVAS VIGENTES DO CONCEITO DE CONFIANÇA

Em um estudo utilizando *Survey*, Ronald Inglehart realizou entrevistas ao redor do mundo e fez a seguinte pergunta: "em geral, você diria que a maioria das pessoas é confiável

[7] Disponível em: CONFIANÇA | Tradução para o inglês - Cambridge Dictionary.
[8] Disponível em: CONFIANÇA | Tradução para o português - Cambridge Dictionary.
[9] Disponível em: DICIONÁRIO ONLINE DE LATIM - Latim - Inglês (online-latin-dictionary.com).
[10] Disponível em: DICIONÁRIO ONLINE DE LATIM - Latim - Inglês (online-latin-dictionary.com).

ou que devemos ser precavido com elas?" (Feres Júnior; Eisenberg, 2006). Essa pesquisa teve início nos anos de 1980 e a mais recente foi publicada em 1999, objetivando comparar opiniões públicas sobre aspectos socioculturais e políticos de vários países. Nesta última edição, o *World Values Survey* abrangeu 65 países nos cinco continentes e tratou das relações entre confiança, bem-estar e democracia (Inglehart, 1999).

As informações desse estudo cobriu 80% da população mundial, e em cada país foram analisados grupos locais e com verbal local, por meio de interpretações em que o nível de confiança interpessoal (relação entre pessoas) é, em grande parte, um produto da cultura política de um povo, e que essa confiança está diretamente relacionada à estabilidade do regime democrático (Feres Júnior; Eisenberg, 2006).

Assim, Inglehart (1999) corroborou que o grau de confiança interpessoal de uma determinada sociedade está enviesadamente direcionado à estabilidade democrática e às tradições culturais-religiosas. Para ele, democracias estáveis e protestantismo promovem um alto grau de confiança interpessoal. Instabilidade democrática e catolicismo, por sua vez, produzem pessoas desconfiadas (Feres Júnior; Eisenberg, 2006).

Historicamente, os países católicos tendem a ter níveis baixos de confiança interpessoal, bem como de desenvolvimento econômico, enquanto os países historicamente protestantes e confucionistas tendem a ser elevados (Inglehart, 1999). É provável, argumenta o autor, que fatores culturais de longo prazo como estes deem uma contribuição forte e independente tanto para o desenvolvimento econômico como para a disposição que estabiliza a democracia.

Embora o desenvolvimento econômico e outros fatores culturais possam contribuir para a confiança interpessoal e o bem-estar subjetivo que estabiliza as democracias, estes mesmos fatores podem coexistir, causando o declínio da confiança nas instituições políticas e na elite. O fato é que, nas democracias estáveis, as instituições políticas e as elites provavelmente não são menos confiáveis do que no passado. Pelo contrário, o declínio da confiança nas instituições reflete provavelmente um declínio mais geral no respeito pela autoridade que surgiu com o desenvolvimento das culturas pós-materiais. Quando as pessoas já não se preocupam com a sua sobrevivência, não precisam de se apegar inquestionavelmente às autoridades que esperam que garantam a sua sobrevivência. Em vez disso, com o bem-estar material aumentando, é provável que a confiança nas instituições políticas e nas elites diminua à medida que os públicos começam a avaliar os seus líderes e as instituições segundo padrões mais exigentes.

Conforme Rotenberg (2022), resultados de enquetes são questionáveis, contudo, têm a

dupla função de expressar preocupação e de moldar opinião pública sobre confiança, isto é, a ansiedade em relação a ela. Esses mesmos resultados também transmitem uma mensagem simples a um público atento.

Não se pode perder de vista, contudo, que Inglehart acostou-se nos escritos de Putnam (2006) e de Fukuyama (1995) acerca da confiança interpessoal, concluindo que ela seria como um elemento fundamental para o desenvolvimento de democracias modernas. Conforme Putnam (2006) e Fukuyama (1995), tal confiança permite a cooperação entre indivíduos de diferentes naturezas, sendo de grande importância, no plano político, para a estabilidade das instituições, no plano econômico, para o funcionamento de sistemas de produção complexos de larga escala. No Brasil, por exemplo, 7% dos entrevistados responderam que a maioria das pessoas é digna de confiança – menor resultado entre os 43 países pesquisados. Há inúmeras maneiras de interpretar estas informações, e muitas delas provavelmente atribuíram o baixo nível de confiança interpessoal dos brasileiros a um conjunto de características de cultura cívica e política do país.

Filgueiras (2007) constatou que a formalidade com que o estudos de Inglehart foram conduzidos em sua abordagem empírica encobriu a volatilidade do termo confiança devido ao fato de diferentes povos terem um conceito distinto do que é confiar em seu semelhante.

> Elementos de definições populares de confiança são (de modo bastante correto) encontrados nos conceitos acadêmicos de confiança. É importante destacar que a conceitualização da confiança em escritos acadêmicos varia consideravelmente segundo a teoria, a estrutura, o modelo ou a abordagem adotados por um pesquisador. Esse fato contribui para os problemas que os pesquisadores com diferentes abordagens têm para se engajar com os conceitos uns dos outros. Essas diferenças contribuem para a divergência ao decidir se o estudo e os resultados serão ou não aceitos pela comunidade acadêmica e publicáveis (Rotenberg, 2022, p. 3-4).

Nesse viés, esgotar conceitos é uma tarefa complexa. Estudá-los e determiná-los requer empenho, conhecimento e domínio. Embora a ideia de confiança esteja compreendida em diversas áreas do saber, sua definição não se exaure e pode-se realçar que isto ocorre porque sua concepção é dinâmica e está associada às mudanças da sociedade.

Analisada pela Psicologia, Ciências Políticas, Sociologia, Economia, Direito e Filosofia, entre outras áreas, a confiança vem sendo pesquisada por meio de lentes distintas: relacionamentos entre organizações; entre indivíduos; em sistemas; e sobretudo, nas relações humanas (Pereira, 2010). A mesma autora complementa que, por muitos anos, seu construto tem captado interesse de várias áreas; nos idos de 1950 e 1960, os pesquisadores descobriram sua importância nos relacionamentos pessoais (estudos que continuaram durante a década de 1970); nos anos de 1980 e 1990, foram publicados muitos estudos sobre o tema nas mais

diversas disciplinas, ampliando os horizontes daquelas mais tradicionais, dando enfoque àquelas que ainda não tinham estudado o tema.

Sua acepção está associada a dicotômicos vocábulos conforme já visto, entre os quais, destacam-se a verdade, a crença, a fé, a segurança, a coragem, a força, a moral, a política etc., que são variáveis essenciais à compreensão das partes do que vem compô-la.

Do ponto de vista de Rotenberg (2022), a confiança é análoga à matéria escura do universo físico. Uma substância extensa, mas de difícil detecção, que liga os planetas e o material terrestre. Do mesmo modo, a confiança é uma força prevalente, muitas vezes silenciosa, conectando as pessoas e garantindo seus relacionamentos; sem isso, o "universo" social não existiria.

> [...], diversas ciências sociais têm dado relevância à confiança que os indivíduos sentem em relação aos outros. Vejamos alguns exemplos: a Sociologia tem-se preocupado sobretudo com a confiança social e interpessoal, e a forma como estas afetam a vida dos indivíduos em sociedade. Tem-se observado, por exemplo, que níveis elevados de confiança levam a uma maior integração social dos indivíduos e a uma maior predisposição para a cooperação. À Psicologia tem igualmente interessado a confiança interpessoal, embora neste caso seja a importância na conduta individual que revele (ou na interacção social, se considerarmos a Psicologia Social). Sob esta perspectiva, a confiança interpessoal é usualmente associada à satisfação dos indivíduos com a sua vida pessoal, ao optimismo, ou ao bom estado de saúde e longevidade (Belchior, 2015, p. 24).

Isso denota que a existência da confiança é imprescindível para o viver na sociedade. Segundo Diniz e Marconatto (2011), duas condições instalam-se para que a confiança seja desenvolvida:

a) **O risco ou a vulnerabilidade:** a probabilidade de se perder algo e/ou alguém, quando interpretada por uma das partes decisórias.
b) **Interdependência:** quando os interesses de uma das partes não podem ser atingidos sem a colaboração da outra.

Para os autores citados, observar a confiança nesses sentidos (individual ou coletivo) se parece com um mecanismo substituto de aparatos formais que se destinam a controlar e a fiscalizar a ação dos agentes em seus relacionamentos, seja ele do tipo patrão-empregado, pessoas-sistemas, pessoas-pessoas. Isto quer dizer, por exemplo, que quanto maior a confiança existente entre dois negociadores, menos a sua relação demandará de marcos regulatórios (como contratos formais), uma vez que há a crença de parte a parte de que um não trairá o outro, ou seja, não incorrerá em comportamentos oportunistas (Diniz; Marconatto, 2011).

Destarte, Barney e Hansen (1994) destacam três diferentes níveis de confiança: fraca,

semiforte e forte.

- Confiança fraca: pressupõe que uma das partes não explorará as vulnerabilidades da outra, pois não existem vulnerabilidades significativas. Aqui, a confiança emerge porquanto não há como os envolvidos agirem de modo oportunista. Esse tipo de confiança acontece em transações nas quais a avaliação do valor e a qualidade dos objetivos trocados podem ser examinados facilmente (Diniz; Marconatto, 2011).
- Confiança semiforte: esse modelo de confiança enfatiza o papel da racionalidade na tomada de decisão, por exemplo, algumas trocas valiosas não podem ser executadas, visto que o custo da estrutura de governança necessária para gerar o nível semiforte de confiança é maior que o ganho esperado na troca. Acontece quando se doa mais e se recebe menos.
- Confiança forte: a confiança não se sustenta sobre mecanismos sociais ou econômicos de governança, como no tipo semiforte, mas a partir de valores, de princípios e de padrões de comportamentos pelas partes envolvidas na troca. As duas partes compartilham mutuamente uma série de vulnerabilidades – de todas as magnitudes e naturezas – mas, independentemente da existência de mecanismos de governança, confiam em si, devido ao que e a quem elas são (Diniz; Marconatto, 2011).

A origem da confiança, segundo Bateson e Hoffman (2001), pode ser destrinchada a partir de uma análise evolutiva da cooperação, relacionada às suas condições de ocorrência ou não. Para eles, existem três tipos de aplicações formada pela cooperação social: a não-manipulativa, quando os indivíduos estão fortemente relacionados; a necessidade de sobrevivência de muitos indivíduos; e quando os benefícios são compartilhados por ambas as partes.

Para Gambetta (2008a), cooperação é o sentido amplo de agentes (indivíduos, empresas e governos) acordarem qualquer conjunto de regras (contrato) dentro de suas interações. Para o autor, os acordos não precisam ser resultado de comunicação prévia, podem surgir implicitamente no curso da própria interação; e as regras não necessitam ser registradas, mas estabelecidas como resultado do hábito ou da experiência anterior bem-sucedida. Assim, a forma mais básica de cooperação humana é a condição de uma interação benéfica, sendo preciso algum nível de confiança em que as partes consigam cumprir certas regras.

> A cooperação exige frequentemente alguma exigência ao nível da confiança, em particular da confiança mútua. Além disso, se a confiança existe apenas unilateralmente, a cooperação também pode falhar [...]. Contudo, dependendo do grau de restrição, de risco e de interesse envolvido, a confiança como uma pré-condição de cooperação pode ser submetida a exigências de diferentes intensidades: dependendo da força dos mecanismos que regem nossas decisões, e também sobre os regimes sociais em que essas decisões se inserem (Gambetta, 2008a, p. 219-220, tradução nossa).

Uma virtude instala-se no sentido de cooperação: a crença. Gambetta (2008a) diz que se tem pouca ideia de como as pessoas realmente adquirem crenças. E, dentre essas crenças, tem-se a confiança como uma expectativa particular em relação ao comportamento provável dos outros. O autor complementa que a cooperação está condicionada à crença de que a outra parte não está disposta a conceder confiança cegamente, porém, acreditando que o outro estará disposto a confiar se algo for executado corretamente. Sendo assim, confiança é uma crença peculiar baseada não em evidências, mas na falta dela (Pagden, 2008). Em contrapartida, essa ação realça a possibilidade de desconfiança (Gambetta, 2008b).

Assim, Gambetta (2008a) define confiança, simetricamente à desconfiança, como um grau particular subjetivo de probabilidade, no qual um agente acredita que outro agente ou grupo realizará uma ação sujeita a afetar a sua própria ação. Quando se diz que se confia em alguém ou que alguém é confiável, significa que a probabilidade dela realizar uma ação é benéfica ou pelo menos não prejudicial, sendo suficiente para que se considere alguma forma de cooperação, nesse sentido. Correspondentemente, quando alguém não é confiável, essa probabilidade é baixa o suficiente para que se abstenha de fazer qualquer ação (Gambetta, 2008a).

Sobre a definição e o exemplo acima, Gambetta (2008a) tece algumas considerações. Em primeiro lugar, “confiar” pode ser visto como um limiar localizado em uma distribuição probabilística de expectativas gerais, que podem levar a uma série de valores entre a completa desconfiança (0) e confiança total (1), e que está centrada em torno um ponto médio (0.50) de incerteza. Assim, tanto a confiança como a desconfiança representam predisposições lexicográficas para atribuir valores de probabilidade e mantê-los incondicionalmente acima de alguma evidência. Em segundo lugar, a confiança é relevante em condições de ignorância ou de incerteza em relação a ações desconhecidas ou incognoscíveis de outros, dando-se por meio da fé, que se traduz em “acreditar”. A este respeito, a confiança inclina-se a ações futuras que condicionam as decisões presentes. Em terceiro lugar, postulando que as próprias ações de um sujeito são baseadas nessa probabilidade, pode-se excluir os casos em que a confiança em alguém não tem influência nas decisões daquele sujeito. Por fim, a confiança aqui está limitada entre os agentes, excluindo aquela entre agentes e eventos naturais. Neste

nível de abstração, a definição de confiança poderia refletir-se nas intenções dos outros de não enganar.

A condição de ignorância ou de incerteza sobre o comportamento de outras pessoas também é central para a noção de confiança, assim como o grau de liberdade, o qual pode ser de cunho positivo ou negativo (traição, decepção) (Luhmann, 2008). A condição de liberdade positiva está relacionada ao limite de a capacidade de o indivíduo alcançar um conhecimento pleno sobre os outros, prevendo suas ações para antecipar qualquer liberdade negativa. Com efeito, a liberdade não é por si só suficiente para caracterizar as questões da confiança. A relação de um indivíduo com outras pessoas é um tipo de liberdade, em que aquele escolhe manter uma relação potencialmente arriscada. Laconicamente, confiar em uma pessoa significa crer que ela não o prejudicará (Gambetta, 2008a).

Luhmann (1996) discorrendo sobre os relacionamentos pessoais, enfatiza que para esse tipo de interação desenvolver-se é exigido ações que dizem respeito à liberdade de agir. Essa liberdade dos indivíduos é o que torna a vida social ainda mais contingente e, por consequência, mais complexa. É a clássica ideia da preocupação com a imprevisibilidade das ações dos outros indivíduos. Sumariamente, essa liberdade traz a responsabilidade das pessoas sobre as suas escolhas, sobre os seus atos (Mota, 2016).

Outra virtude direcionada à confiança é a restrição, relevante não apenas para se decidir até onde o indivíduo precisa confiar nos outros, mas também para os outros decidirem até onde podem confiar neste indivíduo; isto é, confiar é importante, contudo ser confiável também. Em Dasgupta (2008), essa ocorrência dá-se por meio de um “pré-compromisso”, que em suas diversas formas (unilateral ou bilateral) é um dispositivo que possibilita impor restrições. Promessas e contratos representam formas mais fracas desses pré-compromissos. O contrato, por exemplo, muda o foco da confiança para a eficácia das sanções caso um acordo seja quebrado. As promessas são interessantes na medida que usa palavras para formalização de contrato, portanto, podendo não acarretar sanções.

E, por último, nos escritos de Gambetta (2008a), há casos em que a família (ou familiaridade) e a amizade são subprodutos da confiança, acontecendo quando as partes envolvidas se conhecem e apresentam respeito e bem-estar um pelo outro. Logo, “a confiança pode emergir aí como subproduto de valores morais e religiosos” (Gambetta, 2008a, p. 230).

Como discutido acima, os principais elementos de confiança para Gambetta estão voltados aos aspectos humanos, destacando a relação com os indivíduos e o sentimento. Essa ideia está basilada no sentimento de segurança. Em síntese, e compactuando Canedo (2012), confiar em um indivíduo é o resultado de várias determinantes ou análises que em conjunto

gera a definição de confiança.

Para que uma pessoa seja considerada confiável, ela precisa levar em consideração atitudes positivas, sendo honesta, colaborativa e otimista, entre outros, em relação às entidades que dependem dela. Nessa óptica, Canedo (2012) diz que confiabilidade é a capacidade de alguém ser confiável e a confiança seria sua consequência, trazendo segurança à pessoa.

Essas análises sobre confiança busca, sobretudo, identificá-la de forma ampla, levando a cabo suas nuances conceituais e suas definições. Com isso, percebe-se que as publicações direcionadas à temática possuem destaque naquelas que se referem à confiança interpessoal e generalizada. A justificativa é que a confiança, primordialmente, inicia-se nas relações pessoais, entre, pelo menos, duas pessoas, como pode ser, por exemplo, observado no Quadro 4, e, a partir disso, desdobra-se nas suas virtudes, produtos e subprodutos.

Quadro 4 – Características da confiança

Características	**Exemplos**
A confiança é relativa a um determinado contexto ou situação.	**A** pode confiar em **B** para lhe oferecer uma carona. Entretanto, **A** não confia em **B** o suficiente para dirigir seu carro.
A confiança tem um direcionamento	**A** pode confiar em **B**, entretanto **B** pode não confiar em **A**.
A confiança pode ser medida.	**A** pode confiar mais em **B** do que confia em **C**.
A confiança possui aspecto temporal e evolutivo.	A confiança que **A** tem em **B** pode aumentar ou diminuir conforme **A** e **B** interagem.
A confiança pode ser influenciada por uma recomendação.	**A** que já confia em **B**, passa a ter certa confiança em **C**, que, por sua vez, lhe foi apresentado por **B**.
A confiança não é transitiva.	Se **A** confia em **B** e **B** confia em **A** e **C**, não significa dizer que **A** confia em **C**.

Fonte: Albuquerque (2008) e Canedo (2012).

Lundåsen (2002), em seu artigo, traz diversos conceitos de confiança generalizada, sobretudo, associado ao capital social, que encerra uma atenção maior sobre os efeitos da confiança entre os cidadãos.

> O espectro vai da economia à psicologia, passando pela sociologia e a ciência política. É óbvio que isso resultou numa variedade de definições do conceito [...]. Diz-se que a confiança generalizada, ao contrário da confiança dentro do grupo e a desconfiança fora do grupo, exerce importantes influências sobre vários aspectos da sociedade e, em seu estudo sobre a Itália, Putnam (1993) sustentou que diferentes níveis de confiança generalizada e, posteriormente, diferentes níveis de capital social levaram a níveis diversos de desenvolvimento. Encontram-se conclusões semelhantes sobre a importância da confiança para os níveis de desenvolvimento das sociedades em Fukuyama (1995) (Lundåsen, 2002, p. 305).

A autora supra, em sua explanação, ressalta que a fé é um mecanismo de confiança ligada ao fato de que alguém manterá sua palavra. Além disso, destaca também a

“previsibilidade” como expectativa para eventos futuros, em que existe a possibilidade de ocorrer algum tipo de perda se a confiança não for correspondida. Em outras palavras, há um elemento de risco envolvido. Para a autora, esses comportamentos são definidos como “patologias da confiança”, não devendo ser confundidos com a confiança verdadeira, mas sim sentimentos que a compõem.

Outros dois elementos correlacionam-se à confiança: a cobiça (ganhar um benefício obtido pela não-cooperação unilateral em vez de mútua) e o medo (ansiedade, por exemplo), agindo como agentes influenciadores da confiança. Hwang e Burgers (1997) acrescentam mais propriedades à confiança, entre elas o fato de que a confiança “não é uma condição suficiente da cooperação”, embora necessária, e que ela atenua dois tipos diferentes de risco: de ser vitimado e de perder um parceiro confiável.

Na concepção de Putnam (1993), a confiança é um elemento que aumenta à medida que é usado e diminui se não for. Robert David Putnam, cientista político norte-americano, relacionou o conceito de confiança ao de capital social. Em uma de suas obras mais emblemáticas “Comunidade e Democracia: a experiência da Itália moderna”, referência no estudo sobre confiança, analisa a Itália, no período entre 1970-1980, estudando 20 governos regionais do país. Para Putnam, os costumes da sociedade e as práticas políticas inter-relacionam-se de forma muito profunda (Belchior, 2015).

Ao observar uma diferença entre o desempenho dos governos regionais no Norte em comparação ao Sul da Itália, menos bem-sucedidos do que os primeiros, Putnam (2006) avança como principal explicação desta diferença o envolvimento cívico das populações. A maior eficiência dos governos do Norte dever-se-ia ao maior envolvimento associativo dos cidadãos, quer dizer, por meio de clubes desportivos, de associações de cariz literário, recreativo, cultural, social entre outros. A inexistência de um forte envolvimento e participação dos cidadãos em associações estaria, para Putnam, associada à prevalência da ineficiência e da corrupção nos governos regionais do Sul de Itália. Assim, a consequência da sociedade agrária ser menos próspera econômica e democraticamente é resquício do baixo capital social nessa parte do país.

> Daí que Putnam tenha concluído que o desempenho das instituições políticas e da própria democracia seriam afetadas pelo ambiente social, econômico e cultural, isto é, por características da organização social, como a confiança, as normas sociais ou as redes de interacção, que melhorariam a eficiência do sistema político ao facilitar o desenvolvimento de acções colectivas coordenadas (Belchior, 2015, p. 28).

Nas regiões cívicas da Itália, a confiança social – comportamento ou interação das pessoas com outras pessoas ou instituições na sociedade – sempre foi um elemento

fundamental do *ethos* que sustentou o dinamismo econômico e o desempenho governamental (Putnam, 2006). E para isso acontecer, complementa o autor, é geralmente necessário haver cooperação entre os Poderes Legislativo-Executivo, entre os operários e os administradores, entre os partidos políticos, entre o governo e a iniciativa privada, entre as pequenas empresas e assim por diante.

Belchior (2015) enfatiza que na obra citada, Putnam alega que seriam as redes de contato e de cooperação estabelecidas entre os indivíduos, o relacionamento entre esses de forma igualitária com base no princípio da reciprocidade, a confiança interpessoal associada à cooperação e os aspectos estimulados pelo envolvimento associativo dos indivíduos, que facilitariam as ações coletivas. Assim, pertencendo a associações, os indivíduos desenvolveriam competências de relacionamento – de confiança mútua, de cooperação, de solidariedade, de tolerância e de reciprocidade –, que potenciariam a eficácia governativa, ao estimular a ação coletiva para o alcance de interesses comuns ou públicos. E putnam (2006) designa esta condição como capital social.

> A confiança é entendida nestes termos como sentimento-chave: apenas confiando nos outros e gerando a confiança destes, a cooperação – fundamento para o desenvolvimento das comunidades – poderá ser frutífera. Claro que, na ausência da confiança, a cooperação é igualmente possível e potencialmente bem-sucedida, mas neste caso terão de ser assegurados mecanismos formais, tais como contratos ou hierarquias, que garantam que as partes cumprem os procedimentos de cooperação. Esta é uma solução de maior complexidade e com custos mais elevados (Belchior, 2015, p. 28).

Sobre o capital social, Putnam (2006) diz ser um fator unificador à prosperidade de um país desde que esteja próxima das questões públicas. Em contrapartida, a baixa do capital social seria causado pelo aumento das taxas de infelicidade e da falta de confiança; alguns exemplos deste tipo de capital: baixa confiança no governo, baixa eficiência política, ou seja, confiança na própria influência; menor participação dos cidadãos nas votações, menos cooperação para se resolver problemas sociais (dilemas de ação coletiva); em suma, a não participação e a não cooperação da sociedade em questões políticas.

Na abordagem do capital social, a confiança é definida como uma propriedade estabelecida entre os membros da sociedade ou das redes sociais que ligam os indivíduos, promovendo normas de cooperação recíproca (Belchior, 2015; Rotenberg, 2022). Tal capital é um constructo multidimensional aplicado às relações fraternais de família e amigos, de bairros, de cidadãos na sociedade, do Estado e das instituições.

> [...] o capital social diz respeito a características da organização social, como confiança, normas e sistemas, que contribuam para aumentar a eficiência da sociedade, facilitando as ações coordenadas: 'assim como outras formas de capital, o capital social é produtivo, possibilitando a realização de certos objetivos que seriam inalcançáveis se ele não existisse [...]. Por exemplo, um grupo cujos membros demonstrem confiabilidade e que depositem ampla confiança uns nos outros é capaz de realizar muito mais do que outro grupo que careça de confiabilidade e confiança [...]. Numa comunidade rural [...] onde um agricultor ajuda o outro a enfardar o seu feno e onde os implementos agrícolas são reciprocamente emprestados, o capital social permite a cada agricultor realizar o seu trabalho com menos capital físico sob a forma de utensílios e equipamento (Putnam, 2006, p. 177).

Em Fukuyama (1995) e em Cunha (2000), capital social é a capacidade de indivíduos (grupos ou organizações) trabalharem em conjunto para uma causa comum, que dependendo do grau de partilha de normas e de valores atendem aos interesses individuais e coletivos. Logo, a confiança é um fator do capital social numa dada sociedade que pode corporizar-se num grupo social menor e mais básico (como uma nação), bem como em todos os grupos intermediários, segundo Fukuyama (1995).

Dessa forma, para Putnam (2006), a confiança é o componente básico do capital social, mas não o único e, quanto mais alto o nível de confiança numa comunidade, maior a probabilidade de cooperação; e quanto maior a cooperação, mais alto o nível de confiança. O autor exemplifica essa teoria: não se confia que uma pessoa (ou uma entidade) fará alguma coisa simplesmente porque ela disse que iria fazer. Confia-se porque conhecendo a disposição e a sua capacidade, espera-se que ela agirá conforme o desejado.

Putnam (1993) enfatizou mais dois tipos de confiança: o denso e o delgado. O denso estabelece-se nas interações face a face e com o conhecimento direto, reduzindo o grau de risco. E, no delgado, a confiança se mede pela maior possibilidade de risco.

A confiança tratada por Putnam nos seus escritos sobre a Itália e que tem o poder de aumentar o capital social, também pode ser chamada de confiança generalizada. Lundåsen (2002) traz uma gama de autores para defini-la e Yamagishi (1998) a descreve como a expectativa de um comportamento idôneo da contraparte, até que se prove o contrário. Obviamente, isto pode refletir num risco ou numa incerteza ou ainda numa insegurança.

Partindo desse pressuposto, Lundåsen (2002) difere "confiança dentro de grupo" de "confiança generalizada". Aquela está relacionada a pessoas que se conhecem pessoalmente e esta não necessariamente – as pessoas não precisam ser conhecidas.

> A confiança generalizada aumentaria a probabilidade de conseguir uma reciprocidade geral e, portanto, facilitaria a ação coletiva. Pode haver muita confiança dentro do grupo, como na família, mas baixa confiança nos outros em geral, tal como descrito no familismo amoral de Banfield. O que não tornaria mútuas essas duas condições (Lundåsen, 2002, p. 310).

Para Lucena (2009), a confiança é uma categoria do conhecimento e o confiante na

confiança é uma categoria de ação. Para ela, a integridade cria a confiança: “Minha integridade potencialmente recompensa sua confiança em mim. O potencial de manter a promessa e ser digno de confiança é primeiro daquele que promete” (Lucena, 2009, p. 35). Essa integridade quando referida a uma comodidade, acomete-se por uma motivação instrumental para aprender alguma coisa útil, e essa motivação e o uso do conhecimento podem ser ambos instrumentais. Mas o conhecimento, intrinsecamente, não é instrumental.

A autora ainda acrescenta, a confiança vem das pessoas (indivíduos); a sociedade não é resultado de uma fabricação; mas remetida à interiorização do indivíduo. Assim, existem dois tipos de confiança: a em si mesmo (pessoal) e a depositada nas outras pessoas (social). A confiança em si mesmo serve para que o indivíduo possa assumir riscos, acreditar em julgamento, e não no de outrem, e estabelecer vínculo afetivo. Em contrapartida, a confiança nas outras pessoas faz com que os poderes sejam delegados e divididos, minimizando as diferenças de valores a partir da tolerância e estimulando o espírito de autoconfiança (Peyrefitte, 1999).

De acordo com Lundåsen (2002), a confiança interpessoal foi associada, à *priori*, a traços de personalidade como misantropia, contudo, muitas teorias também trouxeram diversas definições e aspectos sobre confiança, mas, segundo a autora, apesar dessa diversificação, a maneira mais comum de operacionalizar a confiança generalizada é por meio de *surveys*.

Filgueiras (2007) enfatiza que o tema confiança interpessoal ganhou pujança nas análises positivas e negativas entre culturas cívicas, descrevendo padrões de interação social, nos escritos de Putnam (2006). O baixo nível de confiança interpessoal está associado a interações de caráter autoritário, em que resulta na existência de corrupção como forma de mediação social; já o alto nível liga-se a interações democráticas e a uma maior prosperidade econômica, esta, gerando estabilização e eficácia das instituições políticas. Tal ideia vai ao encontro dos postulados de Feres Júnior e de Eisenberg (2006), em que a confiança interpessoal carece de substância política de qualidade, dependente de um aparato institucional presente em leis.

> O exercício da confiança não se dá meramente por raízes religiosas de determinada cultura, mas pelo modo como as instituições são capazes de reduzir o risco em sociedades complexas. A confiança interpessoal, portanto, é inadequada a uma teoria democrática moderna, porque em sociedades complexas os padrões de interação são mediados por instituições (Filgueiras, 2007, p. 881).

Para Luhmann (1996), Mota (2016) e Rocha e Barreto [200-], a confiança interpessoal pode ser dividida em dois momentos. No primeiro, o indivíduo pode confiar em sua própria

confiança em outra pessoa, atribuindo à sua confiança a habilidade para motivar terceiros. No segundo, o indivíduo pode confiar na confiança que outros têm nele. Nesses dois momentos (podendo-se falar então em duas dimensões), a confiança se apresenta como confiança reflexiva.

Desse modo, Couch e Jones (1997) e Lundåsen (2002) e Reis (2003) ramificam a confiança em três níveis: a confiança relacional (ligada a pessoas conhecidas e específicas); a confiança na rede (ligada às redes sociais ou familiares) e a confiança generalizada (na natureza humana).

Ketzer (2015) destaca que o tipo de relações de confiança em que os teóricos estão mais interessados são as relações interpessoais que envolvem fiar-se na boa vontade do confiado, mais do que em formas de confiança diretamente cognitivas. Consoante a autora, quem confia coloca-se numa posição vulnerável de risco de traição. Isto é, confiança é uma relação que envolve direitos e obrigações; é o tipo de laço social indicador de sucesso nas relações interpessoais. Ela ainda adita que, embora o conceito de confiança seja utilizado numa série de áreas científicas como a Política, a Sociologia ou o Direito, ele é oriundo da Filosofia Moral, que aponta para necessidade da boa vontade para que relações se estabeleçam.

Assim, o objetivo da tese da autora supra é distinguir o nível de confiança, por meio do conceito de "confiar" de "fiar-se". Fiar-se é o nível mais básico, o qual também é denomidado de fiabilidade (*reliability*), que se define pelas relações dos indivíduos com o mundo, com as instituições e com desconhecidos, sendo necessária para a vida diária; já o outro nível, chamado de confiança (*trust*) é mais profundo, no qual a confiança é explícita e pode envolver a instituição de promessas como acordos.

> A análise do conceito de confiança em Filosofia Moral aponta para dois conceitos distintos: fiar-se (*rely*), um conceito mais básico, ligado a coisas materiais (o despertador, o semáforo), uma fiabilidade básica no funcionamento das coisas e do mundo; e confiança (*trust*), que caracteriza uma relação mais profunda entre seres humanos, e que envolve boa vontade, promessa, responsabilidade e delegar ao outro, em quem se confia. Esse delegar ao outro pode ser em termos de ações que o outro terá que realizar ou em termos de acreditar no que o outro diz e tomar suas palavras como verdadeiras com o objetivo de adquirir conhecimento (Ketzer, 2015, p. 26, grifo nosso).

A fiabilidade é um tipo de relação que envolve sentimentos como desapontamento. No entanto, confiança (*trust*) está para as relações morais, pressupondo boa vontade das partes, como a promessa daquele que é confiado em corresponder ao sentimento de confiança que lhe foi depositado, corroborando uma relação explícita. Quando a *trust* é rompida, a sensação é de

traição; entretanto, isso não compromete a relação com o mundo, mas com aquela pessoa que rompeu a relação.

McMyler (2011) diz que há realmente uma diferença entre confiar (*trust*) e fiar-se (fiabilidade). Este, concebido por uma perspectiva mais individualista, tratando-se de uma espécie de dependência entre os agentes e as suas fontes de conhecimento para aceitar algo como evidências. Aquele, envolve mais do que fiar-se, pressupõe a boa vontade do outro em auxiliar alguém, mais do que simplesmente crer que a palavra do outro é verdadeira.

Ketzer (2015) considera que confiança e fidedignidade (*trust* e *trustworthy*) são formas especiais de dependência do conhecimento e que conferem ao falante obtê-lo e compartilhá-lo. Ela expôs que os defensores dessa perspectiva relatam que o ouvinte geralmente aceita as palavras do falante e as toma para si, assumindo o testemunho do falante autoridade, e nesses casos parece que há confiança. São casos nos quais o ouvinte não busca uma conclusão própria para sua crença, mas um estímulo externo.

Portanto, confiar é ter a noção de dependência de algo ou alguém e fidedignidade é a propriedade que alguém tem de ser competente e comprometida com o que lhe é confiado. Fricker (1998) demonstra que a fidedignidade é uma característica que alguém possui quando tem posição de prestígio no meio em que vive. Por exemplo, alguém que é fidedigno e competente tem autoridade racional, e retendo ambas características, possui credibilidade. Contudo, "mera credibilidade" significa dizer que o indivíduo nem é confiável, nem competente, mas por algum motivo lhe estão concedendo autoridade.

Para Faulkner (2011), a confiança pode ser uma ação ou uma atitude. A primeira dá-se quando o indivíduo depende de outra pessoa para algo e a segunda quando se cria expectativa que algo irá ser realizado conforme se espera. A confiança como atitude subdivide-se em dois tipos: a "confiança preditiva", que envolve a crença, espelho da fiabilidade; e a "confiança afetiva", que envolve esperar que a confiança motive o confiado, isto é, envolvem sentimentos e atitudes como o de boa vontade ao depender de outra pessoa (Faulkner, 2011; Ketzer, 2015).

> Confiança afetiva envolve uma expectativa que é diferenciada do tipo de expectativa presente na confiança preditiva. Esse esperar não envolve crença no futuro, previsão de que o outro irá agir de forma fidedigna. Trata-se de uma espera normativa, que está diretamente relacionada à responsabilidade para com aquele que nos deposita confiança (Ketzer, 2015, p. 14).

A autora faz um panorama dos conceitos essenciais de confiança em sua tese: 1. fiar-se – relação de dependência que o indivíduo estabelece com o mundo e com as coisas dele; ou seja, fia-se em algum objeto por uma necessidade: relógios, semáforos, instituições bancárias

e educacionais, no trânsito e em pessoas que não se conhece; 2. fiabilidade (*reliability*) – aquele que possui uma determinada propriedade em que se pode fiar; 3. fiável (*reliable*) – aquele que é digno de fiabilidade; 4. confiança (*trust*) – fiabilidade na boa vontade e na competência do outro; 5. fidedignidade (*trustworthiness*) – propriedade daquele em quem se pode confiar; 6. fidedigno (*trustworthy*) – aquele que é digno de confiança. A síntese disso é que a confiança sempre acomete três partes: confio em algo ou em alguém para algo ou alguma coisa, nesta ordem – eu-o outro-algo.

A análise de Giddens (1991) está centrada nos "ambientes de confiança e de risco" nas culturas pré-modernas e modernas para entendê-los na "sociedade contemporânea". Acerca da cultura pré-moderna, a confiança é localizada em ambientes como as relações de parentescos (familiar), religiosas e de tradições. Na cultura moderna, os ambientes de confiança estão localizados nos sistemas abstratos desencaixados, ou seja, nas relações pessoais orientadas ao futuro. Cunha (2000) relata que Giddens trabalha na formatação de uma teoria social crítica que dê conta da sociedade contemporânea, revisitando as culturas passadas.

> A confiança pode ser definida como crença na credibilidade de uma pessoa ou sistema, tendo em vista um dado conjunto de resultados ou eventos em que essa crença expressa uma fé na probidade ou amor de um outro, ou na correção de princípios abstratos (conhecimento técnico) (Giddens, 1991, p. 41).

Para o autor, a confiança é uma forma de fé na qual há uma segurança adquirida em resultados prováveis; ela é um tipo de crença. A partir daqui, tem-se uma visão ampla sobre a análise de Giddens (1991) acerca da confiança, chegando ao fator que a confiança pode ser definida como a crença na credibilidade de uma pessoa ou sistema, tendo em vista um conjunto de resultados ou eventos, que expresse crença e fé na correção de princípios abstratos (conhecimento técnico). Nesse sentido, o autor sugere conceituar a confiança e suas noções, dispondo de dez pontos, conforme o Quadro 5.

Quadro 5 – Os dez pontos do conceito de confiança de Guiddens

1. A confiança relaciona-se à ausência no tempo e no espaço. Não haveria necessidade de se confiar em alguém cujas atividades fossem continuamente visíveis e cujos processos de pensamento fossem transparentes, ou de se confiar em algum sistema cujos procedimentos fossem inteiramente conhecidos e compreendidos. A confiança é um dispositivo para lidar com a liberdade dos outros, contudo, a principal condição à confiança não é a falta de poder, mas a falta de informação plena.
2. A confiança está basicamente vinculada à contingência e não necessariamente ao risco. A confiança sempre leva à conotação de credibilidade em face de resultados contingentes, ou melhor, às ações de indivíduos ou à operação de sistemas. No caso da confiança nas pessoas, a suposição de credibilidade envolve a atribuição de "probidade" (honra) ou amor; é uma consequência da pessoa que confia em alguém.

3. A confiança não é o mesmo que fé na credibilidade de uma pessoa ou sistema; ela é o que deriva desta fé. A confiança é o elo entre fé e crença, e é isto o que a distingue do conhecimento indutivo fraco. Este conhecimento é a crença baseada em algum tipo de domínio das circunstâncias em que se tem justificativa. Toda confiança é num certo sentido cega.
4. Existe também a confiança em fichas simbólicas (meios de intercâmbio sem ter em vista as características específicas dos indivíduos ou grupos que lidam com eles em qualquer conjuntura particular, por exemplo, o dinheiro) ou em sistemas peritos (sistemas de excelência técnica ou competência profissional que organizam grandes áreas dos ambientes material e social em que se vive, por exemplo, são profissionais ou peritos que são consultados para um fim); mas isto se baseia na fé, na correção de princípios dos quais se é ignorante; não na "probidade moral" (boas intenções) de outros.
5. Neste ponto, tem-se uma definição de confiança: crença na credibilidade de uma pessoa ou de um sistema, tendo em vista um dado conjunto de resultados ou de eventos, em que essa crença expressa uma fé na probidade ou no amor de uma pessoa, ou na correção de princípios abstratos (conhecimento técnico).
6. A confiança existe no contexto de: (a) a consciência geral de que a atividade humana, incluindo nesta expressão o impacto da tecnologia sobre o mundo material, é criada socialmente, e não dada pela natureza das coisas ou por influência divina; (b) o escopo transformativo amplamente aumentado da ação humana, levado a cabo pelo caráter dinâmico das instituições sociais modernas.
7. Perigo e risco estão intimamente relacionados, entretanto, não são a mesma coisa. O risco pressupõe perigo (não necessariamente a consciência do perigo). Uma pessoa que arrisca algo flerta com o perigo, compreendido como uma ameaça aos resultados desejados. Qualquer um que assume um "risco calculado" está consciente da ameaça que isso pode acarretar.
8. Risco e confiança entrelaçam-se. Confiança serve para reduzir os perigos aos quais os indivíduos estão sujeitos. Há certas circunstâncias nas quais os padrões de risco são institucionalizados (investimentos no mercado de ações, esportes fisicamente perigosos ou confiança em um *software* de gestão de documentos, por exemplo). Risco aceitável é a minimização do perigo que varia em diferentes contextos, mas é geralmente central na manutenção da confiança. Assim, viajar pelo ar pode parecer uma atividade inerentemente perigosa, dado que o aeroplano parece desafiar as leis da gravidade. As pessoas envolvidas com o funcionamento das linhas aéreas respondem a isto demonstrando estatisticamente o quão baixos são os riscos da viagem aérea.
9. O risco não é apenas uma questão de ação individual. Há ambientes de risco que afetam coletivamente grandes massas de indivíduos, como no caso de risco de desastres ambientais ou guerra nuclear. A partir disso, pode-se definir "segurança" como uma situação na qual um conjunto específico de perigos está neutralizado ou minimizado.
10. As observações anteriores nada dizem sobre o que constitui o oposto da confiança, que não é a desconfiança, mas dependendo da circunstância pode adequar-se. Tampouco estes pontos oferecem muito no que diz respeito às condições sob as quais a confiança é gerada ou dissolvida.

Fonte: Giddens (1991).

Sobre a desconfiança, Giddens (1991) ressalta que o termo se aplica mais facilmente quando se fala na relação de um agente com um sistema, ou entre indivíduos. Direcionada a pessoas, a desconfiança significa duvidar ou desacreditar das reivindicações de integridade que suas ações personificam ou demonstram.

Na concepção de Giddens, vê-se que a fé, a crença e a confiança estão intimamente ligadas. Para Luhmann (1996), essas virtudes se complementam, mas há distinções. Para o sociólogo alemão, a confiança deve ser entendida especificamente em relação ao risco. Essa noção originou-se por meio de que resultados inesperados são consequências das atividades e das decisões dos indivíduos. Risco substitui em grande parte o que antes era pensado como

destino e torna-se separado das cosmologias. “A confiança pressupõe consciência das circunstâncias de risco, o que não ocorre com a crença. Tanto a confiança como a crença referem-se a expectativas que podem ser frustradas ou desencorajadas” (Giddens, 1991, p. 33).

Luhmann (1996) afirma que ter confiança, também é sentir seus antônimos, tais como insegurança, risco, perda, medo e falta. A visão de sua teoria sobre os sistemas sociais possui marca registrada como um elemento de redução da complexidade. Para ele, a confiança é um fato da vida social, de tal maneira que sua ausência impediria, por exemplo, de o indivíduo acordar pela manhã. É como se, para existir, o ser humano pusesse suas forças e suas crenças na natureza do mundo ou em suas relações próprias.

> Ausente a confiança, não há formação de expectativas e uma sociedade sem expectativas legítimas não é capaz de assegurar um convívio harmônico. A confiança substitui as informações insuficientes, se garantidas as expectativas criadas, pela garantia da segurança essencial. Portanto, os meios de comunicação – responsáveis pela formação de opiniões, pelas informações que veiculam, pelos produtos que vendem – ao gerar expectativas legítimas devem honrá-las à sua medida, para que a segurança no mercado seja mantida e a confiança não desapareça, sendo capaz de cumprir seu papel de crença no presente, por meio das atitudes do passado, de que o futuro prometido será assegurado (Pereira, 2010, p. 494).

Luhmann (1996) complementa que o sistema social representado pela confiança é único e carrega regras influenciadas pelo próprio sistema social e pela personalidade do indivíduo. Sendo assim, não existe garantia de uma certeza absoluta das coisas por intermédio da confiança; mas permite que um futuro incerto se faça confiável; ou seja, é uma aposta feita no presente em experiências passadas. Laconicamente, a maior contribuição de Niklas Luhmann é destacar a confiança como artifício de redução da complexidade, por conseguinte, trazendo segurança em orientação ao futuro (Mota, 2016). Na visão luhmanniana, a crença refere-se a uma atitude mais ou menos tida como certa de que as coisas familiares permanecerão estáveis.

> Você está crente que suas expectativas não serão desapontadas: que os políticos tentarão evitar a guerra, que os carros não quebrarão ou deixarão subitamente o meio da rua para atingi-lo em seu passeio de domingo à tarde. Você não pode viver sem formar expectativas no que toca a eventos contingentes e você tem que negligenciar, mais ou menos, a possibilidade de desapontamento. Você negligencia isto porque se trata de uma possibilidade muito rara, mas também porque não sabe mais o que fazer. A alternativa é viver num estado de incerteza permanente e privar-se das expectativas sem ter nada com o que substituí-las. (Luhmann, 2008, p. 97).

Luhmann (2008) ainda admite que o indivíduo considera conscientemente as alternativas para seguir um curso específico de ação, ou seja, alguém que compra um carro

usado, arrisca-se a adquirir uma dor de cabeça. O comprador deposita confiança no vendedor ou na reputação da empresa para tentar evitar que isto ocorra. Um indivíduo que não considera alternativas está numa situação de crença, enquanto alguém que reconhece essas alternativas e tenta calcular os riscos, engaja-se em confiança (Giddens, 1991).

Numa situação realmente de crença, um indivíduo reage ao desapontamento culpando outros; em circunstâncias de confiança ele deve assumir parcialmente a responsabilidade e pode se arrepender de ter depositado confiança em alguém ou alguma coisa. A distinção entre confiança e crença depende da possibilidade de frustração ser influenciada pelo próprio comportamento prévio da pessoa, portanto, de uma discriminação correlata entre risco e perigo.

A noção de risco é relativamente recente na confiança, segundo Giddens (1991). E, levando em consideração que perigo envolve risco, Luhmann (2008) faz sua separação. Eles surgem da compreensão de que a maioria das contingências que afetam as atividades humanas são criadas por nós, e não dada por Deus ou pela natureza. Assim, o perigo existe em circunstâncias de risco e serve para defini-lo. Giddens (1991) corrobora que seguramente Luhmann está certo em dicotomizar confiança e crença, e risco e perigo, bem como em afirmar que todos estes estão de alguma maneira intimamente ligados entre si.

Barbosa (2017) compactua dessa ideia e ressalta que a confiança representa um risco. Esta se diferencia da familiaridade, do algo comum, e também de uma simples confidência. A confidência baseia-se em questões que não envolvem decisões, como estar confidente (confiante) que o dinheiro ainda existirá amanhã.

A confiança e os seus elementos estudados por Luhmann serviram à construção de sua teoria dos sistemas sociais, visando trazer soluções a conflitos decorrentes de uma sociedade hipercomplexa e atualmente conectada, em que as mutações efêmeras trazem inseguranças e incertezas tanto quanto às suas abrangências e aos seus resultados. Os sistemas sociais, assim, possuem o objetivo de apreensão e diminuição da complexidade e servem à mediação com o mundo e com os humanos (Luhmann 1996). De acordo com Engelmann e Klein (2020), a complexidade é a totalidade dos conhecimentos possíveis, como um mecanismo básico que faça uma pré-seleção das possibilidades; esse redutor comunicativo é o sentido.

Dessa forma, pode-se enfatizar que Niklas Luhmann observou a confiança como um elemento fundamental do cotidiano humano que consiste num redutor de complexidade social e, por isso, dedicou algumas de suas obras à temática, com o livro "*Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität"*, em 1968, que, traduzido em diferentes línguas, oferece uma definição clara do que é o fenômeno da confiança.

> No ato de confiar, a complexidade do mundo futuro é reduzida. O agente cheio de confiança se engaja como se no futuro só houvesse algumas determinadas possibilidades. Ele define seu presente futuro num futuro presente. Ele faz aos outros seres humanos a oferta de um determinado futuro em um futuro comum, que não segue se resignando ao passado comum, mas que ao invés disso abrange algo novo. Familiaridade e confiança são, portanto, meios complementares de absorção de complexidade, e, como passado e futuro, atados um ao outro. As garantias mais concretas, que dão um ar de proteção à situação na qual o indivíduo que confia se encontra, jazem na ideia de que o indivíduo, objeto da confiança, deseje, por qualquer razão, o prolongamento do relacionamento e, portanto, tema as sanções implícitas para a ocasião em que este deseje quebrar a confiança daquele (Engelmann e Klein, 2020, p 101-102).

Hardin (2002) e Luhmann (1996) identificaram que entre duas pessoas a confiança só se mantém pelo desejo de ambos em continuar o relacionamento, sendo uma ideia reacional, pois, sem a confiança, apenas formas simples de cooperação humana seriam possíveis, as mais complexas seriam deixadas de fora.

O conceito adotado pelos autores citados, quando correlacionado às tecnologias da TD, traz algo em comum, principalmente, na necessidade de que seus usuários sintam a "segurança" de que a inovação utilizada perdure por muito tempo, o que a reveste de confiabilidade tanto no que tange à sua segurança de utilização quanto à sua efetiva garantia de prosperidade social (Engelmann e Klein, 2020, p 101-102).

Os autores supra reconhecem que, por intermédio da confiança, um sistema ganha tempo, e o tempo é a variável crítica na construção de estruturas sistêmicas mais complexas. Nessa ideia, Rocha e Barreto [200-] corroboram que para a confiança operar necessita-se de tempo, isto é, a confiança é uma forma que possibilita o controle do tempo; ela se encontra entre o passado e o futuro, possibilitando que, no presente, reduza-se complexidade. Complementam os autores, confiar não é necessariamente eliminar os perigos existentes no futuro, -"que, por sua vez, é incerto e permanecerá sendo incerto –, mas agir como se o futuro fosse certo, ou melhor: confiável (Rocha; Barreto [200-]).

Luhmann (1996) enfatiza que quem demonstra confiança, antecipa o futuro; o indivíduo age assim, como se para ele o futuro fosse mais seguro. Dessa forma, o passado é de complexidade reduzida. É evento já realizado, escolha já feita e aceita. Por isso, o passado serve como referência para as ações futuras. Essa dimensão temporal da confiança dissolve o problema de uma ação inesperada, ocultando a contingência social. "Aquele sistema ou indivíduo que cumpre com os comportamentos esperados, torna-se mais previsível, portanto, mais seguro na vista dos outros, torna-se familiar. Da mesma forma, quem costuma romper com as convenções sociais torna-se 'insegurança', imprevisível." (Mota, 2016, p. 190). Luhmann (1996) corrobora, familiaridade, assim, possibilita expectativas relativamente seguras e com isso também uma absorção de riscos permanecidos Assim, um indivíduo ou um

sistema é familiar se seu comportamento for o comportamento aceito como tendo sentido.

Nessa perspectiva, existe uma outra dimensão de confiança mostrada por Luhmann (1996) conhecida como confiança sistêmica, que para operar depende dos meios de comunicação simbolicamente generalizados. A confiança sistêmica é mecanismo adicional à linguagem cotidiana, sendo: a verdade, o poder, o amor e o dinheiro. Eles possibilitam a formação de estruturas, diminuindo a contingência existente na sociedade. Luhmann (1996) não se refere, especificamente, ao estabelecimento de uma relação de confiança entre pessoas, mas na confiança que elas depositam em tais mecanismos e, consequentemente, em um sistema (Rocha; Barreto [200-]).

A verdade, por exemplo, desempenha um papel fundamental, pois estabelece uma relação de confiança sistêmica concomitantemente com outros meios, isto é, com o dinheiro ou o poder. Desse modo, a verdade e o dinheiro são os meios presentes em uma relação contratual (Rocha; Barreto [200-]). A base racional da confiança sistêmica está na confiança do outro (Luhmann, 1996).

Mota (2016) destaca que é primordial entender que a confiança e a desconfiança são dois lados da mesma moeda; são equivalentes funcionais, ambos reduzem a complexidade social, só que enquanto a confiança o faz mirando expectativas positivas no seu objeto, a desconfiança observa essas expectativas como negativas. Nas relações pessoais, por exemplo, a desconfiança é transformada em comportamento desconfiado, podendo ensejar insatisfação.

Para sintetizar o pensamento Luhmanniano, destaca-se que a confiança manifesta-se sob diversas formas na vida humana, podendo estar presente tanto nas relações mais íntimas quanto nas relações com figuras abstratas (instituições e as organizações sociais).

> Ela traz o passado bem-sucedido para as expectativas de um futuro mais seguro, menos complexo, fazendo, normalmente, com que esta profecia se autorrrealize, mas tendo sempre presente a possibilidade de que o contrário ocorra. Colocamos cobertas nas contingências para não as enxergar e dessa forma podermos agir com menos receio. Se isto não for possível, invertemos os polos e mostramos toda nossa insatisfação através da desconfiança (Engelmann e Klein, 2020, p 101-102).

Os autores admitem que esse conceito aplica-se a uma tecnologia que vem ganhando notoriedade entre a sociedade e seu meio corporativo, haja vista as suas possibilidades de difusão e, principalmente, de segurança e transparência, que é a plataforma *blockchain.* Hodiernamente, a percepção de Rotenberg (2022) é que o acesso a informações que revelam a falta de confiabilidade das pessoas é maior do que em qualquer momento da história humana. Assim, com a tecnologia e as redes sociais digitais, cada ação é transmitida a milhões de pessoas conservada para escrutínio público. Essa mudança resultou em uma oportunidade sem igual para avaliação crítica do comportamento das pessoas, detecção de não confiabilidade e

expressão de falta de confiança nos outros, especialmente, em relação aos indivíduos expostos à opinião pública.

Pode-se dizer que a confiança ocorre por vias de canais. Este canal tanto pode ser algo ou alguém, no qual é possível se segurar e criar expectativas. Por exemplo, pode-se confiar em documentos normativos, como leis e diretrizes (algo)? Afirma-se que sim, pois são dispositivos que passaram pelo crivo de uma comunidade (alguém) que o legitimou, ou seja, pessoas que detêm o poder de passar segurança, verdade e fidedignidade àquele instrumento. Esses mecanismos servem de pontes para a confiança existir, em que há viabilidade para o seu desenvolvimento; mas, quando isso é rompido, quebra-se as expectativas e vem os sentimentos de desconfiança e desinteresse, por exemplo, antônimos à confiança. Assim, uma norma será compreendida como válida se se observar o conjunto de operações do sistema jurídico, em que uma comunicação se entrelaça à outra em um processo contínuo (Pereira, 2010).

3.2 A CONFIANÇA COMO PRINCÍPIO

Viver em sociedade, hodiernamente, requer a intrínseca ideia de boa convivência, isto se torna possível, pois os indivíduos se localizam sob a umbela de regras. Na ausência desses preceitos, os números de conflitos seriam significativos, colocando em risco a política de bem-estar das pessoas. A esses conjuntos de procedimentos comportamentais imprescindíveis para a boa convivência cabe o princípio da confiança. Esse princípio tem como finalidade realizar condutas nos parâmetros “normais” qualificados pela sociedade, esperando por parte de terceiros que atuem nessa normalidade (Canhetti; Ferreira, 2011).

Confiar não é nada além de uma necessidade social. O ser humano precisa reduzir, de alguma forma, as complexidades para permitir uma intervenção mais eficaz nas suas redes de relações. Então, apesar da confiança ter diversos matizes e graduações, como discutido anteriormente, sua ideia básica é que os sujeitos adiram às relações jurídicas em virtude de representações manifestadas por terceiros; esse fato se dá, exclusivamente, pela confiança depositada na outra pessoa ou na própria relação com outrem (Martins, 2008). Este autor afirma que, quando se confia, o sujeito baixa suas guardas e não leva em consideração o que pode ocorrer caso sua confiança seja violada, por exemplos tem-se o caso da mãe que confia o filho a uma babá, ou do motorista que confia em que os demais carros obedecerão às regras de trânsito. “Sabe-se lá de todos os efeitos que uma violação dessa confiança pode representar...” (Martins, 2008, p. 12).

Advindo da área do Direito, o princípio da confiança, também chamado de princípio da proteção da confiança ou princípio da confiança legítima, recebe resistência por não ser considerado como um verdadeiro princípio, pois não é legislado. A ocorrência desse fato se dá por ser avulto a um critério de interpretação e de fixação dos limites do dever objetivo de cuidado, criado pela jurisprudência alemã, contudo, não é, como qualquer princípio, absoluto, e nem tem extensão suficiente para possibilitar, no âmbito penal, a compensação de culpas, que há muito é rechaçada pela doutrina e pela jurisprudência (Canhetti; Ferreira, 2011).

Este princípio se caracteriza pelo olhar social sob a necessidade de manutenção do ato administrativo, ainda que ilegítimo, quando verificada a confiança gerada no particular, sobre o fato que afetou sua esfera individual, a fim de que este ato se estabilize.

Marques (2002) alega que o princípio da confiança é imanente de todo o direito e se apresenta como elemento básico da vida em sociedade. O caso primeiro, expositor de sua criação, ocorreu na Alemanha, na década de 1950. Quando reconhecido nos tribunais passou a ser tratado como prática. A Espanha também utilizou desse princípio de forma pioneira. Logo após esses casos, a Europa ampliou sua aceitação.

Na doutrina alemã, elegeu-se o termo "princípio da proteção à confiança", ao passo que, para o Direito Comunitário, firmou-se o termo "princípio da proteção à confiança legítima"; na *Common Law*[11], popularizou-se o termo "legítimas expectativas" (Maioli, 2012).

> Ainda durante a separação entre Alemanha Oriental e Alemanha Ocidental uma decisão do Tribunal Administrativo Superior de Berlim, em 14/11/1956 é apontada como *leading case* na proteção à confiança. Uma viúva que residia na República Democrática Alemã, sob a promessa de percepção de pensão se mudou para a Berlim Ocidental, onde percebeu o benefício prometido, durante um ano. Passado este tempo, a administração revogou o ato concessivo em razão de ter verificado que a viúva não preenchia os requisitos para ser incluída como beneficiária. Além de suspender o pagamento, cobrou todos os valores que já haviam sido pagos.
> Submetida a questão ao Tribunal Administrativo Superior de Berlim, este decidiu que o princípio da confiança deveria prevalecer frente à legalidade e, mesmo não havendo fundamento normativo que subsidiasse a concessão do benefício este não poderia ser revogado. Esta decisão foi confirmada pelo Tribunal Administrativo Federal. (Rocha; Diniz, [20--], p. 171).

Os mesmos autores dissertam – foi após a consolidação da jurisprudência pela proteção à confiança, a Lei do Processo Administrativo Federal alemã, de 1976, nos §§48 e 49, positivou regras relativas ao princípio, sobretudo, no tocante aos efeitos e à possibilidade de revogação de atos administrativos beneficentes.

[11] Ou "lei comum" refere-se a um sistema jurídico em que decisões judiciais que surgem a partir de outras já dadas em tribunais, a jurisprudência é sua principal fonte.

Segundo Maioli (2012), para o princípio de confiança acontecer, pressupõe-se a existência de pelo menos seis elementos: um sujeito, o Estado, um ato jurídico base da confiança, a confiança, um ato demonstrativo da confiança e um ato jurídico frustrante da confiança que gera prejuízo para quem confiou. Assim, a proteção da confiança tem por necessidade a estabilização das relações entre os indivíduos.

E, complementando, destaca-se que a relação de obrigação não surge do contrato; mas do contato social entre as partes e é a partir desse ponto que a relação se resolve para a satisfação das partes envolvidas. É a vinculabilidade pela confiança que previne a formação de representações falsas, temerárias e infundadas (Martins-Costa, 2006). É nesse ponto que se pode destacar a adequada aplicação do princípio da confiança, o ordenamento não apenas garante a segurança e a confiabilidade nas relações sociais, mas também, acaba por fortalecer a própria "confiança".

Os outros princípios estão para complemento da confiança e vice-versa, mas que de forma equivocada, segundo alguns autores do Direito, não significa o mesmo que confiança, são eles os princípios da boa-fé e da segurança jurídica (Sousa, 2011). O da boa-fé possui acepção subjetiva e objetiva: a primeira é a intenção de responsabilidade e reflete-se no "sentimento pessoal de atuação conforme a ordem jurídica"; e a segunda se satisfaz quando o comportamento das partes respeita, reciprocamente, o comportamento esperado para uma determinada relação jurídica (Rocha; Diniz, [20--]).

Na gênese da boa-fé, cada um deve cumprir a própria palavra e que a confiança se componha pelo fundamento-chave das relações humanas, então, não podendo ser mal utilizada; cada um deve agir de forma coerente e legítima (Martins, 2012).

A aproximação entre a significação do princípio da confiança e da boa-fé está em seu elemento objetivo. A distinção seria que na boa-fé, a reciprocidade é indispensável; já na confiança, o ato administrativo, em algumas hipóteses, deveria ser mantido independente da apuração das intenções do administrado (Rocha; Diniz, [20--]).

A instituição da *bona fides* (boa fé) oriundo do direito romano é associada à proteção da confiança. Proveniente do Direito privado, a boa fé é considerada princípio geral do Direito, obviamente que devidamente adaptada às realidades do Direito público e às peculiaridades do direito administrativo.

Mais uma distinção feita por Barbosa (2008) entra a *bona fides* e a confiança (*cum fides*) é que a primeira é o princípio que informa o modo pelo qual a cooperação entre as partes será devida, enquanto a última liga à proteção das expectativas legítimas e atua como justificativa ou explicação à vinculabilidade jurídica.

O princípio da segurança jurídica, presente no ordenamento jurídico brasileiro, se dá pela proteção da imobilidade ou da estabilidade das relações jurídicas, contra todas aquelas tentativas de inová-las, por meios que vão contra. Sua implicação no que tange à proteção da confiança é quando o indivíduo deposita em determinada relação jurídica, de forma que mudanças de comportamento não possam mudar as expectativas geradas, por quem quer que seja (Martins, 2008).

Como visto, esses dois princípios encontram-se relacionados. Enquanto a segurança jurídica está em conexão com elementos de ordem objetiva na esfera jurídica, a proteção da confiança está nos aspectos subjetivos de segurança. Contudo, ambas demandam, dentre outras, as seguintes características: transparência dos atos do poder, racionalidade, clareza de ideias e palavras e fiabilidade (Ferreira, 2008).

Segundo Maioli (2012), a jurisprudência brasileira refere-se indiscriminadamente à segurança jurídica e à proteção à confiança, ou até mesmo à boa-fé objetiva sem atentar para a precisão técnica necessária para o correto desenvolvimento e a evolução do Direito, muitas vezes, tratando-as do mesmo jeito.

A Constituição da República Federativa do Brasil de 1988 não menciona a segurança jurídica taxativamente, porém, trata-se de elemento essencial ao Estado Democrático de Direito. O princípio da confiança no Brasil é constantemente confundido com o princípio da segurança jurídica, com o da boa-fé, como se fossem sinônimos. Isso mostra que o Direito brasileiro necessita ainda de um debate mais aprofundado sobre o princípio da confiança. Contudo, de forma singular, Luís Roberto Barroso sustenta que a segurança jurídica está atrelada a muitos valores, dentre eles a confiança nos atos do poder público; a estabilidade das relações jurídicas; a previsibilidade de comportamentos, dentre outras características (Barroso, 2006).

Complementa Martins (2008), a proteção da confiança não é apenas uma questão meramente ética ou moral, antes disso consubstancia em uma necessidade do próprio modelo jurídico e do contexto social, que, conforme apontado pela própria doutrina brasileira, a proteção da confiança legítima assume duplo papel no ordenamento: 1) atua como uma proteção das legítimas expectativas; e 2) ao mesmo tempo, funciona como justificativa da vinculabilidade das partes à relação jurídica.

A importância de compreender o princípio da confiança se dá pelo fato de como ele age na sociedade em relação às suas práticas, seja ela contratual entre pessoas ou por mecanismo. Nas linhas deste estudo, sua conotação está posta como um mecanismo de ter uma necessidade em quem confiar, que aqui se insere pela análise das do Conarq, que dão

diretrizes para reduzir a complexidade social no que tange a normas para confiabilidade aos documentos, melhorando a relação do sistema-usuário.

4 PRESERVAÇÃO DIGITAL: HISTÓRICO

A perspectiva do entendimentos sobre preservação pode ser remontada aos primórdios da vida humana. Desde que existiu a intenção de provar algo, tornou-se necessário utilizar estratégias para solidificação e para conservação de testemunhos. Por exemplo, na Idade Antiga e na Idade Média, títulos de nobreza e de posse de terras precisavam de cuidados à sua integridade, isto é, preservá-los para as gerações futuras, o que garantia aos seus descendentes a proteção de direitos.

Tal prática foi se acoplando à sociedade como uma ação cotidiana. Lugares considerados de guarda foram sendo imprescindíveis para acondicionar registros: os arquivos e as bibliotecas, servindo, muitas vezes, de depósitos de artefatos, de livros, de documentos ou de qualquer registro que servisse para atestar algo. Agentes que atuavam nesses espaços laborais, a título dos escribas, eram os "guardiões" da informação e tinham ligação direta ao alto escalão à época, cargo reputado a pessoas eruditas e letradas.

A atribuição pelos romanos à organização arquivística levou-os a definir o estatuto do arquivista (*tabularius*), função desempenhada por um escrivão, conferindo-lhe atribuições no âmbito da conservação, da reprodução e da validação dos documentos, prescrevendo as condições de acesso, bem como o escalonamento da própria carreira (Silva *et al.*, 2009).

Monges e mosteiros também desempenharam um papel vital na preservação e na distribuição de livros. Foi o trabalho deles que forneceu muito do conhecimento atual acerca do passado antigo e da rica herança das tradições grega, romana e árabe; com o advento da imprensa, essa tradição monástica desapareceu. No entanto, a reverência pelo registro histórico do texto tem sido realizada por bibliotecários e por arquivistas em bibliotecas públicas e privadas até hoje (Kuny, 1997).

Dessa forma, um dos grandes problemas, mas também solução para a longevidade e para a integridade dos documentos se põe ao que a preservação simboliza, uma vez que engloba fatores como custo, tecnologia, logística e ética para a sua manutenção.

Segundo Hazen *et al.* (2001), a preservação é um agrupamento de três principais tipos de atividades: o primeiro está concentrado nos ambientes de biblioteca e nas maneiras de torná-los mais apropriados a seus conteúdos (incluindo os arquivos, os museus e qualquer unidade ou sistema custodiador(a) de informações); o segundo incorpora esforços para estender a vida física de documentos; o terceiro envolve a transferência de conteúdo intelectual ou informativo de um formato ou matriz para o outro.

Em nenhum desses casos, a preservação pode ser uma atividade definitiva, pois a

permanência do suporte tem durabilidade finita, contudo, seu conteúdo, sempiterno. Assim, faz-se necessário elencar alguns conceitos no âmbito da salvaguarda à informação, a saber, conservação (preventiva e reparadora), restauração e preservação. Pode-se entendê-los fazendo alusão a um guarda-chuva, conforme a Figura 2, em que existe uma haste para segurá-lo com as mãos e firmá-lo sobre corpo do indivíduo, além de um material que reveste a cabeça, mantendo-o protegidos de agentes externos.

Figura 2 – Guarda-chuva da proteção documental

Fonte: Spinelli, Brandão e França (2011).

A conservação está compreendida nos cuidados prestados aos documentos. A política moderna de conservação a longo prazo orienta-se pela luta contra as causas de deterioração e no maior prolongamento vital possível dos documentos, devendo ser adotada como filosofia por uma instituição (Spinelle Junior, 1997).

Para o mesmo autor, a conservação preventiva é um conjunto de medidas e de estratégias em âmbito político, operacional e administrativo, contribuindo para a conservação da integridade dos acervos e dos prédios que os acondicionam. Suas ações são a adequação do controle ambiental, os modos de acondicionamento e de acesso, que visam prevenir e retardar a degradação, por meio de higienização e de reparos. A conservação reparadora é toda intervenção na estrutura dos materiais que compõem os documentos, a fim de melhorar o seu estado físico e a sua legibilidade. Já a restauração, um conjunto de medidas que estabilizam ou revertem danos físicos e químicos adquiridos pelo documento ao longo do tempo, intervindo de modo a não comprometer sua integridade e seu caráter histórico. Em um sentido amplo, a preservação trata-se de toda ação destinada à permanência dos registros documentais.

Segundo o Brasil (2005), preservação é a prevenção da deterioração e de danos em documentos, por meio de controle ambiental e de tratamento físico ou químico. Esse conceito restringe o ato de preservar apenas aos documentos físicos. E, complementarmente, Camargo e Bellotto (2010) dizem ser a preservação, função arquivística destinada a assegurar as atividades de acondicionamento, de conservação e de restauração de documentos. Essa é uma óptica mais abrangente, mas que não circunda o campo tecnológico digital, entretanto, englobam os atos de conservação e de restauração.

Cassares (2000) remonta a preservação a um conjunto de medidas e de estratégias de ordem administrativa e política operacional, que pode contribuir direta ou indiretamente à integridade dos materiais. Aqui, encontra-se a visão do campo das estratégias nas organizações, o qual acopla a manutenção documental, porém, não menciona a preocupação com o seu conteúdo.

Esses primeiros conceitos sobre preservação estão voltados para a integridade dos suportes, mais do que para o conteúdo dos documentos. Para o ambiente digital, outros elementos de relevante importância são realçados: a autenticidade e a confiabilidade, que possibilitam protuberar o cuidado com os conteúdos informativos dos documentos, ou seja, o suporte aqui não é mais tão importante quanto na preservação física. Isso tem justificativa, já que é unânime entre os estudiosos desta área: o suporte carrega problemas elementares – sua instabilidade e o fatídico horizonte de obsolescência. Então, pode-se antecipar que a questão da preservação não é apenas uma solução para problemas técnicos, mas sim um desafio muito mais institucional e social. Como resultado, dois fatores se destacam ao reforçar esta ideia: o planejamento e a política de gerenciamento dos objetos digitais.

Ao se considerar o seu contexto histórico, a preservação digital é um termo relativamente recente. Hirtle (2008) revela que uma de suas primeiras referências não apareceu na biblioteca ou na literatura arquivística, mas na revista *Theatre Crafts*, em 1992, por um artigo intitulado “Preservação digital”, o qual descrevia uma tecnologia para serra de mesa:

> O sistema BladeGuardTM da serra de mesa Biesemeyer foi projetado com a conveniência do operador em mente. A proteção transparente é larga o suficiente para acomodar qualquer ângulo da lâmina e é contrabalançada para que a proteção deslize facilmente. A proteção é montada em uma longa lança que se conecta a qualquer serra de mesa e garante que a coluna de suporte vertical fique bem fora do caminho do trabalho. O protetor levanta com um toque de dedo e trava fora do caminho para trocar a lâmina, mas um alarme com um interruptor de chave soa para avisar o operador se a serra for iniciada com o protetor na posição de armazenamento. Assim, em 1992, a “preservação digital” era tão provável que significasse manter os dedos ao usar uma serra de mesa quanto significava a preservação de dados digitais (Hirtle, 2008, p. 123-124, tradução nossa).

Em contrapartida, vale ressaltar que a preservação de registros eletrônicos tem sido uma preocupação dos arquivistas desde pelo menos o início dos anos 1960, quando a seção de registros legíveis por máquina foi formada no Arquivo Nacional. Além disso, o Consórcio Interuniversitário para Pesquisa Política e Social (ICPSR), um arquivo de dados da Universidade de Michigan, também começou nessa época. Embora esses primeiros programas estivessem preocupados com a preservação da informação digital, tendiam a não utilizar o termo "preservação digital", preferindo falar em arquivamento de registros eletrônicos ou preservação de conjuntos de dados.

Arellano (2008) descreve que, de fato, as primeiras considerações sobre a preservação digital partiram da Arquivologia. Fatores como tempo e custo de armazenamento de longo prazo foram adicionados a decisões sobre volume e formato do material a ser preservado. Também foram os arquivistas que propuseram algumas das características das ferramentas necessárias para a proteção, o cuidado e a manutenção de coleções digitais.

Em inglês, por exemplo, a referência mais antiga sobre "preservação digital", consoante Hirtle (2008), ocorreu no contexto da pesquisa que Anne Kenney e Lynne Personnius empreenderam, em 1990, na Biblioteca da Universidade Cornell, em conjunto com a Xerox Corporation. Esse conceito foi originalmente desenvolvido em bibliotecas, não em arquivos, como um auxílio aos esforços contínuos de preservação analógica de bibliotecas, que inicialmente não se preocupava com a preservação da informação nascida no ambiente digital.

As comunidades de bibliotecas e de arquivos preocupadas com a gestão da informação em formato eletrônico se uniram em 1994, por meio da criação da Comissão de Preservação e Acesso/Grupo de Pesquisa de Bibliotecas (CPA/RLG) e da Força-Tarefa sobre Arquivamento de Informação Digital. Embora formada por dois grupos, principalmente, associados a bibliotecas, a Força-Tarefa incluía dois arquivistas entre seus membros.

Em 1998, as informações criadas em formato eletrônico foram redefinidas como recursos "natos digitais" (nomenclatura conhecida na atualidade). A criação do campo da preservação digital como uma atividade da comunidade bibliotecária fez com que algumas questões importantes para os arquivistas pudessem ter recebido menos atenção.

As primeiras iniciativas baseadas em bibliotecas, por exemplo, seguiram o modelo de preservação analógica, o qual enfatizava a transferência de informações para mídias estáveis que podiam ser gerenciadas facilmente. Logo no princípio, os arquivistas perceberam que toda mídia eletrônica requeriam gerenciamento ativo. Ademais, os bibliotecários se concentraram em capturar e preservar as informações encontradas nos documentos, enquanto

os arquivistas também estavam interessados em preservar a autenticidade e a confiabilidade dos registros. Além de preservar o conteúdo dos documentos, os arquivistas enfatizaram a necessidade de manter a capacidade dos registros eletrônicos de servirem como evidência.

4.1 CONCEITOS BASILARES DA PRESERVAÇÃO DIGITAL

O documento é um estoque de informação que carrega consigo elementos da realidade. Em nossa sociedade, tal dispositivo serve de mecanismo para desburocratizar ações e legitimar práticas. Essa condição no ambiente digital muda, pois, semelhante alteração faz com que computadores sirvam de pêndulos para a comunicação. Por ser considerado um local que requer cautela e proteção, o meio *online* necessita de cuidados e de estratégias que considerem a vida útil dos documentos prolongadas.

Arellano (2004) confirma que é necessário dar importância ao contexto do objeto digital, para que usuários possam entender o ambiente tecnológico no qual ele foi criado, e complementa: a preservação documental continua a ser determinada pela capacidade de o objeto informacional servir às utilizações que lhe são imputadas, às suas atribuições que garantam que ele continue sendo satisfatório à posterioridade; mas, no caso específico dos documentos em formato digital, a preservação dependerá, principalmente, da solução tecnológica adotada e dos custos envolvidos.

Ao contrário das práticas de conservação em que um item pode, muitas vezes, ser tratado, armazenado e essencialmente esquecido por algum período, os objetos digitais exigirão atualizações e cópias frequentes em uma nova mídia de armazenamento. Manter o artefato digital “original” não é importante (Kuny, 1997).

Os objetos ou materiais digitais são informações representadas por sequências de dígitos binários (linguagem computacional), tanto as nascidas digitalmente como as digitalizadas. O grande mote da obsolescência faz com que políticas sejam instituídas e implementadas para evitar a perda desse materiais, e, nesse sentido, há o desafio das instituições para manter os documentos legíveis à sociedade. Ferreira (2006) divide os objetos digitais em quatro nuanças:

- **objeto físico:** aquilo que o *hardware* é capaz de interpretar, transformando símbolos inscritos no suporte físico em um conjunto de dados que o *software* será capaz de manipular;

- **objeto lógico:** é a estruturação de dados designado por formato do objeto digital. O *software* é responsável por preparar esse objeto para que seja apresentado a um receptor humano, por meio de um periférico de saída;
- **objeto conceitual:** assume uma forma familiar aos seres humanos, como livros, filmes ou fotografias (documentos), constituindo aquilo que deve ser preservado;
- **objeto experimentado:** é a experiência, a interpretação ou o entendimento feito pelo emissor/receptor do objeto.

Preservar digitalmente significava, genericamente, usar tecnologias para reformatar mídias analógicas como parte de um processo. Informações reformatadas, ou o que veio a ser conhecidas como "documentos digitais", são consideradas as matérias-primas, bem como as primeiras iniciativas que fizeram da preservação digital ter seu significado como tal. Hoje, essa ideia se expande e, além de englobar esses documentos, utiliza uma perspectiva ativa, se valendo de normas e de padrões para assegurar sua autenticidade.

Em um sentido abstrato, a preservação de materiais digitais não é complexa. Enquanto a relação entre *hardware-software* e *humanware* (organizações e pessoas) for mantida, uma espécie de "nexo de preservação" existe e um objeto digital pode ser preservado a longo prazo.

O problema são as forças centrífugas, como tempo e dinheiro, que separam cada um desses elementos – o *software* e o *hardware* ficam desatualizados, a migração de informações pode exigir uma recodificação cara e as organizações não terem recursos para resolver esses entraves. Isso cria um ambiente onde o objeto é basicamente deixado em um limbo digital, preso em um formato obsoleto ou capturado em um meio ilegível, ou sem capacidade administrativa, sem recursos e sem disposição para atualizar os dados (Kuny, 1997).

Assim, pode-se entender a preservação digital imersa em dois procedimentos, o primeiro estrutural e o segundo operacional:

> A preservação digital é composta por procedimentos de manutenção, que podem ser denominados estruturais e por procedimentos de preservação dos componentes, os quais podem ser denominados como operacionais. Os procedimentos estruturais se referem aos estágios iniciais, definindo questões como a infraestrutura, normas, escolha de padrões, financiamentos e definição de metadados. Já os procedimentos operacionais se referem a atividades que objetivam a preservação física, lógica e intelectual dos documentos digitais através de ações como a migração, a emulação e o encapsulamento (Santos; Flores, 2015, p. 203-204).

Para Bodê (2016), a definição de preservação digital toma como sustentáculo o termo "documentos digitais" e considera seu objetivo principal direcionado à "garantia do acesso", no sentido de "garantir o funcionamento" desses documentos ao longo do tempo. Ainda

corrobora – a preservação digital se dá pelo conjunto de todas as ações possíveis de serem executadas, em qualquer nível operacional, que garanta o funcionamento adequado e a percepção para os humanos do conteúdo de documentos digitais pelos prazos que forem definidos como necessários.

Santos e Flores (2015) dizem que o foco da preservação de documentos digitais está no objeto conceitual e consiste na atividade de garantir acesso à informação, ao mesmo tempo que mantém sua autenticidade. Os documentos que estão nesse processo deverão ser interpretados por uma plataforma tecnológica do futuro que será diferente da que foi utilizada em sua criação, e sua finalidade é o conteúdo informacional.

A questão da preservação digital não deve se restringir apenas à seleção do que vai ser preservado, possui relação também com a responsabilidade dos agentes, os custos, a autorização de acesso e as estratégias para certificar a eficiência de todo o seu ciclo de vida. Assim, Formenton, Gracioso e Castro (2015) advogam que esse processo se caracteriza pela implantação de uma infraestrutura física e tecnológica dos recursos disponíveis na instituição; mas, principalmente, por um planejamento detalhado das funções e atividades bem-sucedidas do acesso aos objetos digitais por longos períodos.

Schäfer e Constante (2012) vão ao encontro dessas ideias, quando descrevem a preservação digital como conjunto de estratégias em que se definem diretrizes e modelos, conceituais e práticos, a fim de minimizar os efeitos da obsolescência tecnológica, garantindo a perenidade da informação, tornando-as acessíveis em longo prazo.

Já Ferreira (2006) a conceitua como sendo a capacidade de assegurar que a informação permaneça acessível com qualidade e fidedignidade no futuro, sendo interpretada por uma plataforma tecnológica. Pode-se perceber que esses conceitos se complementam e se entrecruzam; seu fim pode ser considerado o mesmo: a garantia de acesso a longo prazo aos documentos.

A elaboração e o estabelecimento de políticas de preservação estão colaborando para que padrões e normas traduzam conceitos e procedimentos de confiança aos documentos. Tem-se, então, as questões de acesso, de direitos autorais, de sistema de armazenamento e de modelos conceituais que dão vazão à legitimidade da preservação digital. Nesse sentido, as estratégias foram criadas, no intuito de manter a autenticidade dos documentos arquivísticos, por meio de práticas que visam à proteção de seus conteúdos.

A ação preventiva assaz empregada no que tange às estratégias de preservação é o *backup* – caracterizado por cópias de segurança. Apenas essa ferramenta não é suficiente para dar conta da completude à proteção documental. Nesse sentido, metodologias mais elaboradas

estão cada vez mais em voga, como, por exemplo, o modelo OAIS, a ISO 16:636/2012, as diretivas do Conarq, além de outras normas.

Schäfer e Constante (2009) apontam que os desafios e as limitações impostas à preservação digital são abrangentes, e por essa razão as recentes iniciativas governamentais, aliadas ao aperfeiçoamento dos arquivistas e dos profissionais da informação, levantam à necessidade de realçá-la à integração entre os sujeitos, isto é, todos os agentes de uma instituição devem estar imersos no comprometimento com a preservação, ação que permitirá excelência e eficácia nas suas rotinas laborais.

Desenvolver programas e políticas de preservação digital requer uma atenção especial, além de uma permanente disponibilidade de recursos. Profissionais capacitados, análise de contexto e disponibilidade financeira são apenas alguns dos elementos imprescindíveis à sua efetivação.

4.2 A TRILHA PARA A PRESERVAÇÃO DIGITAL SISTÊMICA

A síntese da ideia de "sistema" preconiza a inter-relação de elementos que partem de um todo para as suas ramificações e/ou de suas ramificações para o todo. E é por essa representação que se compreende a Preservação Digital Sistêmica (PDS), em razão de se formar, por meio da cooperação de vários conceitos.

Termos como custódia, cadeia de custódia (ininterrupta), cadeia de preservação e Cadeia de Custódia Digital Arquivística (CCDA) são alguns dos espelhos dessa temática na Arquivologia. Para ampliar a óptica sobre a PDS, pauta-se na Teoria Geral dos Sistemas (TGS) de Ludwig Von Bertalanffy.

O vocábulo custódia, consoante Silva (2019), possui origem latina e significa guardar/proteger. Para a mesma autora, sua semântica precede a necessidade de um agente para custodiar documentos e mantê-los incorruptíveis. Semelhante ideia é corroborada no campo jurídico, definido-o como um *lócus* em que alguma coisa é guardada e cuidada; caso em que um custodiante deve assumir a responsabilidade pela coisa custodiada (Santos, 2001).

> A guarda significa que existe um lugar de preservação e que os documentos ali custodiados estão sob a posse de um custodiante, ou seja, os arquivos estão retidos e preservados. A proteção significa que os arquivos são materiais que precisam ser cuidados e estar em segurança, em virtude da sua fragilidade e vulnerabilidade. Envolve, portanto, a responsabilidade jurídica da instituição custodiante (produtora ou preservadora) pela segurança e preservação dos documentos, os quais não podem ser corrompidos, alterados ou subtraídos (Silva, 2019, p. 51).

Hilary Jenkinson, arquivista britânico e teórico da Arquivologia Clássica e Custodial, foi um dos pioneiros a se preocupar com a custódia como um conceito arquivístico. Schmidt (2012) explica que a obra do inglês teve a intenção original de dissertar sobre o tratamento de arquivos no período da Primeira Guerra, mas, como não havia publicação em língua inglesa, decidiu não reduzir seu Manual a esse objetivo primeiro, sendo o principal ponto de seu livro a "preservação na custódia oficial", na década 1920.

Em formatos mais abrangentes, o Dicionário de Terminologia Arquivística diz ser a custódia a responsabilidade jurídica de guarda e de proteção de arquivos, independente de vínculo de propriedade (Brasil, 2005b).

Camargo e Bellotto (2010) também noutro Dicionário de Terminologia Arquivística compactuam dessa concepção, então, sendo a custódia a responsabilidade jurídica, que pode ser definitiva ou temporária, da guarda e da proteção de documentos dos quais não detém a propriedade.

O *Multilingual Archival Terminology* (MAT)[12] define custódia (*custody)* como a responsabilidade pelo cuidado dos documentos baseada em sua posse física e nem sempre inclui a propriedade legal ou o direito de controlar o acesso aos documentos. Para Silva (2019), essa "responsabilidade" é sinônimo de "cuidado" pelo material que está sob a guarda de um custodiante, cuja posse física significa estar fisicamente sob a tutela de um responsável.

Em síntese, o termo "responsabilidade" se põe a todas as definições apontadas de custódia acima, implicando dizer que tal habilidade deve estar ao encargo de alguém com atribuição para preservar documentos. Contudo, a "responsabilidade jurídica" se asserta à proteção documental regulamentada por legislação ou outros atos normativos (Silva, 2015).

Jenkinson, em sua obra, discutiu várias ideias pouco exploradas à sua época e entre elas considerou a Arquivologia como área distinta da História. Enfatizou também que os termos *record* e *archives* (arquivo)[13] são sinônimos. Para o britânico, os arquivos guardavam duas verdades: a **histórica**, representada pelo conteúdo do documento, e a **arquivística**[14], que se dá pelo contexto de produção e pela relação do produtor com os documentos (custódia-

[12] Disponível em: Banco de Dados de Terminologia de Arquivo Multilíngue (ciscra.org).
[13] Segundo Jenkinson (1922), arquivos são os documentos que formam parte de uma transação oficial, sendo preservado para referência, servindo como evidência dessa transação. *Records* e *archives* são sinônimos, porém, considero mais apropriado o uso do *archives* por ser comumente utilizado por outras línguas (Jenkinson, 1922, tradução nossa).
[14] A verdade arquivística é a possibilidade de representar, de forma fiável, o contexto de origem e as funções do documento de arquivo, o compreendendo plenamente em um conjunto relacionado pelo vínculo arquivístico. E são as funções arquivísticas, por meio de seus procedimentos, que tornam essa verdade possível, isto é, dão lógica ao objetivo da Arquivologia, os documentos de arquivo, que é o acesso (Schmidt, 2012).

custodiador) e, principalmente, pela existência de mais dois elementos, a permanência da imparcialidade e da autenticidade documental.

> A obra de Jenkinson abordou ainda problemáticas concernentes ao aumento da produção de documentos pós-fim da Primeira Guerra Mundial, sendo que por isso seria necessário passar a avaliá-los. Nesse sentido, acreditava que os arquivos "do passado" não deveriam ser destruídos e que os arquivos "do futuro" deveriam ser avaliados pela própria administração, devendo ser encaminhado para custódia dos arquivos somente o que fosse importante de preservar para o futuro (Schmidt, 2012, p. 121).

Jenkinson (1922), em sua visão clássica, considerava arquivos somente aqueles em papéis, detendo quatro qualidades essenciais:[15] imparcialidade, autenticidade, naturalidade e interdependência. Para o autor, os arquivos viviam em uma zona militarizada, pois estavam sempre em situação de risco (mesmo em sua gênese) e aos arquivistas ficavam duas incumbências: a defesa física e moral dos arquivos e a proteção de suas qualidades essenciais.

A defesa física é, sobretudo, externa e se caracteriza por várias ações, incluindo todos os procedimentos possíveis de salvaguardar os documentos, como, por exemplo, medidas de segurança, de conservação, de restauração; e não depende exclusivamente do arquivista. A defesa moral é a permanência da autenticidade documental, a não adulteração dos arquivos e o respeito às atividades arquivísticas, que podem ser as regras de arranjo e de descrição, a guarda da relação orgânica do produtor-documento, entre outros fatores (Jenkinson, 1922).

A originalidade do pensamento jenkinsoniano está ligada à preservação dos arquivos, em que duas de suas características se destacam, a imparcialidade e a autenticidade, propriedades essas que se refletem em elementos de confiança.

Schellenberg (2006) também citou a custódia em sua obra, percebendo-a como uma atribuição que deve ser incorporada ao documento para tornar seu uso possível no futuro, ou seja, promover acesso à informação por parte dos usuários (Silva, 2015). Por meio desse enfoque, que leva em consideração a informação para a posterioridade, o arquivista norte-americano dividiu os documentos de arquivo em dois tipos: *record*[16] e em *archives*[17], assim como Jenkinson, mas com visões diferenciadas.

---

[15] A imparcialidade está relacionada à razão de criação do documento e à sua capacidade em refletir de maneira fiel as atividades de produção, ao passo que a autenticidade condiciona-se aos procedimentos de custódia contínua para garantia do valor de prova. A naturalidade também está atrelada à criação do documento, porém, na perspectiva de resultado "natural" da atividade, e por fim a interdependência, relacionada à participação e ao papel do documento no conjunto de documentos de arquivos. Vale ressaltar que nossa opção por adentrar nestas definições deu-se com vistas a compreendermos, no decorrer deste trabalho, sobre quais premissas os arquivistas "Modernos" e "Contemporâneos" estabelecem críticas contundentes às ideias de Jenkinson (Schmidt, 2012, p. 120).

[16] *Records* são todos os livros, papéis, mapas, fotografias ou outras espécies documentárias, independentemente

> Para que os documentos sejam arquivados devem ser preservados por razões outras que não apenas aquelas para as quais foram criados ou acumulados. Essas razões podem ser oficiais ou culturais (Schellenberg, 2006, p. 38).

Para que sejam considerados arquivos, primeiramente, os documentos devem cumprir a função para os quais foram criados (acumulados para algum objetivo, que numa repartição governamental é o cumprimento de sua finalidade oficial: administrativa, jurídica, de negócio ou social), acompanhados de uma outra razão: a ordem cultural, que é quando são preservados para uso de outros além de seus próprios criadores (Schellenberg, 2006).

> Se as razões de sua criação são internas, pois dizem respeito ao cumprimento da finalidade oficial, as razões de preservação são externas, pois dizem respeito a outros fins diferentes de sua produção. Há aqui um corte entre a razão oficial para produzir um arquivo, e a razão cultural para preservá-lo, expressas nas definições de *records* e *archives*. (Silva, 2019, p. 154).

A custódia como elemento-chave para a transmissão dos *records* e sua passagem à categoria *archives*, não é o critério essencial para incluir documentos considerados *records* na categoria arquivos.

> Os documentos modernos existem em grande volume, são de origem complexa e sua criação é, muitas vezes, casual. A maneira pela qual são produzidos torna infrutífera qualquer tentativa de controlar os documentos de *per si*, ou, em outras palavras, de seguir "linhas imaculadas" de "custódia intacta" (Schellenberg, 2006, p. 39).

A citação acima de Schellenberg corrobora em um desencontro à visão de Jenkinson, no que diz respeito à necessidade de uma cadeia de custódia para determinar se documentos são arquivísticos. Isso acontecia porque o volume e o descontrole nos procedimentos de criação dos documentos da administração pública americana impediam qualquer tentativa de controlar o seu vínculo, acarretando também na quebra da cadeia de custódia.

> [...], se forem oferecidos documentos modernos a um arquivo, serão aceitos como arquivos, desde que satisfaçam os outros quesitos essenciais, na "suposição razoável" de que sejam realmente documentos do órgão que os oferece (Schellenberg, 2006, p. 39).

---

de sua apresentação física ou características, expedidos ou recebidos por qualquer entidade pública ou privada, no exercício de seus encargos legais ou em função das suas atividades e preservados ou depositados para preservação por aquela entidade ou por seus legítimos sucessores como prova de suas funções, sua política, decisões, métodos, operações ou outras atividades, ou em virtude do valor informacional dos dados nele contidos (Schellenberg, 2006, p. 41).

[17] *Archives* são documentos de qualquer instituição pública ou privada que hajam sido considerados de valor, merecendo preservação permanente para fins de referência e de pesquisa e que hajam sido depositados ou selecionados para depósito, num arquivo de custódia permanente (Schellenberg, 2006, p. 41).

Esses quesitos essenciais[18], que são três, são caracterizados pela qualidade que os documentos recebem dos órgãos para a sua guarda e conservação de acordo com o arranjo dado no curso das atividades arquivísticas.

4.2.1 Cadeia de Custódia Arquivística (ininterrupta)

Como visto acima, o termo custódia pode ser encontrado nos referenciais teóricos da Arquivologia e da Ciência da Informação, já em contrapartida a expressão "cadeia de custódia", não aparece com tanta frequência. Mas o seu sentido se assemelha à concepção de custódia, acrescendo os princípios de gestão, de segurança e de preservação aos documentos.

Para Silva (2019), o sentido mais amplo de cadeia de custódia denota que seus materiais (documentos) não podem estar corrompidos e os, custodiantes, possuem papel central nessa seguridade.

> A cadeia de custódia documental pode ser entendida como o ambiente no qual perpassa o ciclo de vida dos documentos. Em outras palavras, ela define quem é o responsável por aplicar os princípios e as funções arquivísticas à documentação. A custódia confiável de documentos arquivísticos tradicionais é mantida através de uma linha ininterrupta, a qual compreende as três idades do arquivo: fases corrente, intermediária e permanente. Dessa forma, a confiabilidade ocorre por intermédio da própria instituição, que faz a própria produção, gestão, preservação e provê acesso aos seus documentos (Flores; Rocco; Santos, 2016, p. 119).

Este conceito de uma linha idônea significa dizer que a autenticidade dos documentos vai depender da capacidade de se manter uma cadeia ininterrupta de custódia. Silva (2019) afirma que o não rompimento da linha idônea fica a cabo de um custodiante responsável e se refere à transmissão dos arquivos ao longo do tempo, de um produtor aos seus sucessores legítimos até o arquivista, cuja função é manter preservados os documentos originais e autênticos das entidades produtoras. A autora ainda corrobora: como os arquivos estão sujeitos a muitas ameaças, os documentos precisam permanecer sem alteração e sem corrompimento – papel essencial da custódia.

O termo "cadeia de custódia" não foi empregado por Jenkinson (1922) em seu manual, mas "custódia ininterrupta" (*unbroken custody*) e "linha imaculada de custodiantes responsáveis" (*unblemished line of responsible custodians*), tendo como atribuição a atuação

[18] 1) Devem ser conservados num todo como documentos desse órgão; 2) devem ser guardados, tanto quanto possível, sob o arranjo que lhes foi dado pelo órgão no curso de suas atividades oficiais; e c) devem ser guardados na sua totalidade, sem mutilação, modificação ou destruição não autorizada de uma parte deles (Schellenberg, 2006, p. 39-40).

dos custodiantes. Estes podem fazer parte da administração ou serem sucessores ou assumidores da custódia, desde que garantam a autenticidade.

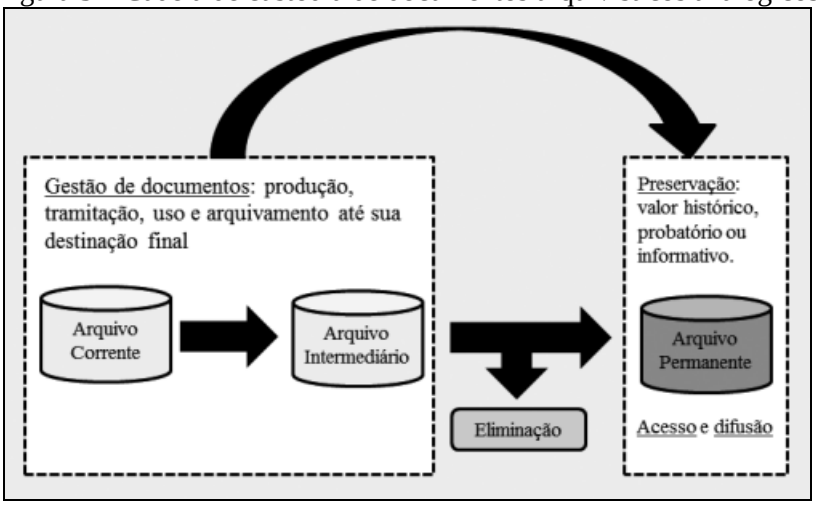
Jenkinson (1922) adita: para serem considerados arquivos, é imprescindível que esse material seja autêntico e o meio para provar tal idoneidade sugere não haver a separação documento-origem. Algumas condições cooperam para que os documentos desconectados da proveniência e trazidos à custódia administrativa não sejam considerados arquivos, a exemplo tem-se documentos oficiais que estão com pessoas privadas, documentos comprados, documentos desmembrados que estão em museus. Logicamente, essa ideia de Jenkinson foi disseminada à época dele; situações em que existiram o rompimento do vínculo documental de seus conjuntos de origem.

Dessarte, havendo *unbroken custody*, o contingente de falsificação torna-se nulo. Porém, a transmissão dos arquivos para seus sucessores não acarreta a interrupção da custódia (*broken custody*):

> Temos visto que o custodiante original dos arquivos é uma pessoa conectada à administração que os produziu. [...] que as funções administrativas e os arquivos podem ser transferidos para uma autoridade administrativa totalmente diferente sem que os arquivos tenham perdido sua característica; mais do que isso, as funções podem caducar e os arquivos serem assumidos por alguma pessoa ou órgão totalmente desconectado com ele e ainda a custódia permanece ininterrupta (Jenkinson, 1922, p. 37-38, tradução nossa).

A Figura 3 sintetiza a abordagem de Jenkinson (1922) sobre cadeia de custódia ininterrupta com uma adaptação complementada por Flores, Rocco e Santos (2016).

Figura 3 – Cadeia de custódia de documentos arquivísticos analógicos



Fonte: Flores, Rocco e Santos (2016, p. 121).

Para os autores, no esquema acima, a gestão e a preservação unem-se pela função da avaliação. Logo, os documentos que não possuem mais o valor primário são avaliados, e se

destituídos de valor secundário serão recolhidos, caso não, eliminados. Todo esse processo deve ser executado por uma instituição arquivística, que se incumbe de manter uma cadeia de custódia ininterrupta.

> A cadeia de custódia, portanto, garante parte da autenticidade e confiabilidade necessária para que o documento seja fixo desde seu uso inicial, momento em que teve uma utilização orgânica, até sua destinação final, seja ela a eliminação ou sua custódia permanente. Este fluxo é chamado Ciclo Vital (Luz; Flores, 2017, p. 176).

Na transferência dos documentos para o arquivo intermediário, seu uso tende a cair e, em muitos casos, migrar para depósitos centralizadores, mantidos pelos mesmos custodiadores do arquivo corrente, pois, como bem se sabe, ao final dos prazos determinados, recolhem-se aos arquivos permanentes (Luz; Flores, 2017). Neste momento, pode ocorrer a quebra na cadeia de custódia,

> por isso é necessário aplicar os processos seguindo o rito arquivístico, a fim de exercer uma sequência de custódia sem interrupção, sem que estes documentos se percam, sejam desviados tanto de instituição como de um sistema que não tenha todos os requisitos arquivísticos e assim comprometa a autenticidade e confiabilidade (Luz; Flores, 2017, p. 177).

A mudança de custodiadores não consagra a maculação da cadeia de custódia, mas a sua quebra, que não reverbera em problemas, uma vez que as qualidades dos documentos precisam ser mantidas. O processo de presunção de autenticidade se baseia nessa ininterrupção e está apoiada na análise da forma fixa e do conteúdo estável dos documentos, que, na abordagem da cadeia de custódia tradicional, informação e suporte são inseparáveis (Santos; Flores, 2020).

Semelhante abstração é insuficiente para os documentos digitais, os quais passam a ser apoiados em requisitos e normas arquivísticas como elementos de verificação de autenticidade e em sistemas informatizados de gestão e de preservação.

4.2.2 Cadeia de Custódia Digital Arquivística

O ciclo de vida dos documentos também pode ser entendido como o ambiente da "cadeia de custódia", que para ser considerada arquivística precisa deter seus princípios, suas normas, seus padrões, suas diretrizes e, se possível, a legislação específica.

Gava e Flores (2020a) destacam: a cadeia de custódia não é sinônimo de ciclo de vida documental, possuem sentidos distintos, mas se entrelaçam, já que aquele é um conceito jurídico, uma necessidade de colocar, em uma linha ininterrupta, os documentos de arquivo.

Isto posto, é com base nos ensinamentos de Jenkinson (1922) e adaptando sua teoria da cadeia de custódia ao ambiente digital, que surge a CCDA.

> [...], há de se evoluir para uma cadeia de custódia digital arquivística, como um modelo de preservação digital, para documentos arquivísticos. Esta preocupação nasceu a partir do momento que começou-se a constatar a produção de documentos digitais que não tinham mais a sua linha de custódia ininterrupta. Ou seja, esses documentos eram exportados, importados, transmitidos sem cadeia de custódia, sem arquivamento, sem recolhimento para os arquivos permanentes, enfim, sem requisitos arquivísticos. Esse cenário não considera uma perspectiva sistêmico-holística da preservação digital, que deve ser sedimentada em padrões, normas e modelos da literatura científica, contemplando todo o ciclo de vida dos documentos. Isso fragiliza a preservação, em longo prazo, de todo o patrimônio arquivístico digital, sob a pena de perda de memória coletiva, e colocando em risco a segurança jurídica de toda uma sociedade (Gava; Flores, 2020b, p. 5-6).

A definição de CCDA ainda se encontra em construção até o momento deste escrito. Foram analisados o Dicionário Brasileiro de Terminologia Arquivística (2005) e o Dicionário de Terminologia Arquivística (Camargo; Bellotto, 2010), além do MAT em inglês, contudo, nada se recuperou acerca da CCDA. Em pouquíssimos referenciais teóricos brasileiros, encontra-se a definição de tal termo, considerando a temática na Ciência da Informação e na Arquivologia.

Em âmbito internacional, para a pesquisadora e coordenadora do InterPARES, Luciana Duranti, *digital chain of custody* (cadeia de custódia digital) tem a mesma acepção de CCDA, sendo a informação preservada e confiável sobre os documentos e as suas modificações, mostrando dados específicos sobre seu estado e outros complementos como datas e horas (Duranti, 2017).

A custódia digital contempla toda informação manifestada em um suporte, registrada em decorrência das funções e das atividades de um órgão, que poderão constituir fonte de prova ou imputar algo na vida das pessoas, incluindo *e-mails*, *websites*, documentos digitais, sistemas informatizados para gestão e para preservação, redes sociais digitais, dados de pesquisa, filmagens de câmeras de videomonitoramento (Santos; Mazuco; Flores, 2020).

A CCDA existe para facilitar o percurso dos documentos arquivísticos digitais que se desenrola em três fases: corrente, intermediária e permanente. Há ambientes distintos para os arquivos de primeira e segunda idade (ambiente de gestão) e de terceira idade (ambiente de preservação e/ou de acesso. Nos sistemas de gestão são realizadas as ações para o correto tratamento dos documentos de valor primário, já nos sistemas de preservação e/ou de acesso são executadas as ações de manutenção e/ou difusão dos documentos de valor secundário.

Mesmo quando há mudança de custódia, a presunção de autenticidade precisa ser mantida nestes ambientes: de um Sigad ou qualquer outro sistema de informação de gestão

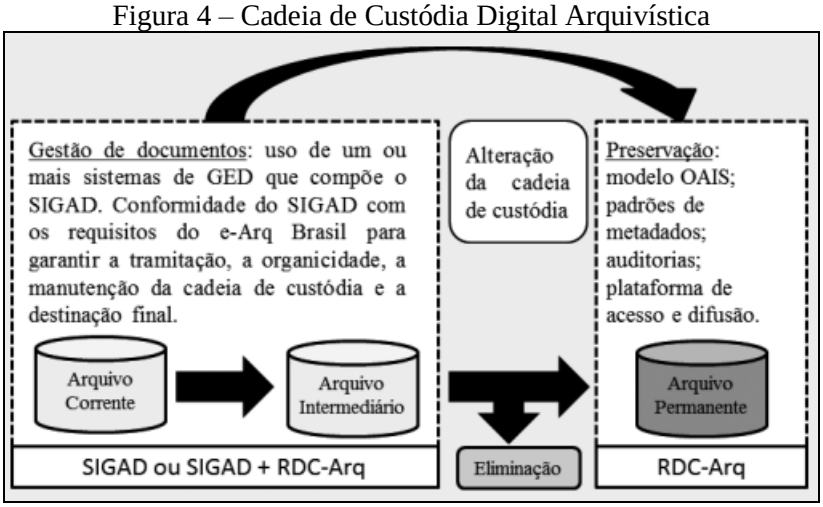
para um RDC-Arq e, caso necessário, a uma plataforma de difusão e acesso. Nestes casos, a presunção deve vir sinalizada pela evidência de que os documentos não foram modificados durante sua transmissão (Gava; Flores, 2020a). Isso implica dizer que a CCDA necessita refletir uma abordagem holística aos documentos, para dar conta de registrar toda e qualquer alteração ao longo do tempo.

Esse processo de preservação em ambientes digitais requer a observância de práticas anteriores à submissão dos objetos a um RDC-Arq, ou seja, ele não deve acontecer apenas nos materiais de caráter permanente. Na verdade, antecede a própria submissão documental num Sigad, deve ocorrer no momento da escolha de normas, de padrões, de pessoal qualificado, de tecnologias.

Por isso, os Sigads têm que estar afinados a padrões recomendados pela comunidade arquivística em sua implementação, como por exemplo, o e-ARQ Brasil; se for no âmbito jurídico, o GestãoDoc (Sistema Informatizado de Gestão de Processos e Documentos), definido pelo MoReq-Jus; e o RDC-Arq definido pela Resolução n.º 51 e pelo Modelo OAIS[19] (Flores; Rocco; Santos, 2016).

Essa comunicação entre sistemas, que é a interoperabilidade arquivística, ajuda na constituição de uma CCDA (Figura 4):

Figura 4 – Cadeia de Custódia Digital Arquivística



Fonte: Flores, Rocco e Santos (2016, p. 128).

O Sigad contempla as fases corrente e intermediária e o RDC-Arq, preferencialmente, a fase permanente. Ao término do valor primário, uma alteração na cadeia de custódia pode

[19] O modelo OAIS detém uma série de recursos relativos à estrutura de metadados utilizados por um sistema informatizado de informação. As metainformações podem registrar procedimentos técnicos de preservação e, assim, especificar permissões de acesso para garantir a autenticidade dos documentos digitais; registram possíveis alterações na cadeia de custódia de um objeto digital, como também identifica-os de forma única, tanto interna, quanto externamente, o que possibilita relacioná-lo ao arquivo a que pertence (Flores; Rocco; Santos, 2016).

ocorrer: a transferência de documentos do Sigad para o RDC-Arq. O que pode acontecer também é a mudança de custodiador, na qual há uma instituição responsável pelo Sigad e outra pelo RDC-Arq (Flores; Rocco; Santos, 2016). Vale destacar que os dois casos não ensejam interrupção na cadeia de custódia, mas sim a transição documental.

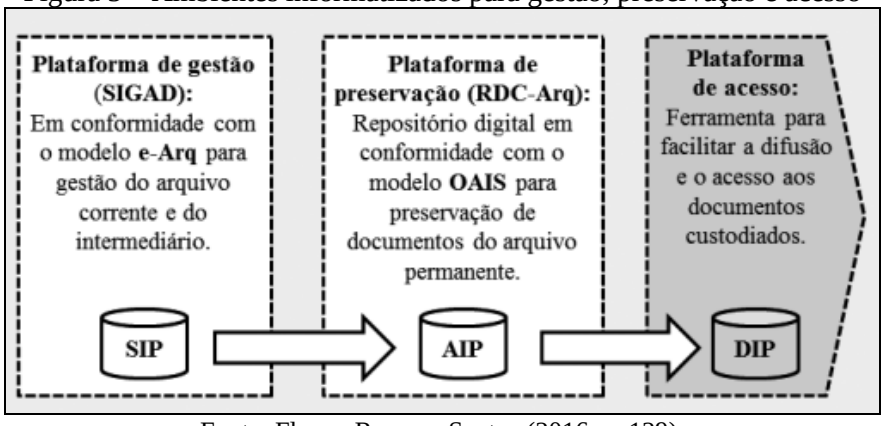
> A construção de uma cadeia de custódia ininterrupta digital requer que o documento esteja inserido no Sigad desde a produção até o seu recolhimento no arquivo permanente, o RDC-Arq, sem que haja alterações, não autorizadas ou não documentadas, em seu conteúdo. Nesse contexto, o incremento na abordagem de Jenkinson é que o produtor passa ao custodiador os documentos digitais por meio de uma interoperabilidade composta por empacotamento e metadados específicos, com plataformas próprias, do Sigad ao RDC-Arq. Os personagens são os mesmos, produtor e custodiador, mas a forma que autentica tal linha ininterrupta é mais complexa, envolvendo inclusive agentes externos, a entidade certificadora, de auditoria, em consonância à ISO 16.363:2012. Tais requisitos irão conferir um *status* aos ambientes digitais, avaliando sua conformidade com modelos pré-definidos em cada região ou país, observando, assim, a efetividade da linha de custódia entre o Sigad e o RDC-Arq (Flores; Rocco; Santos, 2016, p. 126-127).

O acesso aos documentos é dado por uma plataforma de acesso, pois não é recomendado diretamente nos RDC-Arqs, já que é uma "zona militarizada", onde não é permitido nenhum tipo de acesso, senão ao próprio administrador ou à pessoa autorizada.

É nesse ambiente de preservação que serão realizadas as intervenções humanas sobre os documentos digitais, que parte de um tratamento intelectual, como, por exemplo, as estratégias de preservação digital. Outrossim, devem estar inclusas nos RDC-Arqs as atividades de arranjo, de descrição, de difusão, visto que seus registros possuem caráter permanente (Flores; Rocco; Santos, 2016).

Os documentos para esses sistemas informatizados são chamados de pacotes de informação, isto é, os SIPs de valor primário são retidos em um Sigad e se de valor secundário transformados em AIPs, recolhidos e armazenados em um RDC-Arq, para que posteriormente possam ser difundidos e acessados, por meio de DIPs, conforme Figura 5.

Figura 5 – Ambientes informatizados para gestão, preservação e acesso



Fonte: Flores, Rocco e Santos (2016, p. 129).

Em decorrência da obsolescência tecnológica e da instabilidade do objeto digital, que podem afetar as ações de preservação, as atividades de gerenciar os documentos de forma autêntica tornam-se imprescindíveis; processo que demanda a existência de ligações, como visto na Figura 5, também chamado de "cadeias", cujo objetivo é transmitir informação pelo tempo-espaço de maneira segura.

Esse sistema de controle que deve se estender ao longo de todo o ciclo de vida dos registros é definido como cadeia de preservação ou *Chain of Preservation* (CoP), que são passos[20] na preservação digital referentes à produção, à manutenção, à avaliação, ao arquivamento e ao acesso, desde que a autenticidade seja mantida. Uma estrutura de CoP inclui todos os elementos de política, de estratégia, de metodologia, entre outros necessários para a administração de documentos.

Uma das primeiras referências sobre a cadeia de preservação foi dada pelo documento da Força-tarefa de Preservação do InterPARES 1 (Thibodeau *et al.*, 2001), sendo continuado no relatório do InterPARES 2 (Interpares 2 Project, 2002). O modelo de CoP é baseado no ciclo de vida dos documentos, levando em consideração a responsabilidade das entidades para preservação a longo prazo.

A parte 5 do relatório do InterPARES 2 diz que o modelo de CoP é aquele que utiliza ferramentas tecnológicas para desenvolver sistemas informatizados, consistindo em uma série de atividades para a manutenção do ciclo vital do documento arquivístico digital. Corrobora o InterPARES 2 (2002), os registros digitais devem ser geridos cuidadosamente durante toda a sua existência, a fim de garantir acesso e legibilidade pelo tempo que for necessário, mantendo intactos sua forma, seu conteúdo e suas relações.

O MAT na versão inglesa define CoP[21] como um sistema de controles que se estende por todo o ciclo de vida dos documentos de forma a assegurar sua identidade e sua integridade ao longo do tempo.

---

[20] Tal processo é sequencial e inclui: definição do escopo e dos objetivos documentos; de recursos; de verificação da autenticidade; de desenvolvimento de planos compartilhados de transferência; de descrição; de armazenamento adequado e de acesso. A cadeia de preservação significa a ação de confiar um documento digital para armazenamento, preservando todos os seus atributos essenciais, de forma a apoiar a declaração de que o documento arquivístico recuperado é um documento autêntico (Gava; Flores, 2020).

[21] Disponível em: Banco de Dados de Terminologia de Arquivo Multilíngue (ciscra.org).

> [...] é possível vislumbrar que a CoP se apresenta de forma muito mais computacional, já que está focada em registrar, por meio de metadados e modelos computacionais, a sua implementação. Trata-se de uma abordagem mais técnica e tecnológica e diferente da abordagem da CoC, que por sua vez, não está focada num modelo computacional, e sim na ideia de um princípio arquivístico, de cuidado, de um querer, de um manter a linha ininterrupta, apresentando a necessidade de cotejar o documento arquivístico digital. A CoP, por sua vez, é a implementação tecnológica da CoC, que agora, precisa ser ressignificada em um ambiente digital, já que a CoP não substitui a CoC enquanto princípio (Gava; Flores, 2020a, p. 89).

Tanto na cadeia de preservação quanto na custódia digital, os documentos arquivísticos necessitam de cuidados especiais levando em consideração conceitos e legislação que garantam a preservação e o acesso em longo prazo (Flores; Pradebon; Cé, 2017).

4.2.3 A Preservação Digital Sistêmica

A preservação digital tradicional, não sistêmica ou passiva, é uma ação que, na atualidade, denota fragilidade à presunção de autenticidade dos documentos e não vislumbra a cadeia de custódia (arquivística) (ininterrupta), sendo ainda, a realidade mais latente no Brasil. Não obstante, vê se desenvolver os conceitos dessa preservação assistêmica, trazendo rupturas teóricas nos campos científicos em que está inserida, a fim de que sejam adaptados e ressignificados. Kuhn (2017) enfatiza que uma virada paradigmática significa o surgimento de novos fatos para abarcar a complexidade em que se vive.

Nessa linha, torna-se imprescindível pensar em um ambiente de cadeia de custódia digital e de como manter esse espaço, que é tendente à vulnerabilidade, em um lugar de confiança arquivística, na garantia da gestão, da preservação e do acesso (Gava; Flores, 2021a). É por essa causa que a preservação digital passou a refletir um caráter sistêmico, respaldada em políticas, em normas, em padrões e em legislações; holístico, representado pelo gerenciamento “correto” de todo o ciclo vital documental; e ativo, podendo ser caracterizado pela comunicação profícua entre sistemas informatizados de informação, sedimentada em modelos da literatura nacional e internacional.

A PDS não se restringe às estratégias para o cuidado com as mídias e a obsolescência dos suportes, mas, antes, tem a preocupação de se firmar em uma CCDA como mecanismo de confiança à informação. Para Santos, Mazuco e Flores (2020), a concepção da preservação digital agora é sistêmica, de modo que se inclua políticas e padrões a serem seguidos em busca da construção de ambientes confiáveis.

Gava e Flores (2021b) definem a PDS como a devida integração de um ambiente de gestão, de preservação, de acesso e de difusão de documentos, visando manter a sua

autenticidade e a sua confiabilidade ao longo do tempo, ou seja, não só no momento da produção, mas também durante todo o ciclo de vida documental pelo tempo que for necessário, mantendo uma cadeia de custódia digital segura e ininterrupta.

> Essa preservação digital, que prevê uma cadeia de custódia digital arquivística, é o que denominamos de Preservação Digital Sistêmica. No entanto, não é isso que se vê nos diferentes cenários de preservação digital vistos atualmente. Muito direcionada em estratégias de preservação altamente focadas na ruptura de suporte, essa Preservação Digital Passiva não leva em conta, pelo menos não de forma adequada, a ruptura do ambiente de produção dos documentos com seu ambiente de preservação, e a quebra nessa cadeia de custódia, que agora é feita em um ambiente digital altamente vulnerável (Gava; Flores, 2021b, p. 12).

A aplicação da PDS requer o gerenciamento dos documentos em ambientes digitais apropriados com requisitos arquivísticos materializados em *software* de gestão, por exemplo, o Sigad definido pelo e-ARQ Brasil e o GestãoDoc subsidiado pelo MoReq-Jus; em *software* de preservação, como o RDC-Arq, respaldado pela Resolução n.º 51; e em *software* de acesso e de difusão afinado em normas de descrição arquivística; fazendo com que a integração desses sistemas assegure a garantia de conceitos importantes para a confiança da informação, como tal: a autenticidade, a confiabilidade e a fixidez pelo tempo que for necessário.

Consoante Santos, Mazuco e Flores (2020), um RDC-Arq pode manter interoperabilidade com Sigads, mas também com sistemas de negócio[22], desde que o último produza documentos potencialmente arquivísticos.[23]

O e-ARQ Brasil em sua nova atualização, publicizada em 2022, pelo Conarq, enfatiza que para os sistemas de negócios, é fundamental os documentos estarem identificados para que sejam submetidos a procedimentos de gestão arquivísticas de maneira adequada: as atividades de **registro, classificação e destinação.** A gestão arquivística de documentos digitais produzidos em sistemas de negócios pode ser feita de três formas:

> 1. Implementação de funcionalidades para que os sistemas de negócio exportem os documentos arquivísticos e seus metadados para um SIGAD (nesse caso os documentos são mantidos e gerenciados no SIGAD).
> 2. Integração dos sistemas de negócio com um SIGAD (nesse caso os documentos são mantidos no sistema de negócio e a gestão arquivística é realizada pelo SIGAD por meio da interação entre os dois sistemas).

[22] É um sistema informatizado cuja principal função é apoiar a realização de atividades específicas na organização, e que produzem e mantêm dados, informações e documentos sobre essas atividades. Alguns exemplos são sistemas de recursos humanos, atividades financeiras, acadêmico, prontuários e informação geográfica. Tradicionalmente, esses sistemas mantêm o registro das atividades na forma de tabelas de banco de dados, podendo, em certos casos, manter documentos em forma manifestada compreensível para os indivíduos, nos formatos os mais diversos, como, por exemplo: pdf, txt, jpg, dwg, shp (Brasil, 2022, p. 29).

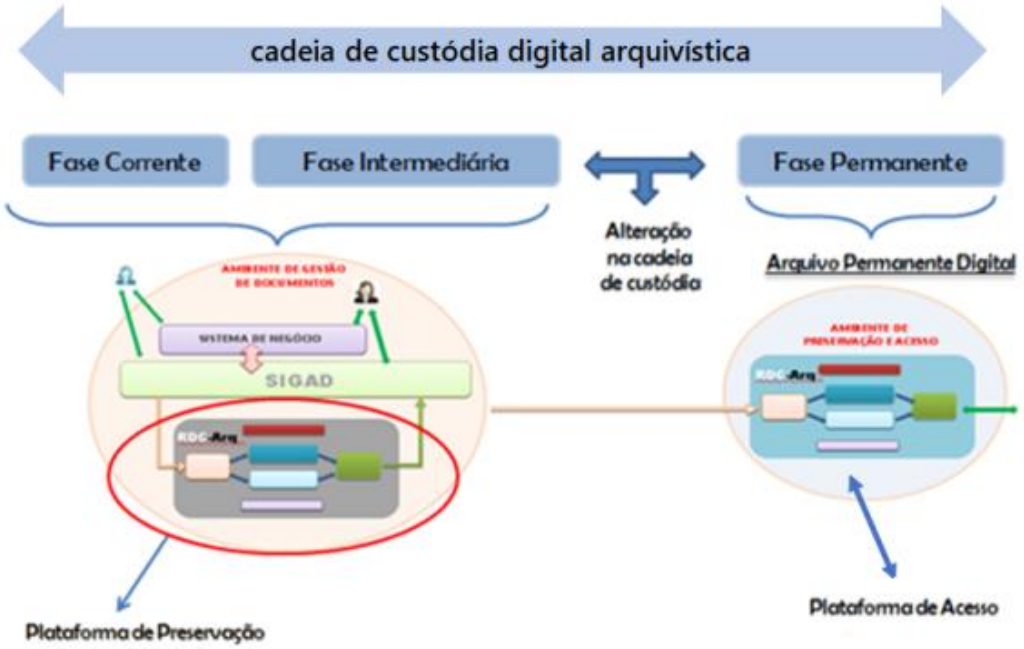
[23] Documentos digitais produzidos e mantidos em sistemas de negócio não cumprem com todas as características diplomáticas, configurando-se como documentos potencialmente arquivísticos. Para serem considerados arquivísticos, os documentos precisam englobar todas as características diplomáticas: ação, forma fixa, conteúdo estável, relação orgânica, pessoas e contexto identificável (Brasil, 2022).

> 3. Implementação de funcionalidades de gestão arquivística de documentos no próprio sistema de negócio (nesse caso os documentos são mantidos e gerenciados no sistema de negócio até a destinação final, ou seja, eliminação ou guarda permanente) (Brasil, 2022, p. 30).

Idealmente, a PDS deve utilizar de sistemas informatizados de gestão arquivística de documentos associados a normas e a padrões, mas se estiver ligada a sistemas de negócio, que mantenha as recomendações supracitadas do e-ARQ Brasil, bem os postulados da Orientação Técnica n.º 3 do Conarq de 2015,[24] a fim de trazer confiabilidade e segurança aos documentos.

Na Arquivologia, a PDS deve atender aos postulados da Resolução n.º 51 do Conarq e do modelo OAIS, sobretudo para que haja uma (boa) comunicação entre Sigad-RDC-Arq; o Sigad atuando apenas nas fases corrente e intermediária dos documentos e o RDC-Arq obrigatório na fase permanente e desejável nas fases corrente e intermediária.

Figura 6 – Interoperabilidade do Sigad com o RDC-Arq



Fonte: Gava e Flores (2020c, p. 94).

Nas fases corrente e intermediária, o RDC-Arq funciona como uma plataforma de preservação e é administrado por um Sigad ou um Sigad de negócio (sistema de negócio com requisitos arquivísticos para gestão de documentos).

O RDC-Arq aplicado na fase permanente torna-se o arquivo permanente digital, que pode ser acessado por meio de uma plataforma de preservação (por exemplo, o *Archivematica* e o Roda), que mesmo sendo uma "zona militarizada, pessoas autorizadas são admitidas; e por

[24] Disponível em: (Microsoft Word - Orienta\347\343o_t\351cnica_RDCarq2015_v8) (www.gov.br).

uma plataforma de acesso, como o AtoM. Com isso, não deve haver a quebra na cadeia de custódia, apenas sua alteração, ao recolher os documentos para a fase permanente, mantendo uma CCDA ininterrupta no ciclo vital dos documentos (Gava; Flores, 2022c).

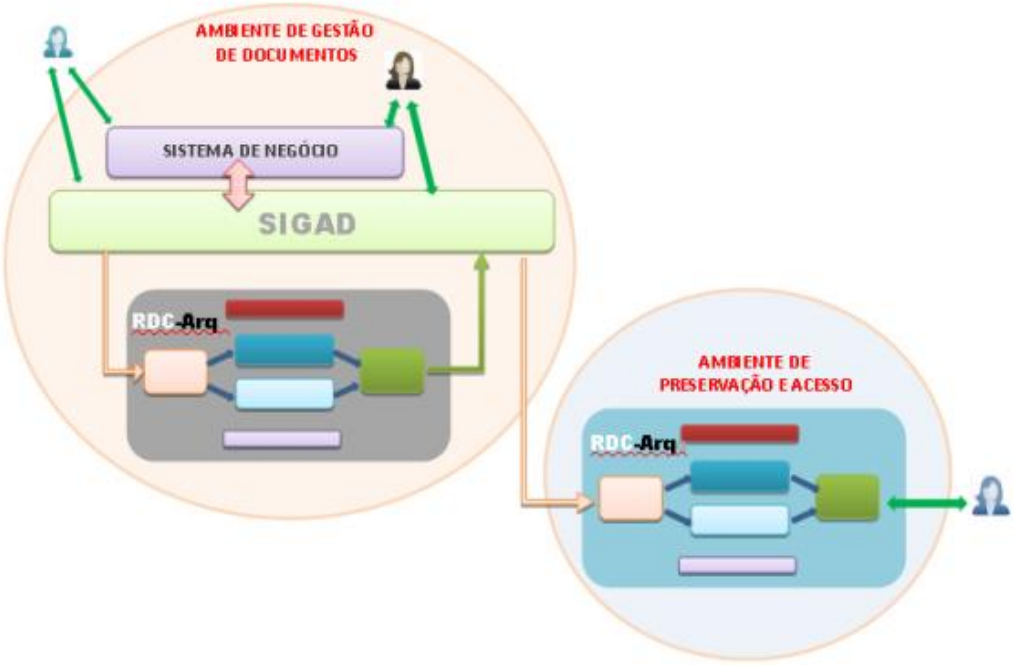
> A custódia arquivística requer a implementação de um Repositório Arquivístico Digital Confiável (RDC-Arq). No caso de documentos de valor permanente, o RDC-Arq requer ênfase em ações como a descrição arquivística, utilizando-se de normas como:
>
> - Norma Geral Internacional de Descrição Arquivística (ISAD (G));
> - Norma Brasileira de Descrição Arquivística (NOBRADE);
> - Norma Internacional de Registro de Autoridade Arquivística para Entidades Coletivas, Pessoas e Famílias (ISAAR (CPF));
> - Norma Internacional para Descrição de Instituições com Acervo Arquivístico (ISDIAH);
> - Norma Internacional para Descrição de Funções (ISDF).
>
> Para custodiar documentos arquivísticos digitais há uma série de normas e padrões que devem ser levados em consideração (Santos; Mazuco; Flores, 2020, p. 253).

Quando da comunicação entre os sistemas informatizados arquivístico, a interoperabilidade, o Conarq na sua Orientação Técnica n.º 3 de 2015, apresenta três possíveis cenários de interação entre um Sigad, um Sigad de negócio com um RDC-Arq (podem ser vistos nos exemplos abaixo), realçando o prisma da preservação digital sistêmica e holística, dentro de uma CCDA.

O gerenciamento dos documentos feito no RDC-Arq não deve ser confundido com o de gestão de documentos realizada por um Sigad; O RDC-Arq administra aspectos como o armazenamento seguro e a aplicação sistemática de estratégias de preservação, já o Sigad, a gestão arquivística dos documentos de valor primário (Conselho…, 2015).

Para ser usado nas duas primeiras idades, o RDC-Arq associa-se a um Sigad, como já mencionado, apoiando a gestão documental, incluindo sua eliminação sistemática. Nas fases corrente e intermediária, não é imprescindível o uso do RDC-Arq, visto que o Sigad garante a autenticidade dos documentos; mas na idade permanente, o RDC-Arq é obrigatório, pois coopera para a melhor maneira de preservação e de acesso.

Figura 7 – Cenário de uso no ciclo de vida total dos documentos de um RDC-Arq em interação com um Sigad

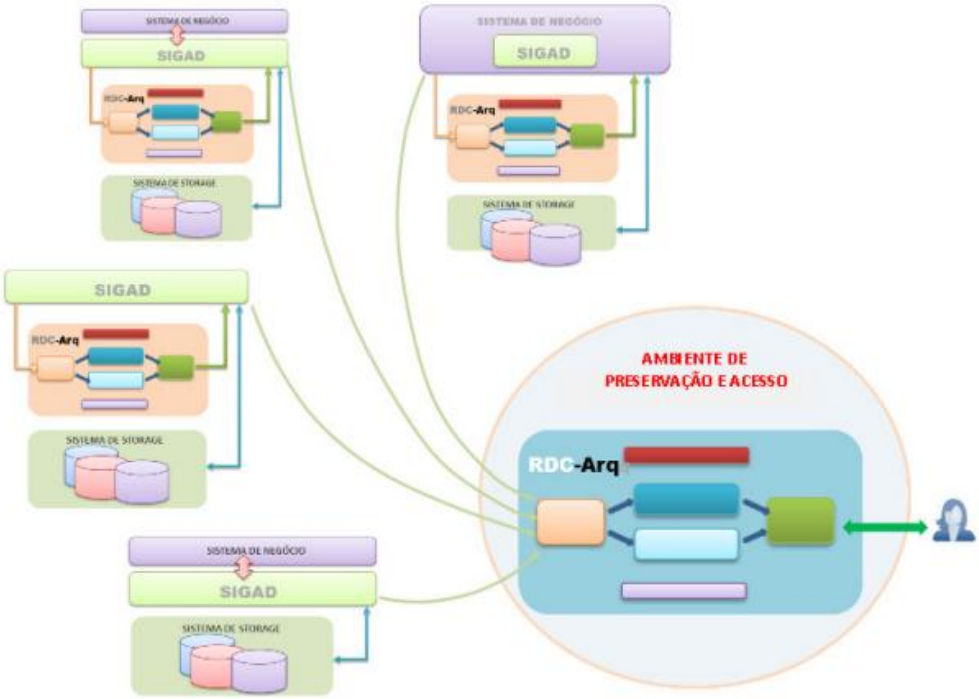


Fonte: Conselho…(2015, p. 4).

Numa conjuntura que englobe o ciclo de vida total dos documentos, conforme a Figura 7, existiria o uso de um RDC-Arq para as idades corrente e intermediária, e outro RDC-Arq para a idade permanente. Neste caso, o RDC-Arq da idade permanente poderia ser o de uma instituição arquivística (como o Arquivo Nacional, por exemplo), envolvendo mudança de custódia, ou o da própria instituição produtora (Conselho…, 2015).

Para as **idades corrente e intermediária**, o uso de um RDC-Arq tem que estar associado ao uso de um Sigad, com o intuito de garantir o cumprimento da destinação, a manutenção da autenticidade e da relação orgânica, para asseverar as características dos documentos de arquivo, em médio e longo prazo. Para a **idade permanente**, os documentos digitais têm que ser mantidos e preservados por um RDC-Arq, de maneira a apoiar o tratamento técnico adequado, incluindo: arranjo, descrição e acesso, promovendo também, a manutenção da autenticidade e da relação orgânica dos documentos.

Figura 8 – Uso do RDC-Arq na fase permanente dos documentos

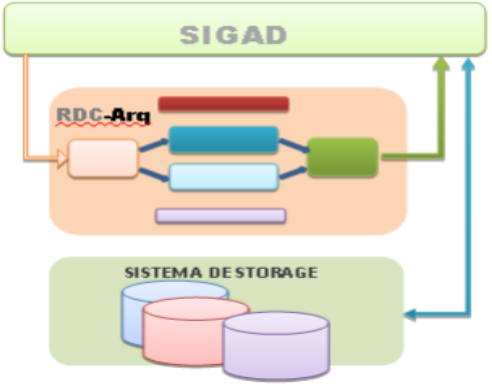


Fonte: Conselho…(2015, p. 8).

A Figura 8 mostra uma possível instituição que dispõe de um RDC-Arq admitindo documentos de Sigads de diversos órgãos, como, por exemplo, o Arquivo Nacional recebendo documentos das entidades da administração pública federal. Abaixo, elencam-se os três cenários distintos para o uso do RDC-Arq em interação com o Sigad, bem como seus exemplos, ambos extraídos da Orientação Técnica n.º 3 do Conarq de 2015:

1) **Cenário:** um Sigad pode gerenciar documentos digitais nas idades corrente e intermediária, armazenando determinados documentos em sistemas de *storage*, e encaminhando outros documentos para um RDC-Arq, de acordo com a política arquivística adotada, como ilustrado na Figura 9.

Figura 9 – Uso simultâneo de armazenamento em sistema de *storage* e de RDC-Arq

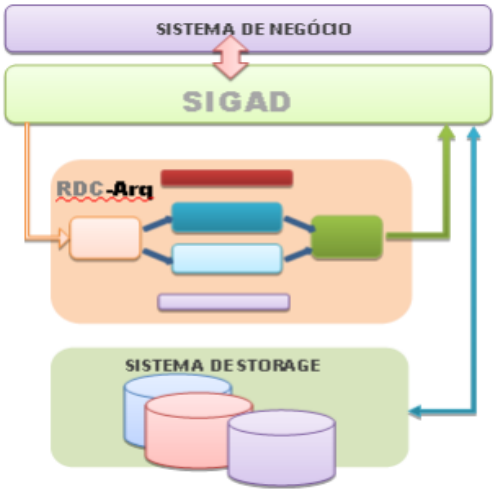


Fonte: Conselho… (2015, p. 5).

No exemplo do primeiro cenário, um órgão determina, com base em seu Código de Classificação de Documentos (CCD) e em sua Tabela de Temporalidade e Destinação de Documentos (TTDD), que todos os documentos com temporalidade prevista menor que cinco anos sejam armazenados no sistema de *storage*, e aqueles com temporalidade prevista acima de cinco anos sejam encaminhados ao RDC-Arq. Isto porque documentos digitais com temporalidade menor que cinco anos, geralmente, não demandam ações que previnam a obsolescência tecnológica e a fragilidade dos suportes, já os de maior duração necessitam de ações de preservação digital próprias de um RDC-Arq.

2) **Cenário:** um sistema de negócio, no ambiente do produtor, pode interoperar com um Sigad, e este com um RDC-Arq e/ou um sistema de *storage*, conforme Figura 9.

Figura 10 – Interoperabilidade entre sistema de négocio-Sigad-RDC-Arq

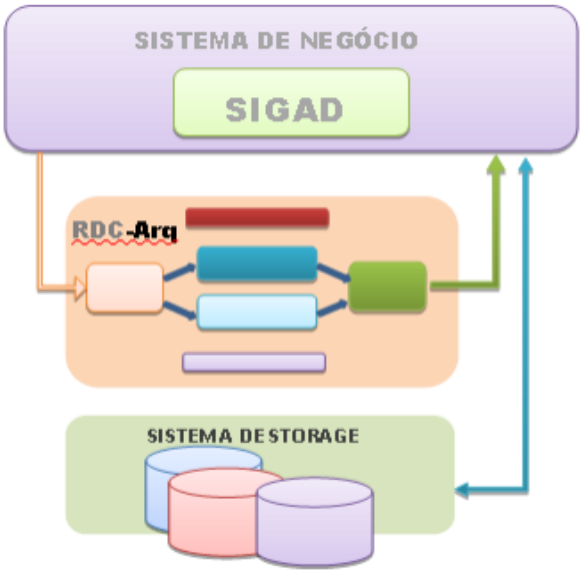


Fonte: Conselho…(2015, p. 6).

No exemplo do segundo cenário, considera-se um sistema acadêmico informatizado de uma instituição de ensino superior que produz documentos, como boletim de notas e frequência, histórico escolar e matrícula em disciplinas. Esses registros são capturados pelo Sigad, que faz a gestão arquivística, armazena os documentos de curta temporalidade no sistema de *storage* e encaminha os de longa temporalidade para o RDC-Arq.

3) **Cenário:** um sistema de negócio no ambiente do produtor que incorpora as funcionalidades de um Sigad e interopera com um RDC-Arq e/ou um sistema de *storage*, conforme Figura 11.

Figura 11 – Sistema de negócio, com requisitos do Sigad, interopera com RDC-Arq



Fonte: Conselho…(2015, p. 7).

No exemplo do terceiro cenário, em uma universidade, o próprio sistema acadêmico informatizado faz a gestão arquivística dos documentos nele produzidos (boletim de notas e frequência, histórico escolar, matrícula em disciplinas, etc.), armazena os de curta temporalidade no sistema de *storage* e encaminha os de longa temporalidade para o RDC-Arq.

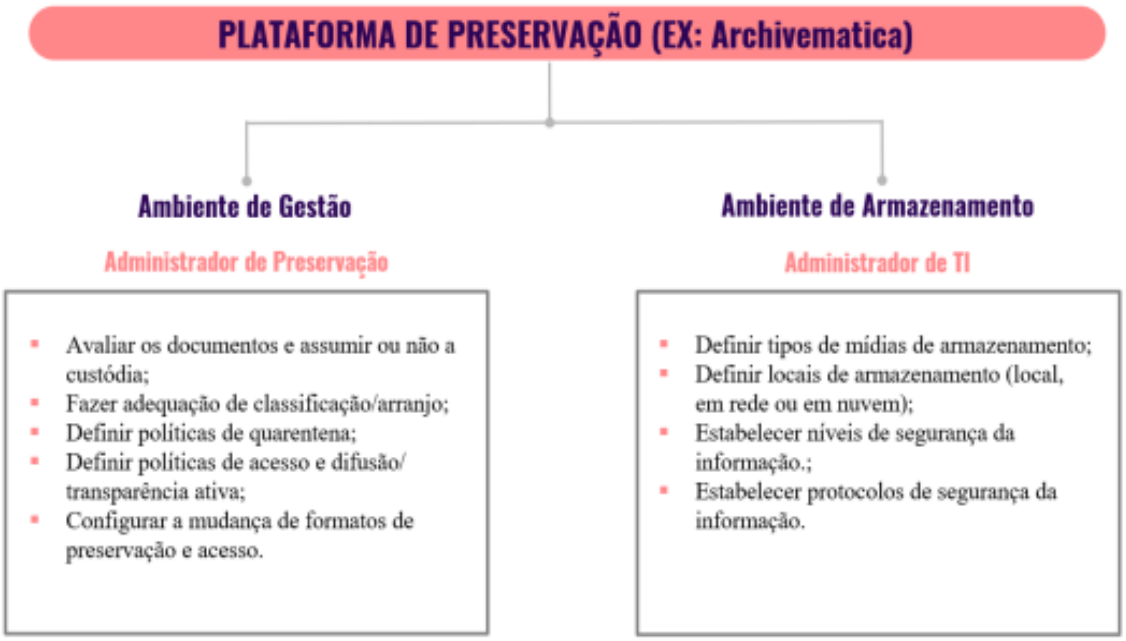
Mas, então, quem são as pessoas que gerenciam esses sistemas informatizados? A essa incumbência estão os papéis ou agentes atuantes na cadeia de custódia, que se definem em três tipos: o produtor, o administrador e o consumidor (entidades definidas pelo modelo OAIS). Ao primeiro tipo cabe a posse da guarda provisória dos documentos, enquantos os utilizam de forma corrente; ao segundo tipo fica a responsabilidade por administrar o conjunto de sistemas de arquivos e que em algum momento passará a custodiá-lo definitivamente; Ao terceiro tipo acomete-se o acesso aos documentos, por meio dos instrumentos de difusão (Luz; Flores, 2017).

Os autores complementam, em relação à administração do administrador, para a área da Arquivologia, esta foi modificada, uma vez que os repositórios passaram a operar em sistemas de dupla checagem, isto é, os responsáveis pelo arquivo e pela área de TI, agora, trabalham conjuntamente por meio de uma "responsabilidade compartilhada", um modelo pós-custodial colocado em sistemas digitais de arquivo. No processo de avaliação dos pacotes de submissão de informação no arquivo permanente digital, a solicitação de eliminação deve ser feita pelo arquivista e o administrador do sistema aplica (ou não) a eliminação. Logo, a

cadeia de custódia é corresponsabilizada por dois papéis; o de guarda (arquivo) e o de manutenção (TI).

Isso denota que o arquivo deve ser considerado como um todo e não o documento individual, ou seja, o produtor e o preservador mantêm uma comunicação/interação profícua, no caso de uma instituição arquivística. Em hodierno, tal acontecimento é considerado pela interoperabilidade para os documentos digitais arquivísticos, dando-se por meio de sistemas informatizados de gestão, de preservação e de acesso (Luz; Flores, 2017).

Figura 12 – Os papéis de administrador de preservação e de TI em uma plataforma de preservação



Fonte: Gava e Flores (2022a, p. 234).

Na PDS, também, dois papéis importantes se sobressaem, segundo Gava e Flores (2022a), o de "administrador de preservação", desempenhado pela(s) pessoa(s) com a responsabilidade de tratar as questões arquivísticas da preservação digital; e o de "administrador de TI", desempenhado pela(s) pessoa(s) com a responsabilidade de tratar as questões tecnológicas de preservação digital. Essas duas funções atuam em dois ambientes diferentes de uma plataforma de preservação, como, por exemplo, no *Archivematica*, conforme Figura 12.

Luz e Flores (2017) consideram que o ambiente do "administrador de preservação" é tratado com base em políticas e planos de preservação digital; e o do "administrador de TI" envolve os aspectos mais tecnológicos da preservação digital.

> Nessa abordagem de preservação digital sistêmica, a eliminação de documentos arquivísticos digitais de longa temporalidade, por exemplo, que cumpriram seus prazos de guarda, e vários outros exemplos, são uma ação conjunta e orquestrada por esses dois papéis, que têm a responsabilidade de manter uma cadeia de custódia arquivística digital ininterrupta e segura, gerindo a transição dos documentos arquivísticos digitais entre os ambientes de gestão documental; de preservação e de acesso e difusão, e baseada em políticas e planos de preservação digital. Ou seja, nessa abordagem não existe mais o cenário em que o profissional do arquivo tem autoridade plena para eliminar documentos arquivísticos. Antes, há a necessidade de se seguir um fluxo de trabalho, e que o administrador de preservação solicite essa exclusão ao administrador de TI, que é responsável pela gestão do ambiente de TI, **que envolve o armazenamento e a segurança dos dados.** Ou seja, as ações de preservação dos documentos arquivísticos digitais tornam-se ações compartilhadas por esses dois papéis, reforçando a necessidade de uma cadeia de custódia digital compartilhada. (Gava; Flores, 2022, p. 10-11, grifo nosso).

Gava e Flores (2022a) dizem que a função do "administrador de preservação" na PDS é replicar e reavaliar os aspectos arquivísticos definidos pela política de preservação digital adotada pela instituição, incluindo a definição dos planos de preservação digital que abrange o processo de admissão, de armazenamento, de preservação, de acesso e difusão dos documentos digitais no ambiente de gestão e da plataforma de preservação adotada, ao longo do tempo. Tais ações envolvem avaliar os documentos e assumir ou não sua custódia; fazer adequação de classificação ou de arranjo; definir políticas de quarentena e de acesso e difusão (transparência ativa); configurar a mudança de formatos de arquivo, tanto de preservação quanto de acesso; cabe a esse papel, apoiar a definição e aplicação das diretrizes definidas na política e planos de preservação digital.

Já o "administrador de TI" tem a função de replicar e reavaliar os aspectos tecnológicos definidos nas políticas e nos planos de preservação digital, abarcando o arquivamento em *storages* dos documentos digitais no ambiente de armazenamento da plataforma de preservação, que analisa e estabelece as tecnologias adequadas para cada uma das demandas tecnológicas da preservação digital. Essas ações são: definir os tipos de mídias de armazenamento e os locais de armazenamento (em rede ou em nuvem); estabelecer níveis e protocolos de segurança da informação como criptografia, replicação de dados (*backups* síncronos) etc.

O arquivista também precisa ter conhecimento sobre essas tecnologias e, dependendo do caso, dar sugestões ou indicar as ferramentas mais adequadas para o gerenciamento dos documentos arquivísticos ao setor ou ao profissional de TI, como: a melhor mídia de armazenamento de acordo com o volume documental, indicação de RDC-Arqs, Sigads e plataformas de acesso etc. Portanto, é fundamental que o estabelecimento desses dois papéis seja respaldado por nomeação em portaria ou em ato administrativo, com mandato e definição de suplentes, embasado na política de preservação (da instituição) (Gava; Flores, 2022a).

Nessa ideia de CCDA compartilhada, o arquivista não detém a custódia documental sozinho, mas permanece com autoridade sobre seu gerenciamento. O que ocorre é o compartilhamento da custódia com o setor de TI, que tem a obrigação de ser sensível às questões arquivísticas, além do embasamento em políticas e planos de preservação, utilizando de normas e de padrões relacionados aos documentos digitais arquivísticos e as melhores estratégias para segurança da informação. Assim, faz-se necessário pensar em uma CDDA não só compartilhada, mas também **distribuída.**

Na CCDA distribuída, particularmente com a transformação digital, existe a demanda no aumento da segurança da informação, exigindo um armazenamento distribuído, em que os dados não se alojem em um único lugar, mas em diversos locais, conectados por meio de uma rede (Gava; Flores, 2022a).

No modelo OAIS, há uma seção registrando a importância de sistemas informatizados estarem distribuídos geograficamente em espaços distintos, com o objetivo de aumentar a proteção contra sinistros e garantir a acessibilidade aos documentos; mas todas as partes sob um mesmo gerenciamento/domínio. O documento OAIS também apresenta vários níveis de interoperabilidade, sendo um deles os “arquivos federados” (*federated archives*), definidos como um grupo de arquivos que concordam em prover acesso ao seu conteúdo, por intermédio de um ou mais instrumentos de buscas em comum.

Os arquivos federados são orientados ao consumidor, que, além da comunidade local (comunidade originalmente atendida pelo arquivo), pode dispor de uma comunidade global (comunidade estendida a usuários que acessam os conteúdos de diversos arquivos OAIS). Os usuários locais tendem a possuir prioridade de acesso, comparado aos usuários globais. A CCDA para se adequar aos modelos dos arquivos federados, poderá não ser mais responsabilidade de uma única instituição arquivística, mas distribuída entre várias delas (Gava; Flores, 2022a).

Dessa forma, o armazenamento dos documentos digitais podem estar na nuvem, geograficamente distante da instituição vernacular, na mesma concepção dos depósitos intermediários para os documentos analógicos. Inclusive, a Instrução Normativa n.º 01, do Ministério da Economia, de 2019, em seu artigo 4, recomenda a contratação de infraestrutura de centro de dados, serviços em nuvem, sala-cofre e sala segura, para respaldar essa CDDA distribuída. O Ministério da Economia expressa que:

> 4.1. Os órgãos e entidades que necessitem criar, ampliar ou renovar infraestrutura de centro de dados deverão fazê-lo por meio da contratação de serviços de computação em nuvem, salvo quando demonstrada a inviabilidade em estudo técnico preliminar da contratação.
> 4.2.1. Os órgãos e entidades devem exigir mediante justificativa prévia, no momento da assinatura do contrato, que fornecedores privados de serviços em nuvem possuam certificações de normas de segurança da informação aplicáveis ao objeto da contratação, assim como outros requisitos que objetivem mitigar riscos relativos à segurança da informação.
> 4.2.2. Os órgãos e entidades devem assegurar, por meio de cláusulas contratuais, que os serviços em nuvem a serem contratados permitirão a portabilidade de dados e softwares e que as informações do contratante estarão disponíveis para transferência de localização, em prazo adequado. (Brasil, 2019, p. 1).

Concorda com Gava e Flores (2020c; 2022a; 2022b), quando identificam a PDS em pelo menos três aspectos importantes: 1) não ser focada no armazenamento dos documentos digitais em mídias externas e na obsolescência dos suportes, um sistema informatizado deve prever essas questões; 2) deve perpassar todos os ambientes envolvidos no ciclo de vida dos documentos digitais; e 3) deve manter a presunção de autenticidade sempre que acontecer a mudança de custódia dos documentos digitais entre esses ambientes.

Isso denota a visão holística e ativa da PSD, representada por uma CCDA colaborativa entre arquivista e tecnólogo da informação de maneira compartilhada e distribuída. Assim, a Arquivologia passa a enfrentar uma ruptura de paradigma, em que a preservação digital salta da exclusividade das estratégias de migração e de conversão da informação de suporte em suporte ou de formato em formato, para uma ação embasada em políticas, apoiada multidisciplinarmente para otimizar o acesso aos documentos no futuro e pelo tempo que for necessário.

Não é de se estranhar que os conceitos de CDDA e de PDS se confundam e sejam utilizados como sinônimos, porquanto possuem definições próximas e complementares. Assim, discute-se sobre a concepções acerca desses dois termos, na tentativa de elucidar pontos que se ajuntam às suas particularidades.

A CCDA é uma linha ininterrupta, ou seja, a comunicação entre os documentos arquivísticos, em suas fases corrente, intermediária e permanente, subsidiada por ambientes digitais distintos, como o de gestão (para as idades corrente e intermediário), de preservação e de acesso (para a idade permanente) por um processo sequencial, e, para isso acontecer, os documentos devem estar inseridos num Sigad ou num sistema de gestão com requisitos arquivísticos, interoperável com um RDC-Arq e, este, com uma plataforma de acesso e difusão, se necessário; perpassando a produção, a avaliação, a preservação até o acesso, conservando as características dos documentos de arquivo, a fim de que permaneçam incorrompidos e sua autenticidade seja garantida. Além disso, envolve as entidades externas

do modelos OAIS, participantes do ciclo de vida documental: o produtor, o preservador e o consumidor, que no caso do espaço de preservação é gerenciado por dois agentes, o administrador de preservação e o administrador de TI, os quais trabalham numa ação cooperada – compartilhada e distribuída – para manter o armazenamento e a manutenção confiável dos documentos digitais arquivísticos.

Já a PSD é uma forma de preservação digital, que utiliza um conjunto de estratégia, para administrar o ciclo de vida dos documentos, perpassando os três ambiente das entidades externas do modelo OAIS, prevendo uma cadeia de custódia digital (arquivística) segura e ininterrupta, em que os sistemas informatizados de gestão, de preservação e de acesso estejam devidamente integrados de maneira holística, da produção ao acesso à informação; todos eles baseados em políticas, em normas e em padrões, que assegurem a autenticidade e, consequentemente, a confiabilidade aos documentos pelo que tempo que for necessário.

A CCDA é uma adaptação dos postulados de Hilary Jenkinson, que inclui a manutenção do ciclo de vida dos documentos arquivísticos inseridos no ambiente digital em uma custódia ininterrupta, por meio de sistemas informatizados de gerenciamento, de preservação e de acesso, visando mitigar as suas vulnerabilidades.

E a PDS é a capacidade de garantir que os documentos digitais permaneçam acessíveis com qualidade suficiente para serem interpretados no futuro, quando recorrido a uma plataforma digital diferente da utilizada no momento de sua criação, por meio de uma comunicação correta, basilada pela imposição de elementos de confiança, como políticas e normas. Ambas são importantes para a Arquivologia, pois visam à preservação e à autenticidade dos documentos digitais.

A CCDA é uma parte importante da PDS que a antecede, uma vez que os conceitos de ambientes de administração documental já existiam e está reforçado pelo respaldo de normas e padrões que visam ao gerenciamento e à correta comunicação dos sistemas de informação para serem considerados confiáveis.

Em suma, a CCDA volta-se com mais afinco à manutenção da autenticidade dos documentos arquivísticos em ambiente digital e a PSD à garantia do acesso e da interpretação dessas informações para o futuro.

5 A TEORIA DE SISTEMAS COMO FUNDAMENTO DA PRESERVAÇÃO DIGITAL

O termo “sistema” está incorporado à linguagem universal, seja em âmbito formal ou trivial, nacional ou internacional, auxiliando também na composição de diversos vocábulos. Com constância, ouve-se falar em expressões como: sistema único de saúde; sistema de transporte público; sistema rodoviário; sistema da empresa, sistema nervoso etc. Entretanto, mesmo fazendo parte do cotidiano, nem sempre seu significado é compreendido e seu uso é empregado de forma correta.

Bertalanffy (2010) salienta que a palavra “sistema” figuraria alto, quiçá em um dos primeiros lugares, caso fizessem uma lista de termos em voga. Hodiernamente, a ideia de sistema está inserida em todos os campos da Ciência, do mesmo modo que tem penetrado no pensamento popular, nos meios de comunicação de massa, tornando-se um jargão comum em todos os setores da sociedade.

A noção de sistema(s), assim como sua teoria, remonta ao mundo antigo, à época dos sumérios, na Mesopotâmia, anterior a 2500 a.C, até os dias atuais, com as tecnologias digitais. Nesse percurso de quase 5000 anos, pode-se resumir a teoria dos sistemas reciclando o mesmo propósito dos tempos antigos: o esforço humano para prever o futuro e sistematizar, conectar e integrar as coisas no mundo.

Os povos sumérios tiveram como primeiro passo a previsão do futuro para compreender o tempo, e, com isso, criaram o calendário. Tal acontecido se deu após a identificação da regularidade na apresentação dos astros, uma vez que o futuro pôde ser previsto porquanto havia uma relação entre as regularidades observadas nos astros e nas cheias dos rios. A partir desse ponto de partida, criou-se a Astrologia e os sistemas de numeração decimal e hexadecimal (Lieber, 2001).

O autor supra ainda ressaltou que foram idealizados os números com significados simbólicos como os dias sagrados (1, 7, 15, 21, 28) em que o trabalho era proibido (aos domingos). Os sumérios também criaram o ano com 12 meses, de acordo com as fases da lua, trazendo para as coisas do mundo uma correspondência de ordem, de lógica e de previsibilidade. Logo, a previsão do futuro passou a reverberar como um procedimento advindo de pressupostos matemáticos, sobretudo, nos milênios e nos séculos seguintes.

Isto posto, corrobora-se que a ideia de “sistema” sempre foi usada como uma questão intuitiva, assim como a ação de classificar. Mesmo as civilizações que não tinham um “letramento” dependiam da noção de sistematizar as coisas para criar referências de

ordenamento, que serviam para compor seus mitos ou para estabelecer suas condições de vivências, por exemplo, a ocupação e a delimitação de espaço.

A Filosofia da Antiguidade também abordou a temática, e sua acepção se direcionava à compreensão dos fenômenos da humanidade de forma global. Os filósofos analisaram as questões humanas sob uma perspectiva macro, levando em conta os diversos saberes e as diversas ramificações do conhecimento. Mas, ao se tentar entender a origem do pensamento sistêmico, tem-se que retornar, provavelmente, à Filosofia pré-socrática.

Etimologicamente, a palavra sistema provém grego "*systema*", significando "combinação", algo estruturado em partes e que atuam em conjunto. Colossi e Baade (2016) reiteram que este sentido é compartilhado pela maioria dos autores da literatura organizacional para expressar a definição de sistema.

Para Chiavenato (2003), sistema (do grego: *sun* = com e *istemi* = colocar junto) pode ser caracterizado por um conjunto de elementos que estão dinamicamente relacionados; o universo, analogamente, está formado por conjunto de sistemas, cada qual contido em outro ainda maior, atuando de modo conectado.

No século XVII, o imperativo de René Descartes teve como recomendação dividir e examinar o problema por parcelas, começando pelas partes mais simples, ascendendo, por partes menores, até as questões mais complexas (Araújo; Gouveia, 2016). Tal abordagem, que ficou conhecida por cartesiana, analítica ou clássica, se preocupava com os elementos enquanto individualidades, assim dizendo, os sistemas eram decompostos em partes menores e mais simples, sendo descritas minuciosamente.

Com base nessa ideia, as Ciências tiveram seus objetos de estudo cada vez mais dissecados: a Física com o átomo, a Biologia com a célula, etc. Todavia, tal abordagem tornou-se insuficiente quando na Física se descobriu uma partícula menor que o átomo – os *quarks* – que eram difíceis de descrever, trazendo uma crise epistemológica à forma como a Ciência estudava e se desenvolvia (Araújo; Gouveia, 2016).

5.1 BASES DA TEORIA DE SISTEMAS NA COMPREENSÃO DA REALIDADE

Sumariamente, sistema é uma formação lógica de apreensão da realidade. Para Lieber (2001), quando se formula o conceito de sistema, não se busca um reflexo do mundo real, mas a descrição de traços cujo conjunto permite a percepção de uma condição de ordem e a proposição para um determinado fim. Então, sistema pode ser entendido como uma coleção

de entidades[25] ou coisas conectadas que formam uma unidade ou um todo, ou que propiciem a consecução de um fim lógico a partir dessas interações conjuntas.

Consoante Chiavenato (2003), sistema é o termo relativo a um conjunto de elementos interdependentes, os quais, juntos, concretizam-se em um elemento unitário. Exemplificativamente, para um circuito elétrico se tornar um elemento único, necessita de componentes ainda menores, os quais dificilmente funcionarão isoladamente. Apenas quando integrados a um sistema maior (elemento unitário), tais componentes poderão funcionar e serem analisados.

Outra analogia feita por Chiavenato (2003) mostra-se por meio do "sistema respiratório", que possui função de transportar oxigênio e as transformações gasosas no corpo: esse sistema interage com outros (digestório, cardiovascular etc.) e, juntamente desses, faz parte de um sistema maior: o ser vivo, que, por sua vez, objetiva a continuação e a prolongação da vida. O ser vivo, por sua vez, faz parte de um sistema maior, composto por outros seres vivos, podendo formar sistemas familiares, empresariais etc.

Sistema também pode ser definido como o conjunto de elementos dinamicamente relacionados para se atingir um fim, operando sobre dados, sobre energia ou sobre matéria (insumos ou entradas de recursos para o sistema operar) para fornecer informação, energia ou matéria (que são as saídas do sistema). A seguir, expõe-se um painel de definição acerca de sistema.

> - Sistema é um conjunto de elementos em interação recíproca.
> - Sistema é um conjunto de partes reunidas que se relacionam entre si formando uma totalidade.
> - Sistema é um conjunto de elementos interdependentes, cujo resultado final é maior do que a soma dos resultados que esses elementos teriam caso operassem de maneira isolada.
> - Sistema é um conjunto de elementos interdependentes e interagentes no sentido de alcançar um objetivo ou finalidade.
> - Sistema é um grupo de unidades combinadas que formam um todo organizado cujas características são diferentes das características das unidades.
> - Sistema é um todo organizado ou complexo; um conjunto ou combinação de coisas ou partes, formando um todo complexo ou unitário orientado para uma finalidade (Chiavenato, 2003, p. 478).

A abordagem sistêmica, que utiliza a teoria dos sistemas para explicar as coisas, opõem-se ao pensamento mecanicista[26], que tem finalidade de dividir organismos em

[25] Entende-se por entidades: pessoas, máquinas, objetos, informações ou mesmo outro sistema, no caso, subsistema. Essas mesmas podem ser inerentes (internas) ao sistema ou transientes (em movimento), ou ainda externo a ele, também chamado de de meio ambiente do sistema (Lieber, 2001).

[26] Mecanicismo (significa invenção engenhosa ou máquina) vem da Filosofia que se difundiu no séc. XVII, a Moderna. A teoria mecanicista considerou a natureza como uma "máquina", um mecanismo em funcionamento,

agregados de células, células em agregados de moléculas, moléculas em agregados de átomos e o comportamento humano em um agregado de reflexos condicionados e incondicionados, segundo Chiavenato (2003). A partir da visão sistêmica surgiu novas denominações às áreas do conhecimento: sistema solar em Astronomia, sistema social em Sociologia, sistema digestivo e respiratório em Fisiologia etc., porém, dentro de uma óptica global e integrada (Araújo; Gouveia, 2016; Bertalanffy, 2010).

A abordagem sistêmica é muito mais ampla que o simples uso de técnicas, pois, como diz Boulding (1966), é uma forma de pensar sobre o trabalho de gerenciar, além de fornecer estruturas para visualizar fatores ambientais internos e externos como um todo integrado. É, antes de qualquer ação, uma forma de pensar, de compreender o mundo empírico sob a égide de uma estrutura teórica. Ou seja, nesta abordagem, um sistema não é apenas a soma de suas partes, mas a integração entre eles. Lieber (2001) adita é competência de um analista, a partir da definição de objetivos e de critérios do sistema, estabelecer claramente o que vai ser incluído ou excluído na análise (processo de inclusão); como vai ser estruturado os atributos (processo de estruturação); processos que devem ser concomitantes.

Churchman (1968) reitera que essa abordagem é um *continuum* de percepção e de ilusão; uma contínua revisão do mundo, do sistema total e de seus componentes; a essência da perspectiva sistêmica é tanto uma confusão quanto um esclarecimento, ambos, aspectos inseparáveis da vida humana. De acordo com essa percepção-ilusão, o autor elenca quatro pontos importantes:

1) A abordagem sistêmica começa quando se enxerga o mundo por meio dos olhos de outrem.
2) A abordagem sistêmica apercebe-se, continuamente, de que toda visão de mundo é restrita. Cada visão de mundo vê apenas uma parte de um sistema maior.
3) Não existe ninguém que seja perito na abordagem sistêmica, ou seja, o problema da abordagem sistêmica é captar o que todos sabem, algo fora do alcance da visão de qualquer especialista.
4) A abordagem sistêmica não é, de todo, uma má ideia. A totalidade não quer dizer generalismo.

---

nos quais os fenômenos físicos seriam explicados pelas leis do movimento. Possui um sentido estritamente cartesiano e postulou que todos os corpos se explicam por meio de dois princípios: a matéria homogênea e o movimento local, que conduz à casualidade.

A teoria clássica foi influenciada por três princípios dominantes, precipuamente, pelas premissas da ciência moderna: o reducionismo, o pensamento analítico e o mecanicismo (este último já explicitado).

- **Reducionismo:** é o princípio baseado na crença de que todas as coisas podem ser decompostas e reduzidas em seus elementos fundamentais, que constituem as suas unidades indivisíveis. Desenvolveu-se, mormente, na Física, na Química, na Biologia, na Sociologia e na Psicologia. Seu foco era "nas partes" e não "no todo".
- **Pensamento analítico:** utiliza o reducionismo como filosofia para explicar as coisas. Sua finalidade é decompor o todo, nas suas partes mais simples, que são mais facilmente solucionadas ou explicadas, para, a *posteriori*, agregar soluções ou explicações parciais para solucionar ou explicar o todo, que constituem a soma ou resultado das soluções ou explicações das partes. O conceito de divisão do trabalho e de especialização do operário são manifestações típicas do pensamento analítico. O relacionamento de interdependência não é considerado neste pensamento.

As teorias modernas e contemporâneas no campo científico fez e faz uso do conceito de sistema. Nesse sentido, o marco moderno mais conhecido na literatura do ocidente, o pensamento do biólogo Ludwig Von Bertalanffy, que postulou, na época do Pós-Segunda Guerra, uma teoria adaptativa para todos os campos do conhecimento, em que as entendidas deveriam se comunicar e interagir, em que "o todo está integrado à(s) parte(s)" (Araújo, 1995).

A teoria dos sistemas é um ramo específico da TGS e os princípios do reducionismo, do pensamento analítico e do mecanicismo passam a ser substituídos por concepções opostas: o expansionismo, o pensamento sintético e a teleologia.

- **Expansionismo:** todo sistema é parte de outro sistema maior que interage entre si. Assim, os sistemas podem ser decompostos em partes menores, mas essas partes não são independentes. O desempenho do sistema depende desse relacionamento, e não mais apenas do desempenho de uma parte isolada.
- **Pensamento sintético:** é uma forma de analisar ou de raciocinar que utiliza as premissas do expansionismo. Se caracteriza como uma parte de um sistema maior que é explicado pelo papel que desempenha nesse sistema maior. As partes são importantes, mas as entender isoladamente não é suficiente. Logo, o sistema é mais do que a simples soma das explicações de suas partes. A análise do sistema é feita de forma dinâmica, relacionando a interação entre seus elementos, e entre o

elemento e o sistema. O relacionamento de interdependência, no pensamento analítico, é considerado. Por exemplo, os órgãos do organismo humano são explicados pelo papel que desempenham no organismo e não pelo comportamento de seus tecidos ou estruturas de organização.

- **Teleologia:**[27] sendo o sistema parte de um todo maior, as causas não podem ser definidas como suficientes para um dado evento acontecer. Ou seja, a relação causa-efeito não é uma relação determinística ou mecanicista, mas simplesmente probabilística. Dessa forma, o comportamento teleológico é explicado por aquilo que ele produz ou por aquilo que é seu propósito ou objetivo produzir. Esse campo dinâmico de forças produz um emergente sistêmico: o todo é diferente de cada uma de suas partes. O sistema apresenta características próprias que não existem em cada uma de suas partes integrantes. Os sistemas são visualizados como entidades globais e funcionais em busca de objetivos. Essa relação acontece, uma vez que não se tem o total controle do ambiente em que o evento ocorre, pois como sistemas abertos que se comunicam com o meio externo, e este é um ambiente altamente mutável e dinâmico, as variáveis influenciadoras no evento surgem e se transformam a todo o momento, ficando difícil a simples definição e afirmação estática destas. Esses aspectos são bem realçados nas Ciências Sociais.

A TGS teve sua gênese com os trabalhos de Ludwig Von Bertalanffy, a qual buscou produzir teorias e formulações conceituais para aplicá-las na realidade empírica (Araújo; Lopes; Oliveira, 2022). Os propósitos da TGS preconizam que:

- há uma tendência à integração das Ciências Naturais e Sociais;
- tal integração parece orientar-se rumo a uma teoria dos sistemas;
- a teoria dos sistemas constitui o modo mais abrangente de estudar os campos não-físicos do conhecimento científico, como as Ciências Sociais;
- a teoria dos sistemas desenvolve princípios unificadores que atravessam os universos particulares das diversas Ciências envolvidas, objetivando a unidade da ciência;
- a teoria dos sistemas conduz a uma integração na educação científica.

Conforme Bertalanffy (2010), a TGS constitui-se na busca da melhor compreensão e unificação dos conhecimentos de uma ampla variedade de áreas especializadas. Não somente os pontos de vistas e os aspectos gerais são iguais em diferentes Ciências, todavia, com

[27] A teleologia é o estudo do comportamento com a finalidade de alcançar objetivos e passou a influenciar as Ciências, sobretudo com avanço da abordagem sistêmica.

frequência, encontram-se leis formalmente idênticas em campos diferentes, que se aplicam a qualquer sistema.

A partir dessas considerações, Bertalanffy (2010) postulou uma nova disciplina científica chamada Teoria Geral dos Sistemas, com o objetivo de formular princípios aos sistemas em geral, independentemente da natureza dos seus elementos e das relações entre eles.

O movimento dos sistemas é pelo menos uma vaga reunião de interesses similares, ligados pelo conceito de sistemas. As ideias emergentes nos vários campos do conhecimento poderiam ser generalizadas pelo enfoque sistêmico, por isso ele é reconhecido como o fundador do movimento de sistemas (Araújo; Baade, 2015). Consoante a essas premissas surgiu a ideia da TGS, cujo objetivo era encorajar o desenvolvimento de sistemas teóricos aplicáveis a mais de uma das tradicionais áreas do conhecimento.

Kuhn (2017) define um momento como esse de revolução científica, já que é feito pelo aparecimento de novos paradigmas conceituais que mostram aspectos antes escondidos na "Ciência convencional". De acordo com essa definição, a implantação da teoria dos sistemas ocasionou uma mudança nos métodos e nas práticas científicas.

Desse modo, a TGS tem como finalidade integrar áreas do conhecimento. Essa integração não tem como propósito reduzir tudo na instância da Física, mas sim, na elaboração de leis que sirvam para todas as áreas. A TGS fundamenta-se em três premissas básicas:

> **a.** *Os sistemas existem dentro de sistemas.* Cada sistema é constituído de subsistemas e, ao mesmo tempo, faz parte de um sistema maior, o supra-sistema. Cada subsistema pode ser detalhado em seus subsistemas componentes, e assim por diante. Também o supra-sistema faz parte de um supra-sistema maior. Esse encadeamento parece ser infinito. As moléculas existem dentro de células, que existem dentro de tecidos, que compõem os órgãos, que compõem os organismos, e assim por diante.
> **b.** *Os sistemas são abertos.* É uma decorrência da premissa anterior. Cada sistema existe dentro de um meio ambiente constituído por outros sistemas. Os sistemas abertos são caracterizados por um processo infinito de intercâmbio com o seu ambiente para trocar energia e informação.
> **c.** *As funções de um sistema dependem de sua estrutura.* Cada sistema tem um objetivo ou finalidade que constitui seu papel no intercâmbio com outros sistemas dentro do meio ambiente (Chiavenato, 2003, p. 474, grifo do autor).

Tudo isso posto, pode-se dizer que a TGS é uma teoria interdisciplinar compreensivista, abrangente e holística, demonstrando o isomorfismo das Ciências, em que os sistemas não podem ser entendidos apenas pela análise separada e exclusiva de suas partes, mas sim numa abordagem da totalidade, do geral para o particular e do particular ligado ao geral.

Mas no que a TGS contribui à PDS? Realçam-se, pelo menos, dois aspectos. Primeiro, porque detém o termo “sistêmica” (que pelo sufixo “-ica”, significa “aquilo que indica relação”, neste caso com o sistema, dando-se pela correta comunicação entre suas partes); e segundo, porque utiliza da abordagem sistêmica para a preservação digital com o objetivo de: fornecer acesso a uma informação autêntica e confiável, como forma de dirimir suas vulnerabilidades, por meio de ambientes informatizados de gestão, de preservação e de acesso, os quais devem estar conectados entre si e aos documentos em todo o seu ciclo vital.

5.2 PARÂMETROS DA TEORIA GERAL DE SISTEMAS NA PRESERVAÇÃO DIGITAL SISTÊMICA

A PDS é um encadeamento de assaz conceitos interligados, os quais auxiliam na sua formação. Por consequência do avanço tecnológico, o termo sistema vem se difundindo cada vez mais, reorientando o pensamento científico para além das áreas consideradas tradicionais, indo ao encontro das Ciências Sociais, que se tornou campo do conhecimento de grande relevância para a TGS.

Esta última área enfatiza a importância de entender as interações e as interconexões entre os elementos de um sistema, buscando compreender seu funcionamento como um todo e não somente como a soma de suas partes individuais. Semelhantemente, a PDS reconhece a complexidade e a interdependência dos sistemas digitais, propondo estratégias e técnicas para garantir a preservação e a acessibilidade a longo prazo, levando em consideração a interação entre as camadas tecnológicas e as dinâmicas e demandas organizacionais, em todo o ciclo de vida dos documentos.

O denominador comum dessas duas áreas é partilhar da abordagem sistêmica ao lidar com sistemas complexos, oferecendo uma base teórica, mas também empírica à análise e à preservação de sistemas (digitais).

Na Arquivologia, a PSD pressupõe a definição de sistema, abarcando uma legião de conceitos que vai da concepção de custódia à CDDA, entidades intercomunicáveis formadoras de um elemento maior. Assim, ao se considerar os documentos arquivísticos digitais como parte de um sistema mais amplo (seu ciclo de vida), torna-se possível desenvolver e utilizar estratégias eficazes para a sua preservação.

Não obstante, a TGS aplicada aos arquivos permite compreendê-lo como um sistema complexo, sob diferentes partes interdependentes, tais como documentos, usuários, técnicas de gestão e de tecnologias etc., com o objetivo de trazer uma análise holística às atividades

arquivísticas, aperfeiçoando os processos de organização, de preservação e de acesso aos registros.

Baseada em seu conhecimento sobre Biologia, a TGS difundida por Bertalanffy procurou evidenciar, inicialmente, as diferenças entre sistemas físicos e biológicos. Ao tentar entender, além do funcionamento isolado dos sistemas menores existentes em um ser vivo, como, por exemplo, o sistema circulatório, nervoso, etc. e a importância do inter-relacionamento desses sistemas menores, entre si e com o próprio sistema maior (o sistema ser vivo), conseguiu mais do que diferenciá-los; o biólogo entendeu o funcionamento genérico de qualquer sistema.

Essa teoria possibilita reconceituar fenômenos dentro de uma abordagem global, permitindo a inter-relação e a integração de assuntos que são, na maioria das vezes, de naturezas completamente distintas. Desse entendimento decorrem também dois conceitos fundamentais, os quais retratam características básicas de qualquer sistema: o de **propósito ou objetivo** e o de **globalismo ou totalidade.**

Todo sistema possui um propósito ou um objetivo a alcançar. Por conseguinte, qualquer sistema tem uma natureza orgânica, na qual uma mudança ocorrida em uma de suas unidades produzirá reações em todas as suas outras unidades, e o efeito total dessas alterações proporcionará o ajustamento de todo o sistema. O sistema sempre reagirá globalmente a qualquer estímulo produzido em qualquer parte ou unidade (Chiavenato, 2003).

E dessas mudanças decorrem dois fenômenos: o da **entropia** (medida da desordem ou da incerteza dentro de um sistema, ou ainda, a perda da comunicação dos sistemas entre si), que na PDS pode ser visto na maneira como a falta de gestão ativa pode levar à “entropia digital”, na qual os documentos digitais se tornam inacessíveis ou inutilizáveis ao longo do tempo; e o da **homeostasia** (equilíbrio entre as partes de um sistema).

Semelhantes eventos acometem os ambientes informatizados de gerenciamento de documentos arquivísticos, especialmente, quando relacionado à autenticidade. O *Archivematica*, como um repositórido digital arquivístico, por exemplo, utiliza de microsserviços para identificar, avaliar e aprovar os elementos de preservação dos documentos. Se esses registros não forem considerados confiáveis por algum motivo, os microsserviços indicam que estão necessitando de melhoramento, imputando correção, antes de passarem para a próxima fase. Ou seja, o próprio sistema é responsável por constatar incongruências nos parâmetros de preservação. Caso a administração do *Archivematica* for manual e autorizar essas inconsistências, o propósito de trazer confiança aos documentos torna-se negativo, quebrando a CoP, o que reverberaria num corrompimento das

características do documento de arquivo, sobretudo à autenticidade, podendo incorrer, o sentido da **entropia**, já que uma parte do sistema tende à desorganização e à desordem. Em contrapartida, o que precisa ser mantida é a **homeostase** – a correta comunicação entre os sistemas informatizados arquivísticos em todo o ciclo de vida dos documentos – Sigad(de negócio)-RDC-Arq-Plataforma de acesso e de difusão numa cadeia ininterrupta.

A classificação dos sistemas dá-se por tipologias – **física/concreta** (composta por equipamentos, por maquinarias, por objetos) ou **abstrata/conceitual** (composta de conceitos, de filosofias, de planos, de hipóteses e de ideias), as quais, no mundo digital, denominam-se *software*.

Com os pressupostos do expansionismo, do pensamento sintético e da teleologia, a TGS permitiu o surgimento de áreas voltadas à tecnologia, como é o caso Cibernética, na década de 1940 e, consequentemente, muitas outras que vieram após ela (Chiavenato, 2003).

A Cibernética[28] emergiu como uma área interdisciplinar na intenção de relacionar todas as outras existentes, incorporando as questões computacionais e informáticas, segundo Bertalanffy (2010). Seu foco era preencher os espaços vazios não pesquisados e permitir que cada Ciência pudesse utilizar os conhecimentos desenvolvidos por outras, ou seja, o propósito era a sinergia.

A princípio, essa área limitava-se à criação de máquinas de comportamento autorregulável, semelhante ao comportamento humano, como robô, computador eletrônico, radar, piloto automático etc. Mas com o passar dos anos, sua aplicação foi necessária à Biologia, à Medicina, à Sociologia, preestabelecendo sua característica interdisciplinar.

O campo de estudo da Cibernética são os sistemas, que considerada uma Ciência da comunicação e do controle, seja nos animais (seres vivos) ou nas máquinas, compreende os processos dos sistemas de organização, de transformação e de processamento da informação e sua concretização em processos físicos, fisiológicos, e psicológicos. Bertalanffy (2010) advoga que tal área está estritamente incorporada à teoria dos sistemas baseada na retroação, quer dizer, na comunicação entre sistema-meio. Outros conceitos estão inseridos na Cibernética, como o de homeostase, de autocontrole, de sinergia, tudo isso, direcionado a uma abordagem organicista da informação.

[28] A Cibernética é uma ciência relativamente jovem e que foi assimilada pela Informática e pela Tecnologia da Informação (TI). A Cibernética foi criada por Norbert Wiener entre os anos de 1943 e 1947, na época em que Von Neuman e Morgenstern (1947) criavam a Teoria dos Jogos, Shannon e Weaver (1949) criavam a Teoria Matemática da Informação e Von Bertalanffy (1947) definia a Teoria Geral dos Sistemas (Chiavenato, 2003, p. 414).

Os sistemas também podem ser caracterizados por **parâmetros** que indicam suas propriedades, por meio de valores e de descrição. Estes parâmetros para fins da PDS são: 1. entrada ou insumo *(input)*; 2. entropia; 3. sinergia; 4. saída, produto ou resultado *(output)*; 5. caixa preta (*black box)*; 6. processamento, processador ou transformador (*throughput*); 7. retroação, retroalimentação, retroinformação (*feedback*) ou alimentação de retorno; 8. ambiente; 9. homeostase (Bertalanffy, 2010; Chiavenato, 2003). Dentro desses conceitos podem haver outros, conforme abordado adiante. Também é válido salientar que todas as nove entidades mencionadas estão respaldadas na abordagem de Bertalanffy (2010) e de Chiavenato (2003), as quais são afinadas à PDS.

1. ***Input:*** é quando um sistema recebe ou admite insumos ou entradas do mundo exterior para poder trabalhar. Pode ser constituída de **informação**, de **energia** e de **materiais**. Recebe também o nome de **importação**.

a) **Informação:** é tudo o que permite reduzir a incerteza, proporcionando orientação e conhecimento a respeito de algo. Permite planejar e programar o funcionamento do sistema. O conceito de informação engloba dois outros, o de **dados** e o de **comunicação.**

- **Dados:** caracterizam-se pelos registros ou anotações em relação a um evento ou uma ocorrência. Analogamente, um banco de dados é o instrumento que acumula e armazena conjunto de dados para a *posteriori* serem combinados ou processados. Quando esse conjunto possui significado, um conjunto de números ao formar uma data, ou um conjunto de letras ao formar uma frase, tem-se informação.

Figura 13 – Exemplos de sistemas de comunicação

SISTEMA	Sistema Telefônico	Porta Automática	Televisão
Fonte	Voz Humana	Afluência de pessoas rompendo raio de luz	Programa de TV
Transmissor	Aparelho Telefônico	Célula fotoelétrica e circuitos auxiliares	Câmara, transmissor e antena transmissora
Canal	Rede de fios condutores que ligam um aparelho a outro	Fio conduzindo ao solenóide que move a porta automática	Espaço livre
Receptor	Outro aparelho telefônico	Mecanismo solenoidal	Antena receptora e aparelho de TV
Destino	Ouvido humano	Porta automática	Telespectador
Ruído	Estática, ruídos, linhas cruzadas, interferências	Mau funcionamento dos dispositivos	Estática, interferência, chuviscos, disfuncionamento dos componentes

Fonte: Chiavenato (2003, p. 424).

- **Comunicação**: informação transmitida a alguém, compartilhada por essa pessoa. Para isso ocorrer, o destinatário da informação deve recebê-la e interpretá-la. Quando essa informação é transmitida, mas não é recebida, ela não é comunicada. O sistema de comunicação tratado pela teoria da informação e da comunicação compõe-se, conforme Figura 13, de seis componentes: fonte, transmissor, canal, receptor, destino e ruído.

Outro conceito fundamental utilizado na perspectiva da teoria da informação e da comunicação é o de redundância, definida pela repetição de mensagem para que sua recepção seja mais garantida. Introduz no sistema a capacidade de eliminar ruídos para prevenir distorções e enganos na admissão da mensagem.

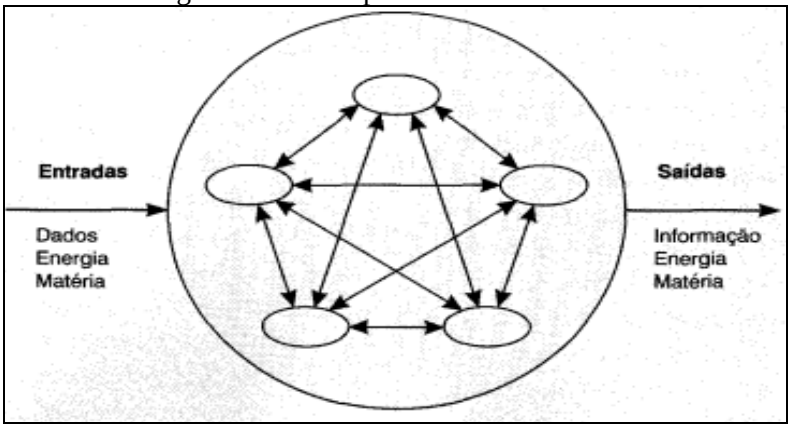
a) **Energia:** é a capacidade de movimentação e de dinamização do sistema, fazendo-o funcionar.

b) **Materiais:** recursos utilizados pelo sistema como meios para produzir as saídas, que são produtos ou serviços. Podem ser operacionais (quando usados para transformar ou converter outros recursos, por exemplo, máquinas, equipamentos, instalações, ferramentas, instruções e utensílios) e produtivos ou matérias-primas (quando são transformados ou convertidos em saídas, ou seja, produtivos ou serviços).

Por meio da entrada, o sistema importa insumos ou recursos do seu meio ambiente para poder trabalhar ou funcionar

2. ***Output***: qualquer sistema produz uma ou mais saídas, que é o resultado final de suas operações. Por meio da saída, o sistema exporta o resultado de suas operações para o meio ambiente. Organizações que produzem bens ou serviços (informações, lucros, pessoas aposentadas ou que se desligam) se caracterizam por uma saída, exemplificativamente.

Figura 14 – Exemplo de sistemas



Fonte: Chiavenato (2003, p. 417).

3. **Processamento:** mecanismo de conversão das entradas em saídas. O processador está empenhado na produção de um resultado. Pode ser representado pela caixa preta, nela entram os insumos e dela saem os produtos.

4. **Caixa preta**: É um sistema cujo interior não pode ser desvendado. Seus elementos internos são desconhecidos e só podem ser conhecidos "por fora", por meio de manipulações externas ou de observações externas; apenas as entradas e saídas são observáveis.

A ideia de “caixa preta” é interdisciplinar e ramifica-se em duas circunstâncias: a primeira se dá pelo sistema considerado impenetrável e inacessível por alguma razão (o cérebro humano ou o corpo humano); e a segunda, pelo sistema considerado complexo, de difícil explicação ou detalhamento (como um computador ou a economia nacional). Exemplo:

> [...] em Medicina, quando o médico observa externamente o paciente queixoso, ou na Psicologia, quando o experimentador observa o comportamento do rato no labirinto quando sujeito a perturbações ou estímulos.
> Na Cibernética, já que é uma área que enfoca as TIs, a caixa preta é um espaço onde existem entradas (insumos) que conduzem perturbações ao interior da caixa, e de onde emergem saídas (resultados), isto é, outras perturbações resultantes das primeiras. Nada se sabe sobre a maneira pela qual as perturbações de entrada se articulam com as perturbações de saída, no interior da caixa. Daí o nome caixa negra, ou seja, interior desconhecido (Chiavenato, 2003, p. 419).

Do ponto de vista arquivístico, a existência de semelhantes “perturbações” devem ser evitadas, uma vez que nos arquivos, os documentos devem estar organizados, classificados, descritos, isto é, expresso. O diagnóstico, por exemplo, é um tipo de instrumento de identificação e de preenchimento de lacunas dos arquivos; mas o que se quer dizer com isso? Esse instrumento é um mecanismo que possibilita conhecer o arquivo como um todo interno-externamente, afastando a ideia de “caixa preta” dessa unidade de informação.

Nos sistemas informatizados de gerenciamento de documento arquivístico, também há funcionalidades que identificam alterações ou adulterações documentais. O foco é desvendar e sanar os problemas informacionais, a fim de não haver *black box*, transformando-a em “caixa branca”, em que os processos internos são visíveis e conhecidos, conforme reitera Chiavenato (2003).

> Diagnóstico. O primeiro passo é o levantamento do defrontamento entre organização e seu ambiente visando às alterações estruturais necessárias. O segundo é o levantamento dos defrontamentos entre grupos, visando às alterações estruturais e comportamentais. O terceiro passo é o levantamento dos defrontamentos entre participantes e a organização, visando às alterações de ordem comportamental. O diagnóstico da situação real e da situação desejada determina a direção para o DO, que deve partir da situação real para a situação desejada (Chiavenato, 2003, p. 398).

Um exemplo de abordagem da “caixa preta” na PDS pode ser o uso de um serviço de preservação digital terceirizado. Nesse caso, a organização fornece os documentos digitais (entrada) e recebe os documentos preservados (saída), mas os processos exatos de preservação (migração de formato, redundância de armazenamento, etc.) podem não ser visíveis para a organização.

Por outro lado, pode-se analisar um sistema de “caixa branca” na PDS, por meio da implementação interna de uma estratégia de preservação digital. Aqui, por exemplo, a organização tem total visibilidade e controle sobre os processos de preservação. Ela pode saber exatamente como e onde os documentos estão sendo armazenados, quais metadados estão sendo capturados e como as migrações de formato estão sendo realizadas.

Esses conceitos têm a incumbência de auxiliar nas decisões sobre como implementar a PDS, isto é, uma organização pode optar por uma perspectiva de “caixa preta” caso não tenha o conhecimento ou recursos para gerenciar a preservação digital internamente; e também por por uma perspectiva de“caixa branca” se quiserem ter mais controle sobre o processo de gerenciamento de sua documentação.

5. **Retroação (*feedback*):** também chamada de servomecanismo, é um subsistema que funciona como mecanismo segundo o qual uma parte da energia de saída de um sistema ou de uma máquina volta à entrada, no sentido de alterá-la de alguma maneira. Serve para comparar a forma como um sistema funciona em relação ao padrão estabelecido para ele funcionar. Caso ocorra alguma diferença entre ambos, a retroação incumbe-se de regular a entrada para que a saída se aproxime do padrão estabelecido.

O objetivo deste parâmetro é o controle, ou seja, o estado de um sistema sujeito a um monitor, que é uma função de guia, de direção e de acompanhamento. A retroação foi planejada para “sentir” a saída (registrando sua intensidade ou sua qualidade) e compará-la com um padrão ou critério preestabelecido para mantê-la controlada dentro daquele padrão ou critério, evitando desvios; impõe correções ao sistema, a fim de adequar suas entradas e suas saídas e reduzir os desvios ou discrepâncias, para regular o seu funcionamento. A finalidade da retroação é impor correções para melhorar o funcionamento dos sistemas, a partir de duas ações:

a) **Retroação positiva:** ação estimuladora da saída que atua sobre a entrada do sistema. Se por acaso, houvesse um sistema informatizado de gerenciamento documental, em que o acesso à informação aumentasse de forma substancialmente, aconteceria a retroação positiva, uma vez que estaria gerando demanda, que se dá pelo processo de busca-solicitação de uma

informação (entrada), estimulando, por meio desse pedido de informação, o acesso (saída). Em suma, essa situação torna-se positiva quando os usuários retornam ao sistema para buscar e para (re)utilizar informações, às quais se pode considerar úteis.

b) **Retroação negativa:** ação inibidora da saída que atua sobre a entrada do sistema. É quando um sistema informatizado de gerenciamento documental diminui sua frequência de solicitação e de acesso à informação, diminuindo a comunicação do sistema-usuário e o sinal de entrada informacional. Ou seja, as informações podem não estarem sendo atrativas aos usuários.

6. **Homeostase:** é obtida por intermédio de dispositivos de retroação, que reagem a uma entrada de informação. O resultado dessa ação-reação transforma-se em uma nova informação, que modifica seu comportamento subsequente. A homeostase é um equilíbrio dinâmico entre as partes de um sistema que dispõe de mecanismos de retroação capazes de restaurar o equilíbrio perturbado por estímulos externos. A base desse equilíbrio é a comunicação e a consequente retroação positiva ou negativa. Na PDS, a homeostase busca manter a integridade e a acessibilidade dos documentos digitais ao longo do tempo, mantendo sua forma fixa e seu conteúdo estável.

Os sistemas têm uma tendência a se adaptar, a fim de alcançar um equilíbrio interno face às mudanças externas do meio ambiente. É também um equilíbrio dinâmico obtido pela autorregulação/autocontrole, em que o sistema deve manter certas variáveis dentro de limites, mesmo quando os estímulos do meio externo forçam essas variáveis a assumirem valores que ultrapassam os limites da normalidade (como é o caso do piloto automático, por exemplo).

> [...]. Todos os seres vivos – desde os mais simples unicelulares até as aves e mamíferos – precisam manter certa estabilidade interna em termos de temperatura, pressão sanguínea etc. Sempre que uma de suas partes sai do equilíbrio, algum mecanismo é acionado para restaurar a normalidade. Os seres vivos vivem em um processo contínuo e incessante de desintegração e de reconstituição: a homeostase. A tendência à manutenção de um equilíbrio interno manifesta-se em todos os níveis da atividade orgânica. [...]. Nos seres mais evoluídos na escala animal, as funções reguladoras são orientadas pelo sistema nervoso e pelos hormônios produzidos pelo sistema endócrino (Chiavenato, 2003, p. 421).

7. **Ambiente:** é o espaço externo que envolve o sistema, onde há uma constante relação de interdependência, de interação e de adaptação entre ambos. Assim, a viabilidade de um sistema depende de sua capacidade de adaptar-se e de responder às exigências e às demandas do ambiente externo. Essa abordagem considerada “ecológica” indica que o ambiente pode ser um recurso positivo para o sistema como também uma ameaça à sua sobrevivência. O processo de adaptação do sistema ao ambiente deve ser sensitivo e

dinâmico, servindo como fonte de energia, de materiais e de informação. Logo, o sistema aberto recebe suas entradas do ambiente, processa-as e efetua saídas ao ambiente.

8. **Entropia**: significa transformação, cujo conceito é controvertido nas Ciências da Comunicação e da Informação. Refere-se à perda de energia em sistemas isolados, levando-os à degradação, à desintegração e ao desaparecimento. A entropia significa que partes do sistema perdem sua integração e comunicação entre si, fazendo com que ele se decomponha, perca energia e informação. Por exemplo, sem estratégias adequadas de preservação digital, os documentos podem se tornar obsoletos à medida que as tecnologias mudam, quando um *software* para ler o formato do arquivo não está mais disponível, ou podem ser perdidos devido à falha do *hardware* ou à corrupção dos dados.

Se a entropia é um processo pelo qual um sistema tende à exaustão, à desorganização, à desintegração e à morte, para sobreviver ele precisa se abrir e se reabastecer de energia e de informação para manter a sua estrutura. Ao processo reativo de obtenção de reservas de energia e de informação dá-se o nome de entropia negativa ou negentropia. À medida que aumenta a informação, diminui a entropia. A negentropia, portanto, utiliza a informação ou a energia do ambiente externo como meio ou instrumento de ordenação do sistema.

A informação também sofre uma perda ao ser transmitida. Isso significa que todo sistema de informação possui uma tendência entrópica. Daí decorre o conceito de ruído. Quando nenhum ruído é introduzido na transmissão, a informação permanece constante.

A garantia de uma gestão adequada dá-se quando os documentos estão corretamente preservados e acessíveis. Isso envolve várias atividades, que vão desde a migração de formato ao monitoramento da integridade da informação. Essas tarefas podem ser vistas como formas de “importar energia” para o sistema de preservação digital. Analogamente, uma migração de formato pode envolver a conversão de documentos digitais para formatos mais recentes ou mais duráveis para garantir seu acesso no futuro. Tal óptica é uma forma de reduzir a “entropia” do sistema, ou seja, a tendência dos documentos se tornarem inacessíveis ou inutilizáveis ao longo do tempo, e aumentar sua “ordem”, isto é, o acesso e a utilidade dos documentos.

9. **Sinergia:** significa trabalho em conjunto, ou seja, cooperação. Há sinergia quando duas ou mais causas produzem, atuando conjuntamente, um efeito maior do que a soma dos efeitos que produziriam atuando individualmente. Quando as partes de um sistema mantêm entre si um estado sólido, uma estreita inter-relação, integração e comunicação, elas se ajudam mutuamente e o resultado passa a ser maior do que a soma dos resultados de suas partes isoladamente.

Sinteticamente, a sinergia refere-se ao fenômeno em que o todo é maior do que a soma de suas partes. Quando um documento digital é preservado com metadados adequados, que fornecem contexto e significado, armazenado em vários locais, para proteção contra perda de dados, e em um formato de arquivo durável, para garantir a acessibilidade a longo prazo, ele será muito mais acessível e utilizável no futuro do que um documento sem essas características. Na PDS, a combinação dessas diferentes estratégias e ferramentas de preservação seria um exemplo de sinergia, uma vez que resultaria em um sistema de preservação mais eficaz do que qualquer uma dessas partes isoladamente. As organizações também são casos típicos de efeitos sinergísticos, assim como a interoperabilidade arquivística.

Em relação à natureza, os sistemas podem ser fechados ou abertos.

a) **Sistemas fechados:** não apresentam troca nem influência com o ambiente. Os sistemas fechados não produzem nada que seja enviado para o ambiente externo. Bertalanffy (2010) realça que não existe um sistema fechado a rigor, ocorre que tal denominação é dada aos sistemas cujo comportamento é determinístico e programado e que operam com pequeno e conhecido intercâmbio de matéria e de energia com o meio ambiente. São também denominados **sistemas mecânicos**, como as máquinas e os equipamentos. A abordagem sistêmica contrapõe-se à microabordagem do sistema fechado.
b) **Sistemas abertos:** apresentam troca e relação com o ambiente por meio de entradas e de saídas. Conservam-se constantemente no mesmo estado (autorregulação) apesar de a matéria e a energia que o integram se renovarem a todo momento (equilíbrio dinâmico/homeostase). Nesse sentido, o sistema aberto é um complexo de interações, influenciado pelo meio ambiente e sobre ele, alcançando um estado de equilíbrio dinâmico (Araújo; Gouveia, 2016). Dessa forma, três acepções são dinamizadas acerca destes sistemas:

> 1. O sistema aberto está em constante interação dual com o ambiente. Dual no sentido de que o influencia e é por ele influenciado. Age ao mesmo tempo, como variável independente e como variável dependente do ambiente. O sistema fechado não interage com o ambiente.
> 2. O sistema aberto tem capacidade de crescimento, mudança, adaptação ao ambiente e até auto-reprodução sob certas condições ambientais. O sistema fechado não tem essa capacidade. Portanto, o estado atual, final ou futuro do sistema aberto não é, necessária nem rigidamente, condicionado por seu estado original ou inicial, porque o sistema aberto tem reversibilidade. Enquanto isso, o estado atual e futuro ou final do sistema fechado será sempre o seu estado original ou inicial.
> 3. É contingência do sistema aberto competir com outros sistemas, o que não ocorre com o sistema fechado (Chiavenato, 2003, p. 179).

Os sistemas abertos são basicamente a representação da TGS, pois preservam características diferenciadas quando relacionados aos sistemas fechados, bem como:

- o **holismo**, trazendo a importância de olhar para o sistema como um todo, em vez de apenas seus componentes individuais, que na PDS se traduz em considerar todo o ciclo de vida dos documentos digitais, desde a sua criação até a preservação-acesso;
- a **interdependência**, referindo-se aos componentes de um sistema como interdependentes, em que a mudança de um componente pode afetar todo o sistema, visto que na PDS a alteração em um documento pode afetar pode afetar sua preservabilidade;
- a **organização,** prevendo uma estrutura organizada nos sistemas, cuja maneira como os documentos são gerenciados podem garantir ou não a sua preservação e o seu acesso;
- a **adaptação**, que sugere uma capacidade adaptativa dos sistemas de mudarem em resposta ao ambiente, ou melhor, como as estratégias de preservação digital podem precisar se adaptar às mudanças tecnológicas.

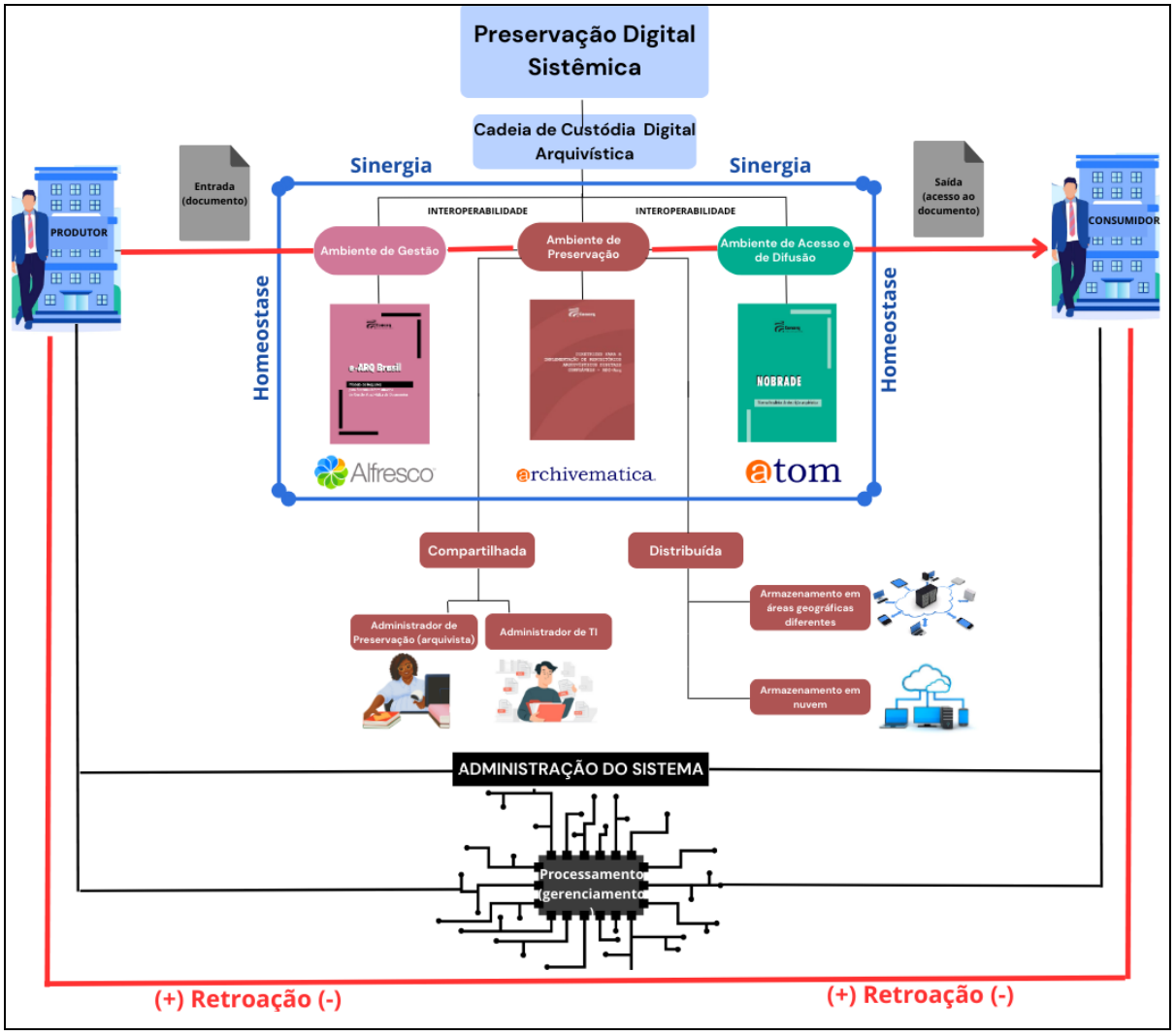
Para Chiavenato (2003), o sistema aberto está organizado pelas seguintes entidades: a) importação (entradas); b) transformação (processamento); c) exportação (saídas); d) por ciclos de eventos que se repetem (importação-transformação-exportação); e) entropia negativa; f) informação como insumo, retroação negativa e processo de codificação g) estado firme e homeostase dinâmica; h) diferenciação[29] i) equifinalidade[30] j) limites ou fronteiras[31]. Em aditivo a essa ideia, os sistemas abertos se compõem pelas seguintes características:

> 1) O todo é superior à soma das suas partes e tem características próprias.
> 2) As partes integrantes de um sistema são interdependentes.
> 3) Sistemas e subsistemas relacionam-se e estão integrados numa cadeia hierárquica (nesta perspectiva pode encarar-se o universo como uma vasta cadeia de sistemas).
> 4) Os sistemas exercem autorregulação e controle, visando a manutenção do seu equilíbrio.
> 5) Os sistemas influenciam o meio exterior e vice-versa (através do input/output de energia e informação).
> 6) A autorregulação dos sistemas implica a capacidade de mudar, como forma de adaptação a alterações do meio exterior.
> 7) Os sistemas têm a capacidade de alcançar os seus objetivos através de vários modos diferentes (Araújo; Gouveia, 2016, p. 9-10).

[29] A diferenciação é a multiplicação e a elaboração de funções especializadas e hierarquizadas.
[30] É quando um sistema pode alcançar, por vários caminhos, o mesmo resultado final, mesmo partindo de diferentes condições iniciais. Na medida em que os sistemas abertos desenvolvem mecanismos regulatórios (homeostase) para regular suas operações, a quantidade de equifinalidade é reduzida.
[31] São barreiras entre o sistema e o ambiente.

A PDS insere-se na perspectiva dos sistemas abertos e adota também os parâmetros e as características explanadas mais acima. Tal relação se dá quando se observa as funcionalidades dos sistemas informatizados em cada um de seus ambientes: o de gestão, o de preservação e o de acesso e difusão. Para sumarizar essa concepção, exepõe-se seu processo na Figura 15.

Figura 15 – Elementos da Teoria Geral dos Sistemas na Preservação Digital Sistêmica



Fonte: Elaborada pelo autor (2023).

A abordagem sistêmica da PDS deve respeitar a CCDA (compartilhada e distribuída). O fluxo documental começa quando o produtor submete um documento a um sistema informatizado arquivístico, em qualquer que seja seu ambiente, sendo este, o dispositivo que recebe ou captura os documentos (entrada), necessitando ser interoperável e, consequentemente sinérgico e homeostático, respaldado por normas como o e-ARQ Brasil (à fase da gestão), a Resolução nº. 51 do Conarq (à fase da preservação) e a Nobrade (à fase da descrição, da difusão e do acesso), ou outras que cumpram os seus requisitos.

Assim, os *software* arquivísticos também concedem acesso (saída) ao consumidor, podendo ter ou não restrição, e utilizam de conversão e migração, além de outras funções, para permitir que documentos de tempos diferentes se comuniquem (processamento).

Como todo sistema tem propósitos, os arquivísticos possuem alguns e entre eles a comunicação com seus usuários para conferir ou ajustar suas funcionalidades, e isso ocorre, por exemplo, por intermédio de *feedback*, que positivo ou negativo, pode ser representado pelo monitoramento e pela avaliação das atividades de sistemas informatizados para informar e melhorar suas funcionalidades.

A existência da homeostase serve para trazer estabilidade aos conteúdos documentais, por meio das funcionalidades dos *software*, como por exemplo, os microsserviços. Oferecendo segurança e confiança à informação. E como já relatado, a homeostase promove o desaparecimento de uma possível entropia. A administração do sistema serve para monitorar tudo o que acontece na PDS, e se necessário, intervir de alguma forma. Logo, não torna-se obrigatório que todos os sistemas possuam todos os parâmetros descritos na TGS, mas aqueles considerados necessários de acordo com sua individualidade.

6 A QUARTA REVOLUÇÃO, A INDÚSTRIA 4.0 E A TRANSFORMAÇÃO DIGITAL: QUE TEM EM COMUM?

A tecnologia sempre foi uma das ferramentas mais importantes para o desenvolvimento humano, sendo utilizada para sanar as suas necessidades. Em analogia a isso, as grandes revoluções (termo que significa mudança) causaram fortes impactos no modo de vida em sociedade, alterando, a cada época, o cotidiano das pessoas.

Conforme Rogers (2017), a primeira alteração profunda em na maneira de viver dos indivíduos, a transição do forrageamento (a busca por alimentos) para a agricultura, ocorreu há pelo menos 10 mil anos e só foi possível graças à domesticação dos animais. Outro exemplo, a Revolução Agrícola, juntou a força desses mesmos animais e a dos humanos para trazer benefícios na produção, no transporte e na comunicação. A Revolução Agrícola foi tão importante que reverberou numa série de outras revoluções, precipuamente, as industriais, iniciadas na segunda metade do século XVIII.

Com o passar do tempo, a produção de alimentos foi se desenvolvendo e gerando o crescimento da população, o que acarretou na urbanização e no surgimento das grandes cidades, ponto-chave para o desencadeamento das Revoluções Industriais, em que as máquinas passaram a desempenhar o trabalho humano, por meio da energia mecânica, para substituir a força muscular.

A **1ª Revolução Industrial (1760-1840)** foi marcada pela construção das ferrovias e pela invenção da máquina a vapor, dando início à produção mecânica e à obsolescência à manufatura artesanal, com grande destaque na Europa e nos EUA.

> Durante a primeira onda da Revolução Industrial, as fábricas dependiam de fontes fixas de energia – primeiro, da energia hidráulica produzida pelas rodas d'água localizadas ao longo dos rios e, mais tarde, da energia a vapor, oriunda de máquinas que queimavam carvão. Embora essas fontes de energia tenham possibilitado o surgimento da produção em massa, elas também enfrentavam graves limitações. De início, impunham a localização das instalações e limitavam a capacidade de produção. Além disso, como as rodas d'água e as máquinas a vapor exigiam que todos os equipamentos da fábrica fossem ligados a um eixo de transmissão central – um único motor extenso que impulsionava todas as máquinas – essas fontes de energia também ditavam o projeto das fábricas e os métodos de trabalho (Rogers, 2017, p. 17).

A **2ª Revolução Industrial (aproximadamente entre os anos de 1870-1914)** destacou-se pelo advento da eletricidade, sobretudo, pela eletrificação das fábricas e das linhas de montagens, emergindo a produção em massa do trabalho derivado do Taylorismo.

Foi uma das descobertas mais significativas do século XIX, a energia elétrica, e eliminou, praticamente, todas as limitações que até então haviam definido as características

das fábricas com a força mecânica. Na década de 1920, um novo ecossistema de fábricas, de trabalhadores, de engenheiros, de produtos e de negócios já tinha tomado forma, tudo em torno da energia elétrica (Rogers, 2017).

A **3ª Revolução Industrial,** ainda no século XX, na década de 1950, ficou conhecida pela **Revolução Digital ou do Computador,** firmando-se no emprego das TICs e pela automação. Foi impulsionada pelo desenvolvimento dos semicondutores, da computação em *mainframe* (década de 1960), da computação pessoal (década de 1970 e 1980) e da *Internet* nos lares da população (década de 1990), afirma Rogers (2017).

O *World Economic Forum*[32], em sua reunião anual de 2016, acontecida em Davos, na Suíça, explorou a temática da **4ª Revolução Industrial**, e Schwab (2016), seu fundador, corrobora vivenciar a gênese de uma revolução que está mudando a forma de viver, de trabalhar e de se relacionar das pessoas.

Para o mesmo autor, essa Revolução iniciada na virada do século (XX-XXI) é baseada na *Internet* ubíqua e móvel, por sensores menores, mais poderosos e mais baratos, pela Inteligência Artificial (IA) e pela aprendizagem automática (ou aprendizado de máquina).

> As tecnologias digitais, fundamentadas no computador, software e redes, não são novas, mas estão causando rupturas à terceira revolução industrial; estão se tornando mais sofisticadas e integradas e, consequentemente, transformando a sociedade e a economia global. Por esse motivo, os professores Erik Brynjolfsson e Andrew McAfee do Massachusetts Institute of Technology (MIT) disseram que este período é "a segunda era da máquina" no título do livro publicado por eles em 2014; estes dois professores afirmam que o mundo está em um ponto de inflexão em que o efeito dessas tecnologias digitais irá se manifestar com "força total" por meio da automação e de "coisas sem precedentes" (Schwab, 2016, p. 6).

A 4ª Revolução é diferente de tudo aquilo que já foi experimentado no decorrer da história. Encontra-se atualmente no processo de compreendê-la, pois sua velocidade e amplitude são incomparáveis em relação aos movimentos anteriores; observam-se bilhões de pessoas conectadas por dispositivos móveis, originando um poder de processamento, de recursos de armazenamento e de acesso ao conhecimento sem precedentes (Schwab, 2016).

Também conhecida pelos sistemas e pelas máquinas inteligentes, não se restringe a esses arquétipos, mas reverbera na fusão de tecnologias e em megatendências que provocam interação entre as chamadas categorias físicas, digitais e biológicas (Schwab, 2006). Nesta linha, numerosas tecnologias vêm abrangendo seu campo: a IA , a robótica, a *Internet* das coisas, os veículos autônomos, a impressão em 3D, a nanotecnologia, a biotecnologia, a ciência dos materiais, o armazenamento de energia , e a computação quântica, entre outras.

[32] O Fórum Econômico Mundial (weforum.org).

Para a **categoria física** existem quatro principais megatendências tecnológicas, que são mais fáceis de enxergar por suas natureza tangível: os veículos autônomos; a impressão em 3D; a robótica avançada e novos os materiais:

- Os veículos autônomos são, por exemplo, os carros sem motoristas, como os caminhões, os drones, os aviões e os barcos.
- A impressão em 3D, também conhecida por "fabricação aditiva", está materializada na criação de objetos físicos por impressão, feitos por camada sobre camada de um modelo ou desenho digital em 3D. Tal impressão começa com um material desarticulado e, em seguida, cria um objeto em três dimensões por meio de um modelo digital. Sua utilização vai desde as grandes turbinas eólicas até aos pequenos implantes médicos
- Na robótica avançada, robôs são utilizados para as várias tarefas, seja na Medicina, na Agricultura ou em outras áreas. A finalidade da robótica é dispor de um rápido progresso na colaboração entre os seres humanos e as máquinas para que seja uma realidade cotidiana.
- Os novos materiais são objetos mais leves, mais fortes, recicláveis e adaptáveis. Suas aplicações estão nos materiais inteligentes com autorreparação ou autolimpeza, nos metais com memória que retomam suas formas originais, nas cerâmicas e nos cristais que transformam pressão em energia. Tem-se também os nanomateriais como o grafeno, que é cerca de 200 vezes mais forte que o aço, milhões de vezes mais fino que um cabelo humano e um eficiente condutor de calor e de eletricidade.

A **categoria digital** é representada pela "*Internet* das Coisas", em inglês, *Internet of Things* (IoT), ou ainda pela "Internet de Todas as Coisas", dá-se pela relação entre as coisas (produtos, serviços, lugares etc.) e as pessoas por meio de plataformas e de tecnologias conectadas. Os sensores são os meios pelo qual as coisas do mundo físico se conectam com as redes virtuais. Dispositivos como *smartphones*, *tablets* e computadores conectados à Internet recebem um sensor, transmissor ou identificação por radiofrequência, permitindo que empresas e clientes rastreiem onde estão e como são movimentados seus objetos em toda a cadeia de fornecimento, qual seu desempenho, como está sendo usado etc.

> A revolução digital está criando abordagens radicalmente novas que revolucionarão o envolvimento e a colaboração entre indivíduos e instituições. Por exemplo, o *blockchain*, muitas vezes descrito como um "livro-razão distribuído", é um protocolo seguro no qual uma rede de computadores verifica de forma coletiva uma transação antes de registrá-la e aprová-la. A tecnologia que sustenta o *blockchain* cria confiança, permitindo que pessoas que não o conheçam (e, portanto, não têm nenhuma base subjacente de confiança) colaborem sem ter de passar por uma autoridade central neutra - ou seja, um depositário ou livro contábil central. Em essência, o *blockchain* é um livro contábil compartilhado, programável, criptograficamente seguro e, portanto, confiável; ele não é controlado por nenhum usuário único, mas pode ser inspecionado por todos (Schwab, 2016, p.17-18 , grifo nosso).

A Tecnologia de Livro-Razão, em inglês, *Distributed Ledger Technology* (DLT) fundamenta-se em registros (como nos livros-razão de contabilidade) adicionados a uma lista de registros de maneira distribuída. É como se vários livros-razão iguais fossem mantidos por várias pessoas (Mori *et al*, 2020). Essa tecnologia atualmente é chamada de *blockchain*.

Surgida no Japão, em 2008, por Satoshi Nakamoto, é qualificada como uma estratégia tecnológica de distribuição, baseada na função de *hashes*, ou chave criptográfica. Emergiu com o propósito de evitar que um mesmo arquivo computacional (arquivo relacionado a criptomoedas) pudesse ser utilizado mais de uma vez, evitando a falsificação da moeda digital (Nakamoto, 2009).

A *blockchain* é como se fosse um livro digital descentralizado ou um banco de dados compartilhado, atualizado e controlado por todos os membros na rede. é uma tecnologia que pode registrar tudo o que tiver valor e for considerado importante: documentos civis, rastreabilidade de produtos e registro de votos (Gonçalves; Rodrigues, 2020).

Sua finalidade primária era permitir a realização de pagamentos em criptomoedas (moedas digitais) entre duas ou mais pessoas, sem intervenção de terceiros como os bancos, os cartórios e os órgãos, de forma rápida, independente e segura nas transações realizadas por meio de suas redes.

A *blockchain* tem como diferencial a sua programação que conta com a criptografia dos dados, geração da função *hash* e auditoria realizada pelos mineradores (os nós) para confirmar a veracidade e a autoria dos dados trafegados via rede (Xavier; Gottschalg-Duque, 2021).

Estruturalmente, a *blockchain* armazena informações de forma cronológica em uma lista de blocos interligados e funciona sob as seguintes características: cadeia de blocos, identificador único da função *hash*, criptografia assimétrica, validação por consenso, distribuição de dados e controle descentralizado, registro do tempo da criação ou modificação do arquivo (*timestamp*) e assinatura digital do autor da alteração do arquivo, conforme

corrobora Xavier e Gottschalg-Duque (2021).

Para melhor elucidar como funciona a tecnologia *blockchain,* apoia-se em toda cadeia de pensamento descrita no exemplo abaixo de Mori *et al.* (2020): considerem-se vários cartórios trabalhando em sincronia para todos os documentos que eles autenticam, emitem ou cancelam. Para qualquer atividade que um único cartório execute, todos os outros recebem tal informação e a anotam em suas respectivas trilhas de atividades executadas (independentemente do cartório que a executou). Isto posto, é de se esperar que todas as trilhas de qualquer um desses cartórios estejam iguais. É como se cada cartório, após criar uma atividade na trilha, a enviasse para os demais cartórios e todos eles teriam trilhas idênticas.

A *blockchain* funciona desta forma, distribuindo as cadeias entre os nós. Os cartórios são computadores (servidores ou nós da rede) que replicam a informação executada por qualquer outro computador na rede. Para cada atividade, todas as trilhas (chamadas de *chain* ou *ledger*) são atualizadas em todos os computadores.

Essa trilha é composta de *hashes*. A característica principal de um *hash* é a geração de uma sequência aleatória de números e de letras de maneira que nunca uma combinação seja igual a outra, mesmo que os dados de origem sejam muito parecidos. Assim, para todas as atividades executadas por um servidor, um *hash* (bloco ou *block*) é gerado e adicionado ao *hash* anterior (cadeia ou *chain*).

Daí provém o termo *blockchain*, pois cada atividade gera um bloco e este bloco é adicionado à cadeia de blocos anterior. Para se adulterar um *blockchain* seria necessário alterar a trilha ou todos os *hashes* de um nó e replicá-lo para os outros nós. Trata-se de uma tarefa árdua. No entanto, o *blockchain* funciona somente com adição de blocos e nunca com alteração ou exclusão deles. Assim, garante-se a autenticidade dos dados e a guarda de um histórico das operações. Logo, os documentos digitais podem ser armazenados seguramente em um *blockchain* e, por meio disso, estabelecer um repositório digital confiável (Mori *et al.*, 2020).

Não é à toa que a aplicação da *blockchain* desperta o interesse da comunidade arquivística, sobretudo, por permitir que qualquer usuário monitore as operações realizadas ou atualize-as, e ainda assim assegurar a imutabilidade e a confiança nos dados armazenados; além de não conferir a sua propriedade e controle a ninguém (Gonçalves; Rodrigues, 2020).

Em outros termos, Schwan (2016) diz que as plataformas digitais tornam possível aquilo que se denomina de economia sob demanda ou economia compartilhada, que reúnem pessoas, ativos e dados, criando formas novas de consumir bens e serviços. O modelo desse

tipo de empresa é a *Uber*, o *Ifood*, a *Shopee*, a *Amazon*, as quais oferecem serviços que vão desde a lavagem de roupas até compras, de tarefas domésticas a estacionamentos, de casas para estada ao compartilhamento de transporte de longa distância. Todas elas possuem uma coisa em comum: semeiam a confiança, pois emparelham oferta e demanda de maneira bastante acessível (baixo custo), além de permitir que as partes interajam, sobretudo pelo *feedback.*

> Em março de 2015, o estrategista de mídia Tom Goodwin escreveu em um artigo para o *TechCrunch*. 'O *Uber*, a maior empresa de táxis do mundo, não possui sequer um veículo. O *Facebook*, o proprietário de mídia mais popular do mundo, não cria nenhum conteúdo. Alibaba, o varejista mais valioso, não possui estoques. E o Airbnb, o maior provedor de hospedagem do mundo, não possui sequer um imóvel' (Schwab, 2016, p. 19).

Na **categoria biológica**, realça-se as inovações na própria Biologia, sobretudo, na Genética, esta reduzindo os custos de seus procedimentos e aumentando a facilidade de suas operações; um genoma humano, por exemplo, pode ser sequenciado em poucas horas por um custo relativamente baixo: dez dólares. A tendência atual é a Biologia Sintética, que oferecerá a capacidade de criar organismos personalizados, escrevendo o DNA deles; outros fatores são importantes destacar, como os biocombustíveis. Lida-se com desdobramentos ainda não ou pouco vistos, em que os *stakeholders* da sociedade global, governos, empresas, universidades e sociedade civil, devem trabalhar juntos com visão compartilhada (Schwab, 2016).

Não há consenso sobre a existência de fato da 4ª Revolução Industrial, algumas correntes acreditam que todas as inovações citadas são apenas mais um aspecto da 3ª Revolução Industrial. Porém, Schwab (2016) realça pelo menos três elementos que os distinguem das Revoluções Industriais passadas: a velocidade, a amplitude e profundidade e o impacto sistêmico.

Nesses termos, a velocidade evolui em um ritmo exponencial e não linear, ao contrário das Revoluções Industriais antecedentes. Esse é o resultado do mundo multifacetado e profundamente interconectado atual; além disso, as novas tecnologias geraram outras mais novas e cada vez mais qualificadas.

A amplitude e a profundidade têm a Revolução Digital como base e combina várias tecnologias, levando a mudanças de paradigmas na economia, nos negócios e na sociedade. A 4ª Revolução não está modificando apenas o "o que" e o "como" fazemos as coisas, mas também "quem" somos. E por fim, o impacto sistêmico, que interliga todos os setores sociais, acarretando à transformação de sistemas inteiros entre países e dentro deles.

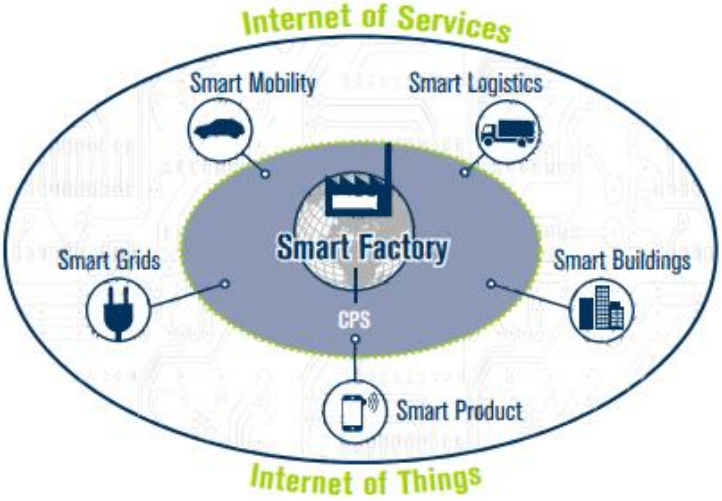
6.1 A INDÚSTRIA 4.0

Um dos fatores que causa o rompimento de paradigmas nessa seara tecnológica é a inovação, foi assim com o desenvolvimento das Revoluções Industriais. Também chamada de 4ª Revolução Industrial por Tessarini Junior e Saltorato (2018), a Indústria 4.0 iniciou suas discussões em meados de 2011, quando uma associação de representantes do governo, empresas e academia alemã apresentou na Feira de *Hannover* uma ideia com séries de estratégias para transformar e otimizar a cadeia de produção global por meio das fábricas inteligentes. O governo alemão apoiou a iniciativa e anunciou que a Indústria 4.0 seria parte de um projeto que ficou conhecido como *High-Tech Strategy 2020 for Germany*, cujo objetivo foi levar a Alemanha à liderança tecnológica, estabelecendo um grupo de trabalho, e sua primeira recomendação foi publicada em abril de 2013 (Azevedo, 2017).

Kagermann, Wahlster e Helbig (2013) realçam que esse fenômeno gerou o que ficou conhecido como *smart factory* (a fábrica inteligente), em que Sistemas Ciberfísicos (CPS) monitoram processos físicos – criando uma cópia virtual do mundo. São compostos de *hardware* e de *software* integrados capazes de controlar e de monitorar equipamentos físicos nos meios de produção, de produtos e de serviços. A *Internet* das Coisas, os robôs e as máquinas em redes fazem uso desses sistemas para se comunicarem entre si e com humanos em tempo real.

Os serviços internos das fábricas inteligentes são oferecidos e praticados no âmbito de uma cadeia de valor, ocorrendo quando as atividades de empresas conectam-se e passam a trocar informações em um ambiente que geram valores para o mercado. Na Figura 16, é possível observar a integração da fábrica inteligente com toda uma cadeia de valor: os serviços de mobilidade inteligente e de logística inteligente, os edifícios inteligentes, os produtos inteligentes e as redes inteligentes.

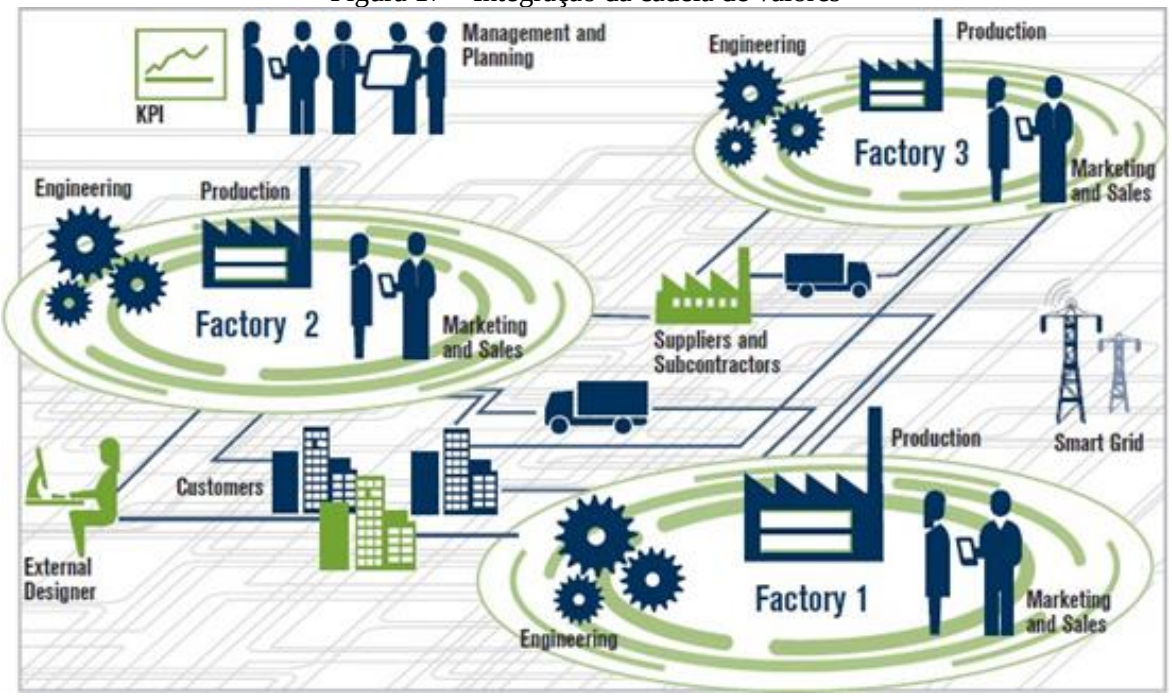
Figura 16 – A Fábrica Inteligente da Indústria 4.0



Fonte: Kagermann, Wahlster e Helbig (2013, p. 19).

Em termos de implementação, a Indústria 4.0 tem como finalidade a otimização de sua cadeia de valor, com uma sistemática de inovação que leva em consideração o potencial econômico e tecnológico, conforme a Figura 17, cujo foco está representado pelos seguintes fatores: a integração horizontal por meio de redes de valores; a integração digital fim a fim da engenharia em toda a cadeia de valor; integração vertical e sistema de manufatura em rede.

Figura 17 – Integração da cadeia de valores



Fonte: Kagermann, Wahlster e Helbig (2013, p. 22).

Azevedo (2017) destaca que o grupo de trabalho alemão definiu oito áreas-chave que necessitam de pesquisa e de aprofundamento para que os conceitos da iniciativa sejam

corretamente implementado à Indústria 4.0:

1. normatização e padrões abertos para uma arquitetura de referência;
2. gestão de sistemas complexos;
3. possuir uma infraestrutura de banda larga abrangente para a indústria;
4. questões de *safety* e *security* como fator crítico para o sucesso da Indústria 4.0;
5. projeto e organização do trabalho adequado para a era digital industrial;
6. treinamento e desenvolvimento profissional contínuo;
7. *framework* regulatório;
8. uso eficiente dos recursos.

Em síntese, a Indústria 4.0 vem transformando o modo de como empresas, por meio de seus serviços, e pessoas se relacionam. Conforme Diogo, Kolbe Junior e Santos (2019), o movimento alemão foi seguido por outros países: a China, o Japão, os EUA, o Brasil, entre outros. Essa mudança tem sido caracterizada pela presença dos CPS.

Tessarini Junior e Saltorato (2018) citam que os EUA, em 2011, anunciaram a *Advanced Manufacturing Partnership* (AMP), consistida na união entre as universidades, as indústrias e o governo federal, para promover investimentos em tecnologias no país. Em 2014, sua sucessora, a *Accelerating US Advanced Manufacturing* (AMP 2.0), trouxe uma série de ações adicionais a ser adotada para alavancar a capacidade de manufatura avançada do país.

Também destacam as ações da China, que em 2015 apresentou o *Made in China* 2025, um programa estratégico para atualizar a indústria no país com diversas metas estabelecidas para 2020 e 2025; e, na Coréia do Sul, onde foi criado o *Korea Advanced Manufacturing System* (KAMS), projeto com a finalidade de desenvolver novos processos e tecnologias para o gerenciamento e a integração dos sistemas de produção. Essas visões, embora em países diferentes, têm objetivos em comum: a inovação tecnológica para um potencial econômico mais competitivo, no que se refere à TD nos setores da sociedade. Entretanto, não são só os CPS que marcam a Indústria 4.0, também chamada de TD por Lydon (2016), outros pilares subsistem (Figura 18).

Figura 18 – Os nove pilares da Indústria 4.0

Fonte: Diogo, Kolbe Junior eSantos (2019, p. 15) adaptado de Lydon (2016).

Durante a tese, alguns desses pilares já foram destrinchados sob à óptica de distintos autores, logo o destaque será para os ainda não explanados.

Na Indústria 4.0 há dois tipos de robôs: **o autônomo e o colaborativo.** A robótica autônoma ficou conhecida pela evolução dos robôs tradicionais presentes desde a 3ª Revolução Industrial, caracterizados pela presença de seis eixos imitando os movimentos antropomórficos. Os colaborativos são aqueles que abarcam sensores avançados reproduzindo a percepção humana em seu volume de trabalho, no intuito de trazer segurança a operações semelhantes. Os robôs colaborativos também se juntam aos trabalhadores em linhas de produção.

***Big Data*, Macrodados, Megadados** ou **Grandes dados** são conjuntos de dados cujo tamanho é fator de impedimento de captura, de armazenamento, de gerenciamento e de análise por parte de ferramentas computacionais tradicionais (Manyika *et al.*, 2011), requerendo formas para processamento de grandes volumes de dados.

De acordo com Armstrong (2019), o *big bata* possui essa nomenclatura por envolver uma enorme quantidade de *bits* de dados, às vezes, da ordem de bilhões. O autor também realça que, para além disso, a quantidade de dados pode levar a falsos positivos, caso seu manuseio não seja adequado. Por isso, atualmente, enfrenta-se os desafios tecnológicos para

coletar, para guardar e para disponibilizar volumosos conjuntos de dados e produzir informação relevante (Rautenberg; Carmo, 2019).

O termo surgiu em meados de 1997, usado pela primeira vez por John Mashey (Armstrong, 2019). Os dados estão crescendo de forma exponencial, e graças às tecnologias da TD, torna-se possível recolhê-los, manipulá-los, analisá-los e exibi-los com mais eficácia, aumentando o seu valor. O *big data* surgiu preconizando três características essenciais, denominadas por Laney (2001) como 3 Vs: Volume, Velocidade e Variedade, porém, outras características foram acrescentadas e hodiernamente se pode falar em, pelo menos, 6 Vs, conforme Akhtar (2018): a Veracidade, a Variabilidade e o Valor.

Figura 19 – 6 Vs do *Big Data*

Fonte: Rautenberg e Carmo (2019) adaptado de Akhtar (2018).

1. **Volume:** relaciona-se aos grandes volumes de dados gerados mediante o uso de recursos computacionais. Com a evolução das mídias sociais e dos serviços da Internet, as pessoas passaram a produzir mais conteúdos, isto é, vídeos, fotos, *tweets*, entre outros tipos de dados.
2. **Velocidade:** os dados são gerados quase que de forma instantânea à medida que os recursos computacionais têm sua capacidade de produção, de captura e de processamento de dados aumentada. Tais fontes vão desde mensagens em redes sociais, radares, sensores, celulares, computadores até coordenadas de drones. Também existem os diferentes formatos e tipos de dados como textos, *e-mail*, áudios, dados de transações financeiras, etc., sendo um dos maiores desafios do *big data* gerenciar todos esses ao mesmo tempo.
3. **Variedade:** os dados provêm de fontes distintas (*e-mails*, *posts* em mídias sociais, arquivos de vídeo, áudio, gráficos, dispositivos, sensores), as quais implementam tecnologias distintas para representação e para armazenamento de recursos digitais.
4. **Veracidade:** refere-se à integridade e à precisão dos dados, contrapondo o fenômeno

Garbage-in, Garbage-out (Gigo), em tradução: lixo entra, lixo sai, na recuperação da informação. Deve-se evitar ruídos e incertezas no armazenamento dos dados de modo a não interferir na análise da informação e no processo de tomada de decisão.

5. **Variabilidade:** é a compreensão e o tratamento dos fenômenos temporariamente presentes nos dados. Por exemplo, alguns eventos específicos virais nas mídias sociais, como a estreia de um filme muito aguardado ou o acontecimento de um fato midiático, podem refletir em padrões de comportamento que não se sustentam ao longo do tempo.
6. **Valor:** uma das características mais importantes dos dados, independente das demais dimensões citadas. É percebido pela análise da precisão dos dados e pela aquisição de informação e *insights* úteis ao processo de tomada de decisão, ou seja, o valor significa "informação útil".

A **Integração Vertical e Horizontal de Sistemas** se dá pela conectividade entre órgãos, empresas e instituições por meio de sistemas computacionais, amparada pela integração e interoperabilidade deles. A integração de sistemas é um conceito presente desde a 3ª Revolução Industrial, mas era feita apenas de forma vertical e somente as grandes empresas conseguiam possuir, por causa do alto custo. A ideia da TD é facilitar essa integração, que também deve dimanar a uma forma horizontal, que vai além das fronteiras das organizações para toda cadeia de suprimentos e de logística. A Gestão do Conhecimento torna-se uma ferramenta essencial para que essa integração seja possível (Diogo; Kolbe Junior; Santos, 2019).

A **Segurança Cibernética**, quando os sensores de mais baixo nível são conectados à Internet, na nuvem e em diversos outros sistemas, eles podem estar sujeitos aos ciberataques. Assim, há de se pensar em defesa e em profundidade, que exige investimentos em arquiteturas de redes confiáveis. Isso exige *know-how* na área de segurança de sistemas de informação.

A **Simulação (Computacional)** acontece quando *hardware* e *software* robustos permitem que fábricas inteiras sejam simuladas com visão tridimensional, que pode estar associada à hologramas à realidade aumentada.

A **Realidade Aumentada** é uma tecnologia que permite a visualização de produtos e de serviços ainda não produzidos. Com o uso dos *smartglasses* e *tablets* ou *smartphones* é possível se ter informações da produção em tempo real com ou sem imersão. Para algumas situações, por intermédio de gestos com as mãos, pode-se interagir com o mundo virtual, manipulando-o no mundo real. Olhando dessa forma, percebe-se que a realidade aumentada ou mista, aliadas à IoT e a integração de sistemas, habilita os CPS, que, consequentemente,

tem muito a colaborar com o trabalho humano.

6.2 TRANSFORMAÇÃO DIGITAL: TECNOLOGIAS EMERGENTES, DISRUPTIVAS E SUSTENTADAS

As mudanças acontecidas no contexto da 4ª Revolução Industrial têm sido representadas pelo conceito de TD, que embora sejam termos difundidos, mas não definidos, no ano de 2000, por Patel e McCarthy[33], estão associados, muitas vezes, à "digitalização". Contudo, Abolhassan (2016) diz: esse fenômeno iniciou-se há pelo menos 60 anos com o desenvolvimento do primeiro supercomputador e da disseminação gradual do processamento de dados e da TI na automatização das indústrias.

Aditam Paixão *et al.* (2020), a TD é um processo de mudança disruptiva ou incremental (sustentada) começado pela doação e pelo uso de meios digitais, que evoluiu para uma conversão holística implícita de uma organização ou da deliberada busca de criação de valor, podendo ser observada sob o pilar de três abordagens: tecnológica, organizacional e social (Cruz, 2023):

- **tecnológica –** baseada no uso de tecnologias digitais, ou melhor, nas mídias sociais e nos dispositivos móveis. Outro modo de compreender esta abordagem é por meio da análise do tipo de uso tecnológico empregado nas atividades organizacionais, as quais representam as fases de seu processo: **digitização**, **digitalização** e a própria TD. Enquanto a digitalização envolve a conversão de dados analógicos em digitais, a digitização significa transformar negócios analógicos em digitais ou criá-los digitalmente. Já a TD representa a transformação efetiva das organizações pela inovação em modelos de negócios com o uso da tecnologia aplicada diretamente ao estabelecimento de um modo diferente de criação, oferta ou captura de valor.
- **organizacional –** requer uma mudança de processos organizacionais ou de criação de novos modelos de negócio. Desse modo, a TD tem por objetivo o redesenho organizacional do negócio pelo uso de tecnologias, trazendo melhores níveis de produtividade, de redução de custos e de desenvolvimento de inovações.
- **social –** influencia todos os aspectos da vida humana. Sob a óptica social, é preciso aceitar como necessidade básica e urgente para os países, fornecer o acesso às

[33] PATEL, K.; MCCARTHY, M. Pat. **The essentials of e-business leadership:** digital transformation. McGraw-Hill: New York, 2000.

> tecnologias a todos, sobretudo, às populações desfavorecidas. Para mais, esse acesso deve ser acompanhado de educação apropriada para gerar oportunidades reais de inclusão e de competitividade que permitam colaborar com o encerramento de uma lacuna que, mais que uma exclusão digital, é social.

Entretanto, torna-se importante enfatizar que perdura uma certa ambiguidade acerca de alguns termos na TD, como as expressões “digitização” e “digitalização”. Há uma diferença significativa entre eles:

> Com efeito, digitalização (*digitization*) significa a conversão de um formato analógico para um formato digital; é a representação da informação com uma linguagem binária (0 e 1). É a representação da informação em qualquer sistema de computador. Por exemplo, podemos digitalizar uma foto com um scanner para armazená-la em um CD. Enquanto digitização (*digitalization*) significa o uso de dados e tecnologia digital para automatizar o manuseio de dados e otimizar processos, é o uso de um sistema de computador para automatizar ou semiautomatizar processos. Deste ponto de vista, informatização é um termo próximo à digitização e às vezes é considerado sinônimo (Mahraz; Benabbou; Berrado, 2019, p. 922, tradução nossa, grifo nosso).

A digitização vem do inglês *digitalization*, referindo-se ao processo de transformar o negócio para o digital, que envolve alterações nos modelos, nos processos e nas estratégias desses negócios, em que empresas podem atuar de forma *online*.

Com isso, uma organização consegue lançar mão de novos processos, sistemas, ferramentas e meios de colaboração, deixando suas atividades mais inteligentes. Um de seus objetivos é auxiliar na redução de custos e de trazer inovação.

É fundamental notar que a digitização não é apenas sobre a transferência de processos físicos para digitais, mas também sobre a transformação de modelos de negócios e de estratégias, eis alguns exemplos:

- Os contratos podem ser criados, geridos e assinados digitalmente, eliminando a necessidade de papel e de caneta, tornando o processo mais eficiente e ecológico.
- Fatura de energia (luz) ou água em papel são digitais. Facilitando o acesso a pagamentos, reduzindo e economizando papéis.
- As agendas analógicas foram substituídas por versões digitais que podem ser acessadas em qualquer dispositivo, o que permite um acessso mais fácil e possibilidades de compartilhamento e de interação com outras pessoas.
- Ferramentas digitais que permitem a organização de atividades de forma mais eficiente, auxilixando o companhamento e a colaboração entre os setores de instituições em tempo real.

- Os canais digitais para facilitar a comunição entre entidades e pessoas.
- A emissão de notas fiscais digitais.
- O armazenamento de dados em plataforma digital entre outro serviços.

Nos seus escritos, Souza (2022) menciona que a digitalização se divide em quatro fases. A primeira fase (pré-1990) é marcada pela experimentação das tecnologias para a geração de dados em formato digital. A segunda (1990 a 2000) pelo surgimento das plataformas digitais de comunicação, as quais reduzem a intermediação nos processos de negócio e, consequentemente, os custos operacionais. A terceira fase (2000 a 2010), o foco esteve na melhoria da eficiência pela exploração de soluções digitais voltadas para otimizar os fluxos de negócio, com destaque para os sistemas de gestão empresarial. E, na última fase, a contemporânea (pós-2010), o fenômeno digital se consolida como perene e disruptivo, em que a conectividade e a integração sistêmica não são mais demandas pontuais, mas sim necessidades básicas e elementares dos processos de trabalho e de negócio. No Quadro 6, apresenta-se a síntese dessas transições.

Quadro 6 – Fases da TD

	Fase 1	Fase 2	Fase 3	Fase 4
Período	Pré-1990	1990–2000	2000–2010	Pós-2010
Fenômeno	Dados digitais	Plataformas digitais de comunicação	Melhoria da eficiência digital	Fenômeno digital consolidado
Foco Principal	Experimentação	Desintermediação	Exploração	Integração
Atividades Dominantes	Tecnologias digitais são exploradas como uma nova forma de trabalhar e de desenvolver negócios	Tecnologias digitais são utilizadas para conectar com os clientes, seja diretamente de uma forma digital de baixo custo ou por meio de plataformas	Tecnologias digitais são usadas para otimizar os fluxos de negócios, principalmente para aumentar a eficiência dos processos de negócios conhecidos	Tecnologias digitais são amplamente difundidas e se tornam um fato aceito nos negócios, em vez de serem especiais ou extraordinárias

Fonte: Souza (2022, p. 6).

Nessa última fase, emerge a digitização como uma especialização da digitalização, buscando a conversão de dados para o formato digital e a sua incorporação aos fluxos e aos processos de trabalho e de negócio, referindo-se à capacidade ou à proficiência necessária para que as organizações gerem e operem dados digitais, criando valor efetivo aos processos de negócio pela transformação de entradas em saídas (Souza, 2022).

Figura 20 – Digitalização x digitalização com digitalização com digitização

Fonte: Souza (2022, p. 7).

Cruz (2023) corrobora que as raízes da TD estão na popularização de tecnologias disruptivas que forçaram empresas e organizações estabelecidas a transformarem seus negócios de modo a permanecerem competitivas no mercado.

Schwab (2016) também complementa essa ideia e diz que esse fenômeno pode provocar, num primeiro momento, efeito destrutivo sobre o emprego quando a tecnologia e a automação substituem trabalhadores, e num segundo momento pode ocorrer um efeito contrário devido à criação de novas profissões, empresas e indústrias. Ainda para o autor, o mais importante é entender em que tempo o segundo momento se sobrepõe sobre o primeiro para iniciar a “prosperidade”.

As visões acerca da TD são as mais diversas. Ainda não se tem todas as suas características e aplicações consolidadas, porém, algumas se destacam no cenário atual, como: as tecnologias inovadoras; o ritmo acelerado da mudança tecnológica; a flexibilidade e soluções individualizadas e a grande diversidade de clientes e de mercados.

Para Nunes e Malagri (2023), as definições da TD vão ao encontro de uma mesma direção, significando o processo de mudança realizado a partir do uso das chamadas tecnologias sociais, móveis, analíticas e tecnologias em nuvem, que afetam pelo menos três dimensões: individual, empresarial e social.

Em outro viés, Paixão *et al.* (2020) dizem que a TD possui uma visão clássica entre autores na literatura, estando imersa na perspectiva do uso das TICs como elemento preponderante na transformação e na reconfiguração de elementos organizacionais, tais são: estratégia, processos, cultura e estruturas. Os autores ainda mencionam, a base de tal fenômeno pode ser vista como um modelo de negócio que incorpora melhorias nas operações, nos produtos, nos serviços e no relacionamento com seus agentes. Assim, a TD seria um desdobramento para os demais setores da estratégia de TI.

Consoante Cruz (2023): no “I Simpósio de Preservação Digital no Tribunal de Justiça do estado de Minas Gerais: desafios e perspectivas", em 2020, o palestrante Dr. Fernando

Zaidan tratou do tema da TD, baseado-a no princípio da digitalização; mas não restrita apenas a isso.

> Afirma ainda que ela se ampara em 4 Ds: desmaterialização, disrupção, democratização das informações e desmonetização. Nesse aspecto, são pilares da transformação digital: pessoas, informações, documentos, processos e tecnologia. Além da digitalização, a palavra da transformação digital no momento, segundo o palestrante, é digitização, que significa transformar os negócios analógicos em negócios digitais. (Cruz, 2023, p. 38-39).

Rogers (2017, p. 12) observa a TD além da aplicação de TI:

> A transformação digital não tem a ver com tecnologia – tem a ver com estratégia e novas maneiras de pensar. Transformar-se para a era digital exige que o negócio atualize sua mentalidade estratégica, muito mais que sua infraestrutura de TI. Essa verdade fica evidente na mudança de papéis do líder de tecnologia nas empresas. A função tradicional do executivo-chefe de informação era usar a tecnologia para otimizar processos, para reduzir riscos e para melhorar a gestão dos negócios existentes. A função emergente do executivo-chefe de atividades digitais é muito mais estratégica, focada no uso da tecnologia para reimaginar e reinventar o core business (negócio principal) em si. A transformação digital exige uma visão holística da estratégia de negócios.

De acordo com o exposto, vê-se que as forças digitais estão reformulando não só o modo de viver em sociedade, mas o de pensar das instituições, sobretudo de como devem operar para serem bem-sucedidas. Assim, Rogers (2017) expõe um *framework* com cinco domínios que devem ser repensados para que a TD possa ocorrer, eis as estratégias: clientes, competição, dados, inovação e valor, que visam descrever o panorama da TD para as empresas de hoje (Figura 21). As empresas que se constituíram antes da Internet precisam conscientizar-se de que muitos de seus pressupostos fundamentais devem ser atualizados.

Figura 21 – cinco domínios da TD

Fonte: Rogers (2017, p. 9).

- **Clientes:** o foco da TD agora é a rede de clientes. É um tipo de modelo que visa explorar a interação entre a empresa e os seus clientes por múltiplas plataformas digitais, como fóruns e redes sociais. Em vez de ver os clientes apenas como alvos de vendas, as empresas precisam reconhecer que os clientes em rede podem ser o melhor grupo de foco, o melhor campeão da marca ou o melhor parceiro de inovação que jamais encontrarão.
- **Competição:** numa perspectiva tradicional, competição e cooperação eram vistas como opostas. Hoje, empresas diferentes ao setor oferecem aos clientes valores competitivos. O resultado dessas mudanças é um grande deslocamento no *lócus* da competição com modelos de negócio muito diferentes, cada uma buscando conquistar mais alavancagem junto ao consumidor. Todos os relacionamentos entre empresas são uma mistura de competição e cooperação, conhecida como "coopetição".
- **Dados:** abrange a forma como as empresas produzem, gerenciam e utilizam a informação. Se anteriormente os dados eram caros, escassos, atualmente, as empresas vivenciam uma baixa de custos. Nesse contexto, as ferramentas da *big data* são de extrema importância, pois habilitam as organizações a lidar com o grande volume de dados de forma a extrair informações estrategicamente relevantes para suas operações. Também criam condições para que as empresas façam novos tipos de previsões, descubram padrões nas atividades de negócios e liberem novas fontes de valor.
- **Inovação:** processo pelo qual novas ideias são desenvolvidas, testadas e lançadas no mercado. A utilização de novas metodologias de trabalho e a aplicação das tecnologias digitais possibilitaram que se acelerasse e se construísse protótipos com baixo custo. Essa nova abordagem à inovação se concentra em experimentos que maximizam o aprendizado ao mesmo tempo em que minimizam os custos. Assim, produtos são desenvolvidos por meio de repetições sucessivas, mediante um processo que economiza tempo, reduz o custo do fracasso e melhora o aprendizado organizacional.
- **Valor:** é quando as tecnologias digitais obrigam as empresas a pensarem de maneira diferente sobre como criar valor para os clientes. A proposta de valor de uma empresa nunca deve ser fixa, mas deve acompanhar a evolução das necessidades do cliente, atentando às mudanças em curso para que possa descobrir a próxima oportunidade de geração de valor e então evoluir.

A inovação pode ser definida como uma série de padrões consistentes que oferece caminhos para que as pessoas olhem para o futuro e prevejam para onde as diferentes tecnologias o levarão (Christensen; Horn; Staker, 2013).

As tecnologias emergentes são aquelas inovadoras em crescimento relativamente acelerado, caracterizadas por persistir no tempo, com potencial de impacto em um contexto sócio-econômico. Também são chamadas assim por ainda não estarem plenamente desenvolvidas e, em geral, nunca estarão totalmente acabadas, porém seu impacto mais importante ocorre no futuro, e, na fase de emergência (Armstrong, 2019).

O autor citado enfatiza que as tecnologias emergentes mais proliferadas são IAs, entidades de inovação com o potencial significativo de disrupção, baseada em três fatores principais: grande volume de dados, aprimoramento dos algoritmos e dos *hardwares*.

A aplicação da IA, considerando o grande volume de dados como um desafio a ser superado permitiu o desenvolvimento do *big data*, resultado do intercâmbio entre tecnologia, metodologia e capacidade de análise, utilizado para pesquisar e cruzar enormes conjuntos de dados, colaborando à aceleração da produção de conhecimento. Seus avanços incluem a melhora da performance organizacional, consequência do aumento da velocidade, inovação e tomada de decisão; tudo suportado pela automação de processos, envolvimento de colaboradores e consumidores em momentos de ideação e obtenção de conhecimento via dados.

As inovações sustentadas, por sua vez, auxiliam organizações a criarem melhores produtos e serviços que frequentemente podem ser vendidos com maiores lucros. Servem aos consumidores de acordo com a definição original, isto é, de acordo com o que o mercado historicamente definiu como “bom” (Christensen; Horn; Staker, 2013).

> Algumas das inovações que melhoram a performance dos produtos são incrementais, e outras são evoluções dramáticas. Porém, chamamos ambas de inovações sustentadas contanto que o propósito dessas inovações incrementais ou dramáticas seja o mesmo — ajudar as empresas a sustentarem seu movimento ascendente, ao longo da trajetória de melhoria de desempenho, para fazerem produtos melhores que possam ser vendidos com maior lucratividade a seus melhores clientes. [...]. As empresas que lideram seus setores na ponta esquerda da linha, antes das batalhas da inovação sustentada começarem, são quase invariavelmente as mesmas que continuam na liderança após o fim dessas batalhas. Não importa o quão tecnologicamente difíceis são essas inovações. Se seu propósito é ajudar as empresas deste setor a fazerem melhores produtos para serem vendidos com maiores lucros para seus melhores clientes, elas invariavelmente encontram uma maneira de fazê-lo (Christensen; Horn; Staker, 2013, p. 9-10).

As inovações sustentadas são vitais para um setor considerado robusto e eficiente, uma vez que as organizações se esforçam para fazer e oferecer melhores produtos e serviços, afastando a ideia uma inovação “ruim”, quando relacionada às tecnologias disruptivas (Christensen; Horn; Staker, 2013).

> As inovações disruptivas, por sua vez, não procuram trazer produtos melhores para clientes existentes em mercados estabelecidos. Em vez disso, elas oferecem uma nova definição do que é bom — assumindo normalmente a forma de produtos mais simples, mais convenientes e mais baratos que atraem clientes novos ou menos exigentes. Com o tempo, elas se aperfeiçoam o suficiente para que possam atender às necessidades de clientes mais exigentes, transformando um setor (Christensen; Horn; Staker, 2013, p. 2).

Flores (2022) argumenta que a disrupção tecnológica não é de todo boa, ao contrário, ela pode ser ruim ao sistema, até porque o mercado lança um novo produto, mas não está baseado em um estudo, ele está baseado em quebrar o *status quo* ao não considerar os referenciais, ao não fazer aquilo a que estão tão acostumados com a Ciência, que seria, analisar, coletar, investigar, fazer uma revisão da literatura; já a inovação sustentada é a mais estruturada.

As inovações disruptivas são marcadas por dois atributos, o da velocidade e o da capacidade transformativa. Quanto mais rápido uma tecnologia prolifera e o quanto a mais de valor gera ao transformar padrões existentes, mais disruptiva é (Armstrong, 2019). Segundo esse autor, o primeiro teórico substancial da disrupção de negócios foi o economista austriaco Joseph Schumpeter. Ele não usou o termo em si, mas escreveu acerca de um fenômeno denominado “destruição criativa” como um elemento do processo de inovação, em que “destrói velhos setores e sistemas econômicos”, que acontece inerentemente ao capitalismo como parte integrante e inevitável de sua própria natureza.

Contudo, Clayton Christensen foi quem lançou a primeira teoria de como ocorria a disrupção. Sua teoria da tecnologia disruptiva (depois renomeada de inovação disruptiva) lançou-se em um artigo de 1995 e num livro subsequente: “O dilema da inovação” (Christensen, 2011).

> A teoria da inovação disruptiva emergiu originalmente de um estudo sobre a indústria de discos para explicar por que as empresas líderes do setor não foram capazes de se manter na liderança de uma geração para a outra. A teoria explica a história de centenas de indústrias e setores onde as organizações recém-chegadas substituíram as empresas ou instituições dominantes. Estes exemplos vão de produtos a serviços, de organizações lucrativas a não-lucrativas, e de mercados de mudança lenta a veloz (Christensen; Horn; Staker, 2013, p. 8).

Entretanto, é importante enfatizar que a teoria de Christensen baseou-se em exemplos extraídos de decisões de compra de empresas e não de consumidores em si dos anos 1990, ou seja, as tecnologias eram vendidas em grande parte a empresas e não consumidores. Mas isso tem explicação – as motivações dos clientes eram impulsionadas por: preço, acessibilidade e desempenho dos produtos. Então, por suas origens em setores de vendas a empresas, a teoria de Christensen explica vários casos de disrupção e ignora outros.

O pensamento de Christensen (2011) dissemina que os desafiantes disruptivos podem expurgar titulares convencionais há muito tempo estabelecidos. Como isso acontece: o disruptor sempre começa vendendo para compradores em um novo mercado, ou seja, aos compradores fora do mercado dos clientes que são atendidos pelo titular convencional. Esse disruptor de "novo mercado" oferece um produto inovador; "inferior" ao tradicional quanto ao desempenho e aos atributos, porém, mais barato e acessível para quem não tem condições de adquirir as ofertas do titular convencional.

Dessa forma, o titular convencional ignora o padrão inferior do desafiante disruptivo, porquanto seus próprios clientes não se interessariam pela nova oferta, e continuam a melhorar o desempenho dos seus produtos de preço mais alto. O desempenho da inovação do desafiante melhora aos poucos, continuando muito mais barato e muito mais acessível.

Numa conjuntura crítica, a nova tecnologia torna-se boa o bastante para ser uma alternativa viável para os próprios clientes do titular convencional, que passam a migrar rapidamente para a alternativa mais barata e mais acessível. Destarte, o titular convencional, que se manteve atrelado ao seu velho produto e ao seu modelo de negócios antigo, constata ser quase impossível competir dessa forma. Sendo assim, há o rápido declínio como uma consequência inevitável. É uma teoria poderosa, que explica excepcionalmente bem as situações de inúmeros setores – computadores, discos rígidos, escavadeiras mecânicas, usinas siderúrgicas, corretoras de ações, prensas de impressão, e muitas outras.

Numa situação que ficou mundialmente conhecida, quando Christensen foi entrevistado sobre o *iPhone* da *Apple*, ele previu que tal produto não geraria disrupção nos fabricantes tradicionais do ramo de telefonia móvel, e não ensejaria sucessos em relação aos celulares da *Nokia*. Após esse acontecido, Christensen mencionou que o produtor tinha sido um disruptor, contudo, o titular convencional que havia sofrido disrupção era o setor de computador.

A teoria da disrupção de Armstrong (2019) não tem a intenção de substituir a de Christensen, mas a ampliar para explicar as novas dinâmicas da disrupção hodierna, impulsionada pelos comportamentos de compra dos consumidores. Essa disrupção é oriunda dos clientes centrais do titular convencional (não dos novos mercados) e induzida pelo valor, não pelo preço, nem pelo acesso. Esse pensamento é baseado em um modelo de negócios como previsão da disrupção de negócios, que é consequência do choque de modelos assimétricos. Tal modelo descreve uma visão totalizante que cria valor, entrega-o ao mercado e em troca captura mais valor.

Um modelo de negócios detalhado pode abranger vários componentes: segmentos de

clientes, propostas de valor, canais, relacionamentos com clientes, fluxos de receitas, de recursos e de atividades e estrutura de custos. Christensen (2011) o define com base em quatro partes: proposta de valor para os clientes, fórmula de lucro, inclusive modelo de receita, estrutura de custos, modelo de margem e velocidade dos recursos, recursos principais e processos principais.

Armstrong (2019) divide seu modelo de negócios em dois lados: a proposta de valor e a rede de valor. O primeiro se caracteriza pelo valor que a empresa oferece ao cliente e o segundo pelas pessoas, parceiros, ativos e processos que capacitam o negócio a criar, a entregar e a captar valor. Neste, incluem-se fatores como canais, preços, estrutura de custos, recursos e segmentos de clientes em que se concentra o negócio. Esses dois diferenciais servem para desestruturar um negócio tradicional.

Uma dicotomia na proposta de valor é deslocar o valor fornecido pelo titular convencional, pelo menos, para alguns clientes. Tal diferença pode decorrer de muitas fontes possíveis, denominada geratriz, que incluem aos disruptores digitais:

- preço mais baixo;
- gratuidade ou oferta "*freemium* (*free* + *premium*)" – as ofertas gratuitas estimulam muito mais tentativas dos clientes do que o preço baixo;
- acesso (a capacidade de acessar o conteúdo ou os serviços a distância);
- simplicidade – visando eliminar o atrito dos processos de vendas, das tomadas de decisões e das compras, para desfrutar um produto muito mais simples e fácil;
- personalização – aos clientes que preferem ter mais opções para escolher um produto ou serviço que atenda às suas necessidades específicas;
- agregação – muitos modelos de negócios de plataforma adicionam valor, agregando muitos vendedores a serem escolhidos pelos clientes;
- desempacotamento – muitas inovações digitais envolvem o desatamento de pacotes tradicionais – grupos de produtos, serviços ou atributos que até então eram oferecidos em pacotes fechados;
- integração (ou reempacotamento) – na direção oposta, os negócios podem gerar um novo valor para os clientes empacotando serviços até então vendidos separadamente. O valor real da integração ocorre quando as várias partes trabalham juntas, de maneira integrada e ininterrupta, como não era possível quando eram partes separadas. Por exemplo, pense em como seus contatos, mapas, agenda, *e-mail*, chamadas telefônicas e textos trabalham juntos e interagem em um

smartphone.);

- social – que é a capacidade de compartilhar a experiência de um produto ou serviço com outras pessoas.

A diferença na rede de valor ergue uma barreira capaz de impedir a imitação pelo titular convencional. Disrupção de negócios ocorre quando o disruptor satisfaz essas duas condições – e para armstrong (2019), só nesse caso. O termo "rede de valor" surgiu na década de 1990 para fornecer um modelo de criação de valor menos atomístico, menos manufatureiro e menos confinado dentro de uma empresa do que o modelo das cadeias de valor. Assim, todo disruptor também necessita de uma diferença na rede de valor que impeça a imitação pelo titular convencional. Os principais elementos a considerar na análise da rede de valor incluem:

- clientes – o desafiante pode perseguir segmentos ou tipos de clientes diferentes daqueles atualmente servidos pelo titular convencional;
- canais – distribuição no varejo ou *online*, entrega direta aos clientes, ou distribuição por meio de intermediários;
- parceiros – são os parceiros de vendas, de fabricação, de cadeia de fornecimento etc., essenciais para a oferta do desafiante;
- redes – rede de clientes ou parceiros que são os consumidores, os anunciantes, os desenvolvedores de aplicativos etc.;
- produtos ou serviços complementares – fornecimento aos clientes de produtos ou de serviços essenciais para o valor decorrente de sua nova oferta, por exemplo, o serviço de música *iTunes* da *Apple*, antecessor do iPhone, que foi adicionado ao valor do produto mais recente;
- marca – reputação, imagem e relacionamento anterior com o cliente podem ser essenciais para a capacidade do desafiante de fornecer o valor da oferta e cobrar o preço certo por ela;
- modelo de receita – abrange o preço, a margem de lucro e o tipo de pagamento. É quando o cliente paga pelo produto, pelo uso, pela assinatura mensal e pela participação na receita, etc.;
- estrutura de custos – abrange os custos fixos e variáveis incorridos pelo desafiante para entregar a oferta ao cliente.
- competências e processos – o desafiante pode ter processos únicos ou diferenciados e competências organizacionais essenciais para o valor que fornece;

- ativos físicos – são as fábricas, os equipamentos, as lojas etc.;
- ativos de PI –incluem propriedades intelectuais, como patentes, direitos, licenças e tecnologias exclusivas.
- ativos de dados – a proposta de valor do desafiante talvez dependa de ativos e capacidades de dados exclusivos, como o uso pela *Amazon* e pelo *Google* de seus dados de clientes para entregar todos os tipos de ofertas personalizadas.

Depois que os indivíduos se passam a encarar qualquer modelo de negócios em termos desses dois lados – a proposta de valor e a rede de valor – encontram-se aptos a aplicá-lo em nova teoria sobre como acontece a disrupção (Armstrong, 2029). Laconicamente, as tecnologias disruptivas podem ser uma resposta alternativa para a criatividade e para a criação de novas coisas. Existem, por exemplo, três maneiras de criar alguma coisa, neste sentido: copiar o que se quer, combinar coisas diferentes, ou mudar alguma coisa para torná-la o que se quer, ou seja, tudo é um *remix* de combinar ou editar materiais existentes.

Isto posto, Flores (2022) corrobora que as inovações disruptivas e sustentadas são tipos básicos da TD direcionadas aos arquivos e à Arquivologia, pois são fenômenos que vêm ocorrendo de forma compulsória, sem a devida consideração da área de negócio; sem um diagnóstico prévio que avalia a condição do Arquivo e acorde as características dessa entidade custodiadora.

Alguns cenários de disrupção acometem a Arquivologia, Flores (2022) cita pelo menos quatro:

1. A própria digitalização (processo de conversão do analógico para o digital) como princípio da TD para os documentos de arquivo vem sendo operacionalizado, muitas vezes, sem considerar os referenciais arquivísticos.
2. A custódia digital dos documentos de arquivo não tem sido mais dos Arquivos. E quem vem tutelando tais registros, salvo exceções, são os setores de TI, inclusive passando a ideia equivocada para os gestores de que os Arquivos estariam incumbidos exclusivamente da custódia e da emanação de políticas somente de documentos analógicos, ou mesmo de que os documentos estariam desmaterializados com os ambientes digitais.
3. Os documentos de arquivo digitais em sistemas de informação digital não estão sendo desenhados nem implementados obedecendo aos requisitos arquivísticos dos modelos de requisitos para a gestão de documentos, colocando em risco a autenticidade, e a preservação que afetam a segurança jurídica da sociedade como um todo.

4. Como uma tecnologia disruptiva, a *blockchain* poderia ter uma aplicação necessária e segura aos arquivos, mas que, ao ter uma adoção sem preservação digital sistêmica, constata-se que ele não preserva o objeto digital, mas sim, preserva os *ledgers* de autenticação, que poderia ter sido uma adoção de inovação sustentada.

Tais considerações levam à reflexão de cenários futuros para os arquivos, atentando para o desenvolvimento de estudos substanciais no que tange à temática que envolvam à confiabilidade dos documentos, sobretudo, atrelados a normas, a políticas, a padrões, a modelos e a requisitos, seja no campo da preservação ou no da segurança da informação frente à TD.

A recomendação de Flores (2022) é que tanto para os arquivos como para a Arquivologia, as TDs ocorram por inovação sustentada; sendo interessante uma disrupção tecnológica, desde que seja fruto de um diagnóstico prévio da instituição. Contudo, caso essa disrupção aconteça, que seja em cenários mais estáveis, como os analógicos, resistentes à transformação, ou muito distantes de possíveis transformações dos modelos de negócio. Logo, à sociedade tanto faz o tipo de tecnologia usada para o gerenciamento dos documentos, o importante é estarem seguramente acessíveis.

6.3 TRANSFORMAÇÃO DIGITAL NO BRASIL A PARTIR DA ÓPTICA GOVERNAMENTAL

O desenvolvimento da TD no setor público brasileiro teve realce em meados dos anos de 1950 (Souza; Nunes, 2021), a *posteriori* da Segunda Guerra Mundial; contudo, esse processo aconteceu de forma tímida quando comparado aos países que detinham maiores incentivos em tecnologias, como na Europa e nos EUA.

A partir de 1980, a lógica da inserção da informatização no Brasil se desencadeou, seguindo o movimento de reforma administrativa, resultante da crise fiscal e do enfraquecimento de um modelo de gestão deveras burocrático; e, por consequência, surgiram os primeiros serviços eletrônicos pela administração pública.

Como política de governo, a incorporação das TICs ocorreu na década 1990, de maneira gradual e em âmbito nacional. Viana (2021) corrobora que foi a disseminação do comércio eletrônico que impulsionou o desenvolvimento da concepção do Governo Eletrônico (e-Gov) brasileiro, referindo-se ao uso das tecnologias. Assim, a administração pública nacional, desde a reforma administrativa, passou a empregar as tecnologias

eletrônicas como forma de consolidação do e-Gov, principalmente, na promoção e na ampliação de acesso à informação (Reck; Hübner, 2021).

O e-Gov surgiu como uma iniciativa instaurada no Programa da Sociedade da Informação de dezembro de 1999, com o propósito de criar um modelo para as atividades relacionadas à TI. Entretanto, sua implementação apenas aconteceu no ano de 2000, por intermédio de um grupo de representantes interministerial do governo federal, que teve como proposta analisar as metas para os anos seguintes, regulamentada em Decreto ainda no ano de 2000[34].

Dessa forma, o e-Gov adveio das perspectivas da "Revolução Digital" e serviu para melhorar a qualidade no serviço público em relação a inovações, principalmente após a popularização da Internet, no sentido de melhorar o relacionamento do governo com os cidadãos sem que fosse necessária a presença física deles (Ministério…, 2023a).

Para Viana (2021), a definição do e-Gov possui um sentido mais restrito, que reside no uso das TICs pelos governos e, um sentido mais amplo, servindo para: a) garantir acesso e entrega por parte do governo aos indivíduos de informações e de uso de serviços; b) possibilitar e implementar eficiência mediante a aplicação desses serviços no âmbito do governo; c) cobrir larga escala de serviços; d) transformar governos; e) compreender o uso das TICs para melhorar a eficiência das agências governamentais e fornecer serviços *online*.

Além dos muitos benefícios, o e-Gov também trouxe algumas problemáticas ordenadas pela divisão e pela exclusão digital, que continua a representar um elemento limitador para a expansão da *Internet*, vigorando até o atual momento. Partindo desse pressuposto, ações surgiram para suprir tais necessidades e uma delas se deu pelo Grupo de Trabalho em Tecnologia da Informação (GTTI), formalizadas pela Portaria da Casa Civil n.º 23, de 12 de maio de 2000, e incorporadas às metas do Programa Sociedade da Informação, coordenado pelo Ministério da Ciência e Tecnologia, concentrando-se em três linhas: a universalização de serviços; o governo ao alcance de todos; e a infraestrutura avançada (Ministério…, 2023a).

Em seu plano político, o e-Gov seguiu um conjunto de diretrizes que atuava numa modalidade triangular: junto ao cidadão; na melhoria da gestão interna; e na integração com parceiros e fornecedores. Buscou-se, neste sentido, compreender a definição de padrões, a de normatização, a de articulação da integração de serviços eletrônicos, a de disponibilização de boas práticas, a de criação e construção de super infraestrutura tecnológica entre outras

[34] Disponível em: Base Legislação da Presidência da República - Decreto de 03 de abril de 2000 (presidencia.gov.br).

(Ministério…, 2023a).

Para além do Programa Sociedade da Informação, outras ações também auxiliaram o e-Gov, sendo assim, algumas normativas foram promulgadas, como, por exemplo, a Medida Provisória nº. 2.200-2, de 24 de agosto de 2001, que criou a ICP-Brasil (Infraestrutura de Chaves Públicas)[35], para o desenvolvimento de um modelo que possibilitou o uso de assinaturas eletrônicas, a certificação digital e a validade legal dos documentos que tramitam por meio eletrônico, diretriz fundamental para a Arquivologia no que tange à preservação e à segurança digital da informação; e o Decreto n°. 3.697, de 21 de dezembro de 2000, revogado pelo Decreto nº. 10.024, de 20 de setembro de 2019,[36] que regulamenta o pregão eletrônico no âmbito da administração federal (Cruz, 2023; Ministério…, 2023a).

Em 2008, a Estratégia Geral de Tecnologia da Informação (EGTI) modificou as atividades da administração pública brasileira. Tal documento objetivou estabelecer as bases para a transição entre a situação de gestão dos ambientes de informática do Executivo federal e elencou um conjunto de metas de melhorias e de princípios norteadores na temática. O trabalho para elaboração desta estratégia teve como fundamento o Acórdão 1603 do Tribunal de Contas da União (TCU) (Cruz, 2023). O e-Gov passou a existir com a institucionalização do Comitê Executivo de Governo Eletrônico (Cege), no ano 2000, em território nacional.

Um fator importante a destacar é que, no ano de 2014, uma parceria com a Universidade Federal da Paraíba (UFPB) foi firmada por intermédio de seu Centro de Informática do Núcleo de Pesquisa e Extensão do Laboratório de Aplicações de Vídeo Digital (Lavid), para o desenvolvimento da Suite VLibras, que é um conjunto de ferramentas computacionais de código aberto e de domínio público, responsável por traduzir automaticamente conteúdos digitais (texto, áudio e vídeo) em Língua Brasileira de Sinais (Libras), tornando computadores, dispositivos móveis e plataformas *Web* acessíveis para pessoas surdas (Ministério…, 2023a, 2023).

No ano seguinte, em 2015, o e-Gov mudou de conceito, ficando conhecido por "Governo Digital", cujo fito é o de tornar mais simples, acessível e eficiente a oferta de serviços aos cidadãos pelas tecnologias digitais. Em janeiro de 2016, a publicação do Decreto nº. 8.638 instituiu a Política de Governança Digital para o Executivo federal e atribuiu ao Ministério do Planejamento, à época, a responsabilidade pela elaboração da Estratégia de Governança Digital da administração pública nessa mesma instância. Logo, sua versão pioneira foi promulgada em março de 2016, e revisada em maio de 2018, abordando três eixos

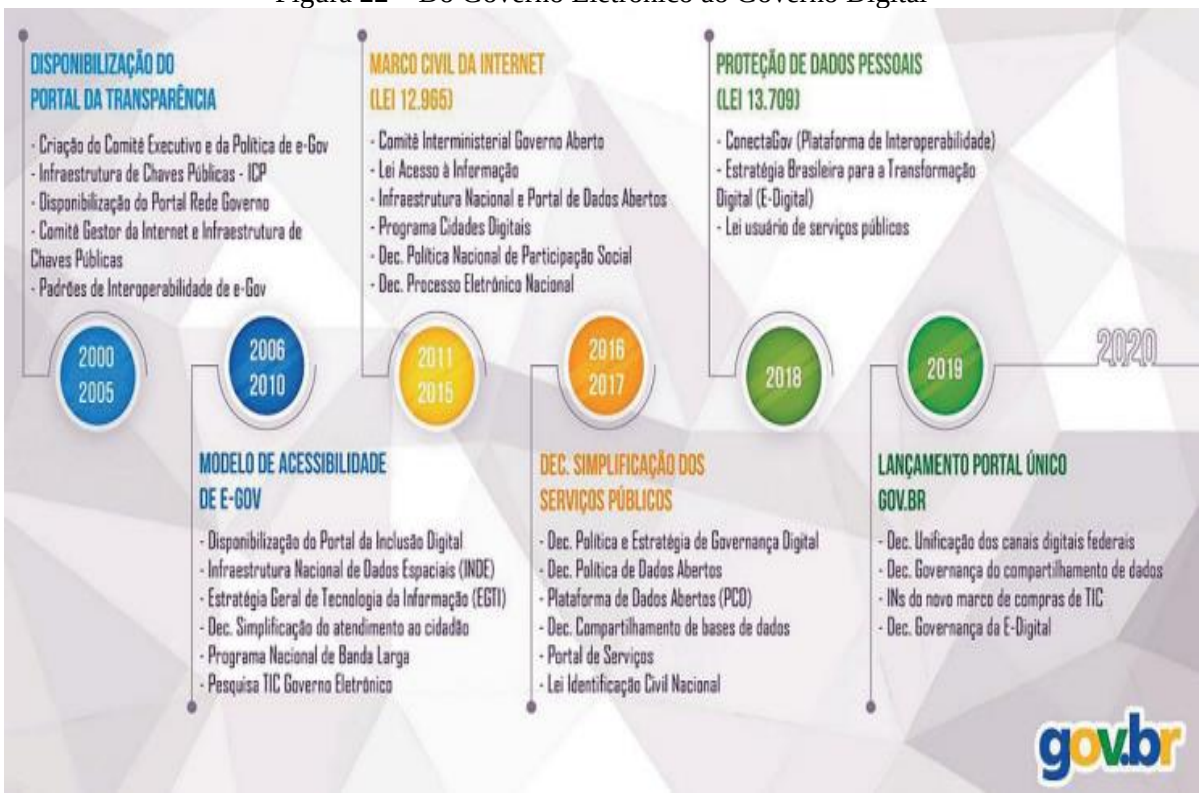
[35] Disponível em: 2200-2 (planalto.gov.br).
[36] Disponível em: D10024 (planalto.gov.br).

estratégicos: acesso à informação, prestação de serviços e a participação social.

A Figura 22 expõe a linha do tempo das ações do governo eletrônico para o digital.

Na versão atual – a Estratégia de Governo Digital (EGD) 2020-2023 (anteriormente chamada de Estratégia de Governança Digital) – foi instituída pelo Decreto nº. 10.332 de 28 de abril de 2020[37], com prazo de prorrogação até o ano de 2023 pelo Decreto nº. 11.260 de 2022[38] (Cruz, 2023).

Figura 22 – Do Governo Eletrônico ao Governo Digital



Fonte: Souza e Nunes (2021, p. 20).

De acordo com o primeiro Decreto citado no parágrafo acima, os instrumentos de planejamento para alcançar os objetivos estabelecidos pela EGD 2020-2023 devem ser elaborados pelas unidades competentes dos órgãos e entidades e aprovados pelo Comitê de Governança Digital. Estes instrumentos são:

> I – Plano de Transformação Digital, que conterá, no mínimo, as ações de:
> a) transformação digital de serviços;
> b) unificação de canais digitais;
> c) interoperabilidade de sistemas; e
> d) segurança e privacidade;
> II – Plano Diretor de Tecnologia da Informação e Comunicação; e
> III – Plano de Dados Abertos. (Cruz, 2023, p. 92).

[37] Disponível em: D10332 (planalto.gov.br).
[38] Disponível em: D11260 (planalto.gov.br).

Os objetivos da EGD 2020-2023 visam, então: oferecer serviços públicos digitais simples e intuitivos, consolidados em plataforma única e com avaliação de satisfação disponível; conceder acesso amplo à informação e aos dados abertos governamentais, para possibilitar o exercício da cidadania e a inovação em tecnologias digitais; promover a integração e a interoperabilidade das bases de dados governamentais; promover políticas públicas baseadas em dados e evidências e em serviços preditivos e personalizados, com utilização de tecnologias emergentes; implementar a Lei Geral de Proteção de Dados (LGPD), no âmbito do governo federal, e garantir a segurança das plataformas Governo Digital; disponibilizar a identificação digital ao cidadão; adotar tecnologia de processos e serviços governamentais em nuvem como parte da estrutura tecnológica dos serviços e setores da administração pública federal; otimizar as infraestruturas de TICs; e formar equipes de governo com competências digitais (Cruz, 2023).

Ainda não existe um documento que materialize a Estratégia de Governo Digital 2020-2023, ou pelo menos, ainda não está disponível na *Internet* para baixar. Todo seu escopo está registrado no *site*[39] do Governo Digital, o qual dispõe de um guia para auxiliar a TD de estados e municípios, com dez passos a serem seguidos (Figura 23).

Figura 23 – 10 passos para a TD

Fonte: Trilha 10 Passos — Governo Digital (www.gov.br).

[39] Disponível em: Estratégia de Governo Digital 2020-2022 — Governo Digital (www.gov.br).

A trilha dos dez passos à TD é uma orientação para todo o território nacional com a intenção de abarcar os estados e os municípios. É verdade que ainda não há um registro documental formal sobre semelhante estratégia até o momento deste escrito. Porém, ao clicar nos ícones desses dez passos, abre-se uma outra página *Web* com instruções que vão desde a formação de pessoal a parcerias, contemplando uma lista de atividades a serem cumpridas (Cruz, 2023). É um guia para ser trabalhado em treinamentos e disseminado em todo o âmbito brasileiro.

A EGD 2020-2023 está organizada em princípios, objetivos e iniciativas norteadoras para a TD. Busca-se com ela oferecer políticas públicas e serviços de melhor qualidade, mais simples, acessíveis a qualquer hora e lugar, a um custo menor para o cidadão. Nessa ideia, até o presente momento, a EGD organiza-se em 6 diretrizes/princípios (Figura 24).

Figura 24 – Seis diretrizes da EGD 2020-2023

Fonte: Estratégia de Governo Digital 2020-2022 — Governo Digital (www.gov.br).

Ainda não existe um documento para *download* centralizando as seis diretrizes mencionadas. Para acessar cada rótulo desses princípios, necessita-se clicar em cada um separadamente e uma página *Web* se abrirá com as devidas informações, resumidas abaixo.

- No governo **centrado no cidadão**, a preocupação é oferecer uma jornada mais amigável, por meio de serviços de alta qualidade (simples, ágeis e personalizados) à experiência do usuário;
- No governo **integrado**, o atendimento ao cidadão é resultado da experiência integrada nos dados e nos serviços da união, dos estados, do Distrito Federal e dos municípios, reduzindo custos, ampliando a oferta de serviços digitais, retirando do

cidadão os ônus do deslocamento e da apresentação de documentos. A interoperabilidade é uma analogia a essa ideia.

> Em 2019, por meio do Decreto nº 10.046, instituímos o primeiro cadastro de referência de informações, o Cadastro Base do Cidadão, disponibilizando para os órgãos uma fonte de consulta confiável para os dados cadastrais fundamentais e a identificação para o atendimento, desonerando a sociedade de fornecimento redundante de informações a cada interação.
> Um bom exemplo do impacto deste tipo de integração é a emissão do passaporte, simplificado a partir do intercâmbio eletrônico de informações de quitações eleitoral e militar, dispensando a apresentação de documentos físicos com informações que o próprio governo já possui. A iniciativa resultou em uma redução de 4 minutos no atendimento da emissão, para os mais de 3 milhões de atendimentos realizados anualmente. Outro exemplo é a concessão do benefício Passe Livre Federal, que oferece transporte interestadual gratuito para pessoas com deficiência. A partir da integração entre os sistemas, os mais de 2,5 milhões de cidadãos com deficiência que já recebem o Benefício de Prestação Continuada (BPC) não precisam apresentar novamente ao governo sua situação de renda e a comprovação de deficiência para ter direito ao passe livre, pois essas informações já foram concedidas anteriormente (Ministério…, 2023b, p. 1).

- No governo **inteligente**, a implementação de políticas se dá com base em dados e evidências e tem a intenção de solucionar as necessidades dos cidadãos e das organizações à tomada de decisões.
- No governo **confiável** figura o respeito da liberdade e da privacidade dos cidadãos, assegurando a resposta adequada aos riscos, às ameaças e aos desafios que surgem com o uso das tecnologias digitais no Estado. Assim, suas plataformas devem se adequar à LGPD, como detentor, não dono, dos dados do cidadão. Além disso, torna-se imprescindível a implementação de controles de segurança cibernética.
- Um governo **transparente e aberto** viabiliza o acompanhamento e a participação da sociedade nas diversas etapas dos serviços e das políticas públicas. Um exemplo disso são os portais de transparências.
- Um governo **eficiente** promove a capacitação de seus profissionais nas melhores práticas de aplicação das plataformas tecnológicas. Otimiza a infraestrutura e os contratos de tecnologia, buscando a redução de custos na oferta de serviços. Como consequência disso, o Programa Capacita[40] busca ampliar a oferta de cursos em algumas áreas: Ciência de Dados, Liderança e Inovação, Segurança e Privacidade e Serviços Digitais voltados ao cidadão.

[40] Disponível em: Enap - Escola Nacional de Administração Pública - Home.

Figura 25 – Indicadores da EGD 2020-2023

Fonte: Indicadores da Estratégia de Governo Digital — Governo Digital (www.gov.br).

Em relação ao cumprimento dessas iniciativas pelo governo federal, tem-se uma amostra dos indicadores em que foram instituídas 59 iniciativas com seus respectivos objetivos a serem cumpridos em cada um dos seus princípios (Figura 25). Todas essas iniciativas foram iniciadas e, dentre elas, 46 foram concluídas e 13 estão em execução. Para o detalhamento de todas as iniciativas, acessar o *link* na fonte da Figura 25.

O governo federal chegou ao final da EGD (2016-2019) com 53% dos serviços disponíveis na versão digital, um recorde diante dos cenários anteriores (Ministério…, 2023c). Já em 2023, o Brasil liderou o *ranking* na América Latina, ocupando 49ª posição no Índice Global de Inovação (IGI)[41], avançando cinco posições, comparado ao ano anterior. Os dados foram divulgados pela Confederação Nacional da Indústria (CNI), em parceria com a Organização Mundial da Propriedade Intelectual (OMPI) (Agência gov, 2023).

Tais informações foram reveladas no 10º Congresso Internacional de Inovação da Indústria, em São Paulo. Assim, o Brasil ultrapassou o Chile, que ocupa a 52ª posição, e o México, na 58ª posição, passando a ser o país com melhor desempenho não só na América Latina, mas no Caribe também, depois de 12 anos fora do recorte das 50 economias mais bem classificadas no IGI (Agência gov, 2023).

Entre os cinco países do Brics, o Brasil está na 3ª colocação, à frente da Rússia, em 51º lugar, e da África do Sul, em 59º lugar. A China é a 12ª colocada e a Índia ocupa o 40º lugar (Agência gov, 2023).

Em relação ao ano de 2022, o Brasil subiu cinco posições, onde figurava o 54º lugar.

[41] Anualmente divulgado desde 2007, o IGI é uma referência à avaliação do avanço da inovação em 132 países. É resultado de um cálculo que divide os indicadores em “insumos de inovação” e “resultados de inovação”. Os insumos se referem às condições e aos elementos disponíveis para apoiar atividades de inovação. A melhor posição do Brasil na lista foi mostrada no ano 2011, com 47ª colocação (Agência gov, 2023, p. 1).

Mas antes disso, o país passou 12 anos fora do grupo das 50 economias mais bem classificadas no IGI. Para exibir mais dados, o país tem pontuações altas nos indicadores de serviços governamentais *online* (14ª posição no mundo) e participação eletrônica (11ª). Atualmente, os dez melhores países do IGI[42] são: Suíça, Suécia, EUA, Reino Unido, Singapura, Finlândia, Holanda, Alemanha, Dinamarca e Coreia do Sul (Uol, 2023).

Mesmo com a projeção do Brasil em 2023 para a ocupação da 10ª maior economia do mundo, sua posição no tange ao IGI é considerada de baixo potencial. Divulgada anualmente, desde 2007, a classificação do IGI é feita pela OMPI em parceria com o *Portulans Institute* e como o apoio de outros parceiros internacionais (Brasil, 2023b).

Outro dado importante é a posição do Brasil em relação aos indicadores da *Internet*. A quantidade de usuários, em 2023, chegou a 5,16 bilhões, número que representa 64,4% da população mundial (com um total de 8,07 bilhões de pessoas). Desse total, 4,76 bilhões têm acesso a redes sociais, ou seja, quase 60% das pessoas no mundo (Souza, 2023).

Concernente ao melhor acesso à *Internet*, o país fica 39ª posição, com 19 a cada 100 pessoas tendo conexão banda larga. E, no que tange "ao país que mais usa a *Internet* por dia", é o 2º colocado. Além também, de se posicionar em 2º lugar no maior tempo de uso, com 9h32min, registrando seu uso por 81% da população (Oliveira, 2023). Em primeiro lugar, vem a África do Sul no *ranking* mundial, onde as pessoas passam 9h38min por dia utilizando a *Internet*. Somente 72% dos sul-africanos a utilizam, índice menor que no Brasil. E somente três em cada 100 pessoas têm conexão banda larga (Oliveira, 2023).

A proporção de brasileiro em 2023 conectados cresceu de 70% em 2019 para 84,3% em 2023, totalizando a marca de 181,3 milhões de internautas. Desde o ano de 2019, o número de brasileiros conectados aumentou 16,6%. A representação disso é o acréscimo de 32,2 milhões de pessoas na *Web*. A maior adoção digital entre a população brasileira tem impactos no consumo de redes sociais e no *e-commerce*. O maior acesso à *Internet* é nas redes sociais e em 2023 esse número chegou a 152,4 milhões (70,6% dos brasileiros) (Oliveira, 2023).

Tais indicadores mostram como está sendo a evolução das partes que compõem a TD no Brasil e globalmente. Vê-se que, para o Brasil, muito se tem o que fazer, sobretudo quando comparado às grandes potências digitais. Em agosto de 2023, foram realizadas seis oficinas temáticas para debater os objetivos da nova EGD, com validade para 2024-2027.

[42]Para dados mais detalhados do IGI 2023 acessar: Índice Global de Inovação 2023: Suíça, Suécia e Estados Unidos lideram a classificação mundial de inovação; inovação mantém-se robusta, mas financiamento para startups é cada vez mais incerto (wipo.int).

Representantes de diversos órgãos federais participaram dos encontros organizados pelo Ministério da Gestão e da Inovação em Serviços Públicos (MGI) em parceria com a Escola Nacional de Administração Pública (Enap). As oficinas debateram temas como governo integrado, confiável e centrado no cidadão, com a finalidade de atender às necessidades da população, pretendendo realizar uma consulta pública para colher contribuições de toda a população brasileira (Ministério…, 2023d).

A nova EGD terá validade para os mais de 200 órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), porém, pouquíssimas informações até o momento foram divulgadas.

6.3.1 A Estratégia Brasileira para a Transformação Digital

Conforme o registro no *site* do governo federal, o primeiro passo para o estabelecimento da estratégia de TD foi identificar o universo de serviços oferecidos.

> Por meio de um Censo de Serviços realizado em 2017, foram identificados, inicialmente, cerca de 2,8 mil serviços prestados à sociedade pela administração direta, indireta e instituições federais de ensino. Nesse processo, foi definido um conceito unificado de serviço público, englobando as atividades do governo prestadas diretamente a usuários, por meio de uma transação individualizada. [...]. À época do Censo, cerca de um terço dos serviços eram totalmente digitais. Atualmente, 90% dos 4,7 mil serviços oferecidos já são (Ministério…, 2023e, p. 1).

Para mais, o governo federal construiu cinco ferramentas (passou a oferecê-las sem custos aos órgão e às entidades da administração pública federal) que passaram a compor a Plataforma de Cidadania Digital, cujo objetivo é ampliar e simplificar o acesso dos cidadãos brasileiros aos serviços públicos digitais, inclusive, por meio de dispositivos móveis (Ministério…, 2023e).

Em 2018, a meta era transformar 100 serviços para testar a eficácia dessa metodologia, e obteve um resultado exitoso, em que os “donos de serviço” (as áreas de negócio que eram responsáveis diretamente pela prestação dos serviços) foram se engajando e o ano terminou com 109 serviços transformados digitalmente (Ministério…, 2023e).

No início de 2019, o governo estabeleceu a meta de transformar 1000 serviços em dois anos. Para isso, houve uma mudança na estratégia, em vez de negociações individuais com cada dono de serviço, apostou-se em mobilizar cada órgão e entidade da administração pública federal, a fim de criar um plano de TD com todos os serviços de um determinado setor de governo (Ministério…, 2023e).

Figura 26 – Ferramentas da TD

Fonte: Plataformas e Ferramentas — Governo Digital (www.gov.br).

Assim, surgiram os planos de TD, com duração de dois anos e o objetivo de coordenar essas ações. Para acelerar ainda mais o processo foi incluída nos planos a oferta complementar das ferramentas da Plataforma de Cidadania Digital (Figura 26).

A Estratégia Brasileira para a Transformação Digital (E-Digital), estabelecida pelo Decreto nº. 9.319, de 21 de março de 2018, é uma iniciativa do governo federal que instituiu o Sistema Nacional para a Transformação Digital (SinDigital) (Cruz, 2023) e contou com participação do grupo de trabalho interministerial em um conjunto de mais de 30 entidades da administração pública (Estratégia…, 2018).

O resultado desse documento refletiu o amplo engajamento do setor produtivo, da comunidade científica e acadêmica e da sociedade civil, sobretudo, por meio de participação nos seminários e nos *workshops* durante o processo de formulação da Estratégia (Estratégia…, 2018).

> Um grupo de trabalho envolvendo diversos órgãos do governo, em colaboração com representações setoriais e com a sociedade civil, traçou diagnósticos e visões de futuro, propondo iniciativas concatenadas com visão estratégica.
> Um enfoque importante para E-Digital é a contextualização das ações estratégicas nas grandes agendas internacionais para o desenvolvimento. Entre elas, destaca-se os Objetivos de Desenvolvimento Sustentável da Agenda 2030 das Nações Unidas (Estratégia…, 2018, p. 6).

Tais ações tiveram foco no papel do governo como habilitador e facilitador da TD no país, na capacitação da sociedade para essa nova realidade, e na atuação do Estado como prestador de serviços e garantidor de direitos.

O documento da E-Digital traz a conclusão de uma jornada iniciada a partir da recomendação do Conselho de Desenvolvimento Econômico Social Sustentável (CDESS), órgão colegiado viabilizador do diálogo entre o governo e a sociedade, estando organizada em dois eixos – o da Economia Digital e o do Governo Digital – e apresenta com detalhes 100 ações de curto e de médio prazo para que o Brasil tenha celeridade na sua TD (Ministério…,

2023a).

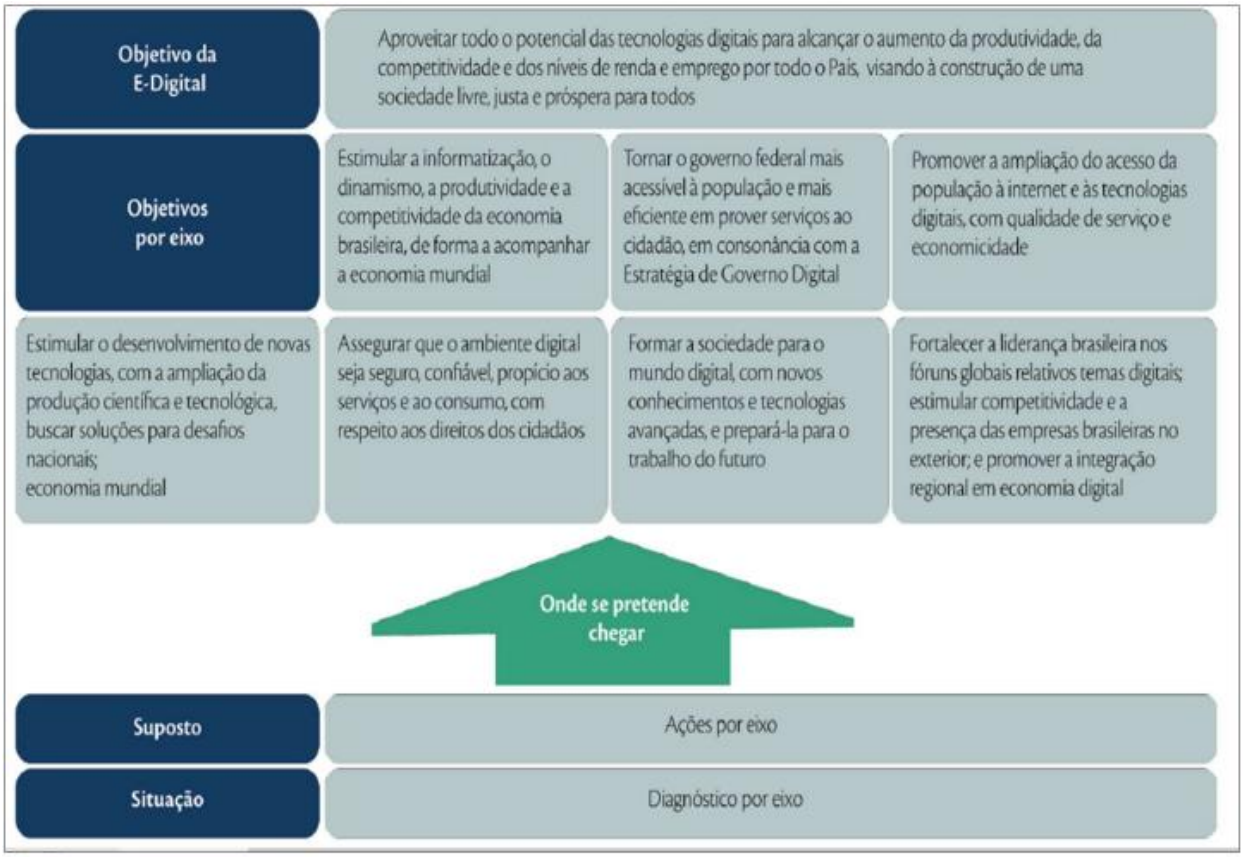
Dessa forma, a EGD passou a ser um documento complementar da E-Digital, com o detalhamento das iniciativas, dos objetivos e das metas da TD do governo, que são:

- ampliar os serviços digitais e alcançar a disponibilização de pelo menos 2 mil diferentes serviços de governo no Portal de Serviços;
- implementar a dispensa de certidões e de documentos para serviços públicos digitais que já constem nas bases de dados do governo;
- implementar um sistema de autenticação única ao cidadão, agregando os principais níveis de segurança em uma só ferramenta;
- consolidar as Plataformas de Governo Digital do governo federal; e,
- aprimorar uma plataforma digital de participação social, como espaço privilegiado para o diálogo entre a administração pública federal e a sociedade civil. (Ministério…, 2023a).

O ciclo de 2022-2023 do E-Digital traz ações que deverão ser implantadas até 2026, conforme a Figura 27, utilizando-se do potencial das tecnologias digitais para o desenvolvimento econômico social sustentável com

inovação e aumento da competitividade, da produtividade e dos níveis de emprego e renda, conforme descreve a apresentação deste documento do governo federal do Brasil (Cruz, 2023).

Figura 27 – Modelo lógico da E-Digital



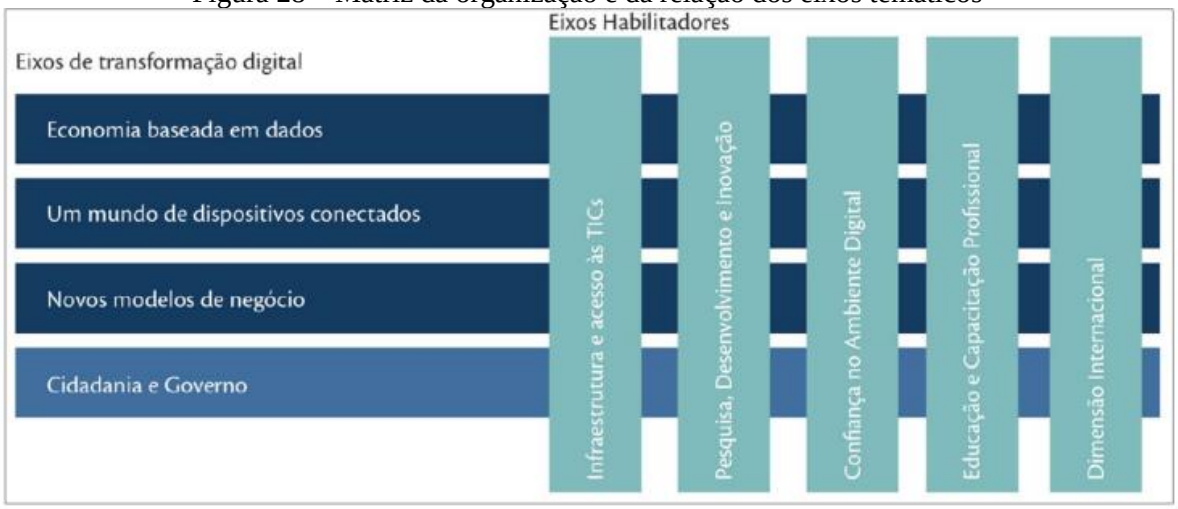
Fonte: Cruz (2023, p. 95) adaptado da E-Digital 2022-2026.

O ciclo da E-Digital 2022-2026[43] preconizou algumas recomendações como: a atualização da Lei de Informática, o lançamento da Estratégia Brasileira de Inteligência Artificial, a implantação da Autoridade Nacional de Proteção de Dados (ANPD), o lançamento do pagamento instantâneo brasileiro (*Pix*), a realização do leilão do 5G e a unificação de serviços governamentais na plataforma gov.br.

A E-Digital é baseada em dois grandes eixos temáticos: os habilitadores de TD (Figura 28).

[43] Disponível em: e-digital_ciclo_2022-2026.pdf (www.gov.br).

Figura 28 – Matriz da organização e da relação dos eixos temáticos



Fonte: Estratégia… (2022, p. 12).

Os eixos habilitadores vão formar as bases para que a TD ocorra, tendo cada um desses eixos, objetivo geral e específico definidos pelo Decreto nº. 9.319, de 21 de março de 2018, a saber:

a) A Infraestrutura e acesso às TIC.
b) Pesquisa, Desenvolvimento e Inovação.
c) Confiança no ambiente digital.
d) Educação e capacitação profissional; e
e) Dimensão internacional. (Estratégia…, 2022).

Os eixos de TD envolvem as estratégias para transformar digitalmente as atividades do governo e da economia, a partir das bases desenvolvidas nos eixos habilitadores. Compõem esse eixos: a TD da economia e a Cidadania e TD do governo.

Cruz (2023) aponta que as ações envolvendo os objetivos deste último eixo traz o conhecimento técnico-científico da Arquivologia com soluções que podem ser aplicadas para atingimento de suas metas possibilitando a gestão, a preservação, o acesso e a difusão de dados, informações e documentos produzidos e recebidos no desempenho das atividades públicas oferecidas por seus serviços, e, como exemplo, cita os Sigads e os RDC-Arqs, pois são amparados por normas e requisitos internacionalmente difundidos e aplicados em grandes estruturas organizacionais governamentais e privadas.

Figura 29 – Eixos da Transformação Digital

Eixos de Transformação Digital	Objetivo geral (Decreto nº 9319/2018)	Objetivos específicos (Decreto nº 9319/2018) (BRASIL, 2018a)
F1. Transformação digital da economia: economia baseada em dados	Estimular a informatização, o dinamismo, a produtividade e a competitividade da economia brasileira, de forma a acompanhar a economia mundial.	• Promover a criação de forte ecossistema para desenvolvimento da economia de dados, com incentivos ao desenvolvimento de infraestrutura de telecomunicações e à atração de *data centers* ao País;
		• Aprimorar capacidades técnicas e humanas relativas ao uso e tratamento de grandes volumes de dados;
		• Promover um ambiente jurídico-regulatório que estimule investimentos e inovação, a fim de conferir segurança aos dados tratados e adequada proteção aos dados pessoais;
F2. Transformação digital da economia: um mundo de dispositivos conectados		• Apoiar a formação e a capacitação profissional em habilidades necessárias para o desenvolvimento e a utilização das novas tecnologias digitais relacionadas aos dispositivos conectados;
		• Promover o desenvolvimento de soluções tecnológicas nas áreas prioritárias de saúde, agropecuária, indústria e cidades inteligentes;
		• Fomentar o ambiente normativo e de negócios que promova a atração de novos investimentos em dispositivos conectados, a fim de assegurar a confiança e a preservação de direitos dos usuários.
F3. Transformação digital da economia: novos modelos de negócio		• Reforçar a atuação de empresas brasileiras no ambiente de negócios digital;
		Estimular e apoiar empresas nascentes de base tecnológica;
		• Desenvolver ambientes regulatórios flexíveis para experimentação de modelos de negócios inovadores.
G. Cidadania e transformação digital do governo	Tornar o governo federal mais acessível à população e mais eficiente no provimento de serviços ao cidadão, em consonância com a Estratégia de Governo Digital.	• Oferecer serviços públicos digitais simples e intuitivos, consolidados em plataforma única e com avaliação de satisfação disponível;
		• Conceder acesso amplo à informação e aos dados abertos governamentais, para possibilitar o exercício da cidadania e a inovação em tecnologias digitais;
		• Promover a integração e a interoperabilidade das bases de dados governamentais;
		• Promover políticas públicas baseadas em dados e evidências e em serviços preditivos e personalizados, com utilização de tecnologias emergentes;
		• Implementar a Lei Geral de Proteção de Dados no âmbito do governo federal e garantir a segurança das plataformas de governo digital;
		• Disponibilizar a identificação digital ao cidadão;
		• Adotar tecnologia de processos e serviços governamentais em nuvem como parte da estrutura tecnológica dos serviços e setores da administração pública federal;
		• Otimizar as infraestruturas de Tecnologia da Informação e Comunicação; e
		• Formar equipes de governo com competências digitais.

Fonte: Estratégia… (2022, p. 11).

O governo federal brasileiro, no ano de 2021, exibiu algumas novidades para aproximar ainda mais o cidadão da esfera pública. Assim, foi criado o Programa *Startup* Gov.br[44] com o objetivo de digitalizar os serviços públicos, priorizando a alocação de profissionais de TICs em projetos estratégicos de alto impacto para a população (Ministério…, 2023a).

[44] Disponível em: Startup gov.br — Governo Digital (www.gov.br).

Também ocorreu o lançamento da plataforma SOUGOV.BR[45], um serviço de aplicativo digital de gestão de pessoas para servidores federais civis ativos, aposentados, pensionistas e anistiados políticos do poder Executivo Federal. E também, em 29 de março de 2021, a Lei do Governo Digital nº. 14.123[46], que dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública, principalmente, por meio da desburocratização, da inovação, da TD e da participação do cidadão. Essa Lei é aplicada aos órgãos da administração pública direta federal dos três poderes, incluído o TCU e o Ministério Público da União; as entidades da administração pública indireta federal, incluídas as empresas públicas e as sociedades de economia mista, suas subsidiárias e controladas, que prestem serviço público, autarquias e fundações públicas; e as administrações diretas e indiretas dos demais entes federados (Brasil, 2021).

Quadro 7 – Princípios e diretrizes da Lei nº. 14.129/2021

I - a desburocratização, a modernização, o fortalecimento e a simplificação da relação do poder público com a sociedade, mediante serviços digitais, acessíveis inclusive por dispositivos móveis;
II - a disponibilização em plataforma única do acesso às informações e aos serviços públicos, [...] quando indispensável, da prestação de caráter presencial;
III - a possibilidade aos cidadãos, às pessoas jurídicas e aos outros entes públicos de demandar e de acessar serviços públicos por meio digital, sem necessidade de solicitação presencial;
IV - a transparência na execução dos serviços públicos e o monitoramento da qualidade desses serviços;
V - o incentivo à participação social no controle e na fiscalização da administração pública; [...]
VIII - o uso da tecnologia para otimizar processos de trabalho da administração pública; [...] X - a simplificação dos procedimentos de solicitação, oferta e acompanhamento dos serviços públicos, com foco na universalização do acesso e no autosserviço;
XI - a eliminação de formalidades e de exigências cujo custo econômico ou social seja superior ao risco envolvido;
XII - a imposição imediata e de uma única vez ao interessado das exigências necessárias à prestação dos serviços públicos, justificada exigência posterior apenas em caso de dúvida superveniente;
XIII - a vedação de exigência de prova de fato já comprovado pela apresentação de documento ou de informação válida;
XIV - a interoperabilidade de sistemas e a promoção de dados abertos;
XV - a presunção de boa-fé do usuário dos serviços públicos;
XVI - a permanência da possibilidade de atendimento presencial, de acordo com as características, a relevância e o público-alvo do serviço;
XVII - a proteção de dados pessoais, nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);
XVIII - o cumprimento de compromissos e de padrões de qualidade divulgados na Carta de Serviços ao Usuário; [...]
XXI - o apoio técnico aos entes federados para implantação e adoção de estratégias que visem à transformação digital da administração pública;
XXII - o estímulo ao uso das assinaturas eletrônicas nas interações e nas comunicações entre órgãos públicos e entre estes e os cidadãos;
XXIII - a implantação do governo como plataforma e a promoção do uso de dados, preferencialmente anonimizados, por pessoas físicas e jurídicas de diferentes setores da sociedade, resguardado o disposto nos arts. 7º e 11 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), com vistas, especialmente, à formulação de políticas públicas, de pesquisas científicas, de geração de negócios e de controle social;
XXIV - o tratamento adequado a idosos, nos termos da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso);
XXV - a adoção preferencial, no uso da internet e de suas aplicações, de tecnologias, de padrões e de formatos abertos e livres, conforme disposto no inciso V do caput do art. 24 e no art. 25 da Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet); e
XXVI - a promoção do desenvolvimento tecnológico e da inovação no setor público.

Fonte: Cruz (2023, p. 100) adaptado da Lei nº. 14.129/2021.

[45] Disponível em: SOUGOV.BR — Portal do Servidor (www.gov.br).
[46] Disponível em: L14129 (planalto.gov.br)

A Lei n.º 14.129/2021 também foi uma forma de concretização da EGD 2020-2022, pois se desenvolveu na observância dos princípios e dos objetivos dessa Estratégia, possibilitando uma universalização ainda maior e o fomento a interação entre a administração pública e o cidadão-usuário de serviços públicos digitais (Reck; Hübner, 2021). Os princípios e as diretrizes da Lei do Governo Digital compõem o Quadro 7.

Laconicamente, o Governo Digital não é uma iniciativa que se restringe ao processo de automação ou apenas de digitização ou digitalização dos serviços públicos, mas intenta aproximar os cidadãos por meio das tecnologias, que é papel essencial do Estado, promovendo eficácia e eficiência em sua comunicação.

Na Região Nordeste, especificamente no estado da Paraíba, os marcos sobre a TD iniciaram-se em 1993 com a implantação do Sistema Integrado de Contabilidade (Estratégia 2021/2026…, 2021). Mais recentemente, no ano de 2012, por meio do Decreto nº 33.050/2012[47], foi implantado o Sistema de Informação ao Cidadão. Em 2017, a criação do Portal da Cidadania trouxe serviços relacionados à mobilidade, à segurança pública, ao governo, à cultura, ao esporte, à saúde, ao meio ambiente, à ouvidoria, à utilidade pública, às guias de pagamento, ao turismo, aos concursos, entre outros. Seu diferencial é a participação digital da população no orçamento democrático estadual, bastando ao cidadão, cadastrar-se e votar nas prioridades de cada região. Com isso, mesmo que o cidadão não possa estar presente em audiências, ele passa a votar digitalmente (Estratégia 2021-2026…, 2021).

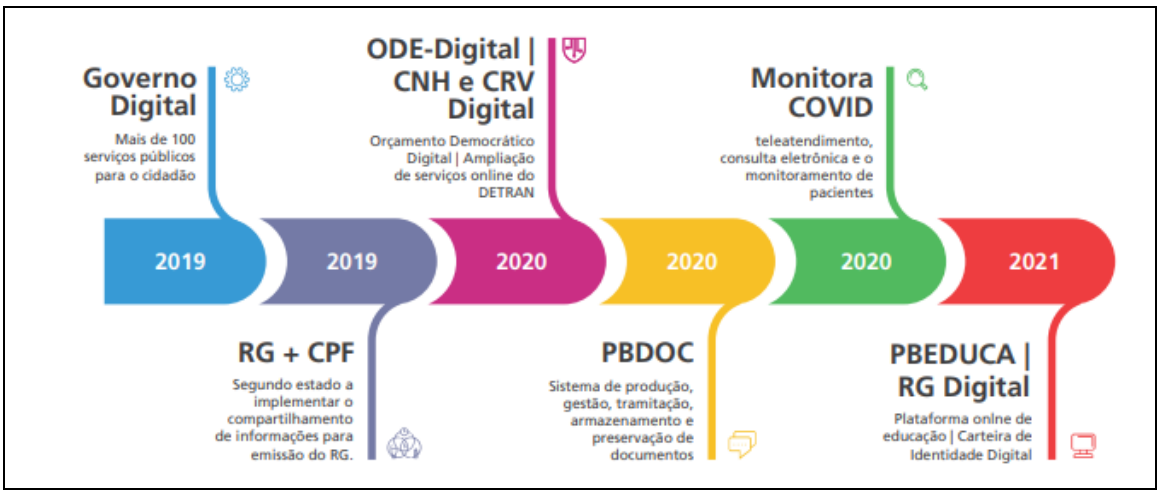
No ano de 2018, houve a implantação do Sistema da Ouvidoria Geral do Estado (Soge) para o registro de solicitações de denúncia, reclamação, sugestão e elogio. Porém, o Programa do Governo Digital do Poder Executivo da Paraíba só foi lançado em 2019, agrupando mais de 100 serviços públicos. Desenvolveu-se também um *chatbot*, chamado Tia Maria, para atendimentos automatizados ao cidadão sobre a prestação dos serviços digitais (Estratégia 2021-2026…, 2021). Outro marco fundamental foi o Comitê Gestor de Governança (CGG), instituído pelo decreto n.º. 39.271, em 2019.

Um ano após, foi lançado o Monitora Covid – teleatendimento. Ainda em 2020, no mês de setembro, o Governo da Paraíba passou a substituir a produção e a tramitação de documentos em papel para o formato digital, conforme o Decreto n.º 40.546, com a instituição do sistema informatizado PBdoc, de produção, de gestão, de tramitação, de armazenamento, de preservação, de segurança e de acesso a documentos, cujo objetivo é trabalhar nos fluxos de processos eletrônicos com segurança e transparência, observadas as disposições da Lei

[47] Disponível em: dec_33_050_regul_lei_12527_internet.pdf (ouvidoria.pb.gov.br).

Federal nº 12.527, de 18 de novembro de 2011[48]. A Figura 30 demonstra alguns dos marcos recentes sobre a TD no estado.

Figura 30 – marcos mais recentes da TD na Paraíba



Fonte: Estratégia 2021/2026…(2021, p. 6).

Em 20 de agosto de 2021, basilada pelo Decreto n.º 41.507[49], a Paraíba instituiu a EGD para o período de 2021 a 2026, no âmbito dos órgãos e das entidades da administração direta, autárquica e fundacional do Poder Executivo estadual.

Outro meio de disseminação da TD deu-se por eventos, como o I e II Seminário de Transformação Digital, em 2021 e 2022, ambos discutindo ações voltadas à educação, ciência e tecnologia. E pelos Simpósios de Governo Digital subsidiados pela Secretaria de Estado da Administração (SEAD), tendo como foco os servidores do estado que estão diretamente ligados à TD, suas diretrizes e estratégias governamentais. As duas edições enfatizaram temas como a Carta de Serviços e TD; o Portal do Governo Digital; o Emprego Público, ocorrido nos anos de 2022 e de 2023.

6.3.2 O Programa Justiça 4.0

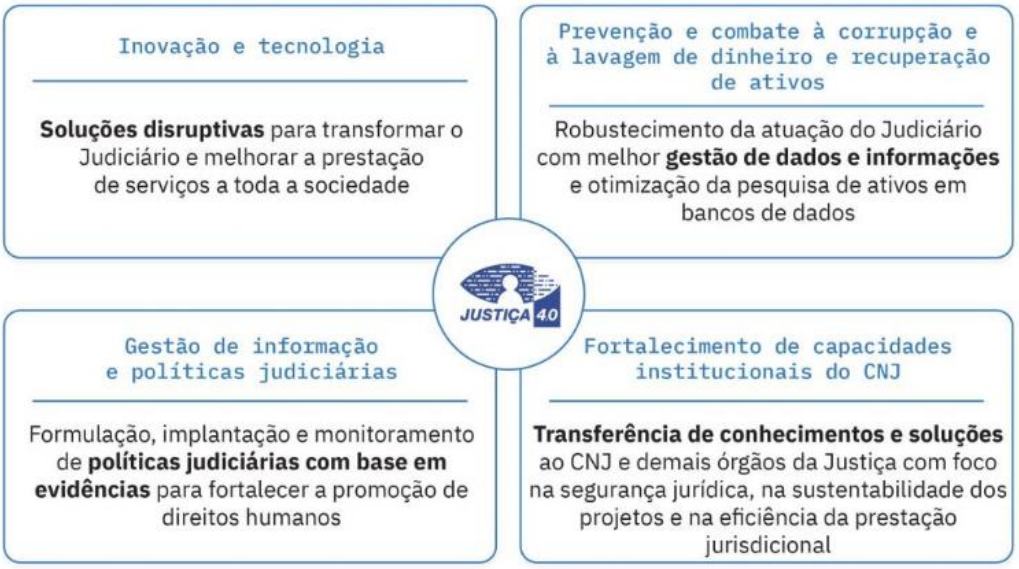
Fora do âmbito do Executivo federal, o Poder Judiciário institui o processo de TD basilada no **Programa Justiça 4.0 – Inovação e Efetividade na Justiça para Todos**, que é exclusivamente voltado ao ambiente digital para efetivar a aproximação do cidadão à Justiça, reduzindo despesas processuais e estruturais, por intermédio da disponibilização de soluções digitais colaborativas que automatizam as atividades dos Tribunais, do trabalho dos

[48] Disponível em: L12527 (planalto.gov.br).
[49] Disponível em: Decreto 41507 2021 de Paraíba PB (leisestaduais.com.br).

magistrados, dos servidores e dos advogados.

O Programa atua em quatro eixos (Figura 31) e foi desenvolvido em parceria entre o Conselho Nacional de Justiça (CNJ), o Programa das Nações Unidas para o Desenvolvimento (PNUD) e o Conselho da Justiça Federal (CJF), com apoio do Tribunal Superior Eleitoral (TSE), Superior Tribunal de Justiça (STJ) e Conselho Superior da Justiça do Trabalho (CSJT).

Figura 31 – Quatro eixos da do Programa Justiça 4.0



Fonte: Justiça 4.0 - Portal CNJ.

Esse movimento nacional se firmou, sobretudo, pela pandemia da Covid-19, permitindo que a Justiça prestasse seus serviços de forma eficiente, célere, econômica e acessível aos cidadãos. Compete ao CNJ, no Brasil, o controle da atuação administrativa e financeira, cabendo elaborar relatório anual, propondo as providências que julgar necessárias, sobre a situação do Poder Judiciário do país, conforme o art. 103-B, § 4º, VII, Constituição Federal (BRASIL, 1988).

Em 10 de setembro de 2020, ao tomar posse no cargo de Presidente do Supremo Tribunal Federal (STF) e do CNJ, o ministro Luiz Fux apresentou cinco eixos[50] de atuação da sua gestão 2020-2022:

1) proteção dos direitos humanos e do meio ambiente;

2) garantia da segurança jurídica no que tange à otimização do ambiente de negócios no Brasil;

3) combate à corrupção, ao crime organizado e à lavagem de dinheiro, com recuperação de ativos;

[50] Disponível em: 5-Eixos-da-Justiça-Ministro-Luiz-Fux-22.09.2020.pdf (cnj.jus.br)

4) incentivo ao acesso à justiça digital;

5) fortalecimento da vocação constitucional do STF. (Jobim; Galvão, 2022).

Tais compromissos foram assumidos pelos Objetivos de Desenvolvimento Sustentável (ODS) da Agenda 2030 da Organização das Nações Unidas (ONU)[51] e a concretização do Eixo 4 deu-se com o Programa Justiça 4.0, que visa também desenvolver políticas judiciais nacionais para uso colaborativo de produtos, empregando novas tecnologias e IA, como: a Base Nacional de Dados do Poder Judiciário (DataJud), a Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br), o Juízo 100%, o Balcão Virtual, os Núcleos da Justiça 4.0, a Plataforma Nacional de Armazenamento, Treinamento Supervisionado, Controle de Versionamento, Distribuição e Auditoria dos Modelos de Inteligência Artificial (Sinapses), a Plataforma nacional Codex e outras iniciativas.

A DataJud[52] foi instituída pela Resolução do CNJ n.º 331/2020 e alterada pela Resolução nº. 437, de 28 de outubro de 2021[53], como fonte primária de dados do Sistema de Estatística do Poder Judiciário (Siespj), a qual é responsável pelo armazenamento centralizado dos dados e dos metadados processuais relativos a todos os processos físicos ou digitais, públicos ou sigilosos dos Tribunais indicados nos incisos II a VII do art. 92 da CF (Justiça 4.0, 2021).

Com o lançamento da PDPJ-Br, em 10 de agosto de 2021, os Tribunais passaram a contar com novas ferramentas de encaminhamento de informações para o DataJud, que, instituída pela Resolução CNJ n.º 335 de 2020[54], tem como objetivo incentivar o desenvolvimento colaborativo entre os Tribunais, preservando os sistemas públicos em produção, mas consolidando a política para a gestão e a expansão do Processo Judicial Eletrônico (PJe), que deixa de ser impositiva, salvo para os Tribunais que utilizam soluções privadas (Justiça 4.0, 2021; Longuini; Denardi, 2021)

Os sistemas judiciais de processo eletrônico vão se conectar à PDPJ-Br a fim de consumir soluções tecnológicas oferecidas como microsserviços. Estes são desenvolvidos pelos Tribunais e pelos órgãos parceiros de forma colaborativa e descentralizada, disponibilizados em um *marketplace* e acessíveis na nuvem. Em médio e longo prazos, leva à uniformidade pretendida, mas não alcançada com o PJe. O funcionamento desse modelo

[51] A Agenda 2030 da ONU é um Plano de ação global, adotado em 2015 por 193 Estados-Membros, reunindo 17 ODS´s, os quais trazem 169 metas, criadas para erradicar a pobreza e promover vida digna para todos, observando as condições que nosso planeta oferece, sem comprometer a qualidade de vida das próximas gerações (Costa, 2021; Silva; Moraes, 2022).
[52] Disponível em: DATAJUD - Portal CNJ.
[53] Disponível em; atos.cnj.jus.br/atos/detalhar/3428.
[54] Disponível em: atos.cnj.jus.br/atos/detalhar/3496.

depende de dois fatores: agregação dos Tribunais e governança. (Justiça 4.0, 2021).

No Juízo 100% Digital (instituído pela Resolução 345/2020 do CNJ[55]), o cidadão utiliza a tecnologia digital para ter acesso à Justiça sem precisar comparecer fisicamente aos fóruns. Todos atos processuais, audiências e sessões de julgamento, são praticados exclusivamente por meio eletrônico e remoto, com videoconferência. Acontece que, nessa ação, os Tribunais devem manter uma ferramenta de videoconferência durante todo seu expediente, permitindo aos advogados e às partes serem atendidos de forma remota, como se estivessem em balcões presenciais. Dessa forma, toda vara e secretaria de órgão judicial deve possuir seu balcão virtual em funcionamento e intermediar o atendimento pelo juiz, caso solicitado (Juízo 100% Digital…, 2020).

Assim, no Balcão Virtual, firmado pela Resolução do CNJ n.º 372 de 2021[56], o usuário do Judiciário tem acesso direto ao atendimento realizado pela secretaria processual do CNJ, sendo possível obter informações sobre os processos em trâmite no sistema PJe remotamente. Como consequência disso, os Tribunais precisam disponibilizar em seus *sites* uma ferramenta de videoconferência que permita o imediato contato com o setor de atendimento de cada unidade judiciária, popularmente denominado como "balcão", durante o horário de atendimento ao público (Conselho…, [202-]).

Os Núcleos de Justiça 4.0 foram projetados para funcionar como unidades judiciárias autônomas, desvinculadas por completo daquelas já existentes, contando com juízes especialmente designados para atuarem em tais órgãos (Rodrigues; Watkins, 2022).

Esses Núcleos são unidades especializadas, com competência sobre toda a extensão territorial que adotam o modelo de processamento de demandas inerente aos Juízos 100% digitais (Rodrigues; Watkins, 2022). A iniciativa que integra o Programa Justiça 4.0 foi formalizada pela Resolução n.º 385/2021 do CNJ[57]. Dessa maneira, cada Núcleo deve contar com pelo menos três juízes, entre os quais um seja o coordenador da unidade (Rodrigues; Watkins, 2022).

Ao menos uma vez por ano, os Tribunais devem avaliar a quantidade de processos distribuídos para magistradas(os) e também o volume de trabalho das equipes. O objetivo é mensurar a necessidade de transformação de unidades físicas em Núcleos, com eventual readequação da sua estrutura de funcionamento ou de alteração da abrangência de área de atuação. O problema afeta principalmente as unidades de comarcas do interior, onde são raras

[55] Disponível em: atos.cnj.jus.br/atos/detalhar/3512.
[56] Disponível em: atos.cnj.jus.br/atos/detalhar/3742.
[57] Disponível em: atos.cnj.jus.br/atos/detalhar/3843.

as varas especializadas e o juiz é responsável por processos judiciais que envolvem diferentes matérias – família, recuperação, falência, crime, saúde, empresarial (Conselho…, 2021a).

Outra ação a destacar é a Plataforma Sinapses[58], aprovada pela Resolução do CNJ nº. 332/2020, que escala o uso de IA, facilitando o compartilhamento de projetos deste segmento no Judiciário. Atualmente, a Plataforma integra as ações do Programa Justiça 4.0, fruto da cooperação técnica entre CNJ, PNUD e o CJF. Assim, a gestão e a responsabilidade pelos modelos e *datasets* cabem a cada um dos órgãos do Poder Judiciário, por meio de seu corpo técnico e usuários colaboradores da Plataforma. O departamento de TI do CNJ é responsável por prover a manutenção da Sinapses.

A Plataforma nacional Codex[59], desenvolvida pelo Tribunal de Justiça de Rondônia (TJRO) em parceria com o CNJ, consolida as bases de dados processuais, provendo o conteúdo textual de documentos e de dados estruturados. Funciona como um *data lake* (repositório de grande capacidade) de informações processuais, que pode ser consumido pelas mais diversas aplicações: a produção de painéis e de relatórios de inteligência de negócios (*business intelligence*); a implementação de pesquisas inteligentes e unificadas; a alimentação automatizada de dados estatísticos; e o fornecimento de dados à criação de modelos de IA (Justiça 4.0, 2021).

O Tribunal de Justiça da Paraíba (TJPB) também aderiu ao Programa Justiça 4.0, sobretudo, aos Núcleos da Justiça 4.0. Há três aplicações destes Núcleos – dois já foram criados e um terceiro está sendo implantado. O primeiro é o Núcleo de Saúde Pública Estadual que atua nas ações no tocante à saúde pública; o segundo, Núcleo de Justiça 4.0 para Crimes de Motivação Político-Partidária, e o terceiro, Núcleo de Análises de Custas Finais (Pacífico, 2023).

Além do Juízo 100% Digital e o Balcão Virtual, o TJPB também implantou o Codex-Sinapse, que já está funcionando no 1º e 2º graus no Judiciário estadual. Foi desenvolvida a IA "Sebastiana", para o 1º grau e está em fase de implementação para o 2º grau (Pacífico, 2023).

Já existem algumas afirmativas sobre a **Justiça 5.0**, sobretudo, advindas das publicações científicas e de incipientes notícias do próprio CNJ. No artigo intitulado "Plataforma digital do Poder Judiciário e acesso à Justiça 5.0: o futuro do Processo Eletrônico Judicial", os autores destacam que a Justiça e o Acesso 5.0 são termos convergidos, representados pela importância da união de esforços para se chegar à Justiça ao alcance de

[58] Disponível em: Plataforma Sinapses / Inteligência Artificial - Portal CNJ.
[59] Disponível em: Plataforma Codex - Portal CNJ.

todos, conforme a efetividade do Programa Justiça 4.0 (Pinho; Monteiro, 2022). Para os autores, a análise da preparação ao Acesso 5.0 observou a mesma estrutura das três ações que sintetizam os objetivos da PDPJ-Br: unificar, desenvolver e inovar.

A ideia de acesso à Justiça 5.0 tem prerrogativa na Sociedade 5.0, que vinda do Japão, caracteriza-se num programa de políticas nos anos de 2016-2021, tendo por objetivo a resolução de desafios humanos por meio das máquinas ao seu favor, tomando como protagonista da inovação e da revolução tecnológica a pessoa humana (EngineBR, 2018). Ou seja, enquanto a justiça é valor-fim, a dignidade da pessoa humana é valor-fonte, o princípio irradiante dos demais princípios (Pinho; Monteiro, 2022).

Na Sociedade 5.0, a desigualdade social e o uso desenfreado dos recursos naturais teriam uma resposta com forte carga axiológica, como o investimento em qualidade de vida, a inclusão e a sustentabilidade (EngineBR, 2018), o que remete, no plano constitucional, aos objetivos fundamentais da República Federativa do Brasil (art. 3º) e, no plano institucional, aos objetivos das ODS da Agenda da ONU de 2030 (Pinho; Monteiro, 2022).

A transposição dessas ideias ao Acesso à Justiça 5.0 implica a convergência de todos os recursos tecnológicos à disposição dos cidadãos e ao objetivo da efetividade e da excelência na prestação jurisdicional como parte da realização de valores, como, por exemplo, a qualidade de vida, com a qual se pode fazer uma correspondência com o bem-estar; a inclusão, que permita o acesso à Justiça para todos; e a sustentabilidade, que pode ser apropriada na racionalidade do uso dos recursos humanos e materiais proposta pela PDPJ-Br (Pinho Monteiro, 2022).

Entende-se que a Justiça 5.0 e suas possíveis ações estão em construção, mas um fato existe, para a sua efetiva existência, o Programa da Justiça 4.0 precisa estar bem desenvolvido e implementado.

A adoção de RDC-Arqs pelos Tribunais brasileiros encontra-se determinada na Resolução n.º 324 de 2020 do CNJ[60], que institui diretrizes e normas de Gestão de Memória e de Gestão Documental e dispõe sobre o Programa Nacional de Gestão Documental e Memória do Poder Judiciário (Proname), considerando as seguintes prerrogativas:

[60] Disponível em: atos.cnj.jus.br/atos/detalhar/3376.

> **Art. 34.** Para fins de preservação digital, os órgãos do Poder Judiciário adotarão repositório arquivístico digital confiável (RDC-Arq), desenvolvido como software livre, gratuito e de código aberto, projetado para manter os dados em padrões de preservação digital e o acesso em longo prazo.
> **Art. 40.** Os órgãos do Poder Judiciário deverão instituir ambientes físico e virtual de preservação e divulgação de informações relativas à memória, produzidas ou custodiadas pelo órgão, seja por meio de Museu, Memorial ou Centro de Memória, de caráter informativo, educativo e de interesse social.
> **§ 1º** O ambiente virtual mencionado no caput será veiculado em espaço permanente do sítio eletrônico do órgão.
> **§ 2º** O acervo digital relacionado à memória institucional será preservado em Repositório Arquivístico Digital Confiável – RDC-Arq, com interoperabilidade de pacotes informacionais (Conselho…, 2020, p. 1).

Duas outras normativas causaram alteração na legislativa 324/2020. A primeira foi a Resolução 408/2021 do CNJ[61] que dispõe sobre o recebimento, o armazenamento e o acesso a documentos digitais relativos a autos de processos administrativos e judiciais, frisando que:

> **Art. 2°** Os órgãos do Poder Judiciário submetidos ao controle administrativo e financeiro do CNJ deverão disponibilizar repositório arquivístico digital confiável – RDC-Arq para a gestão e o tratamento arquivístico de documentos e mídias digitais cujo tamanho ou extensão sejam incompatíveis com o sistema de processo eletrônico oficial, com observância de garantia de acesso às partes.
> **Parágrafo único.** Os sistemas processuais deverão permitir o acesso contínuo aos documentos e às mídias digitais referenciados no caput por meio de *links* ou indicação do respectivo endereço de acesso registrado nos autos físicos ou eletrônicos.
> **Art. 5º** Os documentos ou as mídias digitais que representem risco à violação da intimidade ou que sejam especialmente sensíveis deverão ser identificados na juntada ao processo eletrônico como documento "reservado/sensível".
> **§ 1º** Ao documento especificado como "reservado/sensível" deverá ser conferido o grau mais elevado de sigilo, limitando o acesso a usuários designados, conforme as funcionalidades e regras do sistema eletrônico.
> **§ 2º** As mesmas regras de sigilo serão aplicadas para acesso ao repositório arquivístico digital confiável – RDC-Arq ou às mídias e aos dispositivos externos que armazenem documentos ou arquivos sensíveis.
> **Art. 6º** Os processos judiciais eletrônicos deverão ser ajustados para marcar a existência de documentos e arquivos digitais em RDC-Arq ou em dispositivos externos.
> **§ 1º** Os sistemas processuais deverão impedir a baixa do processo, físico ou eletrônico, até que seja definida a destinação legal, conforme as regras de tratamento arquivístico dos documentos e das mídias digitais mantidos em RDC-Arq ou em dispositivos externos (Conselho…, 2021b, p. 1).

E a segunda foi Resolução 469/2022 do CNJ[62], que estabelece diretrizes e normas sobre a digitalização de documentos judiciais e administrativos e de gestão de documentos digitalizados do Poder Judiciário, preconizando:

---

[61] Disponível em: atos.cnj.jus.br/atos/detalhar/4065.
[62] Disponível em: atos.cnj.jus.br/atos/detalhar/4719.

> **Art. 4º** Constituem diretrizes da digitalização de documentos e processos judiciais e administrativos do Poder Judiciário:
> **XII –** a garantia de preservação digital a longo prazo da documentação digitalizada em Repositório Arquivístico Digital Confiável (RDC-Arq).
> **Art. 21.** Os documentos administrativos e judiciais de guarda permanente, inalienáveis e imprescritíveis, constituem patrimônio arquivístico do Poder Judiciário e poderão ser digitalizados, conforme definido em política própria, para possibilitar o amplo acesso, a difusão, a pesquisa e a salvaguarda dos originais físicos, observados os seguintes requisitos:
> **VIII –** a documentação permanente digitalizada será incluída em RDC-Arq, desenvolvido com software livre, gratuito e de código aberto, projetado para manter os dados em padrões de preservação digital e acesso em longo prazo; (Conselho…, 2022, p. 1).

Essas normativas são importantes, pois identificam boas práticas necessárias à preservação, à memória e, consequentemente, à gestão dos registros no Judiciário. Nesse aspecto, aos documentos arquivísticos de valor primário, tem-se a Resolução n.º 91/2009, alterada pela n.º 522 de 18/09/2023[63], ambas do CNJ, que institui o Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus) e disciplina a obrigatoriedade da sua utilização no desenvolvimento e na manutenção de sistemas informatizados para as atividades judiciárias e administrativas no âmbito do Poder Judiciário.

> **Art. 2º** Os sistemas informatizados de gestão de processos e documentos utilizados em atividades judiciais e administrativas dos órgãos integrantes do Poder Judiciário, ainda que segmentados em aplicações, módulos e microsserviços, deverão aderir aos requisitos do MoReq-Jus, com o objetivo de assegurar a confidencialidade, a integridade, a disponibilidade, a autenticidade, o não repúdio, a conformidade e a preservação de processos e documentos do Poder Judiciário.
> **Art. 7º** Os sistemas atualmente em desuso e aqueles que vierem a ser descontinuados deverão preservar os dados e metadados, garantir o direito de certidão e de acesso à informação para fins legais e ter seus processos, dossiês e documentos:
> **§ 2º** Os processos, dossiês e documentos de guarda longa ou permanente deverão ser armazenados em Repositório Arquivístico Digital Confiável (RDC-Arq) (Conselho…, 2023, p. 1).

O Conselho Nacional do Ministério Público por meio da Portaria CNMP-SG n.º 105, de 10 de março de 2022[64], que institui a Política de Gestão de Documentos e Informação do Conselho Nacional do Ministério Público, também salienta a relevância dos RDC-Arqs e prescreve:

[63] Disponível em: atos.cnj.jus.br/atos/detalhar/5266.
[64] Disponível em: Atos e Normas - Conselho Nacional do Ministério Público (cnmp.mp.br).

> **Art. 16** Os documentos arquivísticos eletrônicos serão custodiados em Repositório Digital com integração de metadados e gerenciamento para captura, armazenamento, recuperação, preservação e acesso.
> **Art. 17** O Repositório Digital Arquivístico do CNMP:
> **I –** será destinado à cadeia de custódia de longo prazo.
> **II –** deve gerenciar os documentos e metadados de acordo com as práticas e normas da Arquivologia, especificamente relacionadas à gestão documental, descrição arquivística multinível e preservação;
> **III –** deve proteger as características do documento arquivístico, em especial a autenticidade (identidade e integridade) e a relação orgânica entre os documentos;
> **Parágrafo único.** A responsabilidade pelo projeto, implantação e manutenção deve ser compartilhada por profissionais de arquivo, biblioteca, direito e tecnologia da informação, de forma a se cumprirem os requisitos legais, tecnológicos e os procedimentos do tratamento arquivístico e de proteção de dados (Conselho Nacional do Ministério Público, 2022, p. 4).

O Ministério da Educação (MEC) também traz a Portaria n.º 613, de 16 de agosto de 2022[65], que regulamenta o art. 4º da Portaria MEC n.º 360, de 18 de maio de 2022, dispondo sobre os procedimentos gerais para conversão e preservação dos documentos do acervo acadêmico digital das Instituições de Ensino Superior (IES). E, no seu Artigo 7, destacam-se os seguintes parágrafos:

> **§ 1º** As IES pertencentes ao sistema federal de ensino superior deverão possuir Repositório de Arquivístico Digital Confiável - RDC-Arq, de acordo com as normas vigentes do Conselho Nacional de Arquivos - Conarq.
> **§ 2º** Os RDC-Arqs das IES deverão possuir cópia de segurança externa à instituição para fins de recuperação de desastres.
> **§ 3º** A contratação de serviço externo de RDC-Arq deverá observar cláusula que garante ao MEC acesso ao acervo, em caso de descredenciamento, e prever a manutenção do acervo durante pelo menos doze meses, em caso de desaparecimento da IES (Ministério da Educação, 2022, p. 1).

Observa-se que o Poder Judiciário e o Poder Executivo têm imensa preocupação com a TD, quando dispõem de legislação e de ferramentas, que possibilitam um maior cuidado e interação com os cidadãos, sobretudo, ao se utilizar dos parâmetros arquivísticos de preservação e de segurança à informação.

[65] Disponível em: PORTARIA Nº 613, DE 18 DE AGOSTO DE 2022 - PORTARIA Nº 613, DE 18 DE AGOSTO DE 2022 - DOU - Imprensa Nacional (in.gov.br).

7 O PROJETO INTERPARES: OS PRIMEIROS ESTUDOS DE REFERÊNCIA CONCEITUAL E METODOLÓGICA À PRESERVAÇÃO DIGITAL

O projeto InterPARES, em português, **Pesquisa Internacional de Registros Autênticos Permanentes em Sistemas Eletrônicos**, desenvolve o conhecimento essencial para a preservação a longo prazo de registros autênticos criados e mantidos em formato digital, fornecendo base para normas, políticas, estratégias e planos de ação. Pode ser considerado uma das primeiras iniciativas quando referido à preservação digital, pois traz à tona conceitos antes não visto, discutindo sobre o cuidado e a proteção documental.

O principal financiador do Projeto é o Conselho de Pesquisa em Ciências Sociais e Humanas das Alianças de Pesquisas Comunidade-Universidade do Canadá (SSHRC-CURA); sendo dirigido pela Professora Doutora Luciana Duranti da Escola de Biblioteconomia, Arquivamento e Estudos da Estudos da Informação da University of British Columbia (UBC), Vancouver, Canadá.

O InterPARES foi lançado em 1999, com o fito de abordar questões levantadas pelo fato de que organizações e indivíduos passaram a confiar na criação, na troca e no processamento de informações digitais sem reconhecer a grave ameaça representada aos registros pela rápida obsolescência e fragilidade de *hardware*, de *software* e de mídias digitais, levando a preocupação com a confiança, a autenticidade, a avaliação e a preservação de documentos.

> Originou-se de uma pesquisa realizada entre abril de 1994 a março de 1997 na Universidade de British Columbia pelo Programa de Mestrado e, Estudos Arquivísticos, em conjunto com o Departamento de Defesa (DoD) dos Estados Unidos da América. Iniciado como projeto da UBC intitulado Preservação da Integridade dos Documentos Arquivísticos Eletrônicos, conhecido simplesmente como projeto UBC, foi capitaneado pela professora Luciana Duranti, a qual foi auxiliadora por Terry Eastwood e Heither MacNeil, cujo resultado doi a publicação da norma DoD Standard 5015.2 (Innarelli, 2015, p. 178-179).

A estrutura intelectual do InterPARES é basilada na Arquivologia e na Diplomática, que envolve um processo interdisciplinar, contando com o espectro acadêmico e profissional nas áreas da Geografia, da Musicologia, da Engenharia da Computação, do Direito, entre outras áreas. Seus pesquisadores incluem indivíduos, organizações e instituições dos cinco continentes, atuando nos setores público e privado (Innarelli, 2015). Dessa forma, serve para fundamentos e aportes conceituais das características dos documentos dos arquivos, por meio da preservação digital a longo prazo. Até a presente data, o Projeto conta com quatro fases consolidadas:

a) A primeira fase (1999-2001) possuiu o foco na preservação da autenticidade dos registros eletrônicos, que não eram mais necessários aos seus órgãos, disseminando conceitos diversos atribuídos aos registros eletrônicos;
b) A segunda fase (2002-2007) também desenvolveu conceitos, princípios, critérios e métodos para garantir a criação e a manutenção de registros confiáveis, além também da preservação a longo prazo de documentos autênticos no contexto das atividades artísticas, científicas e governamentais;
c) A terceira fase (2007-2012) traduziu teorias e métodos de preservação digital extraídos de suas pesquisas, mostrando: (1) como a teoria geral e os métodos podem ser implementados em arquivos e unidades de pequeno e médio porte de forma eficaz; (2) quais fatores determinam o tipo de implementação que é apropriado para cada conjunto de registros em cada contexto; e (3) quais habilidades os profissionais exigirão para conduzir tais operações;
d) A quarta e última fase (2012-2019) explorou questões de confiança e confiabilidade de registros e dados em ambiente *online*. Seu objetivo é gerar os quadros teóricos e metodológicos para desenvolver políticas, procedimentos, regulamentos, normas e legislações locais, nacionais e internacionais, a fim de garantir a confiança pública baseada em evidências de boa governança, uma economia digital forte e uma memória digital persistente.

Pode-se salientar que, em âmbito internacional, o InterPARES pode ser considerado como um dos maiores campos de estudo sobre preservação digital, o qual cria e incorpora conceitos, métodos e teorias. Contudo, aqui no Brasil, percebe-se uma escassez de publicação: seja na seara científica (nas bases de dados e periódicos), ou não científica (veículos de informação popular).

Com inferência, entende-se que uma das causas para esse acontecimento adveio da barreira linguística, isto é, a maioria de suas publicações não está vernacular ao idioma português. Em contrapartida, a equipe brasileira teve o início de sua participação no Projeto InterPARES 3, que ficou conhecido como Team Brasil. A coordenação da equipe à época coube à Claúdia Lacombe Rocha, do Arquivo Nacional, contando com a participação dos demais servidores que integravam o quadro dos membros que estudavam os documentos digitais: Brenda Rocco, Carlos Ditadi e Margareth da Silva.

Assim, foram desenvolvidos nove estudos de caso, que fizeram testes em conjuntos documentais da Universidade Estadual de Campinas (Unicamp), Ministério da Saúde, Câmara dos Deputados, Governo do Estado de São Paulo e Prefeitura de Porto Alegre (Arquivo

Nacional, 2018). Arquivistas e outros profissionais participaram desses campos de testes.

O Arquivo Nacional também colaborou coma a quarta fase do InterPARES pelo Team América Latina, desenvolvendo um estudo de caso sobre a preservação de documentos produzidos no Sistema de Gestão de Pessoas do Poder Executivo Federal (Sigepe). Mesmo com a atuação do Brasil, nas duas últimas etapas do Projeto, percebe-se a necessidade de uma adaptação, bem como a tradução dos relatórios das duas primeiras fases do InterPARES, uma vez que permitiria aos interessados entenderem a gênese e o desenvolvimento dos conceitos que compõem a preservação digital.

As informações apresentadas a seguir, que elencarão as quatro fases do InterPARES, estão dispostas em seu sítio[66] oficial e são apresentadas aqui por duas razões: (1) por ir ao encontro da temática da pesquisa, que busca entender a preservação digital nas suas questões mais vigentes, e auxilia na compreensão do conceito de confiança em uma perspectiva tecnológica digital; e (2) para expor a importância dos seus estudos à preservação digital.

7.1 O PROJETO INTERPARES 1

O InterPARES 1 debruçou-se sobre os estudos de preservação da autenticidade dos registros eletrônicos[67], sendo aqueles documentos que não eram mais de uso imediato às instituições criadoras, portanto, dispensáveis. Os documentos analisados nesta primeira etapa foram, principalmente, textuais, mantidos em banco de dados e sistemas de gerenciamento de documentos. Os frutos colhidos nesta etapa produziram requisitos conceituais para autenticidade e métodos destinados à seleção e à preservação de registros eletrônicos autênticos.

A conclusão de um projeto anterior intitulado “A preservação da Integridade dos Registros Eletrônico”, também conhecido como projeto UBC, serviu de base para o InterPARES 1.

Em colaboração com o Departamento de Defesa dos EUA e conduzido por pesquisadores da UBC de 1994 a 1997, teve como objetivo estabelecer padrões para criar registros eletrônicos confiáveis e manter sua autenticidade durante sua vida ativa e semiativa. Um de seus produtos foi o DoD Standard 5015.2. Nesse sentido, buscou estabelecer os meios para avaliar e manter a autenticidade dos registros eletrônicos, uma vez que se tornam inativos

[66] Disponível em: http://www.interpares.org/welcome.cfm.
[67] Os termos “registro eletrônico” para fins desta tese serão entendidos como sinônimos de documentos de arquivo em meio digital.

e são selecionados para preservação permanente.

No âmbito do Projeto, inseriram-se acadêmicos e profissionais de diversas disciplinas, a saber, Direito, História, Ciência da Computação e Engenharia, Ciência da Informação e Química; mas vale ressaltar que os principais conceitos e metodologias foram extraídos da Diplomática e da Arquivologia.

Os países envolvidos como coinvestigadores representaram universidades, instituições arquivísticas, empresas e indústrias, são eles: Canadá, Estados Unidos, Reino Unido, Austrália, China e Hong Kong, França, Irlanda, Itália, Holanda, Suécia e Portugal.

A responsável pela direção administrativa, financeira e intelectual do InterPARES 1 foi de exclusividade da Dra. Luciana Duranti. Dessa forma, o Projeto teve como finalidade formular modelos de políticas, de estratégias e de padrões capazes de garantir a preservação. Para cumprir essa primeira etapa da pesquisa, quatro domínios de investigação surgiram: o domínio de autenticidade, o domínio de avaliação, o domínio de preservação e o domínio de estratégia (Quadro 8):

Quadro 8 – Domínios do InterPARES 1

Domínio de autenticidade	
Objetivo: identificar requisitos conceituais para avaliar e para manter a autenticidade dos registros eletrônicos.	**Metodologia (duas abordagens metodológicas foram adotadas):** uma abordagem teórica e dedutiva, baseada na Diplomática Arquivística Contemporânea e uma abordagem indutiva e empírica que empregou estudos de caso selecionados com base na teoria fundamentada para compreender os registros gerados por uma variedade de sistemas eletrônicos existentes.
Domínio de avaliação	
Objetivo: determinar se a seleção de registros eletrônicos deve ser baseada nos mesmos critérios ou em critérios diferentes dos registros tradicionais e como as tecnologias digitais afetam a metodologia de avaliação.	**Metodologia (três diferentes metodologias foram adotadas em sequência):** uma revisão da literatura sobre avaliação de registros eletrônicos, um estudo de políticas de arquivamento, procedimentos, métodos e relatórios de avaliação, e modelagem das atividades envolvidas na seleção dos registros eletrônicos.
Domínio de preservação	
Objetivo: desenvolver métodos de preservação para registros eletrônicos autênticos.	**Metodologia (tanto uma abordagem empírica quanto uma analítica foram adotadas, incluindo):** um levantamento dos programas existentes, planos e tecnologias para preservar registros eletrônicos, e uma modelagem das atividades envolvidas na preservação de registros eletrônicos autênticos, que levou em consideração as conclusões das Forças-Tarefa de Avaliação e Autenticidade.
Domínio de estratégia	
Objetivo: para desenvolver uma estrutura intelectual para a articulação de políticas, de estratégias e de padrões internacionais, nacionais e organizacionais para a preservação a longo prazo de registros eletrônicos autênticos.	**Metodologia:** sua estrutura intelectual foi desenvolvida destilando princípios e critérios das descobertas dos outros três domínios.

Fonte: InterPARES 1 Project (1999).

Esses domínios, também denominados Forças-tarefas, possuem composição interdisciplinar. Assim, foram confecionados relatórios em cada temática: Força-tarefa de Autenticidade, Força-Tarefa de Avaliação, Força-Tarefa de Preservação e Força-Tarefa de Estratégia.

7.1.1 Relatório da Força-tarefa de Autenticidade

Os relatórios finais das Forças-tarefas do InterPARES 1 são encontrados em língua inglesa, por isso foram trazidos aqui, como forma de aclarar as informações contidas neles. Traduziram-se esses documentos por sua representatividade no campo da preservação digital, não apenas por ser um Projeto famigerado; mas por suas descobertas, sobretudo conceituais, que desencadearam o aporte para o desenvolvimento de pesquisas significativas.

A finalidade do Relatório da Força-tarefa de Autenticidade foi o de identificar requisitos conceituais para avaliar e manter a autenticidade dos registros eletrônicos. Assim, cinco questões foram elaboradas neste no domínio:

- Quais são os elementos que todos os registros eletrônicos compartilham?
- Quais são os elementos que nos permitem diferenciar entre os diferentes tipos de eletrônicos registros?
- esses elementos, o que nos permitirá verificar sua autenticidade ao longo do tempo?
- Os elementos para verificar a autenticidade ao longo do tempo são os mesmos que permitem verificar sua autenticidade no tempo, ou seja, no ponto em que foram originalmente criados e transmitidos?
- É possível mover os elementos de sua posição atual para um lugar onde eles possam ser mais facilmente preservados, sem afetar a validade?

Foram adotadas duas pesquisas com abordagens complementares neste Relatório. A primeira, teórica e dedutiva, baseada na Diplomática e na Diplomática Arquivística[68], envolvendo a identificação e a definição dos elementos de um registro eletrônico "ideal". A segunda abordagem foi indutiva e empírica, fazendo uso de estudos de caso nos sistemas eletrônicos existentes à época. Ambas as abordagens visavam à construção de teorias, bem como de conceitos e de requisitos para avaliar a autenticidade dos documentos.

O resultado do trabalho desta Força-tarefa foi o desenvolvimento de dois conjuntos de requisitos: um inclui os que suportam a **presunção da autenticidade** de registros eletrônicos antes de serem transferidos para a custódia do preservador; o outro inclui requisitos que

[68] Também chamada de Diplomática Contemporânea ou Diplomática Arquivística.

suportam a produção de **cópias autênticas,** após terem sido transferidos para a custódia do preservador.

O InterPARES 1 define alguns conceitos importantes neste relatório, são eles:

a) Registro: qualquer documento feito ou recebido e guardado no decorrer de uma atividade prática.

b) Autenticidade: qualidade de ser autêntico, ou aquilo com direito a aceitação. O termo autêntico significa, digno de aceitação ou crença baseada em fatos, sendo sinônimo do termo genuíno. Genuíno é algo com caráter real e não falsificado, imitado ou adulterado. *Bona fide* implica boa fé e sinceridade de intenção. A partir dessas definições um registro autêntico é aquele que pretende ser e estar livre de adulteração/corrupção.

c) Autenticação: declaração de um registro autêntico em um determinado momento por uma pessoa física ou jurídica a quem foi confiada a autoridade. Assume a forma de uma declaração oficial (palavras ou símbolos), atestando-o como autêntico. Um exemplo disso são as assinaturas digitais[69], desenvolvida para abordar comunicação eletrônica em redes – a *Internet*;

d) Registro autêntico: documento livre de adulteração/corrupção.

Tanto na Arquivologia como na área do Direito, documentos precisam presumir autenticidade. Vê-se que o ambiente *Web* está continuamente em risco. Assim, a autenticidade dos documentos sempre é ameaçada quando são transferidos através do espaço (ou seja, quando enviados entre pessoas, sistemas ou aplicativos) ou do tempo (quando eles são armazenados *offline*, ou quando o *hardware* ou o *software* é usado para processar, comunicar ou mantê-los atualizados ou substituídos).

Abordagem teórico-dedutiva

Nesta etapa, estabeleceu-se teorias e um Modelo de Análise. Para a confecção desse modelo, gerou-se um *template* baseado nas premissas da Diplomática Arquivística.

[69] Essas assinaturas identificam o remetente de um objeto de dados e verificam se eles não foram alterados na transmissão. Podem suportar a autenticação de um registro, mas não é o suficiente para estabelecer a identidade e demonstrar a integridade de um documento a longo prazo.

> A Diplomática surgiu no século XVII como uma técnica analítica para determinar a autenticidade de registros emitidos por autoridades soberanas em séculos anteriores. Seu objetivo principal era averiguar 'a realidade dos direitos ou veracidade dos fatos' contidas nesses documentos. Os princípios e métodos da Diplomática foram estabelecidos no ano de 1681, em um tratado escrito por Jean Mabillon, monge beneditino. Mabillon examinou, entre outras coisas, a linguagem dos documentos, suas partes características, seus selos e os seus sistemas de cronologia. (Mcneil *et al.*, 2001, p. 3, tradução nossa).

A questão primária da Diplomática era a de determinar a autenticidade; esse uso continuou no século XVIII, quando muitas faculdades de Direito europeias incorporaram seus conceitos e princípios. No final do século XIX, no entanto, sob a influência da Filologia Clássica e da escola científica de historiografia, a Diplomática surgiu como uma ferramenta para avaliar a autoridade dos registros medievais como fontes históricas.

Nas últimas décadas, houve inúmeras chamadas dentro do ambiente arquivístico para adaptar a Diplomática para desburocratizar o entendimento acerca do documento digital. Em 1989, o CIA recomendou o desenvolvimento dessa área para a pesquisa. Na Europa, precisamente na Holanda, existiram os esforços dos arquivos para construir uma Diplomática Moderna, com o propósito de desenvolver tipologias de registros criados por organizações desde o século XIX e a adaptação de conceitos e de métodos diplomáticos tradicionais.

Na América do Norte, o esforço mais abrangente para adaptar a Diplomática Tradicional às práticas contemporâneas estão incorporadas no trabalho de Luciana Duranti, em uma série de artigos, que circundaram os anos de 1989-1992. Duranti examinou os princípios e os conceitos desenvolvidos por teóricos diplomáticos para avaliar a autenticidade de documentos medievais e determinar se eles poderiam ser adaptados à aplicação dos registros modernos. Ao longo dos seis artigos, ela refinou e reinterpretou os conceitos clássicos e introduziu novos, levando em consideração a variedade e a complexidade dos ambientes eletrônicos (Mcneil *et al.*, 2001).

Uma das características da análise da Diplomática Arquivística é a identificação da forma fixa e do conteúdo estável do documento. Isso participa ou apoia uma ação, seja processual ou como parte da tomada de uma decisão (significa que sua criação pode ser obrigatória ou discricionária); e pelo menos três pessoas (autor, escritor e destinatário) estão envolvidos na sua criação (essas três pessoas conceituais podem ser físicas ou jurídicas).

A hipótese de trabalho da Força-Tarefa de Autenticidade foi que, embora possam se manifestar de maneiras diferentes, esses elementos estão presentes explicita ou implicitamente na memória eletrônica. O **Modelo de Análise** foi criado para testar essa hipótese. Os elementos incluídos nesse Modelo se enquadram em quatro categorias: forma documental, anotações, contexto e meio:

A forma documental é definida como as regras de representação segundo as quais o conteúdo de um registro, seu contexto administrativo e documental imediato e sua autoridade são comunicados; possui tanto elementos intrínsecos, como extrínsecos. Os intrínsecos são as partes discursivas do registro que comunicam a ação em que o registro participa e o contexto imediato. Eles se enquadram em três grupos:

a) elementos que transmitem aspectos do contexto jurídico e administrativo do registro (o nome do autor, do destinatário e a data);
b) elementos que comunicam a própria ação (a indicação e a descrição da ação ou matéria);
c) elementos que transmitem aspectos do contexto documental do registro e seus meios de validação (o nome do redator, o atestado e a corroboração).

Os elementos extrínsecos referem-se às características específicas do registro que são instrumentais em comunicar e alcançar o propósito para o qual foi criado, são eles:

• características gerais de apresentação (textual, gráfico, imagem, som, ou alguma combinação desses);

• recursos de apresentação específicos (*layouts* especiais, *hiperlinks*, cores, taxa de amostragem de arquivos de som);

• assinaturas e selos eletrônicos (assinaturas digitais);

• selos de tempo digitais;

• outros sinais especiais (marcas d'água digitais, marca de uma organização ou logotipo pessoal).

As anotações são acréscimos feitos a um registro após sua criação. Eles se enquadram em três grupos básicos:

a) adições feitas no registro após a sua criação, como parte de sua execução (a data e hora da transmissão adicionada a um registro de *e-mail* no momento em que é enviado, ou a indicação de anexos adicionados antes de serem transmitidos);
b) acréscimos feitos no registro no curso do tratamento de um assunto comercial em que o registro participa (comentários anotados na capa do registro, ou incorporados a ele, e datas de transmissão);
c) adições feitas no registro durante o manuseio de seu gerenciamento (o código de classificação ou número do arquivo atribuído ao registro, seu rascunho e/ou o número da versão, referências cruzadas para outros registos e uma indicação de programação ações).

O contexto muda a análise do próprio registro para uma forma mais ampla,

procedimental e estrutural do documento, na qual o registro é criado e gerenciado. Os elementos que foram identificados correspondem a uma hierarquia que vão do geral ao específico. Eles incluem o contexto jurídico-administrativo, o de proveniência, o de procedimento, o documental e o tecnológico. O conhecimento desses elementos é fundamental para a compreensão dos processos de negócio, no qual registros eletrônicos são criados, mantidos e usados.

O meio (suporte físico que armazena registro) provou ser um construto problemático do ponto de vista da análise Diplomática, uma vez que precisava-se entendê-lo como parte do próprio registro ou como parte de seu contexto tecnológico. Para os diplomáticos que examinavam os documentos medievais, o meio era o componente essencial do registro, porque o exame do suporte físico significava uma das provas mais latentes de sua autenticidade.

O desenvolvimento inicial do Modelo ocorreu ao longo de um período de nove meses, de janeiro a setembro de 1999. Durante esse tempo, foi revisado, várias vezes, tanto pela Força-Tarefa de Autenticidade, quanto pela comunidade internacional do InterPARES. Em junho de 1999, o *template* foi considerado suficientemente desenvolvido para o início do processo de teste e de refinamento, por meio dos estudos de caso dos sistemas eletrônicos.

Abordagem empírico-dedutiva

Conforme explicitado, o Modelo para Análise começou como um protótipo baseado no conhecimento prévio de arquivamento para os tipos de registros "ideias" (registro autêntico tratado pelo InterPARES) e delineou os possíveis elementos que um documento poderia conter. No entanto, um dos objetivos do Projeto era desenvolver um modelo preditivo que ajudasse os arquivistas a identificar novos tipos de registros e os requisitos necessários para manter sua autenticidade ao longo do tempo.

No primeiro ano do Projeto, os pesquisadores determinaram que poderiam desenvolver uma imagem mais rica dos registros eletrônicos se eles triangulassem a abordagem diplomática dedutiva à abordagem empírica indutiva. Esse exame foi conduzido por meio de um estudo de caso interpretativo não aleatório em sistemas eletrônicos.

A adição desta abordagem, "de baixo para cima" estendeu consideravelmente as atividades de pesquisa do InterPARES, além das originalmente previstas. Forneceu um rico conjunto de dados e um desenvolvimento teórico, indicando o papel crescente do contexto processual e tecnológico na garantia de manter a autenticidade dos documentos.

O estudo de caso

Entre os anos de 1999 a 2001, quatro rodadas de estudos de caso foram conduzidas por pesquisadores institucionais e estudantis em agências governamentais, universitárias e corporativas no Canadá, nos EUA, na Itália, no Reino Unido, na Holanda e na China. Esses estudos incluíram bancos de dados em grande escala (como patentes e sistemas de registro de alunos), sistemas de informação geográfica e aplicativos interativos baseados na *Web*.

Os atuantes da Força-tarefa adotaram a abordagem da teoria fundamentada, a fim de identificar e descrever fenômenos associados aos registros e seus contextos. Essa teoria é um método para descobrir conceitos e hipóteses por meio de dados observados para ajudar a expandir ou refinar conceitos ou teorias que já foram desenvolvidas. Assim, por causa de tal abordagem, os pesquisadores empregaram teorias ao invés de amostragem estatística.

Nas primeiras duas rodadas, o foco foi sistemas eletrônicos. A tradução dos dados fora estruturada em um formulário que podia ser analisado diplomaticamente, usando o Instrumento de Coleta de Dados de Elemento de Modelo (TEDGI). As informações coletadas também foram disponibilizadas as Forças-tarefas de Avaliação e de Preservação.

Essas duas primeiras análises indicaram que poucos sistemas continham os "registros ideais" promulgados no Modelo. A abordagem da teoria fundamentada, com base no que a Força-tarefa aprendera nos dois primeiros turnos; modificaram os critérios de seleção do estudo de caso para a terceira e quarta rodada. Por meio dessa redefinição, os pesquisadores incorporaram os seguintes indicadores de sistemas que são conhecidos por criar registros ou têm o potencial para tal:

a) se a ação em que o sistema participa é juridicamente exigida;
b) se houver um procedimento comercial em vigor para realizar dessa ação;
c) se o sistema opera dentro dos níveis de gestão ou de tomada de decisão estratégica da organização.

O objetivo principal de analisar os estudos de caso a partir da Diplomática Arquivística era consolidar informações necessárias para a elaboração de conceitos e de requisitos para avaliar a autenticidade dos registros eletrônicos e para o desenvolvimento de uma tipologia de registros eletrônicos com base nesses requisitos.

O processo de análise ocorreu em três fases: os estudos das rodadas um e dois foram analisados na primeira fase (2000); os da terceira rodada, na segunda fase (janeiro 2001); e os da quarta rodada, na terceira fase (maio de 2001).

O produto final foi constituído por um "relatório final" para cada sistema analisado.

Tais relatórios foram escritos para vinte e dois dos vinte e seis estudos de caso concluídos. Quatro dos estudos de caso foram excluídos da análise diplomática devido a informações insuficientes ou dificuldades de linguagem com a documentação técnica.

Resultado da pesquisa da Força-tarefa de Autenticidade

O objetivo de desenvolver o Modelo de Análise e testar sua eficácia por meio de quatro rodadas, deu-se na visão de estabelecer requisitos conceituais para avaliar e manter a autenticidade dos registros eletrônicos a longo prazo. Dessa forma, o ímpeto desta Força-tarefa firmou-se em uma descoberta conceitual. Então, para avaliar a autenticidade de um registro eletrônico, o preservador deve ser capaz de estabelecer sua **identidade**[70] e demonstrar sua **integridade**.

A identidade de um arquivo na perspectiva diplomática inclui atributos variados: os nomes das pessoas que concorrem em sua formação (autor, destinatário, escritor e originador); sua data de criação (a data em que foi feita, recebida e reservada) de transmissão; indicação da ação ou matéria da qual participa; expressão de seu vínculo arquivístico, que conecta a outros registros, participando da mesma ação (por exemplo, um código de classificação ou outro identificador único).

A integridade dá-se quando o registro está completo e incorrupto em todos os seus aspectos. Isso não significa que ele deve ser exatamente o mesmo de quando foi criado para que sua integridade exista e seja demonstrada. Mesmo no mundo do papel, com o passar do tempo, os documentos estão sujeitos à deterioração, à alteração ou à perda. No meio eletrônico, a fragilidade da mídia, a obsolescência da tecnologia e as idiossincrasias dos sistemas também afetam a sua integridade. Quando se refere aos documentos eletrônicos, esses são considerados como essencialmente completos e não corrompidos, se a mensagem comunicada atingir seu propósito: permanecer inalterada.

Outros personagens surgem nesse ínterim da avaliação e da manutenção da autenticidade: o preservador[71] e o criador. Antes que os registros sejam transferidos para a custódia arquivística, o preservador deve estabelecer, como parte do processo de avaliação, em qual medida eles foram mantidos pelo criador, usando tecnologias e procedimentos administrativos que garantam sua autenticidade ou, pelo menos, minimizar os riscos de

[70] Refere-se ao caráter distintivo de um registro, ou seja, aos atributos que o caracterizam de maneira única e o distinguem de outros.

[71] O preservador deve avaliar a autenticidade dos registros eletrônicos antes que sejam transferidos para a custódia arquivística e mantê-los após a transferência. A avaliação é parte integrante dos registros, enquanto a manutenção é parte integrante de sua preservação a longo prazo.

mudança.

Para isso, o preservador deve manter o sistema eletrônico de acordo com os procedimentos que garantam sua autenticidade contínua e produzam cópias. Diante do exposto, a Força-Tarefa de Autenticidade desenvolveu dois conjuntos de requisitos. O primeiro, denominado "Requisitos de Referência", inclui requisitos que suportam a presunção da autenticidade dos registros eletrônicos do criador, antes de serem transferidos à custódia do preservador. O segundo, "Requisitos de Linha de Base", apoia a produção de cópias autênticas que foram transferidos para a custódia do preservador.

Os Requisitos de Referência e de Linha de Base são firmados na noção de confiança à manutenção e à preservação de registros; o primeiro direcionado a um sistema de manutenção de registro confiável [72] e o segundo na função do preservador como custodiante de confiança.[73]

O papel do preservador como guardião de confiança remonta à antiguidade romana, quando os cidadãos depositariam registros privados no *tabularium* com o propósito expresso de torná-los autênticos. Como guardiões de confiança, antigas instituições arquivísticas sustentavam e emprestavam credibilidade às relações contratuais entre os cidadãos. Eles também emprestaram credibilidade ao implícito contrato social entre os cidadãos e o estado, preservando os registros do passado do estado. Hodiernamente, o papel do preservador como um custodiante de confiança também é análogo ao do guardião de registros terceirizado de confiança em contratação eletrônica.

Nesse sentido, outra característica de avaliação de documentos se destaca: a presunção de autenticidade[74], que possui norma publicada nas resoluções do Conarq; mas sua concepção foi associada, primeiramente, nesta Força-tarefa, para verificar a passível veracidade dos registros.[75]

No processo de verificação, os fatos conhecidos sobre o registro e seus contextos fornecem as bases para apoiar ou refutar a alegação de sua autenticidade. Ao contrário da

---

[72] Tipo de sistema que as regras governam quais documentos são elegíveis para inclusão no sistema, tornando-se possível inseri-los e recuperá-los, além de determinar sua vida útil.

[73] Para ser considerado um custodiante de confiança, o preservador deve demonstrar que não há razão para alterar os registros preservados, ou permitir que outros os alterem, e que é capaz de implementar os requisitos básicos.

[74] Inferência extraída de fatos conhecidos sobre a maneira como um registro foi criado, manipulado e mantido (suas evidências). A presunção de autenticidade será baseada no número e grau de requisitos que foram atendidos. Portanto, quanto maior o número e o grau de requisitos satisfeitos, maior a presunção. É por isso que são chamados de "*benchmark*". Vale destacar que o Conarq possui documento diretivo no que se refere à presunção de autenticidade de documentos arquivísticos digitais pela Resolução n.º 37, de 19 de dezembro de 2012, a qual é objeto de estudo desta pesquisa.

[75] A verificação da autenticidade é o ato ou o processo de estabelecer uma correspondência entre fatos conhecidos sobre o registro e os vários contextos em que têm criado e mantido.

presunção de autenticidade, que é estabelecida com base nos Requisitos de Referência.

Para concluir as análises desta Força-tarefa, salienta-se haver um exame comparativo para os requisitos de autenticidade expostos no ato de sua criação. Três padrões foram escolhidos para essa relação: a ISO/DIS 15489: o Rascunho de Padrão Internacional sobre gerenciamento de registros[76]; o Padrão de Gerenciamento de Registros 5015.2 do Departamento de Defesa dos EUA; [77] e a Especificação de Requisitos do Modelo da Comissão Europeia (CE).

Assim, os documentos ISO e CE identificam disposições que podem ser considerados como contrapartida aos requisitos de *benchmark*, enquanto o DoD funciona, paralelamente, às estipulações contidas nos requisitos básicos e *benchmark*.

7.1.2 Relatório da Força-tarefa de Avaliação

A Força-tarefa de Avaliação se estabeleceu para os registros eletrônicos e não os tradicionais. Seu domínio insere-se na completude de sete perguntas:

- Qual é a influência da tecnologia digital na avaliação?
- Qual é a influência da recuperabilidade, da inteligibilidade, da funcionalidade e das necessidades de pesquisa sobre avaliação?
- Quais são as influências do meio e da forma física do registro na avaliação?
- Quando, no curso de sua existência, os registros eletrônicos devem ser avaliados?
- Caso os registros eletrônicos sejam avaliados mais de uma vez no curso de sua existência, e, em caso afirmativo, isso deve ocorrer em quais circunstâncias?
- Quem deve ser responsável pela avaliação dos registros eletrônicos?
- Quais são os critérios e métodos de avaliação para registros eletrônicos autênticos?

A pesquisa passou por três fases. Uma revisão da literatura sobre avaliação de prontuários eletrônicos. Em seguida, examinou-se a documentação de instituições arquivísticas sobre suas políticas e seus procedimentos de avaliação. A fase final, e a mais importante, envolveu o desenvolvimento de um Modelo de Função de Seleção de registros eletrônicos, a fim de obter compreensão detalhada da natureza das atividades na avaliação para uma preservação autêntica.

Conceitualmente, essa determinação envolve a responsabilidade pela preservação do criador para entidades. O aspecto mais importante dessa transferência de responsabilidade é

---

[76] *International Organization for Standardization. ISO/DIS 15489: Draft International Standard on Records Management.*

[77] *The U.S. Department of Defense's (DoD) 5015.2 Records Management Standard.*

garantir, tanto quanto possível, que a identidade e a integridade dos registros possam ser estabelecidas e preservadas ao longo do tempo. Os requisitos conceituais para avaliar a autenticidade são, portanto, um guia importante no processo de identificação de registros à sua integridade. Seu principal resultado é o Modelo de Função do Processo de Seleção.

Definição de avaliação segundo o relatório da Força-tarefa de Avaliação

No uso comum, avaliação pode ser definida como o ato de estimar a natureza, a qualidade, ou a importância de alguma coisa. Na Arquivologia, pode-se entendê-la como um elemento básico para sua função, que visa determinar a disposição dos documentos, isto é, sua preservação ou eliminação.

Assim, essa atividade envolve fazer um julgamento ou uma estimativa do valor de preservação de registros. Mais comumente, o preservador[78] avalia os documentos e determina o seu valor e a sua disposição. Em situações que o preservador tem responsabilidade pela avaliação, muitas vezes, chega a decisões sobre o destino dos registros em consulta com o criador. Realizar a disposição também é frequentemente uma responsabilidade compartilhada entre o criador-preservador. A responsabilidade de eliminar os registros pode cair para o criador ou para o preservador, ou ser compartilhados por eles.

Qualquer que seja a divisão de responsabilidades, é necessário realizar uma avaliação para identificar registros dignos de existência continuada e, em seguida, atribuí-lo valor. É esta função de seleção, ao invés das diferenças na forma como a responsabilidade por eles é realmente atribuída, que interessa a esta Força-tarefa.

Projeto de pesquisa e de metodologia

Na primeira fase de sua pesquisa, a Força-tarefa de Avaliação conduziu uma revisão e análise das literaturas sobre avaliação de registros eletrônicos. A revisão se deu em um consenso – os documentos eletrônicos devem ser avaliados sob a mesma óptica teórica e metodológica dos registros tradicionais. Em contrapartida, os arquivistas lutaram com o problema do que fazer com a dinâmica dos bancos de dados, muitos dos quais estavam envolvidos na manutenção de registros; mas na verdade, não os produziam.

A maioria dos autores escolhidos nessa temática concluiu que a avaliação precisa ser

[78] O preservador é a pessoa jurídica cuja principal responsabilidade é a preservação a longo prazo de registros autênticos. O preservador pode ser uma instituição arquivística (nacional, estadual ou municipal). Pode ser um escritório de uma organização, igrejas, empresas e universidades. Em suma, deve haver alguma entidade a quem é atribuída a responsabilidade pela preservação.

atribuída à gênese dos sistemas eletrônicos para acontecer um gerenciamento coerente de informação; obviamente, levando em consideração a utilização das estratégias de manutenção e de preservação. Outra questão elencada foi que os autores raramente abordavam a aplicação do conceito de autenticidade para avaliação. Eles presumiram que a função da "preservação" é a forma segura e confiável de gerenciamento. A avaliação determina quais registros devem ser preservados; fica então, a cargo do preservador, garantir a continuidade de sua identidade e integridade. Embora isso seja verdade, o trabalho da Força-tarefa mostrou que o conceito de autenticidade tem aplicação importante durante a avaliação.

A revisão das políticas e procedimentos das instituições e dos programas arquivísticos ampliou os resultados da revisão da literatura. Também revelou que apenas um pequeno número de instituições e de programas tinham qualquer coisa parecida com uma vasta experiência na avaliação de registros eletrônicos.

As principais documentações de valor revelaram-se nos laudos. Esses relatórios expuseram que os arquivistas gastaram muito tempo para apreciar os vários contextos dos registros, incluindo, o tecnológico. Juntos, as revisões da literatura e das políticas e procedimentos forneceram um corpo de conhecimento empírico usado nos principais exercícios para desenvolver o Modelo de Função de Seleção. Este Modelo representou as várias atividades de um processo funcional em uma série de diagramas. A Força-tarefa usou IDEF (0) ou Definição de Integração para Modelagem de Função, que é derivado de Análise Estruturada e Técnica de Projeto. O DEF (0) é uma informação federal dos EUA para Padrão de Processamento.

O objetivo do Modelo foi caracterizar as relações das atividades envolvidas na seleção de registros eletrônicos autênticos para a preservação a longo prazo. O Modelo é produzido a partir do ponto de vista da entidade responsável pela preservação contínua de uma organização. O pressuposto é que as mesmas atividades ocorrem em qualquer contexto que a seleção é realizada.

Resultados da pesquisa Força-tarefa de Avaliação

O trabalho no Modelo começou no início dos anos 2000. Nessa época, a Força-Tarefa de Autenticidade já havia desenvolvido o "Template para Análise de Prontuários Eletrônicos" a ser utilizado pelo Projeto e, posteriormente, os Requisitos para Avaliar e Manter a Autenticidade" dos registros eletrônicos forneceram uma importante estrutura conceitual para o pensamento por trás da modelagem.

O escopo das principais atividades na seleção (diagrama A0)

Do ponto de vista do preservador, a avaliação é o primeiro passo no processo de preservação. Selecionar registros eletrônicos envolve avaliá-los e realizar suas disposições. Muitos problemas que ocorrem no tratamento de arquivos decorrem de mudanças no contexto dos documentos ao longo do tempo. Monitorar essas nuanças é uma atividade distinta; isso garante que informações atualizadas sobre os documentos sejam compiladas e as decisões de avaliação atualizadas. Em grande medida, monitorar registros eletrônicos selecionados para a preservação é a resposta à pergunta da pesquisa da Força-Tarefa de Avaliação: Quando no curso de sua existência os registros eletrônicos devem ser avaliados? A resposta é frequentemente ditada pelo circunstâncias de mudança de contexto.

Nos casos em que a decisão de avaliação é embutida no projeto de sistemas eletrônicos, como por programação de registros, ou onde é conduzido algum tempo depois de um sistema estar em operação, monitorar registros selecionados para preservação e fazer os ajustes necessários faz parte do processo de seleção. Este processo, portanto, abrange quatro atividades principais: (1) gerenciar a função de seleção, (2) avaliação de registros eletrônicos, (3) monitoramento de registros eletrônicos selecionados para preservação, e (4) realizar a disposição dos registros eletrônicos.

A visão geral da seleção (A0)

Seleção de registros eletrônicos para preservação a longo prazo – como a seleção de registros em geral – responde, de um modo geral, às necessidades da sociedade e às dos seus criadores. Todas as atividades de seleção são realizadas com uma compreensão de teoria, de metodologia e de prática da arquivística. Gerenciar a função da seleção é, em grande parte, uma questão de levar esses fatores condicionantes ao desenvolvimento de políticas, de estratégias, de procedimentos e de padrões

Em particular, as informações sobre o contexto tecnológico dos registros eletrônicos entram em jogo nos dois estágios vitais de seleção: quando avaliar a autenticidade e quando determinar a viabilidade de preservá-los. As demais informações contextuais (jurídico-administrativas, de proveniência, processual e documental) tendem a ser relevante ao avaliar os documentos, isto é, julgando sua capacidade de servir aos interesses da sociedade e de seus criadores. Assim, dois tipos de informações resultam do processo de avaliação, as informações sobre a decisão de avaliação e as informações sobre os registros eletrônicos

selecionados para preservação como parte de uma transferência do criador para o preservador.

Gerenciando a função de seleção (A0, A1)

No que tange às “restrições de acesso”, o preservador precisa estabelecer, implementar e manter uma estrutura de políticas e de procedimentos que orientem a função de seleção. O objetivo da gestão é garantir que os requisitos do preservador à seleção de registros eletrônicos autênticos sejam atendidos de forma eficaz e eficiente. Gerenciar a função de seleção significa assumir a responsabilidade por todo o processo, tanto da qualidade do resultado, quanto da eficiência do processo. Sua principal responsabilidade é garantir que esses documentos sejam identificados e capazes de serem mantidos de acordo com os requisitos de autenticidade adequados.

Fatores externos, como as necessidades do criador e da sociedade, assim como os requisitos legais, variam de uma situação para outra, podendo influenciar no juízo de valor durante a avaliação. Já os estudos arquivístticos são outras questões mais aplicadas, mas não menos importantes.

As “informações necessárias” para a gestão se dão em quatro tipos, servindo para apoiar o desenvolvimento de políticas, de estratégias e de procedimentos que norteiam a seleção: informações sobre o contexto dos registros, informações sobre as decisões de avaliação, informações sobre as decisões de avaliação atualizadas e informações sobre a disposição.

Outro elemento a destacar, posterior a etapa acima, dá-se pelo “resultado de gerenciamento”, divididos em dois aspectos estruturais. O primeiro é uma convergência que rege as “estratégias de avaliação, que opera como controle sobre os processos e o monitoramento de registros eletrônicos selecionados para preservação. Essas estratégias abrangem:

a) critérios de avaliação;
b) diretrizes sobre como aplicar os requisitos de autenticidade;
c) procedimentos para realizar a avaliação;
d) diretrizes para relatar os resultados das avaliações;
e) procedimentos para relatar atividades de avaliação.

O segundo aspecto é um conjunto de regras e procedimentos que regem a conduta de disposição e atuam como uma espécie de controle sobre essa atividade. Essas regras e esses procedimentos incluem:

a) procedimentos para realizar a disposição (por exemplo, funções e

responsabilidades do criador e do preservador);

b) regras para disposição (por exemplo, formatos aceitáveis para transferência, meios de transmissão de registros, etc.);
c) procedimentos para relatar atividades de disposição (por exemplo, caráter e volume de registros adquiridos e/ou destruídos).

Avaliação de registros eletrônicos (A2)

Quando aplicada a qualquer conjunto de registros, a seleção pode ser dividida em dois principais processos, que são a tomada de decisão com relação à disposição dos documentos: se eles serão transferidos ou eliminados.

Além disso, a criação de "pacotes" de informações para documentar a decisão de avaliação e dos registros a serem preservados são cruciais para permitir o desempenho de outras funções arquivísticas, como a de preservação e de descrição. Sendo assim, a avaliação é a atividade durante a qual informações relevantes são coletadas e compiladas, em que uma decisão sobre sua disposição é tomada.

A avaliação é composta de algumas atividades distintas: compilar informações sobre os registros e os seus contextos; mensurar o valor dos registros, determinando as viabilidades de preservá-los; e, por fim, por uma tomada de decisão. Esta divisão é baseada em uma decomposição da avaliação em suas atividades ou funções de componentes lógicos, e não se destina a especificar um fluxo de trabalho preciso. Não faz suposições sobre a organização do ambiente no qual as atividades acontecem.

Avaliar um conjunto de registros eletrônicos é decidir sobre sua disposição. Se eles forem considerados para atender à alguma necessidade duradoura de seu criador ou sociedade, serão preservados.

Avaliando valor (A22)

Para entender o valor dos documentos, parte-se da decomposição de três atividades: avaliar o valor permanente dos registros eletrônicos, avaliar sua autenticidade; e determinar seu valor.

A primeira atividade resulta em uma declaração das razões pelas quais os registros devem ou não ser preservados, de acordo com critérios definidos pela instituição (podendo envolver juízo de valor).

A segunda atividade dar-se-á quando o avaliador fundamenta a presunção da

autenticidade, garantindo sua integridade. Como exemplo, pode-se citar: restrições de acesso, procedimentos para entrada e validação de dados, *backups* e armazenamento em diferentes locais. Já os requisitos de *benchmark* devem fornecer detalhes a serem analisados ao avaliar a autenticidade. O primeiro passo para gerenciar essas funções é reunir as evidências que sustentam a presunção de autenticidade, que é medida pelos Requisitos de Referência. Se uma avaliação não produz uma alta presunção de autenticidade, o arquivista deve tentar verificá-la por outros meios, como comparar diferentes versões ou cópias de registros, examinar trilhas de auditoria do sistema ou entrevistar o pessoal envolvido na criação, no uso e na preservação dos documentos.

Na terceira atividade, avaliar a autenticidade dos documentos não é uma tarefa simples. Por exemplo, supõe-se que um dos objetivos da avaliação seja identificar os registros que documentam um processo ou função desempenhada por seu criador. Para fazer isso, um avaliador define os registros que permitirão ao preservador manter uma reflexão precisa desse processo. Além disso, se houver evidências de práticas deficientes de manutenção de registros e de possíveis adulteração intencional ou fraudulenta, torna-se mais importante, ainda, preservá-los para atestar tal ocorrência.

A avaliação de como a autenticidade afeta o valor dos documentos, em grande parte, é uma questão de coleta e de monitoramento de evidências do que aconteceu com eles durante o curso de sua existência. Contudo, nos casos em que os registros não residem mais em seu ambiente original através, por exemplo, de conversão ou migração, é necessário determinar se o que está sendo avaliado é o que existia originalmente; e se essas alterações prejudicaram sua capacidade de atuar como peça da atividade que os gerou.

Nos casos em que a cadeia de custódia e de preservação forem quebradas ou que a migração resulte em registros perdidos, ou em documentação inadequada, faz-se primordial identificá-los(las). Se o avaliador suspeitar que esses registros não refletem mais o que eram no momento de sua criação, pode decidir não preservá-los.

Determinando a viabilidade de preservação (A23)

Só avaliar os registros não é suficiente. O avaliador também deve determinar a viabilidade de preservá-los como documentos autênticos. Mais precisamente, esse agente decide se os componentes digitais que incorporam os elementos essenciais que conferem identidade e garantem integridade dos registros podem ser preservados. Isso incluiria estado de conhecimento de preservação; capacidade de *hardware* e de *software*; experiência da

equipe; e recursos financeiros. A atividade para determinar a viabilidade de preservar registros eletrônicos autênticos é tida por três fases:

a) O avaliador determina os elementos dos documentos por meio do seu conteúdo informativo, identificando aqueles que precisam ser preservados de acordo com os requisitos de autenticidade dos Requisitos de Referência da Força-tarefa de Autenticidade.
b) O avaliador identifica onde esses elementos se manifestam em documento digital e quais devem ser preservados.
c) O avaliador concilia esses requisitos de preservação com a capacidade de gerenciamento da instituição responsável pelos documentos avaliados.

A primeira atividade para determinar a viabilidade de preservar um conjunto de registros que está sendo avaliado é identificar quais elementos devem ser preservados para garantir autenticidade. Essa atividade elenca os elementos extrínsecos e intrínsecos, conforme descrito no *benchmark.*

No ambiente analógico, esses elementos extrínsecos e intrínsecos são tipicamente unidos no meio; entretanto, não é assim no ambiente digital. Os elementos identificados no domínio digital podem se manifestar em várias formas – que o Projeto chamou de componentes digitais.[79].

7.1.3 Relatório da Força-tarefa de Preservação

O plano de pesquisa original do InterPARES afirmava: o objetivo da pesquisa neste domínio é identificar e desenvolver os procedimentos e os recursos necessários para a implementação dos requisitos conceituais e dos critérios nos primeiros dois Domínios. Assim, esta Força-tarefa articulou-se nas seguintes questões:

- Quais métodos, procedimentos e regras de preservação de longo prazo estão em uso ou sendo desenvolvidos?
- Quais destes atendem aos requisitos conceituais de autenticidade identificados no Domínio 1?
- Quais métodos de preservação de longo prazo precisam ser desenvolvidos?
- Quais desses métodos são necessários ou sujeitos a padrões, regulamentos e

[79] A Força-tarefa de Preservação do InterPARES define componente digital como um objeto digital que contém todo ou parte do conteúdo de um registro eletrônico e/ou metadados necessários para ordenar, estruturar ou manifestar esse conteúdo, requerendo métodos específicos para preservação de um ou mais documentos. Em complemento, o conceito de objeto digital tem suas raízes no paradigma orientado a esses objetos, sendo apresentado por um *software.*

diretrizes em contextos institucionais específicos?

- Quais são os métodos procedimentais de autenticação para registros eletrônicos preservados?
  a) De que forma a descrição arquivística pode ser um método de autenticação para uso de registros eletrônicos?
  b) De que forma os relatórios de avaliação e de aquisição/adesão podem ser construídos para permite a autenticação de registros eletrônicos?
  c) Quais são os procedimentos para a certificação de registros eletrônicos quando eles se cruzam limites técnicos (por exemplo, atualização, cópia, migração) para preservar sua autenticidade?

Quais são os métodos técnicos de autenticação para registros eletrônicos preservados?

Quais são os princípios e os critérios para gerenciamento de mídia e de armazenamento necessários para a preservação de registros eletrônicos autênticos?

Quais são as responsabilidades para a preservação a longo prazo de produtos eletrônicos autênticos registros?

Embora este Domínio tenha sido encarregado de abordar essas questões, várias delas pressupõem um conhecimento que só seria desenvolvido pelos outros grupos do InterPARES. Todas as cinco perguntas estão relacionadas à autenticidade e à autenticação, e suas respostas dependem, especificamente, da articulação desses conceitos e requisitos relacionados pela Força-tarefa de Autenticidade.

Por um lado, reuniu dados empíricos sobre programas, planos e tecnologias existentes para preservação. Por outro lado, realizou uma análise estruturada desse processo.

No campo empírico, esta Força-tarefa executou uma pesquisa de programas que estão preservando, estão planejando preservar, ou estão conduzindo pesquisas relacionadas à preservação documentos, e desenvolveu um *white paper*[80] sobre mídia para armazenamento de informações digitais. Ela também coletou dados sobre os métodos de autenticação usados em organizações que participam do InterPARES; no entanto, na ausência de critérios de autenticação, estes dados não puderam ser analisados.

Na esfera analítica, abordou a preservação de registros eletrônicos autênticos. A questão-chave foi:

Quais atividades são necessárias para preservar os registros eletrônicos?

[80] Documento informativo que exibe informações e dados sobre um determinado assunto, expondo um ponto de vista ou soluções para problemas.

a) Quais são as entradas para este processo?
b) Quais controles governam o processo?
c) Que o processo produz; ou seja, quais são seus resultados?
d) Quais recursos ou mecanismos são necessários para realizar o processo de preservação dos registros eletrônicos?

Ao abordar a questão acima e suas subquestões, a Força-tarefa explorou:

Como os requisitos de autenticidade impactam o processo de preservação?

a) Como é demonstrada a conformidade com os requisitos de autenticidade?
b) Como os métodos tecnológicos podem ser avaliados à luz dos requisitos para autenticidade?

Como a avaliação dos registros eletrônicos impacta o processo de preservação?

a) Como a preservação impacta na avaliação?

A pesquisa também abordou as perguntas iniciais do Domínio 3 e fez três adicionais como resultado das respostas iniciais:

Qual é o significado de preservação?

a) O significado muda quando é aplicado em formato eletrônico em vez de papel?

As estratégias atuais para preservação de registros eletrônicos garantirão longevidade e autenticidade?

Quais os custos da preservação de registros eletrônicos? Modelo de custo efetivo foram desenvolvidos?

Metodologia: método de modelagem

A Força-tarefa de Preservação desenvolveu um Modelo Funcional seguindo o método de Definição de Integrada prescrito pelo InterPARES.O IDEF (0)[81] é um modelo estruturado para representação de funções, de atividades ou de processos dentro de sistemas, que inclui entidades.

Três tipos de entidades entram neste processo: Entradas (I), que são transformadas ou consumidas no processo; os Controles (C), que administram sua execução; e os Mecanismos (M), necessários para executá-los. Apenas um tipo de entidade sai deste processo, as Saídas

[81] Definição de Integração para Função e Modelagem. Nos documentos da ala desta Força-tarefa, no *site* da InterPARES 1, encontram-se todos os modelos, que são compostos por diagramas. Não se tem o intuito aqui de descrevê-lo; apenas dar seu significado neste trabalho. Sua exposição não é diferente das entidades do Modelo OAIS, sua ideia baseia-se em um fluxo semelhante.

(O), que são produzidas pela atuação nas entradas sob condições e restrições impostas pelos controles.

O processo descrito no Modelo Preservar Registros Eletrônicos[82] começa com a transferência de documentos de seu criador ao preservador, que tem responsabilidades mais amplas do que o próprio processo de preservação. Presume-se, por exemplo, que o preservador é o responsável pela seleção dos registros a serem preservados. No Modelo, o ponto de vista é literal e estritamente o de "a pessoa responsável pela preservação", que inclui garantir a transmissão de registros eletrônicos autênticos ao longo do tempo.

Embora o Modelo seja sistemático, ele não prescreve uma implementação. Em vez de definir um sistema de preservação, fornece um roteiro abrangente, preciso e coerente que instituições e pessoas possam usar na concepção, no desenvolvimento e na avaliação de sistemas que atendem aos seus requisitos, seus objetivos e suas restrições.

Resultados da pesquisa da Força-tarefa de Preservação

As respostas ao levantamento das práticas, dos planos e das pesquisas de preservação digital indicam três temas amplos. Em primeiro lugar, a percepção do que é preservação vai além do arquivo e da biblioteca. Em segundo lugar, a preservação envolve o uso de tecnologias. Terceiro, o exercício da função de preservação também será regido pelos requisitos da instituição em que esta função é realizada.

Resultados da modelagem analítica

Os critérios de avaliação de tecnologias derivam dos requisitos arquivísticos e institucionais que determinam as metas e os objetivos da preservação em atuar como controle de processo. Assim, a viabilidade enseja acessibilidade. Enquanto o *Preserve Electronic Records* não inclui ou assume custo, ele prevê a aplicação de um modelo de custo para desenvolver estratégias e planos de preservação para sua execução.

A descoberta mais fundamental da Preservação de Registros Eletrônicos foi a mudança paradigmática no seu conceito, provocando dimensões tanto na Arquivologia, quanto no campo tecnológico. Enquanto a frase "preservar um registro eletrônico" é conveniente e, sem

[82] O também chamado modelo *Preserve Electronic Records* é intencionalmente genérico. Ele identifica e descreve os processos necessários para preservar os registros eletrônicos, articula as entradas necessárias para cada processo, os controles sob os quais opera, os mecanismos necessários para realizar o processo e a(s) saída(s) produzida(s) por cada processo. O modelo define os relacionamentos entre essas entidades e processos.

dúvida, continuará a ser usada; em muitas variações é uma expressão abreviada que desmente a realidade. **Empiricamente, não é possível preservar documento digital: só se pode preservar a capacidade de reprodução do registro** (Thibodeau *et al*., 2001).

Há, inevitavelmente, uma diferença substancial entre a representação digital do registro em armazenamento e a forma como ele é apresentado para uso. É sempre necessário utilizar algum *software* para traduzir os *bits* armazenados na forma documental. Isso acarreta um risco, independentemente de quão bem os dados digitais forem protegidos, eles podem ser alterados.

Assim, em contraste às noções prevalecentes sobre a preservação de registros em cópia, o processo de preservação vai muito além de mantê-lo seguro no armazenamento. Esse processo começa com o ato inicial de captura e se estende através da reprodução documental. Para refletir uma situação empírica, esta Força-tarefa construiu o conceito de um "componente digital". Os componentes digitais não têm relação necessária com os elementos da forma documental reconhecida na análise diplomática. Em vez disso, eles são determinados, tecnologicamente, pela forma como os *bits* são armazenados e pelos métodos (*software*) que devem ser aplicados.

O processo de preservação de registros eletrônicos

Três mecanismos são necessários para realizar o processo de preservação: informação e infraestrutura de tecnologia de comunicações; instalações onde os registros eletrônicos serão armazenados e processados; e pessoas competentes para realizar o processo. A infraestrutura de tecnologia compreende *hardware*, *software* e mídia física para armazenar e processar os componentes digitais; esses mecanismos são usados em todas as atividades de preservação.

Existem duas entradas principais para execução desse processo, a primeira é transferências dos documentos selecionados. A segunda consiste em solicitações de registros ou de informações sobre eles. O processo de preservação também precisa de uma terceira entrada – informações sobre os documentos que foram selecionados para preservação, fundamentais para determinar quais métodos, tecnologias, instalações e pessoal serão necessários à organização no processo e na garantia de sua autenticidade.

O processo de preservação também produz duas saídas principais: os registros eletrônicos reproduzidos e os reproduzíveis. Um sistema de preservação produz um registro eletrônico reproduzido quando é reconstituído e apresentado dentro do próprio sistema. No entanto, em muitos casos, aqueles que desejam acessá-lo fora do sistema, fá-lo em

navegadores da *Web*. Nesses casos, o sistema de preservação pode produzir apenas o(s) componente(s) digital(is) junto com instruções sobre como reconstituir e apresentar o registro; ou seja, ele produz um registro eletrônico reproduzível.

Existem duas outras saídas derivadas do processo de preservação: um certificado de autenticidade, que atesta a autenticidade de um registro reproduzido; e as informações sobre preservação – atesta a integridade e a confiabilidade do processo de preservação em geral. Um certificado de autenticidade é produzido quando um solicitante exige evidências tangíveis de que um documento é autêntico.

Para cada corpo de registros selecionado para preservação se requer a articulação de uma estratégia de preservação[83]. Esse mecanismo atua como um controle sobre os processos de execução. Uma estratégia de preservação irá envolver requisitos de infraestrutura de tecnologia da informação específica. A gestão da preservação, portanto, inclui subprocessos para identificar e adquirir a infraestrutura tecnológica e os métodos de preservação tecnológica que serão usados na preservação dos registros.

Os métodos de preservação tecnológica usados para preservar os registros são específicos para classes de componentes digitais e controlam o seu processamento e a sua manutenção ao longo do tempo, bem com a sua reprodução; a infraestrutura tecnológica permite a execução desses métodos. Por exemplo, uma estratégia de preservação pode prescrever que, no caso de registros textuais, que sua aparência visual é crítica para autenticidade, esses serão preservados como imagens em *bitmap*. Métodos de preservação usados para implementar tal estratégia incluiria *software* para converter registros textuais de outros formatos, como arquivos de processamento de texto para *bitmaps*.

Uma estratégia de preservação também define ações específicas que devem ser realizadas em relação ao corpo de registros, seja em momentos especificados, como quando os registros são trazidos pela primeira vez para o sistema de preservação, ou sob condições específicas, como quando a mídia em que o componente digital precisa ser substituído. Cada processo de execução deve produzir informações sobre si mesmo e sobre os resultados alcançados na sua execução que seja apropriada e adequada para permitir que a gestão determine se uma estratégia de preservação foi bem-sucedida e, se não, qual ação corretiva é necessária.

Por fim, a base para o conteúdo do Modelo de Processo de Preservação foi

[83] A estratégia de preservação engloba um conjunto de regras ou procedimentos para o processamento dos registros em cada uma das atividades de execução; critérios para determinar se cada processo definido na estratégia é executado corretamente e atinge o resultado desejado; além da tecnologia específica e métodos que serão usados para preservar os registros para sua reprodução.

fundamentada na norma padrão ISO OAIS. À época, estava sendo desenvolvida, ao mesmo tempo em que a Força-tarefa de Preservação criava seu protótipo. o modelo OAIS tem um escopo muito mais amplo do que o *Preserve Electronic Records*, ou seja, pode ser aplicado a qualquer tipo de informação.

7.1.4 Relatório da Força-tarefa de Estratégia

O objetivo desta Força-tarefa foi definir os princípios para o desenvolvimento de estratégias e de padrões internacionais à preservação a longo prazo de registros eletrônicos autênticos, bem como os critérios para as suas políticas. Presidido pelo diretor do Projeto, seus membros foram os presidentes dos três primeiros domínios: de autenticidade, de avaliação e de preservação; um especialista em questões legais e políticas (Jason Barão); e um especialista em padrões, especialmente aqueles relacionados a direitos autorais (Sharon Farb).

A estrutura intelectual desenvolvida aqui deriva da síntese das conclusões das Forças-tarefa anteriores. O plano de pesquisa original do InterPARES identificou três questões que deveriam ser abordadas dentro do Domínio 4:

- Quais princípios devem orientar a formulação de políticas internacionais, estratégias e padrões relacionados à preservação a longo prazo de registros eletrônicos autênticos?
- Quais devem ser os critérios para o desenvolvimento de políticas, de estratégias e de padrões nacionais?
- Quais devem ser os critérios para o desenvolvimento de políticas organizacionais, estratégias e padrões?

A distinção entre políticas[84] (internacional, nacional e organizacional), estratégias[85] e padrões[86] derivam do reconhecimento de seu *lócus*. Em cada caso, sua articulação refletirá a síntese dos requisitos de arquivamento para registros eletrônicos autênticos. Este documento fornece um quadro para a articulação de políticas, de estratégias e de padrões, garantindo que sejam bem fundamentados e consistentes.

[84] Declaração formal de direção ou orientação sobre como uma organização executará seu mandato, funções ou atividades, motivadas por determinados interesses ou programas.
[85] Complexo de práticas formalmente articuladas por uma entidade para atingir um propósito específico, que é um plano ou um roteiro para implementação de políticas.
[86] Complexo de normas estabelecidas com o objetivo de tomar a característica de um produto, processo ou serviço uniforma dentro ou através de um setor, país ou sistema.

O desenvolvimento da estrutura intelectual

Frameworks são mapas compartilhados para o avanço da compreensão e da implementação de conceitos, de ideias e de questões. Estruturas intelectuais são usadas para modelar conceitos. Seu principal objetivo é servir de modelo de um instrumento de compreensão.

A Força-tarefa de Estratégia desenvolveu a estrutura intelectual por meio da análise e síntese de resultados do trabalho nos três primeiros Domínios do InterPARES. Tomando esses resultados como seus dados, articularam princípios e critérios para a formulação de políticas, de estratégias e de padrões. Essa estrutura refletiu uma colaboração multidisciplinar entre as equipes de pesquisa internacionais e nacionais.

Com base no trabalho realizado por Lal Verman, relacionado ao desenvolvimento de um modelo lógico de padronização e Yesha Y. Sivan, direcionado ao desenvolvimento de uma estrutura de cinco dimensões para o desenvolvimento de padrões, este Domínio projetou uma estrutura intelectual que pode ser usada por órgãos internacionais e nacionais, e organizações individuais.

Uma estrutura intelectual não pretende ser uma ferramenta para desenvolver teoria; em vez disso, pode ser usada para promover e comunicar uma compreensão compartilhada dos principais conceitos, problemas e soluções propostas relacionadas à preservação a longo prazo de registros eletrônicos autênticos. Esse esquema possui três dimensões: propósito, princípios e critérios.

As investigações do projeto InterPARES projetou um conjunto de 14 princípios e critérios correspondentes ao desenvolvimento de políticas, de estratégias e de padrões. Assim, qualquer política, estratégia ou padrão de preservação de registros deve atender aos princípios e aos critérios estabeleciso no Quadro 9.

Quadro 9 – Estrutural intelectual da Relatório da Força-tarefa de Estratégia

Princípios	Critérios
1. endereçar registros específicos, ao invés de objetos digitais em geral; ou seja, deve-se abordar os documentos feitos ou recebidos e reservados no decorrer da atividade prática	Um registro se distingue de outros objetos digitais em virtude de possuir uma forma fixa, um conteúdo estável, um vínculo com outros registros, e um contexto identificável. Ele participa ou apoia uma ação e pelo menos três pessoas estão envolvidas em sua criação (um autor, um escritor e um destinatário).
2. Foco em registros eletrônicos autênticos.	Um registro eletrônico é aquele que afirma ser o que é e está livre de adulteração ou corrupção. Assim, comprovar sua autenticidade envolve estabelecer: identidade e demonstrar sua integridade com base nos Requisitos de Referência e de Linha de Base. Quando nos referimos a um registro eletrônico, consideramos essencialmente completo e não corrompido se a mensagem de que é destinada a se comunicar a fim de alcançar seu propósito é inalterada.
3. Reconhecer e prever o fato de que a autenticidade corre risco quando os registros são transmitidos através do espaço (quando enviado entre pessoas, sistemas ou aplicativos) ou tempo (tanto quando eles são armazenados *offline*, ou quando o *hardware* ou o *software* usado para processar, comunicar ou mantê-los é atualizado ou substituído).	Os registros eletrônicos são mais suscetíveis à adulteração e à corrupção do que os tradicionais. Um sistema pode ser projetado para que, uma vez arquivado, o registro nunca fica fora dele: os usuários obtêm acesso apenas às cópias. No entanto, tais controles só são eficazes dentro dos limites de um sistema. Quando um registro é retirado dele, ou quando o próprio sistema é modificado, o documento está em risco.
4. Reconhecer que a preservação de registros eletrônicos autênticos é um processo contínuo que começa com o processo de criação de registros e cujo objetivo é transmiti-lo através do tempo e do espaço.	Esse processo é definido como "cadeia de preservação", ou seja, um sistema de controle que se estende ao longo do todo o ciclo de vida dos registros, garantindo sua identidade e integridade em qualquer ação. O que se realça pelos Requisitos *benchmark* e de Linha de Base.
5. Basear-se no conceito de confiança para os registros, assim como os de manutenção e preservação, destacando, para isso o papel do preservador como um custodiante confiável.	Os registros devem ser feitos e mantidos em um sistema de manutenção de registros confiável e preservado por um custodiante de confiança. Um sistema confiável de manutenção de registros compreende o conjunto das regras que controlam a criação, a manutenção e o uso dos registros pelo criador, fornecendo uma circunstancial probabilidade da autenticidade dentro de um sistema. Para ser considerado um guardião de confiança, o preservador deve demonstrar que não tem razão para alterar os registros preservados ou permitir que outrem os faça, sendo capaz de implementar de todos os requisitos básicos.
6. Ser baseado no entendimento de que não é possível preservar um registro eletrônico como um objeto físico armazenado: só é possível preservar a capacidade de reproduzir o registro.	Reproduzir um registro eletrônico significa ser capaz de renderizá-lo com o conteúdo e qualquer elemento da forma documental, acrescido de anotações que tal registro possuía antes da reprodução.
7. Reconhecer que os componentes físico e intelectual de um registro eletrônico não, necessariamente, coincidem e que o conceito componente digital é diferente do de forma documental.	Um componente digital é diferente de um elemento da forma documental com base no fato de que o primeiro é um objeto digital que contém todo ou parte do conteúdo de um registro e/ou dados ou metadados necessários para ordenar, estruturar ou manifestar o conteúdo, por meio de métodos específicos de preservação. No contraste, elementos extrínsecos e intrínsecos da forma documental são as características de um registro que constituem sua aparência externa e transmitem sua ação.

8. Especificar que os requisitos de uma cópia de um registro devem ser considerados equivalente a um original.	Em princípio, um registro eletrônico original é o primeiro registro completo e efetivo. No entanto, em um ambiente eletrônico, se nenhum original sobreviveu? Cada cópia fiel do conteúdo de tal registro e de sua forma documental deve ser considerada uma cópia em forma de original, que equivale ao original quanto às suas consequências. Qualquer tipo de cópia que é declarada autêntica por um oficial confiado a tal responsabilidade também é equivalente ao original.
9. Integrar a avaliação de registros no contínuo processo de preservação.	Os registros devem ser selecionados para longo prazo na preservação com base em seu valor contínuo, na avaliação de sua autenticidade e na viabilidade de sua preservação.
10. Integrar a descrição arquivística no contínuo processo de preservação.	A descrição arquivística deve servir como um coletivo para comprovação da autenticidade dos registros e seus relacionamentos contextuais.
11. Declarar explicitamente que todo o processo de preservação deve ser completamente documentado como um meio primário para proteger e avaliar autenticidade a longo prazo.	Para apoiar a afirmação da autenticidade de registros eletrônicos, o preservador deve documentar, no mínimo: as práticas para apoiar a presunção de autenticidades, de acordo com os requisitos de *benchmark*; os processos de manter os registros ao longo do tempo e sua reprodução com os Requisitos de Linha de Base para a produção de cópias autênticas.
12. Reconhecer explicitamente que o princípio tradicional que todos os registros se basearam no habitual e curso normal de negócios pode ser a presunção de autenticidade.	Além da evidência de que foram criados e usados no seu curso normal, os registros devem ser presumidos autênticos com base nos critérios listados com referência nos requisitos da Força-tarefa de Autenticidade ou verificado como autêntico pelo preservado.
13. Reconhecer que o preservador está preocupado tanto com a avaliação quanto à manutenção da autenticidade dos registros eletrônicos. A avaliação da autenticidade dos registros eletrônicos ocorre antes que os registros sejam transferidos para a custódia do preservador como parte do processo de avaliação; enquanto a manutenção da autenticidade das cópias dos registros eletrônicos ocorre, uma vez que eles tenham sido transferidos para a custódia do preservador como parte do processo de preservação a longo prazo.	Na avaliação da autenticidade do sistema eletrônico, os registros devem ser baseados no *benchmark*, enquanto a manutenção da autenticidade das cópias dos registros eletrônicos deve basear-se nos Requisitos de Linha de Base.
14. Traçar uma distinção clara entre a preservação da autenticidade dos registros e a autenticação de um registro.	A autenticação é uma declaração de autenticidade um registro em um momento específico por uma pessoa jurídica a quem foi confiada a autoridade para fazer tal declaração. Tem a forma de uma declaração oficial, que pode ser por palavras ou símbolos, adicionado no registro, atestando que o registro é autêntico.

Fonte: Duranti *et al.* (2001).

O Projeto InterPARES 1 foi executado por um grupo internacional e multidisciplinar que conduziu investigações no contexto de unidades de pesquisa trabalhando separadamente. No entanto, o desenvolvimento dessa estrutura intelectual foi inestimável para testar a coerência real dos três relatórios finais sobre autenticidade, avaliação e preservação,

fornecendo uma base abrangente na garantia e na consistência à preservação de registros eletrônicos autênticos.

7.2 O PROJETO INTERPARES 2: A EXPERIÊNCIA INTERATIVA E DINÂMICA

O Projeto InterPARES 2 teve como objetivo desenvolver e articular conceitos, princípios, critérios e métodos, como forma de garantir a criação e a manutenção de registros confiáveis e a preservação digital a longo prazo no contexto de atividades artísticas, científicas e governamentais que são realizadas usando tecnologia de computador experiencial, interativa e dinâmica.

Como continuação da primeira versão, esta fase demandou, circundando os anos de 2002-2007, uma equipe colaborativa multi e interdisciplinar, aplicando uma abordagem multimétodo ao desenvolvimento de conceitos, de processos e de ferramentas para ajudar a garantir um ambiente protegido e duradouro aos documentos autênticos.

Acadêmicos em artes e ciências, arquivistas, especialistas de tipos diferentes de instituições e representantes governamentais de todo o mundo convergiram para enfrentar o desafio apresentado pela manipulabilidade e incompatibilidade de sistemas digitais.

O InterPARES 2, de o início, debruçou-se sob duas questões já identificadas no Projeto 1: a constatação de que a preservação dos documentos arquivísticos digitais se inicia na produção e que esses documentos podem ser experienciais, interativos e dinâmicos; e a outra questão se relaciona ao *eletronic record*, que passou a ser chamado de *digital record* no contexto do InterPARES 2 e 3 (Innarelli, 2015). O termo *record* foi protuberante por ser alvo de estudos, o qual possuindo um entendimento conceitual e epistemológico, difere dependendo do seu contexto.

> O InterPARES 1 teve suas raízes epistemológicas nas ciências humanas, especificamente na diplomática e na arquivística. Em contraste, o InterPARES 2, embora planejando como uma parte de sua pesquisa para testar alguns dos resultados do InterPARES 1 em uma variedade de configurações aplicadas, não abraçou nenhuma perspectiva epistemológica ou definições intelectuais a priori. Em vez disso, os pesquisadores em cada grupo de trabalho identificaram a(s) perspectiva(s), o desenho da pesquisa e os métodos que eles acreditavam ser os mais apropriados para sua investigação. A razão para essa abertura foi que o InterPARES 2 foi concebido para funcionar como um ambiente de 'conhecimento em camadas' (InterPARES 2 Project, 2002, p. 1).

Diversos países participaram desta edição: Canadá, Irlanda, França, Bélgica, Austrália, EUA, Holanda, Singapura, China, Itália, Reino Unido e África do Sul; todos os continentes foram envolvidos. Vale destacar, também, a participação de duas pesquisadores brasileiras: Claudia Lacombe, do Arquivo Nacional, e Rosely Curi Rondinelli, da Fundação Cada de Rui

Barbosa (Innarelli, 2015).

A estrutura intelectual do Projeto dividiu-se em três focos de investigação, cada um abordando os registros criados no decorrer de um tipo de atividade. O Foco 1 estudou os registros de atividades artísticas; o Foco 2 estudou os registros de atividades científicas; e o Foco 3 estudou registros de atividades governamentais. Além disso, desenvolveu quatro Domínios, são eles:

a) A Terminologia *Cross-domain*, que controla o uso de termos e de definições relacionados a todas as áreas de pesquisa;
b) O *Cross-domain Policy*, que analisa as políticas, as estratégias e as diretrizes para criação, manutenção e preservação de registros digitais e desenvolve novos conforme necessário;
c) A Descrição *Cross-domain*, que examina esquemas descritivos em cada disciplina envolvida no Projeto e desenvolve novos capazes de apoiar a criação, a manutenção e a preservação a longo prazo de registros digitais precisos, confiáveis e autênticos;
d) O *Modeling Cross-domain*, que articula as funções, as informações e os recursos envolvidos na criação, na manutenção e na preservação de registros digitais precisos, confiáveis e autênticos, apoiando a representação e a análise dos resultados dos estudos de caso.

Figura 32 – Estrutura intelectual do InterPARES 2

	FOCUS 1 **Artistic activities**	**FOCUS 2** **Scientific activities**	**FOCUS 3** **Governmental activities**
DOMAIN 1 **Records creation & maintenance**	**Working Group 1.1** Creation and Maintenance of Artistic Records	**Working Group 1.2** Creation and Maintenance of Scientific Records	**Working Group 1.3** Creation and Maintenance of E-Government Records
DOMAIN 2 **Authenticity, accuracy & reliability**	**Working Group 2.1** Accuracy, Reliability, Authenticity of Artistic Records	**Working Group 2.2** Accuracy, Reliability, Authenticity of Scientific Records	**Working Group 2.3** Accuracy, Reliability, Authenticity of E-Government Records
DOMAIN 3 **Methods of appraisal & preservation**	**Working Group 3.1** Appraisal and Preservation of Artistic Records	**Working Group 3.2** Appraisal and Preservation of Scientific Records	**Working Group 3.3** Appraisal and Preservation of E-Government Records

Terminology Cross-domain

Policy Cross-domain

Description Cross-domain

Modeling Cross-domain

Fonte: http://www.interpares.org/ip2/ip2_intellectual_organization.cfm.Acesso.

- **Domínio 1 (produção e manutenção dos documentos arquivísticos no contexto das atividades artísticas, científicas e governamentais):** a Força-tarefa deste Domínio investigou os conceitos centrais relativos aos registros e aos processos de sua criação e manutenção, mas, para isso, desenvolveu questionários. Embora os estudos de caso tenham sido conduzidos no contexto do Domínio 1, os dados coletados foram relevantes para o trabalho de todos os três domínios. A análise diplomática também foi necessária, sendo usada para descrever os elementos formais dos documentos e seu processo de criação e para identificar as informações que precisavam ser preservadas. Os resultados desta pesquisa foram: questionários, visões gerais de estudos de caso, modelos para análise, modelos de entidade e de atividade, fluxos de trabalho e declarações de metodologia.
- **Domínio 2 (os conceitos de confiabilidade, precisão e autenticidade):** testou a aplicabilidade dos conceitos arquivísticos de confiabilidade, de precisão e de autenticidade. Os grupos de trabalho, aqui, pesquisaram a literatura de cada disciplina e se basearam na pesquisa de estudo de caso para formar uma compreensão do significado dos termos citados em cada área. A partir desse entendimento, foi elaborada uma teoria dos processos dos registros e manutenção. Modelos de atividades de alto nível desenvolveram-se, no intuito de refletir semelhanças e variações nesses processos. Tiveram como resultados: artigos acadêmicos, discutindo os significados dos conceitos em questão, comparando-os e reconciliando-os; outros artigos acadêmicos, apresentando uma teoria de registro confiável; e, por fim, “As Diretrizes para os Criadores de Registros”, descrevendo métodos para a produção confiável e manutenção de registros que podem ser preservados autenticamente (essas Diretrizes foram traduzidas para o francês, espanhol, catalão e português).
- **Domínio 3** (**os métodos de avaliação e de preservação):** usou o conhecimento adquirido no curso dos estudos de caso para testar a aplicabilidade das diretrizes de avaliação e preservação propostas pelo InterPARES 1. A metodologia foi a de prototipagem rápida, que permite aos projetistas de sistemas implementar requisitos conforme articulado por usuários em potencial. Posteriormente, o desenvolvimento de cada sistema testou a viabilidade das diretrizes em etapas, permitindo modificações quando necessárias. Os resultados foram: protótipos de sistemas de avaliação e de preservação, modelos de atividades e as Diretrizes para

Preservadores de Registros (esta última, também traduzida para o francês, espanhol, catalão e português).

- **Descrição *cross-domain:*** deu-se por pesquisar questões relacionadas às regras e aos requisitos de apresentação e de manutenção dos metadados de confiabilidade e de autenticidade na preservação de documentos arquivísticos digitais autênticos. A *Description cross-domain* aplicou vários métodos na condução das seguintes atividades: análise de garantia literária, mapeamento de metadados, modelagem conceitual, modelagem de atividades, metamodelagem e instanciação empírica. Seus resultados serviram para o desenvolvimento de um esquema de metadados de registros e especificações de ferramentas automatizadas, além de um esboço para Modelo de Cadeia de Preservação.
- **Políticas entre Domínios:** as primeiras tarefas da *Policy cross-domain* foram pesquisar e analisar as políticas, as estratégias, as diretrizes e os padrões existentes em cada uma das áreas de Foco em relação aos Domínios – examinar como eles podem ser aplicados aos ambientes digitais sob investigação; reconhecer pontos em comum e identificar lacunas, principalmente, em relação às novas questões decorrentes da acessibilidade, do uso, da manipulabilidade e da fragilidade dos tipos de documentos. Posteriormente, investigou os resultados dos estudos de caso e do trabalho realizado nos três domínios.
- **Terminologia entre domínios:** criou ferramentas terminológicas – glossário, dicionários, tesauro, banco de dados, ontologias de registros.
- **Modelagem entre vários domínios:** o *Modeling cross-domain* investigou várias técnicas, incluindo as já desenvolvidas no InterPARES 1, ficando escolhida o IDEFØ como a principal técnica de modelagem para o Projeto. Usando IDEFØ, os modelos do projeto UBC-DoD (Universidade de British Columbia e Departamento de Defesa dos EUA) e o InterPARES 1 foram integrados em um Modelo Unificado (MU). Os resultados mais significativos foram dois projetos de consulta de modelos unificados em IDEFØ:
    a) O Modelo de Cadeia de Preservação, que é um modelo de "ciclo de vida de registros" baseado na perspectiva da entidade responsável pela preservação de longo prazo de registros digitais;
    b) O modelo BDR (*Business-Driven Recordkeeping*), que é um modelo de "registros contínuo" baseado na perspectiva da entidade criadora.

A partir das informações acima, o relatório final do InterPARES 2[87] foi composto de oito partes, com vinte e três apêndices, bibliografia e glossário. Sintetizam-se aqui as oito partes como forma de um entendimento geral, pois a intenção não é pormenorizá-las, e sim encabeçar suas ideias para fins desta tese.

Parte 1 (Relatório da Força-tarefa Focal) – Casos e fundamentação teórica no contexto das atividades artísticas, científicas e governamentais

Este primeiro relatório teve gênese nas bases teóricas e na contextualização dos demais grupos de trabalho formados para pesquisar o foco e o domínio de sua competência. Subdividida em outras três Forças-tarefas, estudou as atividades artísticas, científicas e governamentais, nas quais cada uma responsabilizou-se por sub-relatórios, são elas: a Força-tarefa Foco 1 (estudo dos documentos arquivísticos digitais advindos das atividades artísticas); a Força-tarefa foco 2 (estudo dos documentos arquivísticos digitais advindos das atividades científicas); e a Força-tarefa Foco 3 (estudo dos documentos arquivísticos digitais advindos das atividades governamentais).

O Foco 1 teve a participação de 52 especialistas de diversas áreas das atividades artísticas (dança, música, cinema, e outras), das TICs, da História e da Arquivologia e limitou-se a estudar os documentos arquivísticos digitais. Sua conclusão delimitou que o uso das tecnologias digitais permite uma nova forma de expressão artísticas, visto que novas mídias podem ser incorporadas em um mesmo processo de criação e produção artísticas, assim como podem ser disseminadas rapidamente. Isto quer dizer que o uso das tecnologias digitais muda de forma significativa a produção, a manutenção e a preservação das produções artísticas. Analogamente, tem-se a fotografia que utilizava recursos analógicos de produção e guarda, atualmente, detém recursos digitais de produção e guarda.

O Foco 2 contou com a participação de 42 especialistas nas atividades científicas, enfatizando a área da Geografia, da Ciência da Computação, das TICs, da Física e da Arquivologia, limitando-se a estudar os documentos arquivísticos produzidos por essa atividade. A conclusão desse relatório foi trazida pelo benefício que as TICs trouxeram à comunidade científica, uma vez que o processamento das informações se torna cada vez mais

[87] O relatório final do InterPARES 2 é composto por um livro com mais de 800 páginas. Devido a essa exaustão para esta tese, utiliza-se, como base para explanar as oito partes mencionadas, os escritos de Innarelli (2015), única tese na BDTD que se debruçou sobre o Projeto InterPARES até o presente momento. Optou-se por não pormenorizar esse relatório, pois não é o intuito deste estudo, mas sim, trazer as principais ideias sobre os meandros metodológicos e conceituais da preservação digital. Diferentemente de como acontecido no Projeto 1, que se esmiuçou, veementemente, nos conceitos estudados neste trabalho.

rápido e disseminável além das fronteiras; sem contar com a crescimento exponencial de sua capacidade de armazenamento.

O Foco 3 contou com a participação de 255 especialistas das atividades governamentais, priorizando as iniciativas de governos eletrônicos, de arquivos públicos e de arquivos universitários, limitando a estudar os documentos arquivísticos digitais dessa atividade. Esse estudo concluiu que, à medida que os sistemas informatizados são desenvolvidos e a cultura do "ser digital" é implementada, no sentido do acesso rápido e remoto, a tecnologia cumpre seu papel primordial: o da acessibilidade. As análises feitas neste foco serviram de base para o desenvolvimento dos relatórios das demais forças-tarefas do InterPARES 2.

Parte 2 (Relatório da Força-tarefa do Domínio 1) – Criação e manutenção dos documentos arquivísticos digitais no contexto das atividades artísticas, científicas e governamentais

Como já explicitado acima, o objetivo do Domínio 1, foco desta parte 2, criou um modelo para análise dos estudos (apêndice 10 do InterPARES 2) com o intuito de identificar os pontos comuns e as divergências dos estudos de casos e os estudos gerais. Esse modelo resultou em relatórios parciais para cada uma das atividades. A distribuição dos estudos gerais e de caso em relação às atividades artísticas, científicas e governamentais é mostrada na Figura 33.

Figura 33 – Estudos gerais e de caso do InterPARES 2

Status	Total	Type	Arts	Sci	Govt
Private	8	Individual	2	0	0
		Corporation	3	1	2
Public	11	Government	0	1	6
		Agency	2	1	0
		Cultural Center	1	0	0
Mixed	4	Partnerships	2	2	0

Fonte: Innarelli (2015, p. 193).

Assim, o *Status*: significa definição de categoria dos documentos; o Total: quantidade de documentos da categoria; o *Type*: tipo do produtor do documento; *Arts Sci e Govt*: atividades artísticas, científicas e governamentais.

Com base nos relatórios parciais, realizou-se uma análise comparativa entre os dois

estudos; o objetivo foi o de determinar os limites das pesquisas e identificar padrões na produção/criação e manutenção dos documentos arquivísticos digitais. A partir da análise das respostas com a aplicação do questionário e do preenchimento do modelo para análise dos estudos gerais e de caso foi possível produzir um documento que sintetizou as práticas de produção, de manutenção, os esquemas de metadados e a tecnologia utilizada pelos produtores dos documentos em cada estudo.

Parte 3 (Relatório da Força-tarefa do Domínio 2) – Autenticidade, confiabilidade e precisão dos registros digitais nos setores artísticos, científico e governamental

A Força-tarefa do Domínio 2 já explicou questões relativas à autenticidade e à confiabilidade dos documentos arquivísticos digitais sob à óptica do InterPARES 1, que teve como desenvolvimento o guia com a diretiva do documento "Diretrizes do Produtor"[88] traduzido, por sua importância, pela CTDE do Conarq, mostrando a preocupação com os documentos de valor primário.

Para o campo desta Força-tarefa, foram desenvolvidas quatro questões aplicadas aos diversos grupos responsáveis pelos estudos gerais e de caso. A pesquisa aqui, enfatizou que, diferente do Projeto InterPARES 1, o InterPARES 2 não foca somente nos documentos arquivísticos digitais considerados ideais, mas nos complexos, os quais podem ser produzidos em decorrência de variadas atividades, como as que foram abordadas nos estudos gerais e de caso relacionados aos três focos propostos. Uma de suas conclusões está relacionada ao fator da obsolescência tecnológica; na falta de procedimento confiável na produção dos documentos, na documentação insuficiente e na incerteza sobre quais documentos devem ser preservados.

Depois dessa análise, foi possível constatar que o setor governamental é o menos complexo em relação à manutenção e à preservação de documentos arquivísticos digitais, pois a padronização dos processos, das atividades e dos documentos impostos pela burocracia, pela organicidade e pela legislação, interferem diretamente na classificação, na organização e na temporalidade dos documentos. Outro aspecto a citar se dá pela forma diferenciada de compreensão que cada instituição possui acerca dos conceitos de confiabilidade, de exatidão/precisão e de autenticidade.

[88] Esta diretiva encontra-se nas publicações técnicas das resoluções do Conarq, englobando em um único documento as "Diretrizes do Produtos e do Preservador".

Parte 4 (Relatório da Força-tarefa do Domínio 3) – Métodos de avaliação e de preservação dos documentos arquivísticos digitais

Um dos destaques deste relatório foi a confecção do guia "Diretrizes do Produtor" também traduzido pela CTDE.

> A principal questão a ser respondida pelo Domínio 3 é se os documentos arquivísticos digitais pesquisados pelo projeto InterPARES 2 – experienciais, interativos e dinâmicos – sugerem a necessidade de novos critérios de avaliação ou inclusão de práticas de avaliação durante o ciclo vital do documento arquivístico digital e desenvolvimento de novas estratégias e práticas de preservação. Ao considerar esta questão, foram formuladas quatro outras questões, as quais foram pesquisadas nos estudos gerais e de caso, a saber: 1 – Como os conceitos de avaliação, os métodos e os modelos desenvolvidos no projeto InterPARES 1 para os documentos arquivísticos digitais administrativos e jurídicos, produzidos a partir de bancos de dados e sistemas informatizados, podem ser aplicados na avaliação dos documentos relacionados às atividades artísticas, científicas e governamentais? 2 – Como os conceitos de preservação, os métodos e os modelos desenvolvidos no projeto InterPARES 1 para os documentos arquivísticos digitais administrativos e jurídicos, produzidos a partir de bancos de dados e sistemas informatizados, podem ser aplicados na preservação dos documentos arquivísticos digitais relacionados às atividades artísticas, científicas e governamentais? 3 – Quais paradigmas da preservação podem ser aplicados nas atividades e tecnologias? Quais paradigmas de preservação são necessários para cada tipo de documento? 4 – Quais metadados são necessários para apoiar a avaliação e a preservação dos documentos arquivísticos digitais autênticos? (Innarelli, 2015, p. 203).

Os pesquisadores, a partir das indagações acima, criaram uma metodologia de pesquisa capaz de avaliar os estudos gerais e de caso a partir de perguntas e respostas sobre os sistemas informatizados de cada instituição. Com a aplicação desse método foi possível avaliar a consistência da metodologia de análise dos sistemas informatizados e dos ambientes de preservação digital nos três contextos analisados. Os resumos e os relatórios de aplicação estão disponíveis para consulta no *site*[89] do projeto InterPARES 2.

O resultado dessa pesquisa mostrou que a maioria dos produtores de documentos arquivísticos digitais, com exceção do setor governamental, não possui ou mesmo desconhece as questões relacionadas à preservação de longo prazo.

No que se refere às atividades artísticas, sua produção, muitas vezes, está ligada ao *hardware* utilizado e as estratégias de preservação. Uma questão problemática apontada foi como a digitalização dos documentos é realizada durante a análise dos estudos gerais e de caso. As instituições utilizam a digitalização em função da falta de espaço físico e da dificuldade de acesso rápido. Para muitas delas, a digitalização é considerada uma forma de acesso e de preservação das informações contidas nos documentos que possivelmente serão

[89] Disponível em: http://www.interpares.org/ip2/ip2_index.cfm.

eliminados, propositalmente ou pela ação do tempo (Innarelli, 2015).

Por fim, destaca-se que existia uma cultura de que alguns produtores passavam a responsabilidade da preservação para outras pessoas ou instituições, os que nem sempre tinham condições ou conhecimento para realizar tal ação.

Parte 5 (Modelando Relatório da Força-tarefa de Domínio Cruzado) – Modelo de produção, manutenção e preservação de documentos arquivísticos digitais

Esta Força-tarefa desenvolveu dois modelos de preservação, são eles: Modelo da Cadeia de Preservação (MCP) e Modelo de Gerenciamento das Diretrizes de Negócio na Gestão de Documentos (MGDN). Os dispositivos apresentados são referências para o desenvolvimento de sistemas informatizados que fazem a manutenção e a preservação de documentos, porém, devem ser adaptados à realidade das instituições, independentemente do setor ou da tecnologia utilizada.

O MCP, utilizando ferramenta das TICs para desenvolver sistemas informatizados, detalha os processos, as entradas e as saídas necessárias para a produção, a manutenção e a preservação dos documentos arquivísticos digitais. Esse Modelo consiste em uma série de diagramas que descrevem as atividades envolvidas na manutenção do ciclo vital do documento arquivístico digital. Seu objetivo foi unificar os três modelos preexistentes[90] em um único modelo que retratasse todas as funções relativas ao ciclo vital dos documentos, garantindo, dessa forma, a manutenção e a preservação dos documentos desde sua produção.

O escopo do MCP considera todas as fases do ciclo vital do documento arquivístico digital, tendo em vista a garantia da autenticidade, da exatidão e da confiabilidade dos registros gerenciados. Já o MGDN traz o gerenciamento dos documentos em um contexto mais amplo: jurídico, econômico, organizacional e cultural. Assim, leva em consideração que os documentos para o cumprimento de suas atividades devam ser preservados a longo prazo por interesses sociais e históricos.

Parte 6 (Relatório da Força-tarefa entre Domínios) – Pesquisa sobre regras e requisitos de apresentação e de gestão dos metadados de confiabilidade e de preservação de documentos arquivísticos digitais autênticos

[90] O modelo desenvolvido no âmbito do projeto da UBC, intitulado A Preservação da Integridade dos Documentos Arquivísticos Eletrônicos e modelos desenvolvidos no projeto no âmbito do InterPARES 1, intitulados Modelo Funcional de Avaliação e Modelo Funcional de Preservação.

As atividades executadas neste relatório permitiram o desenvolvimento do Padrão de Metadados, Descrição Arquivística de Documentos e Sistema de Análise (Madras), resultando em quatro objetivos básicos: dar suporte ao registro de metadados; apoiar a análise dos registros de metadados; padronizar a estrutura de metadados e produzir dados analíticos para o grupo que desenvolve o padrão ISO 23081.

Esse padrão foi desenvolvido utilizando a tecnologia XML-DTD para estruturação dos metadados. Sua escolha veio à tona por ser de fácil compreensão na implementação de sistemas informatizados abertos. Seu propósito é reforçar a ideia de que os metadados fazem parte do processo de preservação dos documentos arquivísticos digitais (Innarelli, 2015).

A maior parte das informações deste domínio é detalhar o Madras, apresentando sua metodologia de desenvolvimento, seus fundamentos teóricos e práticos, seus metadados, suas aplicações e as tecnologias utilizadas por ele.

Parte 7 (Relatório da Força-tarefa de Política Cruzada) – Relação entre os produtores e os preservadores dos documentos arquivísticos digitais

O principal objetivo aqui foi estabelecer o relacionamento entre cada Domínio e cada Foco, apresentando princípios que orientam o desenvolvimento de políticas, de estratégias e de normas para produção, manutenção e preservação dos documentos.

Como produto, foi gerado um trabalho intelectual compreendendo dois princípios. O primeiro foi instrumentalizar as instituições com ferramentas e modelos que apoiam o desenvolvimento de políticas e de estratégias de preservação. O segundo ofereceu aos produtores e aos preservadores diretrizes para o desenvolvimento de políticas organizacionais que visam garantir a preservação, orientando a aplicação correta de cada um dos princípios investigados pelo Projeto InterPARES.

Um dos primeiros trabalhos realizados nesta Força-tarefa foi um estudo teórico sobre cinco temáticas fundamentais; propriedade intelectual; privacidade e políticas de acesso livre à informação; legislação relacionada aos documentos arquivísticos; autenticidade de documentos arquivísticos e o uso de *software* de código aberto e de padrões para a preservação de documentos. Ao final do trabalho, constatou-se que poucas instituições estavam preparadas para enfrentar o desafio do digital.

As discussões feitas aqui serviram de base para a elaboração de um dos principais documentos do InterPARES 2, as “Diretrizes para Desenvolvimento de Políticas, de

Estratégias e de Padrões para Preservação de Longo Prazo de Documentos Arquivísticos Digitais".

Parte 8 – Ferramentas tecnológicas

Os vários termos e conceitos pesquisados pelas diversas Forças-tarefa e grupos de pesquisa do InterPARES estão alocados neste Domínio, cujo objetivo foi definir os termos propostos para uso oficial no âmbito do Projeto, no intuito de garantir a comunicação entre as equipes e os pesquisadores das mais variadas áreas.

O principal desafio elencado no campo da terminologia consistiu em atribuir precisão aos termos utilizados no Projeto; que envolveu uma equipe multidisciplinar e multinacional, composta por pesquisadores de 20 países.

O termo "documento arquivístico" é considerado um dos exemplos basilares do trabalho que a Força-tarefa teve, pois havia, nas diversas áreas pesquisadas, variadas formas de conceituá-lo (Innarelli, 2015). Nesse sentido, a Força-tarefa de Terminologia desenvolveu três ferramentas terminológicas: um glossário com aproximadamente 450 termos; um dicionário com aproximadamente 900 termos e um *thesaurus* com aproximadamente 1.200 termos. Um banco de dados também foi criado para dar conta das questões terminológicas do InterPARES 2.

7.3 O PROJETO INTERPARES 3: PRESERVAÇÃO EM ORGANIZAÇÃO DE PEQUENO E MÉDIO PORTE

O InterPARES 3 foi uma convergência internacional composta de várias equipes regionais, nacionais e multinacionais. O projeto foi financiado com subsídio da Alianças de Pesquisa Comunidade-Universidade (Cura) do Conselho de Pesquisa em Ciências Sociais e Humanas do Canadá, que também apoiou a Equipe (*Team*) Canadá, cujo nome deriva do título específico desta terceira fase – Elaborações Teóricas em Gestão de Arquivos (Team): implementação da teoria de preservação de documentos autênticos em sistemas digitais em organizações arquivísticas de pequeno e médio porte[91].

12 equipes estão entrelaçadas no Projeto: *Team* África; *Team* Brasil; *Team* Canadá; *Team* Catalunha; *Team* China; *Team* Colômbia; *Team* Itália; *Team* Coreia; *Team* Malásia;

[91] *Theoretical Elaborations into Archival Management* (Team)*: Implementing the theory of preservation of authentic records in digital systems in small and medium-sized archival organizations.*

Team México; *Team* Noruega e *Team* Turquia.

Desenvolvido no período de setembro de 2007 a abril de 2012, o InterPARES 3 teve como contribuição os ensinamentos das duas primeiras fases do Projeto. Seu objetivo principal foi capacitar os programas e as instituições arquivísticas de médio e pequeno porte, responsáveis pelo gerenciamento de documentos arquivísticos digitais resultantes de atividades de governo, de pesquisas artísticas e de entretenimento, sociais e comunitárias, na preservação contínua (Innarelli, 2015).

> […], uma conclusão importante, […], do InterPARES, é que, embora o corpo de conceitos, princípios e métodos desenvolvidos por meio da pesquisa científica constitua a base essencial e a estrutura das melhores práticas, qualquer solução para os problemas de preservação digital é específica para cada situação e deve ser elaborada por preservadores levando em consideração: a) o contexto cultural, administrativo, jurídico e funcional em que operam; b) a natureza e as características das organizações que produzem o material digital a ser preservado; c) a tipologia do material produzido e suas características documentais e tecnológicas; d) as limitações impostas pelos recursos financeiros e humanos disponíveis; e) a cultura organizacional tanto do produtor do material quanto do preservador; e g) acesso a profissionais qualificados ou programas e recursos educacionais. (InterPARES 3 Project, 2007, p. 14).

Os princípios metodológicos nesta fase são marcados por uma colaboração internacional multidisciplinar, aplicando uma abordagem multimétodo ao desenvolvimento de práticas, de processos e de ferramentas que ajudam garantir um ambiente protegido e duradouro para os registros digitais produzidos por arquivos de poucos recursos.

Ainda, considera, por ter um grande número de colaboradores, estudos gerais e de caso para compor seus documentos, tendo como elementos constitutivos: a interdisciplinaridade, multidisciplinaridade e transdisciplinaridade; a transferibilidade; a investigação aberta e modelo de múltiplos métodos. Todas essas características são de gênese prática, epistemológica e conceitual, isto inclui dizer, que existe a *práxis* arquivística.

Tal abordagem metodológica permitiu a expansão da comunicação do InterPARES com os países do mundo, incluindo-os nas chamadas *Teams* (responsáveis por coordenar estudos de casos em seus países), acarretando o desenvolvimento de ferramentas que garantissem um ambiente tecnológico seguro aos documentos arquivísticos digitais produzidos em instâncias de arquivos de pequeno e médio porte. Destaca-se o Brasil como país envolvido nesse processo com dez estudos de caso.

Os estudos de caso desta fase foram baseados na pesquisa-ação, caracterizada pelo conjunto de práticas materiais disciplinadas que incluem diálogo colaborativo e tomada de decisão participativa. A pesquisa-ação pode assumir a forma de investigação etnográfica ou de desenvolvimento de protótipos. Suas etapas foram:

a) **Identificação do problema** – cada parceiro de teste identificou um conjunto de materiais digitais, estando ou não sob sua custódia, para os quais um plano de retenção pudesse ser desenvolvido. Como alternativa, as *Teams* identificavam uma necessidade de política ou um sistema para projetar e implementar.
b) **Coleta de dados** – os dados foram coletados por meio de metodologias, de entrevistas, de análise diplomática e de modelagem de arquivo, a fim de compreender o contexto e os limites das equipes.
c) **Primeiras interações** – testando soluções em contextos diferentes, todos os membros das *Teams* (copesquisadores, colaboradores, bancos de ensaio e parceiros de pesquisa, alunos) refletiram sobre os dados coletados para cada estudo de caso, e articularam várias soluções possíveis, a partir das quais planos de ação surgiram e foram testados (estratégias, protocolos, requisitos funcionais, procedimentos e resultados esperados conforme necessário). Os resultados incluíram a avaliação de desempenho dos planos em relação aos *benchmarks* e aos Linhas de Base.
d) **Comparação das primeiras interações** – os resultados dos testes foram compartilhados entre todos os pesquisadores das *Teams* e analisados.
e) **Segunda interação** – essa interação leva em conta os prós e os contras registrados nos resultados dos testes, comparando os diferentes contextos. A segunda interação foi constituída de diversas mini-interações, até que se definisse um plano de ação definitivo para cada contexto.
f) **Comparação das segundas interações** – os dados foram comparados por outros semelhantes – organizações parceiras do mesmo tipo (por exemplo, arquivos estaduais, arquivos universitários, arquivos municipais) – para estabelecer quais os fatores críticos que determinaram a solução mais adequada para esses contextos e se eles estão relacionados a formas documentais, tecnologias, culturas ou funções organizacionais.
g) **Reflexão, análise e síntese** – por meio da pesquisa, copesquisadores e colaboradores formularam considerações teóricas.

A metodologia que deu suporte ao InterPARES 3 utilizou os seguintes documentos: Roteiro para análise contextual dos estudos de caso; Arcabouço intelectual; Diretrizes do produtor; Diretrizes do Preservador; Modelo para análise diplomática; Política organizacional; Roteiro de perguntas que os pesquisadores devem responder nos estudos de caso de documentos arquivísticos; Roteiro de perguntas que os pesquisadores devem responder nos estudos de caso de políticas; Roteiro de perguntas que os pesquisadores devem responder nos

estudos de caso de sistemas de gestão e Base de dados de terminologia geral e específica para cada uma das Equipes. Como conclusão, gerou-se relatórios sobre os casos analisados, que foram publicados e serviram como subsídio de conhecimento para as novas etapas do Projeto (Innarelli, 2015). Os produtos desenvolvidos no InterPARES 3 confeccionaram mais de 140 documentos, entre eles estão materiais educacionais, relatórios de pesquisa, estudos de casos e documentos diversos que deram suporte à pesquisa. Vale elencar que, dentre os produtos, onze temas se destacaram:

> I. **Documentos que dão suporte à pesquisa:** são 37 documentos distintos que dão suporte à pesquisa realizada. Por exemplo: Modelo para Análise Diplomática e Roteiro para Análise Contextual dos Estudos de Caso.
> II. **Material educacional:** são 32 documentos conceituais que auxiliam o entendimento sobre a temática. Por exemplo: Diretrizes do Preservador e Diretrizes do Produtor.
> III. ***E-mail:*** são 12 documentos que abordam as questões referentes à preservação de mensagens de correio eletrônico (*e-mail*);
> IV. **Metadados:** são 5 documentos que abordam as questões referentes ao uso de metadados nos processos de preservação digital;
> V. **Cultura organizacional:** são 12 documentos que abordam as culturas organizacionais no que diz respeito às políticas de preservação digital existentes nas instituições;
> VI. **Documentos pessoais:** são 8 documentos que abordam as questões referentes à preservação de documentos arquivísticos digitais pessoais;
> VII. **Políticas:** são 45 documentos que abordam questões relacionadas às políticas de preservação de documentos arquivísticos digitais;
> VIII. **Preservação:** são 43 documentos que estão relacionados a estudos gerais e de caso que visam à preservação digital de seus acervos digitais;
> IX. **Manutenção:** são 35 documentos que abordam questões relacionadas à manutenção dos documentos arquivísticos digitais;
> X. ***Websites:*** são 12 documentos que abordam questões referentes à preservação de *websites;*
> XI. **Base de Dados de Terminologia do InterPARES 3:** são 8 glossários e 8 dicionários produzidos em 8 línguas diferentes. (Innarelli, 2015, p. 218-219).

Esses documentos podem ser todos encontrados no sítio[92] de InterPARES 3, fomentando os casos que envolvem a realidade de cada país no Projeto.

Aqui, com o destaque à *Team* Brasil, sua coordenação ficou a cabo de Claudia Lacombe Rocha e contou a participação de vários pesquisadores, sendo capitaneado pelo Arquivo Nacional. Seus componentes dividiram-se, contando com sarquivistas e outros profissionais, em: diretoria (sete profissionais); coinvestigadores (27 profissionais); colaboradores (dois profissionais) e assistentes de pesquisa (19 profissionais). As instituições parceiras foram: Câmara dos Deputados; Ministério da Saúde; Unicamp e Sistema de Arquivos do Estado de São Paulo (Saesp).

A oportunidade de participar do Projeto nesta fase serviu para colocar em prática

[92] Disponível em: http://www.interpares.org/ip3/ip3_products.cfm?item=1.

propostas teórico-metodológicas acerca da preservação digital, além de gerar aprendizado para os servidores do Arquivo Nacional. Isto foi frutífero para os estudos arquivísticos na área e teve como materialização relatórios.

A equipe brasileira foi assídua em sua atuação e produziu um legado com: a sistematização do conhecimento produzido no Brasil sobre a temática, por meio de palestras, oficinas, seminários, encontros, reuniões, colóquios etc.; a tradução de vários documentos do Projeto InterPARES; a aplicação da metodologia dos estudos de caso em quatro instituições brasileiras; um glossário com 225 termos e um dicionário com 227 termos do InterPARES 3 em português; os relatórios dos dez estudos de caso desenvolvidos no Brasil e o relatório final do projeto no Brasil (Innarelli, 2015).

Frente a essas ponderações, destaca-se que os estudos de caso da *Team* Brasil levaram em consideração a necessidade, cada vez mais veemente, da análise diplomática dos documentos para alcançar sua confiabilidade na preservação digital, isto salienta que as instituições brasileiras necessitam estar situadas e preparadas para os novos desafios do ambiente virtual, sobretudo pela obsolescência

7.4 O PROJETO INTERPARES 4 (CONFIANÇA E CONFIABILIDADE)

O InterPARES 4, também conhecido pelo acrônimo *Trust* ou *ITrust* (2012-2019), é um projeto de pesquisa multinacional e interdisciplinar que explorou questões de confiança e de confiabilidade em documentos e dados *onlines*. Seu objetivo foi criar mapas teóricos e metodológicos para desenvolver políticas, procedimentos, regulamentos, normas e legislação locais, nacionais e internacionais, a fim de garantir a confiança pública baseada em evidências de boa governança, uma economia digital forte e uma memória digital persistente.

Contando com mais parceiros nesta edição, o Projeto abarcou mais de 50 universidades e organizações, nacionais e multinacionais, públicas e privadas, na América do Norte, América Latina, Europa, África, Australásia e Ásia (a Aliança Internacional). Os profissionais envolvidos foram da Arquivologia, da Gestão de Registros, da Diplomática, do Direito, da TI, da Comunicação e Mídia, do Jornalismo, do *E-commerce*, da Informática em Saúde, da Cibersegurança, da Governança e Garantia da Informação, da *Digital Forense*, da Engenharia da Computação e da Política de Informação.

Sua parceria formal teve sete *Team*s que se reuniam uma vez por ano em *workshops* para relatar os avanços da pesquisa, são eles: *Team* América do Norte; *Team* Europa; *Team* América Latina (do qual fez parte o Brasil); *Team* Ásia; *Team* Australásia; *Team* África e

Team Transnacional. Essas equipes regionais, contam, cada uma, com um diretor que, sob a direção do diretor de Projeto, formam o comitê de diretores internacional.

A equipe do Projeto na UBC apoiou o trabalho da Aliança Internacional como um todo; mas deu suporte, principalmente, ao trabalho da *Team* América do Norte. Os resultados alcançados pelo InterPARES 4 foram:

a) o desenvolvimento de requisitos e de especificações funcionais para sistemas digitais *online* seguros; e estruturas analíticas para avaliar modelos de negócios inovadores emergentes do ambiente da *Internet* em evolução;
b) o alcance e equilíbrio entre privacidade e acesso, sigilo e transparência, o direito de saber e o direito ao esquecimento em redes globalmente conectadas;
c) recomendações legislativas relacionadas a evidências eletrônicas, crimes cibernéticos, identidade, segurança, comércio eletrônico, propriedade intelectual, descoberta eletrônica e privacidade;
d) a autenticação adequada de identidade na *Internet* e a proteção contra fraudes;
e) o apoio a todas as facetas da propriedade intelectual: patentes, direitos autorais, marcas registradas, segredos comerciais, gerenciamento de direitos digitais, compartilhamento de arquivos, licenciamento, domínio público e convenções internacionais;
f) o fornecimento de uma base sólida para articular modelos de políticas e procedimentos e padrões para gerenciá-los;
g) o desenvolvimento de módulos de educação e de ferramentas de treinamento para profissionais; e currículos acadêmicos para programas de pós-graduação.

O *site*[93] desta versão do InterPARES está desmembrado das três primeiras etapas do Projeto. As informações contidas na sua página eletrônica são mais intuitivas, pois seus rótulos são mais sucintos e de fácil navegação, porém, nesta fase, muito dos trabalhos publicados são monetizados.

O domínio da pesquisa está distribuído em cinco temas: Infraestrutura; Segurança; Controle; Acesso; Jurídico. As subdivisões dessas temáticas são caracterizadas pelos domínios cruzados e cobre tópicos e questões de relevância em todos os cinco domínios citados, a saber: Terminologia; Recursos; Educação; Política e Questões sociais/societais.

a) Infraestrutura: dá-se por questões relacionadas à arquitetura do sistema e da infraestrutura relacionada, pois afetam os registros mantidos em ambientes

[93] Disponível em: https://interparestrust.org/trust.

online. Exemplos de áreas a serem investigadas incluem tópicos como: tipos de nuvem e sua confiabilidade; tipos de acordos contratuais e sua negociação, cobertura, flexibilidade, etc.; custos, adiantados e ocultos;

b) Segurança: debruça-se sobre as questões de registros relacionadas à segurança de dados online, incluindo: métodos de segurança (criptografia, fragmentação, ofuscação, localização geográfica); violações de dados; cibercrime; riscos associados a servidores compartilhados; garantia de informação; auditorias e auditabilidade; prontidão *forense*; avaliação de risco; e *backup*.

c) Controle: difere do domínio de segurança em seu foco no gerenciamento de material digital em ambientes *online.* Aborda questões como: autenticidade, confiabilidade e precisão dos dados; metadados de integridade; cadeia de custódia; retenção e disposição; transferência e aquisição; controle intelectual e controles de acesso.

d) Acesso: acesso aberto; privacidade; responsabilidade; e transparência.

e) Jurídico: considera questões como a aplicação do privilégio jurídico (incluindo a questão da extraterritorialidade); a retenção legal; cadeia de evidências; utenticação de evidências oferecidas no julgamento; certificação; e leis não vinculativas (em particular os instrumentos de definição de padrões da ONU) – mapeamento, escopo, impacto potencial e restrições;

f) Terminologia: preocupa-se com a produção contínua de um glossário multilíngue; um dicionário multilíngue; ontologias; e ensaios que explicam o uso de termos e de conceitos dentro do projeto.

g) Recursos: preocupa-se com a produção contínua de bibliografias, identificando artigos publicados, livros, jurisprudência, políticas, estatutos, normas, *blogs* e literatura cinzenta semelhante;

h) Educação: preocupa-se com o desenvolvimento de diferentes modelos de currículos para a transmissão dos novos conhecimentos produzidos pelo Projeto.

i) Política considera questões relacionadas a políticas emergentes dos cinco domínios; por exemplo, questões de política relativas ao desenvolvimento e à implementação de infraestrutura ou de padrões de segurança. Em geral, aborda questões de manutenção de registros associadas ao desenvolvimento e à implementação de políticas que têm impacto sobre a gestão de registros em um ambiente *online*. As políticas podem ser amplas, como uma política nacional de gerenciamento de informações, ou muito específicas, como uma política sobre a

adoção de certos padrões dentro de uma organização.

j) Questões Sociais/Societais: preocupa-se com a análise da mudança social consequente ao uso da *Internet*, incluindo, mas não se limitando ao uso/uso indevido de mídia social de todos os tipos, confiabilidade de notícias, vazamento de dados (intencional ou acidental/força maior), questões de cultura organizacional e de comportamento individual.

O InterPARES 4 teve mais de 200 publicações (livros, artigos, anais, documentos de pesquisa, teses e mídias sociais), além de mais de 200 apresentações (palestras, *workshops*, seminários e conferências). o Brasil seguiu participando dessa iniciativa com apoio do Arquivo Nacional, fazendo parte da *Team* América Latina e contribuiu com um estudo de caso [94]sobre a preservação de documentos produzidos no Sigepe.

[94] Disponível em: https://interparestrust.org/assets/public/dissemination/IPT_LA01_Report_port_2017.pdf.

8 DESCRIÇÃO DAS PUBLICAÇÕES TÉCNICAS DE PRESERVAÇÃO DIGITAL DO CONSELHO NACIONAL DE ARQUIVOS

A seguir, expõem-se, de maneira descritiva, as Publicações Técnicas do Conarq que enfocam a temática da preservação digital. Devemos levar em consideração à época em que cada documento foi produzido, bem como a sua conjuntura, sabendo que o horizonte temporal das tecnologias digitais é muito efêmero quando comparado às questões analógicas.

Cada diretiva, muitas vezes, dispõe do mesmo conceito e do mesmo termo, contudo, em alguns casos, sua definição pode divergir de uma para outra. Procuramos fazer uma síntese acurada das informações dispostas em cada diretriz, mas sobretudo, no intuito de analisar o conceito de confiança, embasados no método indiciário e na Teoria do Conceito Dahlberg.

Para este entendimento, acostamo-nos no nosso Referencial Teórico acerca do que significa confiança, compilando o que os autores evidenciaram aos postulados das normativas em questão. Além disso, os registros nas subseções abaixo foram extraídos das próprias Publicações Técnicas do Conarq, em que abarcamos o máximo de informações possíveis dessas diretivas. Claro que nem todas as recomendações e diretrizes foram contempladas, pois não eram necessárias, contudo, apenas informações que traziam, de alguma forma, o enfoque da confiança. As diretrizes analisadas:

1. A Carta para a Preservação do Patrimônio Público Arquivístico Digital.
2. Diretrizes do Produtor – A elaboração e a manutenção de materiais digitais: diretrizes para indivíduos.
3. Diretrizes do Preservador – A preservação de documentos arquivísticos digitais: diretrizes para organização.
4. Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais.
5. Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos – e-ARQ Brasil – versão 2.
6. Diretrizes para a Implementação de Repositórios Arquivísticos Digitais Confiáveis – RDC-Arq – versão 2.

No final de cada subseção, quadros foram elaborados para sintetizar os elementos de confiança de cada norma. Tais elementos elencam: conceitos e definições. Os conceitos podem ser representados por um único termo ou mais de um.

8.1 CARTA PARA A PRESERVAÇÃO DO PATRIMÔNIO PÚBLICO ARQUIVÍSTICO DIGITAL

A primeira Publicação Técnica do Conarq a evidenciar a preservação digital para os documentos arquivísticos foi a “Carta para a Preservação do Patrimônio Arquivístico Digital”, redigida em quatro idiomas: português brasileiro, francês, espanhol e inglês.

Aprovada em 2004 e publicada em 2005, esta recomendação possui o objetivo de conscientizar e de ampliar discussões acerca da informação em formato digital enquanto patrimônio cultural, que se encontra em perigo de perda de confiabilidade.

A Carta manifesta a necessidade de se estabelecer políticas, estratégias e ações que garantam a preservação a longo prazo e o acesso contínuo aos documentos arquivísticos digitais, e para isso traz algumas recomendações:

- a informação arquivística digital produzida, recebida, utilizada e conservada em sistema informatizado vem constituindo o legado do patrimônio arquivístico digital, e dessa forma, encontra-se em perigo de desaparecimentos e de falta de confiabilidade e a preocupação em preservar essas informações deve ser urgente;
- A Unesco prescreveu que seus Estados-membros, entre eles o Brasil, estabeleçam políticas e ações de proteção ao patrimônio digital. Sob essa égide, o Conarq, órgão responsável pela política nacional dos arquivos públicos e privados, aprovou o texto desta Carta como conscientização à preservação dos documentos arquivísticos digitais.
- Pensando nisso, os documentos arquivísticos digitais precisam ser autênticos e fidedignos para fornecerem evidências das suas atividades, devendo contribuir para a memória da sociedade como um todo.
- A eficácia do documento arquivístico em todo o seu ciclo depende da qualidade e do rigor dos procedimentos de produção e de manutenção realizados pelas organizações produtoras.
- Para isso, torna-se necessário que os sistemas eletrônicos/digitais, a fim de que não haja perda nem adulteração dos registros arquivísticos, garantam que esses documentos permaneçam disponíveis, recuperáveis e compreensíveis pelo tempo que for necessário.

Os postulados da Carta enfatizam que a preservação de documentos arquivísticos digitais deve garantir a sua autenticidade e facultar o seu acesso, mas para isso, eles necessitam estar em condições de serem utilizados e compreendidos. O acesso contínuo aos seus conteúdos e às suas funcionalidades dão-se por meio de recursos tecnológicos disponíveis.

Por isso, é importante a conscientização dos governos, das organizações públicas e privadas, das instituições de ensino e de pesquisa e de todos os setores da sociedade brasileira comprometidos com a inclusão informacional para problemas como:

- a dependência social da informação digital para o exercício de suas atividades;
- a obsolescência da tecnologia digital que ameaça a vida dos documentos;
- a incapacidade dos atuais sistemas eletrônicos/digitais de informação em assegurar a preservação de longo prazo;
- a fragilidade intrínseca do armazenamento digital, pois são mais instáveis que os meios analógicos;
- a complexidade e os custos da preservação digital, visto que tecnologias precisam estar sempre atualizadas, tanto *hardware* quanto *software*;
- a multiplicidade de atores envolvidos, uma vez que a preservação não se limita ao domínio tecnológico, envolve também questões administrativas, legais, políticas, econômico-financeiras e, sobretudo, de descrição dessa informação por meio de estruturas de metadados.

Nesta Carta há o manifesto sobre a importância das instituições arquivísticas, do poder público, da indústria de tecnologia da informação e da comunicação e das instituições de ensino e pesquisa, implementarem ações de preservação digital, especialmente no que concerne:

1. à elaboração de estratégias e de políticas que envolvem a gestão arquivística de documentos; a instrumentalização dos arquivos; o governo digital e as ações cooperativas;
2. ao estabelecimento de normas que envolvem padrões e protocolos; requisitos funcionais; metadados e segurança da informação digital.
3. à promoção do conhecimento que envolve agenda de pesquisa; ensino e formação de recursos humanos e disseminação do conhecimento.

Identificamos os elementos do conceito de confiança na Carta a partir desses três pilares mencionados (Quadro 10).

Quadro 10 – Elementos do conceito de confiança extraídos da Carta para a Preservação do Patrimônio Arquivístico Digital

Conceitos	Definições
Gestão arquivística de documentos	Tem o objetivo de garantir a produção e a manutenção de documentos fidedignos, autênticos, acessíveis, compreensíveis e preservável.
Instrumentalização dos arquivos	Visa orientar à criação de infraestrutura nas instituições arquivísticas e nas organizações produtoras e acumuladoras de documentos, no que concerne a equipamentos, a sistemas, a metodologias e a recursos humanos, para que possam desempenhar um papel ativo na gestão da preservação dos documentos digitais.
Governo digital	Promove a participação de representantes das instituições arquivísticas nos projetos de governo digital, para a definição de estratégias, de padrões e de normas de gestão, de preservação e de acesso a documentos e informações, conforme orientação do Conselho Internacional de Arquivos e da Unesco.
Ações cooperativas	Visa incentivar programas cooperativos de preservação de documentos digitais para aplicação e compartilhamento de recursos sob a forma de acordos, consórcios, convênios e parcerias.
Padrões e protocolos	Versa sobre definir e/ou recomendar a utilização de padrões e de protocolos abertos e de aceitação ampla na criação, no uso, na transmissão e no armazenamento de documentos digitais; e desenvolver soluções em cooperação com organizações de pesquisa e a indústria de tecnologia da informação e comunicação.
Requisitos funcionais	Visa definir requisitos funcionais e estimular sua adoção para orientar o desenvolvimento e a aquisição de sistemas digitais de gestão arquivística, que sejam adequados às especificidades da legislação e das práticas arquivísticas brasileiras.
Metadados	Tem o objetivo de definir estruturas padronizadas de metadados e determinar a sua utilização nos sistemas digitais de gestão arquivística, com o propósito de gerir a preservação e a acessibilidade dos documentos digitais.
Segurança da informação digital	Define a política de segurança da informação, que considere os aspectos legais, organizacionais, humanos e tecnológicos, de modo a garantir a autenticidade dos documentos digitais e o sigilo da informação, bem como a proteção contra perdas, acidentes e intervenções não autorizadas.
Agenda de pesquisa	Desenvolve uma agenda nacional de pesquisa para a preservação e longevidade dos documentos digitais, alinhada às principais iniciativas nacionais e internacionais, com a participação das agências governamentais de fomento e de amparo à pesquisa, universidades e outras entidades dos setores público e privado.
Ensino e formação de recursos humanos	Visa estimular a inserção do tema Preservação do Patrimônio Arquivístico Digital na formação dos profissionais de informação, especialmente dos arquivistas, nos cursos de graduação e de pós-graduação.
Disseminação do conhecimento	Visa estabelecer ações de identificação, de disseminação e de compartilhamento do conhecimento e a utilização de metodologias e técnicas para a gestão e a preservação de documentos arquivísticos digitais.

Fonte: Brasil (2005a).

Esses elementos do conceito de confiança da Carta promovem, em algum grau, a comunicação com o pensamento dos autores do nosso Referencial Teórico do conceito de

confiança, no intuito de reforçar os esforços para garantir a preservação e o acesso contínuo aos documentos digitais, sendo uma condição fundamental para a democratização da informação arquivística em nosso país e a preservação da memória nacional.

8.2 DIRETRIZES DO PRODUTOR. A ELABORAÇÃO E A MANUTENÇÃO DE MATERIAIS DIGITAIS: DIRETRIZES PARA INDIVÍDUOS

Quando falamos em "Diretrizes do Produtor e do Preservador"[95], não esqueçamos do Projeto InterPARES, e especialmente dos seus "Recursos de Preservação" – conjunto de diretrizes das fases 1 e 2 do Projeto – que apoiam o entendimento da natureza dos documentos arquivísticos digitais e do desenvolvimento de métodos para a sua produção confiável e para a sua manutenção e preservação de forma acurada e autêntica. São ferramentas que podem ser usadas por indivíduos e por organizações como diretrizes e instrumentos, a fim de lidar com problemas relacionados aos documentos. Vimos alguns desses recursos-chave na seção sobre o Projeto Interpares, contudo para fins de discriminá-los de acordo com as Diretrizes do Produtor, eis:

Quadro 11 – Recursos de Preservação do Projeto Interpares 1 e 2

Requisitos de autenticidade	Este recurso do InterPARES 1 é composto de dois conjuntos de exigências para avaliar e para manter a autenticidade dos documentos arquivísticos digitais; um é destinado a produtores e o outro, a preservadores de documentos. O primeiro conjunto, conhecido como "Requisitos de Referência para a Autenticidade", contém as exigências que apoiam a presunção de autenticidade dos documentos arquivísticos digitais de um produtor, antes que eles sejam transferidos para a custódia do preservador. O segundo conjunto, "Requisitos de Base para a Autenticidade", é composto por exigências que apoiam a produção de cópias autênticas dos materiais digitais transferidos para a custódia do preservador e mantidos em seu sistema de preservação.
Modelo de análise	Recurso do InterPARES 1. Propicia a decomposição do documento digital em suas quatro partes constituintes necessárias: a forma documental, as anotações, o suporte e os contextos (isto é, tudo o que envolve a ação da qual o documento participa, que inclui seus contextos administrativo, de procedimento, documental, tecnológico e de proveniência. O modelo define cada parte e elemento

[95] É importante ressaltar que as "Diretrizes do Produtor e do Preservador" estão registradas em um único documento nas Publicações Técnicas do Conarq, a partir da Resolução n.º 38, de 9 de julho de 2013, publicada pioneiramente, no âmbito do InterPARES, visando ao aperfeiçoamento da gestão e da preservação dos documentos de arquivo em formato digital. Disponível em: Resolução nº 38, de 9 de julho de 2013 — Conselho Nacional de Arquivos (www.gov.br).

	da forma, explica seu propósito e indica até que ponto tal parte ou elemento é útil para avaliar a autenticidade do documento. Em um nível mais básico, o modelo serve como uma lista com definições que ajudam os usuários a determinar se eles estão lidando com um documento arquivístico de fato.
Arcabouço de políticas	Recurso do InterPARES 2. É composto de dois conjuntos complementares de princípios para a produção e para a preservação de documentos digitais autênticos que, juntos, ajudam a estruturar a relação entre os produtores e os preservadores, fornecendo um guia para estabelecer um arcabouço intelectual abrangente, dentro do qual eles podem desenvolver ambientes com políticas consistentes e integradas que conduzam à preservação efetiva e coordenada dos documentos digitais.
Diretrizes para produtores	Recurso do InterPARES 2. Tem a finalidade de recomendar e de auxiliar agentes a tomarem decisões de como elaborar e manter materiais digitais, a fim de assegurar sua preservação pelo tempo que for necessário. Pode ser aplicado a vários tipos de publicações, de documentos e de dados digitais, mas especialmente aos documentos arquivísticos digitais.
Diretrizes para preservadores	Recurso do InterPARES 2. Fornece recomendações concretas para qualquer organização responsável pela preservação a longo prazo de documentos digitais.
Dois modelos de gestão de documentos arquivísticos	Estes modelos do InterPARES 2 descrevem, de forma gráfica e narrativa, todas as atividades e ações importantes e específicas que devem ser tomadas, bem como as entradas, as saídas, os mecanismos de capacitação e as restrições ou controles, com o objetivo de produzir, de gerenciar e de preservar documentos arquivísticos digitais confiáveis e autênticos. Desta forma, ambos os modelos caracterizam os dados e as informações que devem ser reunidas, armazenadas e utilizadas para apoiar os vários processos de gestão ao longo da vida do documento.
O modelo da Cadeia de Preservação	Baseia-se na tradicional abordagem do "ciclo de vida dos documentos", apresenta as perspectivas específicas nas situações do produtor, do gestor e do preservador dos documentos.
Modelo de Manutenção de Documentos Orientada pelas Atividades do Produtor	Baseia-se na abordagem do *records continuum* (modelo de gestão de documentos australiano), adota a perspectiva do produtor de documentos arquivísticos.
Bases de dados de terminologia	Este recurso do InterPARES 2 contém três instrumentos de terminologia: glossário, dicionário e ontologias. O glossário é uma lista de termos autorizados e definições que são fundamentais para nosso entendimento dos ambientes de produção, de manutenção e de preservação de documentos. O

	dicionário é usado para facilitar a comunicação interdisciplinar. Ele contém múltiplas definições para termos de diversas disciplinas. Ao usar esta ferramenta, os usuários podem ver como a Arquivologia utiliza a terminologia em comparação com a Ciência da Computação, com a Biblioteconomia e com a Ciência da Informação, com as Artes e com outras áreas. As ontologias identificam as relações explícitas entre conceitos de documentos arquivísticos. Isto é útil para comunicar as nuances da Diplomática no ambiente digital interativo, experiencial e dinâmico.
Sistema de Análise e de Registro de Descrição Arquivística e Metadados (siglas em inglês, Madras)	Recurso *online* interativo do InterPARES 2. É um repositório de esquemas destinado a ajudar na identificação dos conjuntos de metadados, ou das combinações de elementos de diferentes conjuntos, que servem para atender a várias necessidades de manutenção e de preservação a longo prazo dos documentos. O Madras fornece recomendações sobre como cada esquema pode ser expandido ou revisado para atender às necessidades de confiabilidade, de autenticidade e de preservação dos documentos digitais produzidos dentro do domínio, da comunidade ou do setor do usuário.

Fonte: Brasil (2013b).

As Diretrizes do Produtor descrevem uma série de atividades para que pessoas, grupos de pessoas e pequenas organizações (tais como consultórios, grupos de pesquisa, ou equipes de pesquisa científica e outros) produzam e mantenham materiais digitais que possam ser presumidos autênticos, acurados e confiáveis. Vale destacar que nem todas as recomendações precisam ser aplicadas; o importante é selecionar e adotar as medidas que respondem a problemas específicos. Além disso, pode haver casos nos quais sejam necessárias medidas adicionais.

Possui o objetivo de fornecer recomendações e de auxiliar na tomada de decisões de como elaborar e manter documentos digitais, a fim de assegurar preservação pelo tempo que for necessário. Pode ser aplicado a vários tipos de publicações, de documentos e de dados digitais, mas especialmente aos documentos arquivísticos digitais. Os documentos preservados por um longo período podem ser armazenados em repositórios arquivísticos.

Este documento apresenta “elementos de preservação digital” que corroboram à completude das recomendações para os produtores que gerenciam documentos, são elas: proteção, integridade, acurácia, forma fixa, autenticidade, interoperabilidade, consciência, obsolescência, fixidez, organização, confiabilidade, autenticação, conteúdo estável, acessibilidade e identidade.

Antes de descrever as dez seções destas Diretrizes, faz-se essencial primeiro, definir

confiabilidade, acurácia e autenticidade. Confiabilidade é a credibilidade do documento digital enquanto conteúdo ou declaração de um fato, estabelecida com base na sua completeza, na sua acurácia e no seu grau de controle exercido no processo de sua produção. É também, a responsabilidade do autor dos documentos, seja ele pessoa física ou pessoa jurídica.

Acurácia é o grau de precisão, de correção, de verdade, de ausência de erros e de distorções nos dados contidos nos documentos. Para assegurar a acurácia, deve-se exercer controle sobre os processos de produção, de transmissão, de manutenção e de preservação dos documentos. Com o tempo, a responsabilidade pela acurácia é passada do autor para o responsável pela manutenção (*keeper*) e, após, para o preservador (se for aplicável).

Autenticidade refere-se ao fato de que os documentos são o que dizem ser e que não foram adulterados ou corrompidos de qualquer outra forma. Aos documentos arquivísticos, a autenticidade refere-se à confiabilidade dos documentos enquanto tais. Para assegurar que a autenticidade possa ser presumida e mantida ao longo do tempo, deve-se definir e conservar a identidade dos materiais e proteger sua integridade. Ao longo do tempo, a responsabilidade pela autenticidade é passada do *keeper* para o preservador.

As recomendações trazidas nas Diretrizes do Produtor são divididas em dez seções. Cada seção possui um elemento ou categoria de preservação como representante principal e a partir dela são elencadas diretrizes e subdiretrizes.

1. Esta seção é representada pela "acessibilidade", preconizando que é fundamental que se selecione hardware, software e formatos de arquivo que ofereçam as melhores expectativas de garantia de que os materiais digitais permanecerão facilmente acessíveis ao longo do tempo.

O acesso aos documentos digitais depende de um *software* apropriado, destinado a uma tarefa específica, trabalhando de maneira eficiente com outros que sirvam para outras tarefas e sistemas (interoperabilidade). Os pontos a seguir tem a intenção de possibilitar garantias de que um *software* e *hardware* mantenham a acessibilidade.

a) **Faz-se necessário a escolha de um *software* que apresente os materiais como eles aparecem originalmente.** Um novo *software* deve ser capaz de ler materiais digitais mais antigos no formato em que os mantém, e de mostrá-los com a mesma forma documental em que eram apresentados originalmente.
b) **É importante que os *software* e os *hardware* escolhidos permitam compartilhar documentos digitais com facilidade.** O *software* deve ser capaz de aceitar e de gerar arquivos em vários formatos. A habilidade de interagir com outra tecnologia é

chamada de interoperabilidade.

c) **Torna-se necessário usar *software* aderentes a padrões (recomendados por organizações nacionais e internacionais).** Para fins destas Diretrizes, os padrões podem ser de direito (de jure)[96] e de fato[97]. Se não existirem estes tipos de padrões, pode-se adotar os que sejam utilizados para longevidade documental. Caso não exista um padrão oficial, semelhantes *software* são comumente considerados um padrão de fato. *Software* de código aberto são os preferíveis.

d) **Deve-se manter as especificações do *software.*** Este tipo de documentação pode ser manual ou qualquer outra descrição mais detalhada sobre *software*, que será essencial, com o avanço tecnológico, para acessar os materiais ou para migrá-los a um novo ambiente computacional. É importante documentar integralmente qualquer *software* que se construa.

e) **Caso personalize um *software*, deve-se certificar de que documentou as mudanças ocorridas.** Uma maneira para fazer isso é incluir a informação sob a forma de comentários no código-fonte do *software*. A informação não será perdida, já que é parte do arquivo, e será útil para quem precisar fazer ajustes posteriormente.

f) **Deve-se documentar a construção (estrutura e funções dos sistemas) do seu sistema para garantir a acessibilidade.** Isto significa identificar os componentes de *hardware* e de *software*, inclusive os periféricos, o sistema operacional e os pacotes de *software*.

g) **Sempre que possível, torna-se necessário escolher formatos independentes de plataforma, amplamente utilizados, não proprietários e não comprimidos, com especificações disponibilizadas gratuitamente**.

2. Esta seção é representada pela "fixidez". Deve-se certificar que os documentos arquivísticos são estáveis e fixos tanto no conteúdo quanto na forma.

Um sistema que contém documentos arquivísticos precisa compô-la com forma fixa e com conteúdo estável. Assim, fixidez pode ser entendida como a qualidade de um documento arquivístico assegurar forma fixa e conteúdo estável.

---

[96]Padrão de direito: adotado por órgãos oficiais de padronização, sejam eles nacionais (Associação Brasileira de Normas Técnicas – ABNT), multinacionais (Comitê Europeu de Normalização – CEN) ou internacionais (Organização Internacional para Padronização – ISO). Para padrões de arquivos de computador, dois padrões de direito recentes são o PDF/A (padrão PDF para arquivamento) e ODF (OASIS Formato de documento aberto) (Brasil, 2013b, p. 4).

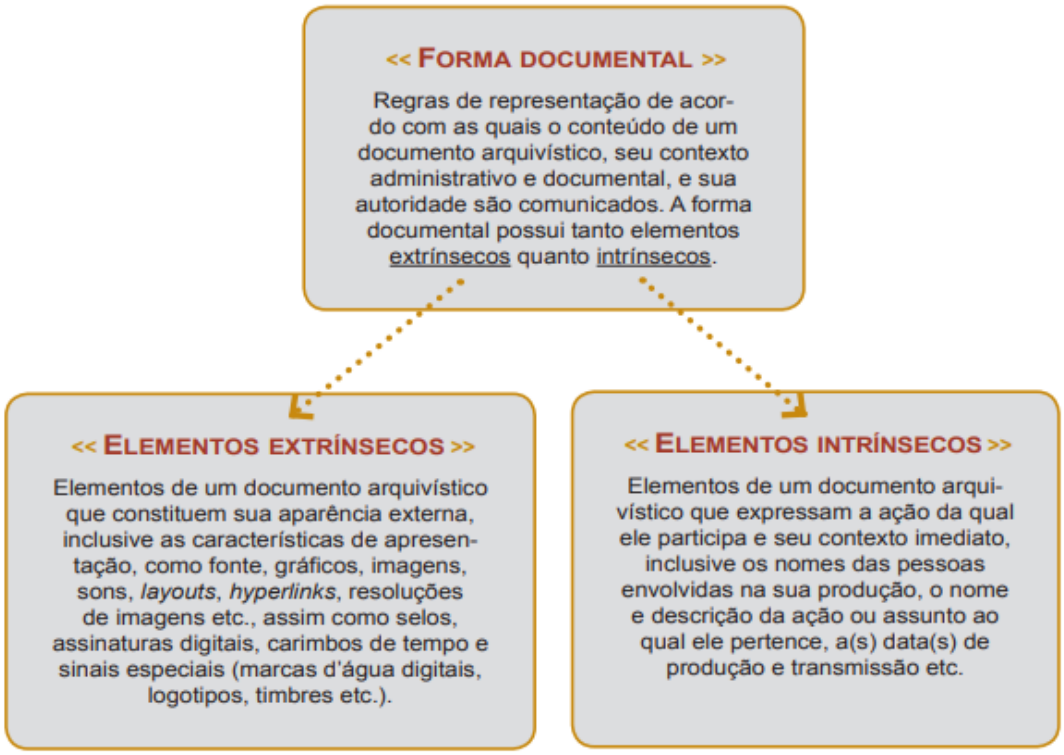
[97]Padrão de fato: que não foi adotado por nenhum órgão oficial de padronização, mas que é amplamente usado e reconhecido pelos usuários como tal. Formatos de arquivos de computador bem conhecidos e amplamente usados que são considerados padrões de fato incluem PDF, TIFF, DOC e ZIP (Brasil, 2013b, p. 4).

O conteúdo estável é a característica de um documento arquivístico que torna a informação e os dados nele contidos imutáveis, exigindo que eventuais mudanças sejam feitas por meio do acréscimo de atualizações ou da produção de uma nova versão. As cadeias de *bits* que compõem o documento digital e determinam sua apresentação digital (isto é, seu formato de arquivo) podem mudar, mas sua apresentação documental não. Exemplo: imaginemos, um documento produzido no *Microsoft Word* e posteriormente salvo como um arquivo PDF. Embora a apresentação digital do documento tenha mudado – de um arquivo ".doc" do *Microsoft Word* para um formato ".pdf" do *Adobe Acrobat* –, sua apresentação documental, também chamada forma documental, não mudou, portanto, podemos corroborar que o documento tem uma forma fixa.

A forma fixa é a qualidade de um documento arquivístico que assegura a mesma aparência ou apresentação documental cada vez que o documento é recuperado. Outro aspecto importante é a "variabilidade limitada", que se dá pela qualidade do documento arquivístico em assegurar suas apresentações de forma limitada e controlada por regras fixas, produzindo um mesmo resultado. Por exemplo, enquanto autor de um documento arquivístico, o indivíduo estabelece regras fixas para a seleção de seu conteúdo e de sua forma documental que permitam apenas uma gama conhecida e estável de variações.

A apresentação dos documentos serve para manter e avaliar a sua confiabilidade e a sua acurácia. Atualizações ou conversões podem resultar em mudanças na forma documental, sendo assim, é fundamental estabelecer a forma dos documentos associados com cada atividade, e após identificar as características essenciais (os elementos extrínsecos e intrínsecos) de cada apresentação ou forma documental.

Figura 34 – Forma documental e suas características essenciais



Fonte: Brasil (2013b, p. 7).

Isto permitirá a identificação em mudanças futuras que impliquem na perda de identidade e de integridade do documento, ajudando no reconhecimento dos direitos de propriedade intelectual, analogamente.

3. Esta seção é representada pelo aspecto da "identidade", que é o conjunto de características de um documento (arquivístico ou não) que o identifica de forma única e o distingue dos demais. A identidade e a integridade constituem a autenticidade. Deve-se certificar que os materiais digitais estão identificados adequadamente, por meio da identidade.

Atribuir um nome a arquivos auxilia na identificação dos seus conteúdos e torna mais fácil localizá-los. Tal processo é fundamental para diferenciar, distinguir versões e fornecer evidências da identidade de um documento arquivístico desde o momento de sua produção. Essas informações acerca de sua identificação são chamadas de metadados. Os metadados servem para descrever os atributos/propriedades dos documentos, sendo necessários para manter e para avaliar sua autenticidade. Os metadados de identidade são:

a) Nomes das pessoas envolvidas na produção dos materiais digitais:
    - **o autor:** a(s) pessoa(s) física(s) ou jurídica(s) responsável(eis) por emitir os documentos;
    - **o redator:** a(s) pessoa(s) física(s) ou cargo(s) responsável(eis) por articular o

conteúdo dos documentos;

- **o originador:** a pessoa física, o cargo ou a unidade administrativa responsável pela conta de correio eletrônico ou pelo ambiente tecnológico onde os documentos são gerados a partir do qual são transmitidos. Isto é mais comumente percebido em casos de mensagens de correio eletrônico nas quais o nome do originador aparece no cabeçalho e/ou nos anexos que foram de autoria ou redigidos por outra pessoa, mas fisicamente manifestados ou transmitidos em nome de tal pessoa pelo originador;
- **o destinatário:** a(s) pessoa(s) física(s) ou jurídica(s) para quem os documentos são destinados;
- **o receptor:** a(s) pessoa(s) física(s) ou jurídica(s) para quem os documentos podem ter sido enviados como cópia ou cópia oculta.

b) **Nome da ação ou assunto:** título ou assunto.

c) **Forma documental:** se é um relatório, uma carta, um contrato, uma tabela, uma lista ou outros tipos.

d) **Apresentação digital:** o formato, o *wrapper* (encapsulamento de documentos digitais, juntamente com seus metadados, para garantir preservação a longo prazo), a codificação e outros tipos.

e) **Data(s) de produção e de transmissão:** data cronológica; data de transmissão; data de recebimento; data de arquivamento (na qual os documentos foram associados a uma pasta ou a um diretório de computador, a um CCD ou a outro esquema).

f) **Expressão do contexto documental:** um código de classificação, um nome da pasta/diretório de computador, uma unidade de arquivamento equivalente dentro do esquema ou CCD ao qual os documentos estão associados, ou a um nome de grupo mais amplo.

g) **Indicação de anexos:** se aplicável.

h) **Indicação de direitos autorais ou outros direitos intelectuais:** se aplicável.

i) **Indicação da presença ou remoção de uma assinatura digital:** se aplicável.

j) **Indicação de outras formas de autenticação:** se aplicável. Pode incluir: a presença de uma corroboração (menção explícita aos meios usados para validar o documento arquivístico); um atestado (validação de um documento por aqueles que participaram de sua emissão, e por testemunhas da ação ou da sua “assinatura”); uma subscrição (nome do autor ou redator aparecendo na parte inferior do documento) ou uma qualificação de assinatura (menção ao título, capacidade e/ou endereço da pessoa ou

pessoas signatárias do documento), ou seja, os elementos diplomáticos.

k) **Indicação da minuta ou do número da versão:** se aplicável.

l) **Existência e localização de materiais duplicados fora do sistema digital:** se aplicável. Se há múltiplas cópias, deve-se indicar qual é a cópia autoritária (documento arquivístico identificado pelo produtor como sendo seu documento oficial).

4. Esta seção é representada pela "integridade", que é a qualidade do documento ser completo e inalterado em todos os aspectos essenciais; junto à identidade, é um componente da autenticidade. Deve-se aqui, certificar-se de que os documentos digitais carregam informações que ajudarão a verificar sua integridade.

Os elementos de integridade podem materializar-se em metadados. Os documentos digitais são íntegros se estiverem intactos e não corrompidos, isto é, se as mensagens para atingir seus objetivos estiverem inalteradas. O conteúdo e os dados são considerados inalterados se forem idênticos ao valor e à apresentação de sua primeira manifestação. Os atributos que se relacionam à integridade dizem respeito à manutenção dos materiais, incluindo a responsabilidade por seu uso apropriado, tais como supervisão e documentação de quaisquer transformações tecnológicas ou transferências para outros sistemas. Eis os metadados de integridade:

a) **Nome da pessoa ou unidade administrativa que utiliza os documentos:** a pessoa ou unidade que utiliza os materiais para conduzir as atividades.

b) **Nome da pessoa ou unidade com responsabilidade primária por manter os materiais:** pode ser o mesmo que a pessoa/unidade que utiliza os documentos.

c) **Indicação de anotações acrescentadas aos materiais:** se aplicável.

d) **Indicação de quaisquer mudanças técnicas nos materiais ou nos aplicativos responsáveis por gerenciar e prover acesso aos documentos:** mudanças de codificação, de *wrapper* ou de formato; atualização de uma versão para outra; conversão de vários componentes digitais inter-relacionados em apenas um componente (por exemplo, componentes digitais que eram apenas conectados a eles, tais como áudio, vídeo e elementos gráficos ou de texto).

e) **Código de restrição de acesso:** indicação da pessoa, do cargo ou da unidade autorizada a ler os materiais, se aplicável.

f) **Código de privilégios de acesso:** indicação da pessoa, do cargo ou da unidade autorizada a fazer anotações nos materiais, apagá-los ou removê-los do sistema, se aplicável.

g) **Código de documento vital (quando aplicável):** indicação do grau de importância do documento arquivístico para dar continuidade à atividade para a qual foi produzido ou à atividade da pessoa/unidade que o produziu. Aplica-se apenas a comunidades de práticas específicas, como na área médica ou jurídica, que devem identificar os documentos vitais para a continuidade de seus negócios em caso de desastre, e que exerceriam medidas de proteção especial sobre tais documentos.
h) **Destinação planejada:** por exemplo, a remoção de materiais do sistema ativo para armazenamento fora dele; transferência para os cuidados de um custodiador confiável; eliminação prevista em TTDD.

5 Esta seção é relacionada à "organização". Assim, deve-se agrupar os documentos digitais de forma lógica.

A organização pode ser baseada nos diferentes tipos de documentos ou na quantidade de tempo pela qual certos tipos devem ser mantidos. Esses agrupamentos podem estar relacionados entre si de uma forma hierárquica ou horizontal, de acordo com necessidades específicas. Seu esquema de organização deve ser registrado em um documento que mostre todos os agrupamentos de materiais, descreva-os de forma breve e indique como eles estão relacionados. Neste caso, pode ser instrumentalizado pelo CCD, também conhecido como Plano de Classificação de Documentos (PCD).

6 Esta seção é representada pela "autenticação" – declaração de autenticidade de um documento arquivístico, num determinado momento, resultante da inserção ou do acréscimo de um elemento ou de uma afirmação por parte de uma pessoa investida de autoridade para tal. Logo, deve-se utilizar técnicas de autenticação que favoreçam a manutenção e a preservação dos materiais digitais.

A autenticidade dos materiais digitais é ameaçada sempre que eles são transmitidos no espaço (quando enviados a um destinatário ou entre sistemas ou aplicativos) ou no tempo (quando os materiais estão armazenados, ou quando o *hardware* ou o *software* usado para armazená-los, processá-los ou comunicá-los é atualizado ou substituído).

Assim, a inferência da autenticidade deve ser apoiada pela evidência em que os documentos foram mantidos, utilizando tecnologias e procedimentos administrativos que garantam a continuidade de sua identidade e de sua integridade, ou que, pelo menos, minimizem os riscos de modificações.

Aqui, a autenticação está dividida em dois tipos. O primeiro é a autenticação independente de tecnologia, destacada pela "presunção de autenticidade", que é uma

inferência estabelecida a partir de fatos conhecidos sobre a forma como um documento foi produzido e mantido. As recomendações são cumulativas: quanto maior o número de recomendações seguidas e maior o grau de satisfação de cada uma delas, maior a presunção de autenticidade.

Já o segundo, é a autenticação dependente de tecnologia, tais como a criptografia. Uma destas técnicas criptográficas é a assinatura digital, que pode ser utilizada quando documentos são transmitidos entre pessoas, sistemas ou aplicativos, para declarar sua autenticidade em um dado momento.

7. Esta seção é representada pelo conceito de"proteção". Deve-se proteger os documentos digitais de ações não autorizadas.

Nessa perspectiva, a autenticidade e a acurácia dos materiais digitais não podem ser presumidas se existir qualquer oportunidade de modificá-los sem deixar vestígios. É preciso demonstrar que seria impossível para qualquer pessoa corrompê-los ou manipulá-los sem que fosse identificada. Aqui, os mecanismos de segurança incluem restringir o acesso físico a lugares onde os computadores são mantidos, assim como o acesso aos documentos nos próprios computadores. Esta última medida pode ser implementada de diversas formas, como o uso de senhas e/ou autenticação biométrica para entrar no sistema ou outros tipos.

8. Esta seção é representada pela necessidade de"cópias de segurança". Deve-se proteger os materiais digitais de perdas acidentais e de corrupção.

As cópias de segurança devem ter regularidade e frequência. Armazená-las em outro local, concede proteção adicional contra sinistros. Há diversas técnicas de proteção neste sentido: pacotes de *software* e serviços de *backup* disponíveis são algumas delas. Atualmente, programas computacionais produzem automaticamente esses esquemas de segurança.

a) É importante que se desenvolva uma política ou rotina rigorosa que assegure aos sistemas fazerem cópias de segurança diariamente. Essas cópias regulares devem ser eliminadas alternadamente, segundo uma estratégia ou programação que seja a mais apropriada às suas exigências, uma vez que cópias não contêm documentos arquivísticos, mas existem para recuperação caso haja falha no sistema. Um exemplo disso é o próprio *backup*. Outros computadores e mídias portáteis, ou disco rígido externo servem para dar mais proteção aos documentos.
b) Deve-se também procurar a melhor tecnologia de cópias de segurança para o seu contexto.

9. Esta seção é representada pelo conceito de "obsolescência". A prevenção contra a obsolescência de software e de hardware deve ser urgente.

Uma estratégia para solucionar este problema é eliminar a dependência de *hardware* e de *software*. Quando partes do ambiente tecnológico tornarem-se obsoletas, a recomendação é atualizá-las para uma tecnologia mais avançada.

10. Esta seção é representada pela ideia de "consciência", considerando os aspectos relacionados à preservação em longo prazo.

Para isso ocorrer, existem custos reais – tanto financeiros quanto humanos – na guarda dos documentos a longo prazo. Semelhante processo começa identificando quem se encarregará dessa preservação: esse papel é do "custodiador confiável", ou seja, um profissional ou um grupo de profissionais, como um arquivo, que tem formação em manutenção e preservação de documentos.

Tal custodiador é o preservador capaz de implementar todos os requisitos à preservação de documentos arquivísticos digitais autênticos. Ele pode demonstrar que não existem razões para alterar ou para permitir que outros alterem documentos preservados.

O conceito de confiança nas Diretrizes do Produtor está representado pelos elementos de preservação digital, os quais identificamos como categorias: a proteção, a integridade, a acurácia, a forma fixa, a autenticidade, a interoperabilidade, a consciência, obsolescência, fixidez, organização, confiabilidade, autenticação, conteúdo estável, acessibilidade e identidade. No caso da forma fixa, do conteúdo estável e da interoperabilidade, estes são elementos que não ensejam categorias, mas compõem seus sistemas.

Quadro 12 – Elementos do conceito de confiança extraídos das Diretrizes do Produtor

Conceitos	Definições
Acessibilidade	As Diretrizes do Produtor não define exatamente "acessibilidade", mas descreve que o acesso aos documentos depende de *software* e de *hardware* apropriados, além de formatos de arquivos, os quais devem oferecer as melhores expectativas de garantia de que os materiais digitais permanecerão facilmente acessíveis ao longo do tempo. A interoperabilidade também é outro conceito que facilita o acesso, uma vez que permite a troca de informações entre sistemas diferentes.
Acurácia	Grau de precisão, de correção, de verdade, de ausência de erros e de distorções nas informações contidas nos documentos. Para a acurácia ser estabelecida, deve-se ter controle sobre os processos de produção, de transmissão, de manutenção e de preservação dos documentos digitais.
Autenticidade	Ocorre quando os materiais são o que eles dizem ser e que não foram adulterados ou corrompidos de qualquer outra forma. Aos documentos arquivísticos, a autenticidade refere-se à confiabilidade enquanto tais. Para garantir a presunção de autenticidade, deve-se definir e conservar a identidade e a integridade dos documentos.
Autenticação	É a declaração de autenticidade de um documento arquivístico, num determinado momento, inserindo algum elemento como acréscimo de uma pessoa investida de

	autoridade para tal. Um exemplo de técnica de autenticação é a criptografia e a assinatura digital.
Confiabilidade	Credibilidade do documento digital enquanto conteúdo ou declaração de um fato, estabelecida com base na sua completeza, na sua acurácia e no seu grau de controle exercido no processo de sua produção.
Consciência	Compreensão acerca dos aspectos que envolvem a preservação digital a longo prazo. Isto é, compreender que a preservação demanda recursos e custos.
Cópias de segurança	Estratégia que visa proteger os documentos digitais de perdas e de corrupção. Liga-se ao armazenamento documental como uma proteção adicional. Há várias técnicas neste sentido: pacotes de *software* e serviços de *backup* são algumas delas.
Fixidez (forma fixa e conteúdo estável)	É a qualidade de um documento arquivístico em assegurar sua forma fixa e seu conteúdo estável. A primeira ocorre quando o documento sustenta a mesma aparência ou apresentação cada vez que é recuperado. O segundo ocorre quando a informação e os dados documentos permanecem imutáveis, exigindo que eventuais mudanças sejam feitas por meio do acréscimo de atualizações ou da produção de uma nova versão.
Identidade	Características de um documento (arquivístico ou não) que o identifica de forma única e o distingue dos demais. A identificação dos documentos digitais é chamada de metadados.
Integridade	Qualidade que um documento possui para ser completo e inalterado em todos os aspectos essenciais; junto à identidade, é um componente da autenticidade. Os elementos de integridade podem materializar-se em metadados. Os documentos digitais são íntegros se estiverem intactos e não corrompidos, isto é, se as mensagens para atingir seus objetivos estiverem inalteradas.
Organização	Qualidade de agrupar os documentos digitais de forma lógica. Tais agrupamentos podem estar relacionados entre si de uma forma hierárquica ou horizontal, de acordo com necessidades específicas, que neste caso pode ser instrumentalizado pelo CCD.
Proteção	Qualidade de proteger os documentos digitais de ações não autorizadas. É preciso demonstrar que seria impossível para qualquer pessoa corrompê-los ou manipulá-los sem que fosse identificada.
Obsolescência	Consciência acerca da prevenção contra a efemeridade do *software* e do *hardware*, a fim de atualizá-los. Estratégia para solucionar dependência de *hardware* e de *software*.

Fonte: Brasil (2023b).

Dez são as seções que compõem as Diretrizes do Produtor. Cada uma possui um elemento de preservação como representante principal e a partir dele há várias recomendações. Como vimos, os elementos de preservação compõem as categorias e as definições de conceito de confiança nestas Diretrizes.

8.3 DIRETRIZES DO PRESERVADOR. A PRESERVAÇÃO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS: DIRETRIZES PARA ORGANIZAÇÃO

Estas Diretrizes foram desenvolvidas com o propósito de fornecer recomendações a instituições, a organizações e a programas responsáveis pela preservação de documentos arquivísticos digitais que podem ser presumidos como autênticos e acurados, enquanto estiverem sob a custódia do preservador. Seu objetivo não é ser abrangente; todavia enfatizar algumas áreas especialmente importantes para a preservação de materiais autênticos.

Do ponto de vista da preservação a longo prazo, todas as atividades para gerenciar os documentos digitais devem estar ligadas sobre uma cadeia interdependente. Se um elo se

rompe, a cadeia não pode executar sua função.

As informações neste documento enfocam a ligação da cadeia de preservação de acordo com a sequência de atividades apresentadas no modelo da Cadeia de Preservação do InterPARES, a qual mostra os vários passos sequenciais à produção, à manutenção e à preservação de documentos autênticos.

Os elementos de preservação digital evidenciados nas Diretrizes do Preservador são: a preservação, a acurácia, a autenticidade, a descrição, a gestão, a obsolescência, a saída, os requisitos de referência e de base, a avaliação e as estratégias de manutenção e de preservação. Antes de começar a destrinchar as recomendações deste documento, vale exibir os seus Apêndices, pois servirão de entendimento das seções subsequentes.

O Apêndice A – Requisitos de Referência para Apoiar a Presunção de Autenticidade dos Documentos Arquivísticos Digitais foi extraído do Relatório da Força da Tarefa de Autenticidade do InterPARES 1.

Tais requisitos são as condições que servem como base para o preservador verificar a autenticidade dos documentos arquivísticos digitais do produtor. Esses requisitos possibilitam ao preservador inferir a autenticidade de documentos arquivísticos, na forma como foram produzidos, utilizados e mantidos pelo produtor. Dentre os Requisitos de Referência, o "Requisito A.1" identifica a informação-chave sobre um documento digital – o contexto imediato de sua produção e a maneira como ele foi utilizado e mantido –, que estabelece sua identidade e prepara o terreno para demonstrar sua integridade.

Os atributos trazidos pelo A.1 e pelo A.2 localizam-se em duas categorias descritas nas Diretrizes do Produtor: os metadados de identidade e de integridade. **Os A.1 de identidade do documentos arquivístico:**

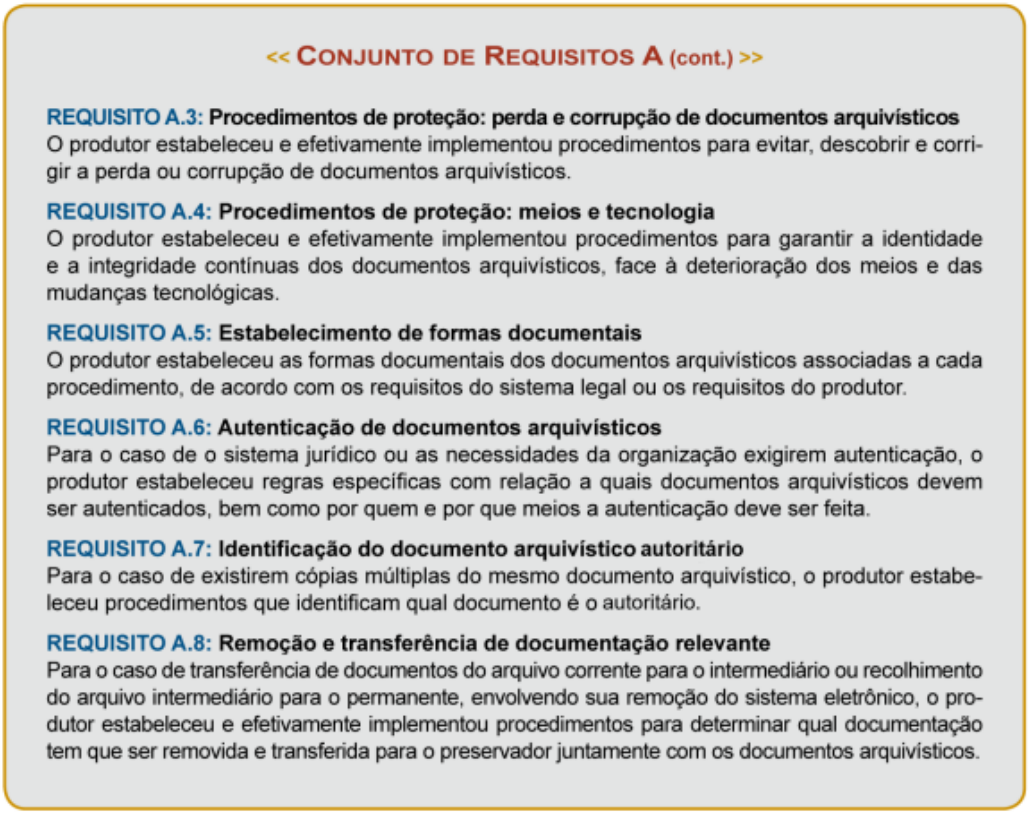
- **Nomes das pessoas que participaram da formação do documento arquivístico:** nome do autor; nome do redator (se for diferente do autor); nome do originador (se for diferente do autor ou do redator); nome do destinatário.
- **Nome da ação ou assunto.**
- **Data(s) de produção e de transmissão:** data cronológica; data de recebimento; data de arquivamento; data(s) de transmissão.
- **Expressão de relação orgânica** (por exemplo, código de classificação, identificador de arquivo).
- **Indicação de anexos.**

Os A.1 de integridade dos documentos arquivísticos são:

- **Nome da unidade responsável pela execução da ação contida no documento.**
- **Nome da unidade que tem a responsabilidade principal (se diferente do anterior).**
- **Indicação de tipos de anotação acrescentada ao documento arquivístico.**
- **Indicação de modificações técnicas.**

Os Requisitos A.2 são direcionados aos "privilégios de acesso", isto é, o produtor é quem define e implementa esses privilégio com relação à produção, à modificação, à anotação, ao remanejamento e à eliminação de documentos arquivísticos, conforme já visto nas Diretrizes anterior. A Figura 35 ilustra a continuação dos "Requisitos A".

Figura 35 – Continuação dos conjuntos de "Requisitos A" do Apêndice A

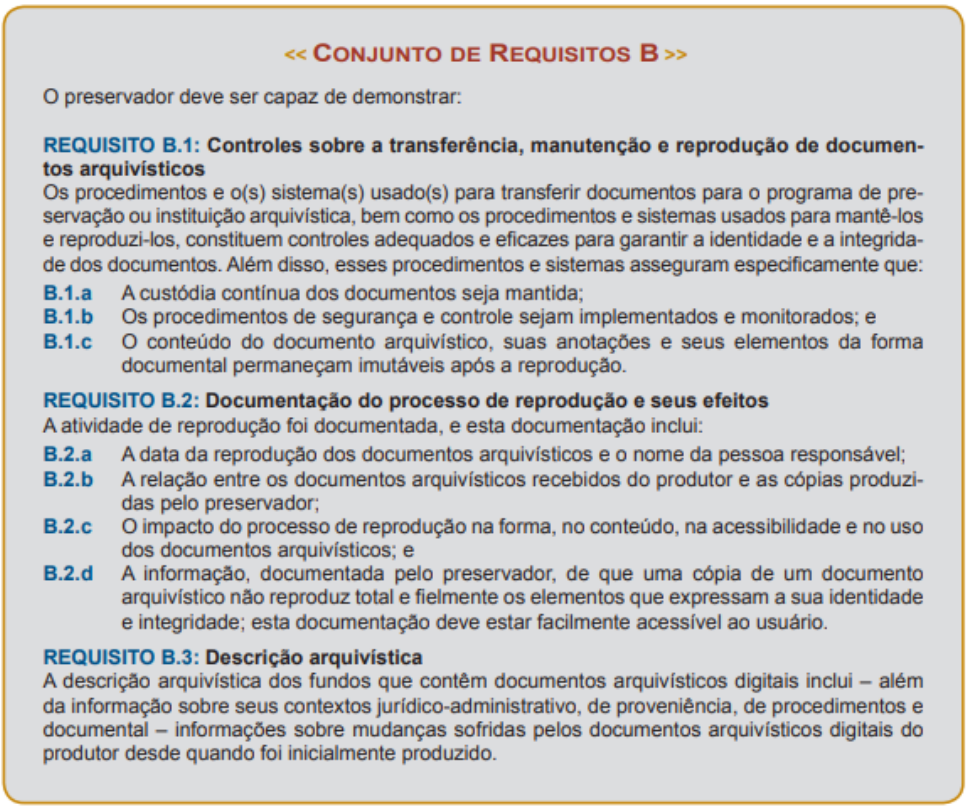


Fonte: Brasil (2013a, p. 38).

O Apêndice B – Requisitos de Base para apoiar a Produção de Cópias Autênticas dos Documentos Arquivísticos Digitais também foi extraído do Relatório da Força-Tarefa de Autenticidade, e delineiam as condições mínimas para o preservador atestar a autenticidade das cópias de documentos arquivísticos digitais de guarda permanente.

Diferentemente dos Requisitos de Referência, todos os Requisitos de Base devem ser atendidos para os documentos serem considerados autênticos.

Figura 36 – Conjunto de Requisitos de Base



<< CONJUNTO DE REQUISITOS B >>

O preservador deve ser capaz de demonstrar:

REQUISITO B.1: Controles sobre a transferência, manutenção e reprodução de documentos arquivísticos

Os procedimentos e o(s) sistema(s) usado(s) para transferir documentos para o programa de preservação ou instituição arquivística, bem como os procedimentos e sistemas usados para mantê-los e reproduzi-los, constituem controles adequados e eficazes para garantir a identidade e a integridade dos documentos. Além disso, esses procedimentos e sistemas asseguram especificamente que:

B.1.a A custódia contínua dos documentos seja mantida;
B.1.b Os procedimentos de segurança e controle sejam implementados e monitorados; e
B.1.c O conteúdo do documento arquivístico, suas anotações e seus elementos da forma documental permaneçam imutáveis após a reprodução.

REQUISITO B.2: Documentação do processo de reprodução e seus efeitos

A atividade de reprodução foi documentada, e esta documentação inclui:

B.2.a A data da reprodução dos documentos arquivísticos e o nome da pessoa responsável;
B.2.b A relação entre os documentos arquivísticos recebidos do produtor e as cópias produzidas pelo preservador;
B.2.c O impacto do processo de reprodução na forma, no conteúdo, na acessibilidade e no uso dos documentos arquivísticos; e
B.2.d A informação, documentada pelo preservador, de que uma cópia de um documento arquivístico não reproduz total e fielmente os elementos que expressam a sua identidade e integridade; esta documentação deve estar facilmente acessível ao usuário.

REQUISITO B.3: Descrição arquivística

A descrição arquivística dos fundos que contêm documentos arquivísticos digitais inclui – além da informação sobre seus contextos jurídico-administrativo, de proveniência, de procedimentos e documental – informações sobre mudanças sofridas pelos documentos arquivísticos digitais do produtor desde quando foi inicialmente produzido.

Fonte: Brasil (2013a, p. 39).

O Apêndice C – Estratégias de Preservação e de Manutenção dos Documentos Arquivísticos Digitais. Compreende estratégias extraídas, em sua maior parte, da obra "Diretrizes para a preservação do patrimônio digital, da Unesco" (original: Guidelines for the Preservation of Digital Heritagen[98]).

Este documento original da Unesco oferece um quadro para a descrição de estratégias de preservação de documentos arquivísticos digitais, que pode ser utilizado para proteger e para manter a acessibilidade de cópias autênticas ao longo da cadeia de preservação. A lista completa de estratégias possíveis adotadas pelo InterPARES 2 está conceitualmente dividida em duas categorias: estratégias de manutenção e estratégias de preservação.

a) As estratégias de manutenção são os requisitos mínimos para proteger e para manter a acessibilidade de cópias autênticas de documentos arquivísticos digitais. Há oito estratégias principais de manutenção (Seção A do Apêndice C):

   1) **Deve-se atribuir responsabilidades claras.** Esta atribuição de gerir o armazenamento e a proteção de documentos arquivísticos é do preservador.
   2) **Deve-se fornecer infraestrutura técnica adequada.** Inclui todos os recursos físicos e administrativos que possibilitam os processos de manutenção de

[98] Disponível em: Guidelines for the preservation of digital heritage - UNESCO Digital Library.

documentos arquivísticos (edificações, *hardware*, redes de computadores e os funcionários auxiliares necessários para mantê-los).

3) **Deve-se ter um plano de manutenção, de suporte e de substituição do sistema.** A implementação de um plano para manutenção, atualização ou substituição de *hardware* e *software*.
4) **Deve-se transferir regularmente dados para novos meios de armazenamento.**
5) **Deve-se adotar condições adequadas para meios de armazenamento.**
6) **Deve-se ter redundância (cópias múltiplas em suportes diferentes) e localização geográfica diferentes para armazenar os documentos.**
7) **Deve-se ter segurança do sistema.** Implementação de controles para assegurar que os componentes digitais dos documentos arquivísticos estejam expostos apenas a usuários ou a processos autorizados. incluem: restrições de acesso físico a locais onde os computadores estão guardados, bem como aos documentos nos próprios computadores (senhas ou autenticação biométrica para se acessar o sistema).
8) **Deve-se ter planejamento em caso de desastre.** Um plano de recuperação de desastres deve conter procedimentos detalhados para restaurar um sistema danificado e para orientar a recuperação dos sistemas de manutenção.

b) As estratégias de preservação (além da de manutenção) preconizam que os preservadores de documentos arquivísticos são responsáveis por estabelecer um sistema de preservação confiável[99] para expressar uma ou mais estratégias de preservação, que são de 13 tipos divididas em quatro grupos (Seção B – Apêndice C):

1) **Deve-se usar padrões.** O uso de padrões aumenta a probabilidade de estabilidade e de um suporte mais duradouro. Esses padrões podem ser de jure, se forem acordados de maneira formal, ou de fato, se forem adotados em larga escala pelas instituições.

1.1) **Formatos autodescritivos.** Análise e marcação de documentos arquivísticos de forma que funções, relacionamentos e estruturas dos elementos específicos possam ser descritos.

1.2) **Encapsulamento.** Ato de juntar um documento arquivístico e os meios

[99] Sistema que compreende todas as regras – e as ferramentas e mecanismos usados para implementá-las –, que orienta a manutenção e o uso intelectual e físico permanente dos documentos arquivísticos sob a custódia do preservador, e que oferece uma probabilidade circunstância de os documentos que se encontram no sistema serem autênticos (Brasil, 2013a, p. 40).

que dão acesso a ele, (normalmente num *wrapper* que descreve o que ele é) de forma que possa ser compreendido por uma vasta gama de tecnologias (tal como um documento XML). O *wrapper*, muitas vezes, inclui metadados que descrevem ou remetem às ferramentas adequadas.

1.3) **Restrição da gama de formatos a serem geridos (normalização).**

1.4) **Conversão.** Transferência de códigos digitais de uma geração de *hardware* ou de *software* para outra.

2) **Nas estratégias de preservação pode-se existir "dependência tecnológica".** Estas estratégias continuam a se basear no *hardware* e no *software* original, sem alterar os documentos arquivísticos.

2.1) **Preservação da tecnologia.** Manutenção do *software* e do *hardware* originais com os quais os documentos foram apresentados.

2.2) **Confiança na compatibilidade descendente ou reversa.** Confiança na capacidade de alguns *software* de interpretar corretamente e apresentar componentes digitais de documentos produzidos com versões anteriores dos mesmos *software.*

2.3) **Reengenharia de *software*.** Transformação do *software* à medida que a tecnologia muda. É semelhante à transformação dos formatos de documentos.

2.4) **Visualizadores e conversão no ponto de acesso.** O uso de ferramentas de *software* ou métodos de transformação que oferecem acessibilidade temporária quando necessário, usando a cadeia de dados original.

2.5) **Emulação.** Uso de um *software* que faz uma tecnologia se comportar como outra.

3) **Abordagens não digitais.** É o ato de copiar os documentos digitais para meios analógicos relativamente estáveis, tais como papel ou microfilme.

4) **Restauração de dados (arqueologia digital).** Recuperação de documentos arquivísticos a partir de suportes físicos. Os métodos de restaurar a inteligibilidade têm sido usados para resgatar documentos em formatos obsoletos. Após esses Apêndices, apresentam-se as recomendações nas cinco seções das Diretrizes do Preservador.

1. Esta seção é representada pelo conceito de "gestão". Deve-se gerenciar a estrutura da cadeia de preservação (A1).

Define os requisitos estruturais, bem como o desenho, a implementação e a

manutenção de uma estrutura de cadeia de preservação. Uma "estrutura de cadeia de preservação" inclui todos os elementos de política, de estratégia, de metodologia, entre outros necessários para o gerenciamento de documentos digitais.

1.1. **Deve-se definir o escopo e os objetivos do gerenciamento.** Esses elementos são definidos pelos responsáveis pela preservação do "programa de preservação digital"[100]. Por exemplo, o preservador poderá optar por preservar apenas o relatório final dos resultados de um estudo ou guardar os dados brutos, normalizados ou agregados, a fim de documentar a metodologia usada e o resultado obtido, bem como assegurar a disponibilidade dos dados para usos futuros. O escopo do programa de preservação ajudará a definir as estratégias do Apêndice C, Seção B.

1.2. **Deve-se adquirir recursos.** Os recursos para preservação digital dão-se em termos de financiamento, de capacidades tecnológicas e de conhecimento especializado. Há várias opções: a) adquirir novos recursos; b) redistribuir recursos existentes ou c) alavancar outros recursos. Para isso, um pré-requisito é fundamental, os recursos têm que ser sustentáveis.

1.3. **Deve-se concentrar nos documentos arquivísticos digitais.** Os preservadores devem assegurar que os recursos de preservação digital tenham como objetivo principal a proteção de cópias oficiais (documento arquivístico que o produtor considera oficial) de documentos digitais, em vez de cópias digitalizadas de documentos analógicos remanescentes.

1.4. **Deve-se oferecer orientação.** A cadeia de preservação de documentos arquivísticos digitais começa na produção, assim os preservadores devem fornecer orientações sobre a produção e a manutenção desses documentos.

1.5. **Deve-se dar um bom exemplo.** Os preservadores devem estabelecer um ambiente de elaboração e de manutenção de documentos que satisfaçam os padrões dos Requisitos de Referência para apoiar a Presunção de Autenticidade de Documentos Arquivísticos Digitais (Apêndice A). As organizações precisam de ambiente interno que ofereça:

---

[100] Ao definir o programa de preservação digital, os preservadores devem se basear em experiências anteriores. A fim de desenvolver políticas e estratégias adequadas, devem consultar o Arcabouço de Políticas do InterPARES 2 para orientação aplicável aos níveis organizacional, setorial, nacional, internacional e supranacional. Com relação às funções do programa de preservação, os responsáveis por ela devem consultar o padrão ISO OAIS e seguir o modelo de Cadeia de Preservação do InterPARES 2 para uma adaptação do padrão OAIS especificamente direcionado para documentos arquivísticos digitais. O planejamento deve também refletir a Lista de Auditoria para a Certificação de Repositórios Digitais (*Audit Checklist for Certifying Digital Repositories*), de autoria da Força-Tarefa sobre Repositórios *Digitais do National Archives and Records Administration* (Nara) e do *Research Libraries Group* (RLG) (Brasil, 2013a, p. 24).

- um treinamento prático para arquivistas sobre as tecnologias;
- o ponto de vista do usuário a respeito das soluções reais de manutenção de documentos arquivísticos e sobre como estas realmente funcionam num ambiente operacional cotidiano;
- um campo de testes onde as atualizações e as inovações possam ser introduzidas e avaliadas;
- um protótipo de trabalho que possa ser usado em demonstrações.

1.6. **Deve-se desenvolver procedimentos.** Isto é, controles sobre a transferência, a manutenção e a reprodução de documentos arquivísticos. Estes controles tem que abarcar os Requisitos de Base (Apêndice B) e procedimentos como: manter a custódia ininterrupta dos documentos arquivísticos; implementar e monitorar procedimentos de segurança e de controle; garantir que o conteúdo dos documentos arquivísticos e sua forma não sofram alterações após a reprodução.

1.7. **Deve-se implementar estratégias de manutenção** (Seção A do Apêndice C).

2. Esta seção é representada pela "avaliação". Deve-se avaliar documentos para preservação permanente (A4.2).

As decisões sobre destinação dos documentos arquivísticos precisam ser tomadas regularmente como parte da gestão de um sistema de manutenção de documentos.

2.1 **A atividade de avaliação deve ser feita assim que possível** (ver Seção 1.4).

2.2 **Dependendo do caso deve-se ter múltiplos proprietários.** Estes devem ser identificados durante o processo de avaliação, a fim de se estimar as ramificações de tal situação na preservação a longo prazo. Isto pode ocorrer, por exemplo, nos casos em que instituições governamentais de vários níveis contribuem com recursos de dados e partilham o acesso a eles.

2.3 **Verificação de autenticidade.** A verificação de autenticidade sempre fez parte do processo tradicional de avaliação de arquivos. Ao avaliar os documentos produzidos num ambiente digital, a verificação de sua autenticidade deve ser um processo mais aberto e mais visível, realizado e documentado pelo preservador. A cadeia de custódia ininterrupta, o conhecimento de práticas de manutenção de documentos e a verificação podem ainda oferecer algumas garantias de autenticidade. Também deve ser acrescentada a verificação da conformidade com cada uma das exigências dos Requisitos de Referência para a Autenticidade, listados na Seção 2.4.

2.4 **Deve-se documentar a verificação de autenticidade.** Tais controles incluem

cada um dos Requisitos de Referência para apoiar a Presunção de Autenticidade (ver Apêndice A do A.1-A.8).

2.5 **Deve-se monitorar documentos identificados para preservação a longo prazo.** Uma vez que a avaliação estiver completa, os documentos arquivísticos identificados para preservação devem ser monitorados em intervalos regulares até que sejam transferidos para o responsável pela preservação. Esse monitoramento inclui confirmar com o produtor que nada mudou no que diz respeito a como as classes de documentos identificadas para transferência ou recolhimento estão sendo criadas ou mantidas; ou confirmar que, caso tenham ocorrido mudanças, estas não afetaram a natureza e os atributos dos documentos, além de seu valor, sua autenticidade ou a sua viabilidade da sua preservação.

2.6. **Deve-se atualizar a avaliação.** As informações obtidas durante uma visita de monitoramento podem fornecer os primeiros indícios de que uma nova avaliação é necessária. No nível mais simples, os sistemas que inicialmente não continham documentos arquivísticos podem ser atualizados para fazê-lo.

2.7 **Deve-se identificar todos os componentes digitais.** Para extrair com sucesso documentos digitais do sistema em que foram produzidos, ou mesmo de um sistema de manutenção secundário, o preservador deve garantir que todos os componentes digitais essenciais sejam identificados e que suas relações sejam explicitadas nos metadados antes que o todo seja transferido.

2.8 **Deve-se determinar a viabilidade da preservação.** A determinação da viabilidade da preservação é essencial para a entidade preservadora entender seus custos, bem como os recursos necessários para a preservar documentos a longo prazo.

3. Esta seção é representada pelo conceito de receber/recepção. Deve-se receber os documentos arquivísticos selecionados para preservação permanente (A4.3).

Essa atividade tem como objetivo a autenticidade e a acessibilidade contínuas dos documentos arquivísticos digitais. O movimento que perpassa a custódia do produtor (ou do sucessor legítimo) para a custódia do preservador é um ponto crítico na cadeia de preservação e tem de ser feito com muito cuidado, para que não haja erros no processo de transferência ou de recolhimento.

3.1. **Deve-se desenvolver um plano compartilhado para a transferência.** Uma transferência ou recolhimento realizada com êxito, do atual custodiador à organização ou ao programa que assume a responsabilidade pela preservação, exige um plano acordado entre ambas as partes. O plano de transferência ou de recolhimento deve ser desenvolvido quando

se confirmar a viabilidade técnica do recebimento e da preservação.

3.2 **Deve-se aplicar procedimentos padronizados.** Os controles sobre transferência ou recolhimento da custódia do produtor-preservador, devem incluir:

- estabelecimento, implementação e monitoramento de procedimentos para registrar a transferência ou o recolhimento de documentos arquivísticos;
- verificação da autoridade para transferência ou para recolhimento;
- exame dos documentos arquivísticos para determinar se correspondem aos documentos arquivísticos que foram selecionados para transferência ou para recolhimento; e
- entrada dos documentos arquivísticos.

Como parte do processo de transferência ou de recolhimento, deve ser verificada a autenticidade dos documentos arquivísticos do produtor, que foi estimada durante o processo de avaliação. Isto inclui a verificação de que os metadados de identidade e integridade foram transferidos junto com seus respectivos documentos e permanecem vinculados a eles. Também deve-se verificar se os documentos estão acompanhados de qualquer documentação relevante sobre o ambiente técnico-administrativo em que foram produzidos e mantidos.

3.3 **Deve-se manter o formato lógico mais antigo disponível**. O formato lógico no qual os documentos arquivísticos foram originalmente produzidos, ou no qual eram mantidos pelo produtor à época da transferência, deve, quando possível, ser mantido pelo preservador, juntamente com quaisquer cópias de referência ou de preservação geradas após o recebimento.

Caso as estratégias de preservação, tais como as conversões, venham a falhar com o tempo, a guarda continuada do formato lógico inicial irá permitir ao preservador reiniciar o processo de preservação com a cópia “mais autoritária” dos documentos.

3.4. **Deve-se evitar duplicatas.** Informações acuradas sobre identidade são um primeiro passo para evitar a duplicação por parte do produtor e do preservador. Além disso, se o preservador fornecer cópias de referência ao produtor, após a transferência dos documentos, estas devem ser claramente identificadas, para evitar transferências acidentais.

3.5 **Deve-se documentar todo o processamento.** Confirmar a identidade do material transferido, verificando a existência de vírus, e confirmar se os arquivos recebidos estão completos torna mais provável que esses se mantenham inalterados. A conversão de arquivos, a renomeação de entidades digitais e o encapsulamento de arquivos são atividades mais invasivas. Nos dois casos, os preservadores devem documentar todo o processamento dos documentos arquivísticos digitais e seus efeitos, enquanto estiverem sob a sua custódia (ver

Apêndice B, Requisito B.2).

4. Esta seção é representada pela "preservação". Deve-se preservar os documentos arquivísticos recebidos (A4.4).

4.1 **Deve-se descrever os documentos arquivísticos** (ver Apêndice B, Requisito B.3, Seção 3.5 e 2.7).

4.2 **Deve-se identificar ramificações legais das ações de preservação.** Quando se escolhe uma estratégia de preservação, deve-se examinar as suas implicações legais. Por exemplo, a conversão de formato, a partir de um ambiente proprietário, poderá envolver o preservador em ações ilegais. Deve-se verificar os direitos autorais, de propriedades e intelectuais.

4.3 **Deve-se confirmar a eficácia da estratégia de preservação escolhida.** Em teoria, a estratégia de preservação selecionada deve ser testada nos documentos arquivísticos antes da sua transferência formal para o preservador, a fim de garantir que o seu desempenho esteja de acordo com o esperado. De forma mais realista, a maioria das organizações ou programas responsáveis pela preservação só podem financiar este tipo de teste excepcionalmente.

4.4 **Deve-se manter um armazenamento adequado.** Esta recomendação é uma das oito estratégias de manutenção obrigatórias da Seção 1.7 e discutidas no Apêndice C, Seção A.

5. Esta seção representa a "saída". Deve-se dar acesso aos documentos arquivísticos (A4.5).

O acesso aos documentos arquivísticos preservados é um componente essencial da cadeia de preservação. Ele deve ser gerenciado pelo preservador com o mesmo senso de responsabilidade e o mesmo grau de competência técnica e profissional empregados na avaliação, no recebimento, na transferência, na descrição e no armazenamento.

5.1 **Deve-se explicar como as cópias de referência foram feitas.** Ver Apêndice B, Requisito B.2.b. Também deve-se documentar como as medidas de controle do processo de reprodução em vigor foram estabelecidas e implementadas, e como são monitoradas a fim de assegurar que o conteúdo dos documentos arquivísticos reproduzidos não sofra alterações no curso da reprodução. Documentar o processo de reprodução é um meio essencial de comprovar que ele é transparente (livre de simulação ou engano). Esta transparência é necessária para o preservador como custodiador confiável.

5.2 **Deve-se explicar os requisitos técnicos para o acesso.** Os preservadores prestam

serviços de referência a diferentes tipos de usuários. Para satisfazer as necessidades desses, o preservador pode ter que realizar processamentos adicionais ou criar ferramentas especiais para apoiar os pesquisadores, por exemplo.

Os elementos de preservação digital evidenciados nas Diretrizes do Preservador foram: a preservação, a acurácia, a autenticidade, a descrição, a gestão, a obsolescência, a recepção, a saída (acesso), os requisitos de referência e de base, a avaliação e as estratégias de manutenção e de preservação. Elementos como a acurácia, a autenticidade, a obsolescência, assim como a identidade e a integridade recebem a mesma definição das Diretrizes do Produtor, portanto é redundante repeti-los.

Quadro 13 – Elementos do conceito de confiança extraídos das Diretrizes do Preservador

Conceitos	Definições
Avaliação	Análise e decisões sobre a destinação dos documentos arquivísticos feitas de forma regular. Nesta atividade, há cooperação entre os agentes envolvidos. Na avaliação é possível verificar a autenticidade dos documentos que serão preservados a longo prazo.
Descrição	Informações sobre os documentos arquivísticos e seus contextos, coletadas durante as fases de avaliação e de processamento. Deve incluir informações sobre direitos de propriedade intelectual ou questões de privacidade. Além disso, informações sobre as mudanças sofridas nos documentos e nos processos de transferência e de preservação.
Estratégias de Preservação e de Manutenção dos Documentos Arquivísticos Digitais	● As estratégias de manutenção são os requisitos mínimos para proteger e para manter a acessibilidade de cópias autênticas de documentos arquivísticos digitais. Como vimos, há oito estratégias principais de manutenção. ● As estratégias de preservação incluem a "dependência tecnológica", baseada na utilização de *hardware* e de *software* confiáveis para a preservação dos documentos a longo prazo. Essas estratégias abarcam 13 tipos divididos em quatro grupos.
Gestão	É fundamental que se faça o gerenciamento da estrutura da cadeia de preservação. Envolve a definição dos requisitos estruturais, bem como o desenho, a implementação e a manutenção de uma estrutura de cadeia de preservação, que inclui todos os elementos de política, de estratégia, de metodologia, entre outros necessários para o gerenciamento de documentos digitais.
Preservação	Proteção aos documentos arquivísticos. São procedimentos para garantir autenticidade em meio às mudanças tecnológicas.
Recepção	Atividade que tem a finalidade de garantir a autenticidade e a acessibilidade contínuas aos documentos arquivísticos digitais. A custódia do produtor-preservador é um ponto crítico na cadeia de preservação e tem de ser feito com muito cuidado, para que não haja erros no processo de transferência ou recolhimento.
Requisitos de Base	Mostram as condições mínimas para o preservador atestar a autenticidade das cópias de documentos arquivísticos digitais de guarda permanente.
Requisitos de Referência	Trazem as condições necessárias que servem como base para o preservador verificar a autenticidade dos documentos arquivísticos digitais do produtor. Elas possibilitam ao preservador inferir a autenticidade de documentos arquivísticos, na forma como foram produzidos, utilizados e mantidos pelo produtor. Isto é, os atributos que os documentos precisam para serem constatados como verdadeiros e autênticos.
Saída/Acesso	Dá-se pelo acesso aos documentos arquivísticos. Envolve o grau de responsabilidade e de competência técnica e profissional do preservador na cadeia de preservação.

Fonte: Brasil (2013a).

As Diretrizes do Produtor e do Preservador focam, em sua grande maioria, nos aspectos da preservação digital passiva. Fala-se em cadeia de custódia ininterrupta, mas não desenvolvem seus reais critérios ou sua importância como um arcabouço sistêmico e ativo. Outro ponto a destacar são os metadados como itens de segurança e de proteção informacional, visto que são elementos que manifestam, em um grau mais básico, pelo menos a presunção de autenticidade aos documentos arquivísticos, sejam eles digitais ou não.

8.4 DIRETRIZES PARA A PRESUNÇÃO DE AUTENTICIDADE DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS

Este documento foi aprovado pela Resolução n.º 37, de 19 de dezembro de 2012.[101] Estabelece diretrizes para a presunção de autenticidade de documentos arquivísticos digitais, com o objetivo de garantir a sua identidade e a sua integridade, minimizando os riscos de modificações, a partir do momento em que foram salvos pela primeira vez e em todos os acessos subsequentes.

Esta norma divide-se em cinco seções: 1. Introdução; 2. Conceitos; 3. Da autenticidade de documentos arquivísticos; 4. Presunção de autenticidade dos documentos arquivísticos digitais; 5. Autenticação dependente de tecnologia. O modo como são dissecadas as informações deste documento não segue a ordem das seções, mas sintetizamo-lo, enfocando, principalmente, a identificação dos elementos do conceito de confiança.

A autenticidade dos documentos arquivísticos digitais é ameaçada sempre que eles são transmitidos através do espaço ou do tempo. A obsolescência tecnológica é um dos fatores que põe os documentos em risco, por isso, deve-se utilizar de mecanismos para superar tal barreira. Uma das resoluções para este problema está na presunção de autenticidade, que acontece pela evidência de que os materiais foram mantidos com uso de tecnologias e de procedimentos administrativos que garantiram a sua autenticidade; ou que, pelo menos, minimizem os riscos de modificações a partir do momento em que foram salvos.

De uma forma geral, presunção de autenticidade é a inferência da autenticidade de um documento arquivístico feita a partir de fatos conhecidos sobre a maneira como aquele foi produzido e mantido. Ela é apoiada na análise de sua forma (aparência ou apresentação do documento) e de seu conteúdo (informação contida no documento), que nos documentos não digitais estão ligados ao suporte, ou seja, a forma, o conteúdo e o suporte são inseparáveis.

[101] Disponível em: Resolução nº 37, de 19 de dezembro de 2012 — Conselho Nacional de Arquivos (www.gov.br).

Baseia-se também numa cadeia de custódia ininterrupta. Uma das justificativas dessa presunção dá-se pelo fato de que os documentos arquivísticos digitais podem ser facilmente duplicados, distribuídos, renomeados, reformados ou convertidos, sem deixar rastros aparentes.

Assim, por meio da análise da forma, do conteúdo, do ambiente de produção, da manutenção, do uso e da preservação de documentos arquivísticos, e não apenas de suas características físicas ou soluções tecnológicas, tem-se a presunção de autenticidade. A mudança de suporte não compromete a autenticidade do documento digital porque, nesse caso, diferentemente dos documentos não digitais, forma e conteúdo estão desvinculados do suporte. Além desses elementos citados, o ambiente presunção dos documentos arquivísticos digitais também deve compreender:

- **procedimentos de controle** – quem produz, mantém/usa e preserva os documentos arquivísticos digitais e como essas ações são realizadas.
- **sistema informatizado confiável** – devendo incluir trilhas de auditoria, controle de acesso de usuários, métodos robustos para garantir a integridade dos documentos (como *checksum* ou *hash*), meios de armazenamento estáveis e medidas de segurança para controlar o acesso indevido à infraestrutura tecnológica (computadores, redes e dispositivos de armazenamento);
- **a entidade produtora e/ou custodiadora dos documentos arquivísticos digitais** – devendo demonstrar capacidade e conhecimento específico para gerenciar os documentos e trazer confiança aos usuários, além de possuir reputação idônea.

Existem três aspectos que envolvem a autenticidade dos documentos arquivísticos neste documento: o legal, o diplomático e o histórico.

1. Os documentos legalmente autênticos dão testemunhos sobre si mesmos, durante ou após sua produção, em que há uma autoridade pública representativa, garantindo seu caráter genuíno.
2. Os documentos diplomaticamente autênticos foram escritos de acordo com o tempo e o lugar indicados no texto, bem como assinados pela(s) pessoa(s) que têm autoridade para tal.
3. Os documentos historicamente autênticos atestam eventos que de fato aconteceram ou informações verdadeiras. É importante frisar que esses aspectos são interdependentes, de modo que um documento não atestado por uma autoridade pode ser diplomática e historicamente autêntico, mas sempre será legalmente inautêntico.

   Para melhorar a proteção e a segurança dos documentos arquivísticos digitais, também

deve-se implementar autenticação. A autenticação dependente de tecnologia são técnicas usadas para fornecer um mecanismo tecnológico que declara a autenticidade dos documentos digitais em um dado momento, por exemplo, a assinatura digital[102].

Como se sabe, autenticação é diferente de autenticidade. A autenticidade dá-se pela qualidade do documento ser verdadeiro; ser exatamente aquele que foi produzido. É composta pela identidade e pela integridade. A primeira define-se pelo conjunto dos atributos de um documento arquivístico que o caracterizam como único e o diferenciam de outros documentos arquivísticos (por exemplo: data, autor, destinatário, assunto, número identificador, número de protocolo). A segunda define-se pela capacidade de um documento arquivístico transmitir exatamente a mensagem que levou à sua produção (sem sofrer alterações de forma e conteúdo) de maneira a atingir seus objetivos. Já a autenticação configura-se pela declaração da autenticidade feita em um dado momento por uma pessoa autorizada tal.

A autenticação não garante necessariamente a autenticidade do documento, uma vez que se pode declarar como autêntico algo que não é. Assim, um documento pode ser considerado autêntico sem que nele conste uma autenticação.

As técnicas de autenticação não são tão efetivas para a transmissão dos documentos no tempo (quando são armazenados no longo prazo ou quando há atualização/substituição de *hardware*, de *software* ou de formatos). Isto porque, em virtude do seu objetivo e de sua forma de funcionamento, as assinaturas digitais não podem ser migradas para as novas cadeias de *bits* resultantes da conversão dos documentos para outros formatos de arquivo.

A assinatura digital não garantirá autenticidade se sua cadeia de *bit* for alterada por motivo de corrompimento, de adulteração ou de qualquer outra coisa, pois tal circunscrição não corresponderá mais a essa nova cadeia. Isto é, embora o documento conceitual seja o mesmo, ele passará a estar relacionado a uma nova cadeia de *bits*, que não tem mais a assinatura daquele momento.

Dessa forma, a assinatura digital garantirá apenas a integridade da cadeia de *bits* original, mas não a do documento conceitual ao longo do tempo. Assim, a não ser que o desenvolvimento da tecnologia dessas assinaturas permita que sua codificação seja preservada na nova cadeia de *bit*s resultante das inevitáveis conversões, a autenticidade não é garantida. Logo, tornam-se necessários outros procedimentos de gestão e de preservação, como a inserção de metadados, para assim trazer a confiabilidade.

---

[102] A legalidade da assinatura digital no Brasil é reconhecida pela ICP-Brasil. Disponível em: 2200-2 (planalto.gov.br).

Quadro 14 – Elementos do conceito de confiança extraídos da Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais

Conceitos	Definições
Assinatura digital	É o resultado de um cálculo matemático que envolve a cadeia de *bits* do documento e a chave da assinatura digital.
Autenticação	Declaração de autenticidade de um documento arquivístico, num determinado momento, resultante do acréscimo de um elemento ou da afirmação por parte de uma pessoa investida de autoridade para tal.
Autenticidade	Qualidade de um documento ser exatamente aquele que foi produzido, não tendo sofrido alteração, corrompimento e adulteração. A autenticidade é composta de identidade e integridade.
Cadeia de custódia ininterrupta	Linha contínua de custodiadores de documentos arquivísticos (desde o seu produtor até o seu legítimo sucessor) pela qual se assegura que esses documentos são os mesmos desde o início, não sofreram nenhum processo de alteração, sendo assim, autênticos.
Composição	Relação entre os dados de forma e conteúdo do documento digital que permite sua apresentação.
Confiabilidade	Credibilidade de um documento arquivístico enquanto uma afirmação do fato. Existe quando um documento arquivístico pode sustentar o fato ao qual se refere, e é estabelecida pelo exame da completeza, da forma do documento e do grau de controle exercido no processo de sua produção.
Conteúdo	Informação contida no documento.
Documento autêntico	Documento que teve sua identidade e sua integridade mantidas ao longo do tempo.
Documento diplomaticamente autêntico	São escritos de acordo com o tempo e o lugar indicados no texto, bem como assinados pela(s) pessoa(s) que têm autoridade para tal.
Documento historicamente autêntico	Atestam eventos que de fato aconteceram ou informações verdadeiras.
Documento legalmente autêntico	Dão testemunhos sobre si mesmos, durante ou após sua produção, em que há uma autoridade pública representativa, garantindo seu caráter genuíno.
Identidade	É o conjunto dos atributos de um documento arquivístico que o caracterizam como único e o diferenciam de outros documentos arquivísticos (ex.: data, autor, destinatário, assunto, número identificador, número de protocolo).
Integridade	é a capacidade de um documento arquivístico transmitir exatamente a mensagem que levou à sua produção (sem sofrer alterações de forma e conteúdo) de maneira a atingir seus objetivos.
Forma	Aparência ou apresentação do documento.
Obsolescência tecnológica	Fator que pode desencadear nos documentos arquivísticos riscos e ameaças de autenticidade através do tempo e espaço.
Presunção de autenticidade	Inferência da autenticidade de um documento arquivístico. Acontece pela evidência de que eles foram mantidos com uso de tecnologias e de procedimentos administrativos que garantiram a sua autenticidade; ou que, pelo menos, minimizem os riscos de modificações dos documentos a partir do momento em que foram salvos.

Fonte: Brasil (2012).

Queremos destacar dois elementos nesta normativa: a presunção de autenticidade e a obsolescência tecnológica. Ambos relacionam-se com o tempo. O primeiro, possibilitando os recursos necessários para a proteção e a segurança dos documentos arquivísticos, encarregado

de trazer subterfúgios, como os metadados, para comprovar a veracidade daquelas informações. O segundo, a consciência de que recursos tecnológicos precisam ser atualizados para dar continuidade aos registros arquivísticos, podendo ser, muitas vezes, um vilão.

8.5 MODELO DE REQUISITOS PARA SISTEMAS INFORMATIZADOS DE GESTÃO ARQUIVÍSTICA DE DOCUMENTOS – E-ARQ BRASIL

O Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos – e-ARQ Brasil foi desenvolvido pela CTDE em consonância com a política do Conarq e está em sua segunda versão, publicada em 2022.

A CTDE foi criada em 1995 pela Portaria nº. 8, de 23 de agosto de 1995, reestruturada em 2002 (Portaria nº. 60, de 7 de março de 2002), e conta com especialistas de vários setores do governo e da sociedade civil, os quais formam um grupo de trabalho multidisciplinar. Seu objetivo é definir e apresentar ao Conarq normas, diretrizes, procedimentos técnicos e instrumentos legais sobre gestão arquivística e preservação dos documentos digitais, em conformidade com os padrões nacionais e internacionais. Os estudos desenvolvidos por essa Câmara circundam os documentos digitais, principalmente, para a área da Arquivologia.

O e-ARQ Brasil, nesta nova configuração, foi aprovado pela Resolução nº 50, de 6 de maio de 2022[103], do Conarq, e específica todas as atividades e as operações técnicas da gestão arquivística de documentos desde a produção, tramitação, utilização e arquivamento até a sua destinação final. Todas essas atividades poderão ser desempenhadas por um Sigad, o qual, tendo sido desenvolvido em conformidade com os requisitos deste documento, confere credibilidade à produção e à manutenção de documentos arquivísticos.

A primeira versão do Modelo de Requisitos foi publicada em 2006 e complementada em 2009. Contudo, as orientações, as políticas e as especificações contidas neste documento atualizado, permanecem similares, estando alinhadas à necessidade de garantir que os documentos arquivísticos digitais sejam produzidos e mantidos de forma confiável, autêntica e acessível.

Esta versão trouxe atualização e adequação terminológica, ajustes com padrões, especificações e legislações mais atuais, e aprimorou a organização dos requisitos e a estrutura de metadados.

Termos como “relação orgânica” e “organicidade”, por exemplo, tiveram revisão em seu conceito. A relação orgânica configura-se pela relação de um documento com os demais que registram a mesma ação, sendo assim, uma característica dos documentos arquivísticos. E

[103] Disponível em: Resolução nº 50, de 06 de maio de 2022 — Conselho Nacional de Arquivos (www.gov.br).

a organicidade relaciona-se ao conjunto documental como um todo, portanto, uma característica do arquivo e não do documento.

A elaboração do e-ARQ Brasil fundamentou-se em documentos similares de âmbito internacional, mas adaptado à realidade e à legislação brasileira. O registro base utilizado foi o Modelo de Requisitos para a Gestão de Arquivos Eletrônicos (MoReq), publicado em 2001 pelo DLM Forum e Comissão Europeia[104], a norma DoD 5015.2-STD e a UK, Public Record Office, bem como os resultados e as publicações do InterPARES 2 e a norma AS ISO 15.489 de 2002.

Outro fator para a elaboração desta normativa partiu da definição dos conceitos de documento arquivístico e de documento arquivístico digital, tendo como fundamentos os estudos da Diplomática e da Arquivologia, enfatizando as *práxis* da gestão de documentos.

A partir disso, pode-se dizer que e-ARQ Brasil é uma especificação de requisitos a serem cumpridos pela organização produtora e recebedora de documentos, pelo sistema de gestão arquivística e pelos próprios documentos, a fim de garantir confiabilidade e autenticidade, assim como seu acesso, pelo tempo que for necessário. Traz também o conceito de Sigad, estabelecendo requisitos mínimos para ele, além de especificar todas as suas atividades e operações técnicas.

O e-ARQ serve para desenvolver um sistema informatizado ou avaliar um que já existe, cuja atividade central seja a gestão arquivística de documentos. Ou seja, ele é aplicável aos sistemas que produzem e mantêm documentos digitais, não digitais e híbridos. Com relação aos documentos não digitais, o sistema apenas apoia o registro dos metadados. No caso dos documentos digitais, o sistema inclui os próprios documentos, ou a referência a documentos digitais externos ao Sigad, além dos metadados.

Esta recomendação tem como objetivos orientar a implantação da gestão arquivística de documentos digitais e não digitais e fornecer especificações técnicas e funcionais, além de metadados, para o desenvolvimento de sistemas informatizados. Todavia, sozinho, não compreende todos os requisitos necessários para qualquer órgão; cada entidade deve considerar as suas especificidades.

Os documentos imagéticos, audiovisuais e sonoros, por exemplo, demandam metadados específicos de gestão e de descrição que não estão contemplados nestas diretrizes. Caso um Sigad contemple tais documentos, deverão ser implementados metadados específicos para garantir sua incorporação no programa de gestão documental da instituição.

---

[104] Disponível em: Fórum DLM - Fórum DLM (dlmforum.eu).

O e-ARQ Brasil está dividido em duas partes. *A Parte I, "Gestão arquivística de documentos"*, abrange um arcabouço teórico e conceitual para se desenvolver um programa de gestão arquivística de documentos. Possui nove seções, alguns em seções, e abarca temas como: política arquivística, planejamento e implantação do programa de gestão arquivística de documentos, procedimentos e controles do Sigad e instrumentos utilizados na gestão de documentos.

Eis as ramificações desta Parte I: 1. Considerações iniciais; 2. Base conceitual; 3. Aspectos essenciais da gestão arquivística de documentos; 4. Definição da política arquivística; 5. Designação de responsabilidades; 6. Planejamento do programa de gestão arquivística de documentos; 7. Implantação do programa de gestão arquivística de documentos; 7.1 Exigências a serem cumpridas pelo programa de gestão arquivística de documentos; 7.2 Metodologia do planejamento e da implantação do programa de gestão; 7.3 Suspensão ou extinção do Sigad; 8. Procedimentos e operações técnicas do sistema de gestão arquivística de documentos digitais e não digitais; 8.1 Captura; 8.2 Avaliação, temporalidade e destinação; 8.3 Pesquisa, localização e apresentação dos documentos; 8.4 Segurança: controle de acesso, trilhas de auditoria e cópias de segurança; 8.5 Armazenamento; 8.6 Preservação; 9. Instrumentos utilizados na gestão arquivística de documentos; 9.1 Plano ou código de classificação; 9.2 Tabela de temporalidade e destinação; 9.3 Manual de gestão arquivística de documentos; 9.4 Esquema de classificação de acesso e segurança; 9.5 Glossário; 9.6 Vocabulário controlado e tesauro.

A Primeira e a Segunda Seção compreendem algumas considerações acerca de definições e de atualizações de conceitos. Mencionamos alguns principais:

- **documento digital** – informação registrada a partir de dígitos binários, acessível e interpretável por meio de sistema computacional.
- **documento arquivístico digital** – informação registrada digital independe do suporte, produzida e/ou recebida por uma instituição pública ou privada, por pessoa física ou jurídica reconhecida e tratada por um sistema computacional.
- **Sistema** – conjunto de elementos interdependentes distribuído por entradas (recursos), por saídas (resultados), por realimentação (controle) e por meio ambiente.
- **Sistema de informação** – conjunto organizado (informatizado ou não) de políticas, de procedimentos, de pessoas e de equipamentos que produzem, processam, armazenam e proveem acesso à informação proveniente de fontes internas e externas para apoiar o desempenho das atividades de um órgão ou entidade.
- **Sistema informatizado** – apoia o acesso e a gestão de dados, de informação e de

documentos em um ambiente computacional.

- **Sistema de gestão arquivística de documentos** – conjunto de procedimentos e de operações técnicas, cuja interação permite a eficiência e a eficácia da gestão arquivística de documentos.
- **Sistema Informatizado de Gestão Arquivística de Documentos (Sigad)** – solução informatizada que controla o ciclo de vida dos documentos, desde a produção até a destinação final, seguindo os princípios da gestão arquivística de documentos. Pode compreender um *software* particular ou um determinado número de *software* integrados, adquiridos ou desenvolvidos por encomenda. Em síntese, é um sistema informatizado que apoia a gestão arquivística de documentos e o seu sucesso depende da implementação de um programa de gestão arquivística de documentos. Sendo assim, deve ser capaz de gerenciar, simultaneamente, documentos digitais e não digitais; considerando também os documentos híbridos, aqueles com partes digitais e não digitais. Para os documentos não digitais, o sistema registra apenas as referências sobre os documentos; e aos documentos digitais o armazenamento e o acesso são feitos por meio do próprio Sigad ou por ele geridos.

Como o Sigad é um *software* arquivístico, deve manter a relação orgânica entre os documentos e garantir a confiabilidade, a autenticidade e o acesso, ao longo do tempo. Suas operações englobam: captura de documentos, aplicação do CCD, controle sobre os prazos de guarda e de destinação, armazenamento seguro e procedimentos que garantam o acesso e a preservação em médio e longo prazos de documentos arquivísticos digitais e não digitais. Para um Sigad ser caracterizado como tal deve atender aos requisitos:

- captura, armazenamento, indexação, recuperação de todos os tipos de documentos arquivísticos e de todos os componentes digitais desse documento como uma unidade complexa (documento arquivístico digital constituído por vários componentes digitais – por exemplo – relatório acompanhado de planilhas, fotografias ou plantas, armazenados em diversos arquivos digitais, desde que considerada a sua relação orgânica);
- gestão dos documentos a partir do CCD para manter a relação orgânica entre os documentos;
- registro de metadados associados aos documentos para descrever os contextos desses mesmos documentos (jurídico-administrativo, de proveniência, de procedimentos, documental e tecnológico);
- estabelecimento de relacionamento entre documentos digitais, não digitais e híbridos;

- manutenção da autenticidade dos documentos;
- aplicação de TTDD, permitindo a seleção dos documentos para eliminação ou para guarda permanente;
- exportação de documentos para apoiar a transferência e o recolhimento;
- apoio à preservação dos documentos.

É importante mencionar que no caso dos documentos arquivísticos digitais, o Sigad deve abranger todos os tipos: textos, filmes, fotografias, registros sonoros, mensagens de correio eletrônico, páginas *Web*, bases de dados, dentre outros. E além disso, diferencia-se dos demais sistemas, isto é, dos Sistemas de Gerenciamento Eletrônico (GED), do *Enterprise Content Management* (ECM) e do Sistema de negócio, pois não necessariamente trazem a abordagem arquivística em suas funcionalidades.

A Terceira Seção envolve os *Aspectos Essenciais da Gestão Arquivística de Documentos*. Para que os documentos consigam desenvolver tal capacidade, eles precisam ser confiáveis, autênticos, acessíveis e compreensíveis, o que só é possível por meio da implantação de um "programa de gestão arquivística", o qual pressupõe a existência de dois instrumentos fundamentais – o CCD e a TTDD. Este programa deve ter como base a política arquivística e a designação de responsabilidades, além de um contexto jurídico-administrativo, de modo que esteja de acordo com a missão institucional e a legislação vigente.

A Quarta Seção traz a *Definição da Política Arquivística*, que tem como objetivo produzir, manter e preservar documentos confiáveis, autênticos, acessíveis e compreensíveis, para apoiar suas funções e atividades. O início dessa política dá-se por uma declaração oficial, de forma resumida, de como será realizada a gestão nas instituições. E para o seu êxito são fundamentais o apoio da direção superior e a alocação de recursos necessários à sua implementação.

Na Quinta Seção, de *Designação de Responsabilidades*, as autoridades responsáveis pelo gerenciamento documental terão de assegurar o cumprimento das normas e dos procedimentos previstos no programa de gestão. As responsabilidades devem ser distribuídas a todos os funcionários de acordo com a função e a posição hierárquica de cada um, envolvendo as seguintes categorias:

- direção superior: autoridade máxima responsável pela viabilidade da política de gestão arquivística de documentos;
- profissionais de arquivo: responsáveis pelo planejamento e implantação do programa de gestão arquivística, assim como pela avaliação e pelo controle dos trabalhos

executados no âmbito do programa;

- gerentes de unidades ou grupos de trabalho: responsáveis por garantir que os membros das equipes produzam e mantenham documentos como parte de suas tarefas, de acordo com o programa de gestão arquivística de documentos;
- usuários finais: responsáveis, em todos os níveis, pela produção e uso dos documentos arquivísticos em suas atividades rotineiras;
- gestores dos sistemas de informação e de tecnologia da informação: equipes responsáveis pelo projeto, desenvolvimento e manutenção de sistemas de informação nos quais os documentos arquivísticos digitais são gerados e usados, e pela operacionalização dos sistemas de computação e de comunicação.

A Sexta Seção, de *Planejamento do Programa de Gestão Arquivística de Documentos*, envolve o levantamento e a análise da realidade institucional, o estabelecimento das diretrizes e dos procedimentos a serem cumpridos pelo órgão ou entidade, o desenho do sistema de gestão arquivística de documentos e a elaboração de instrumentos e de manuais. Iniciando-se com o diagnóstico, por exemplo.

A sétima seção inclui a *Implantação do Programa de Gestão Arquivística de Documentos*, que carrega a execução e o acompanhamento de ações e de projetos, referindo-se à capacitação de pessoal, à implantação de sistemas de gestão arquivística, à integração com os sistemas de informação existentes e os processos administrativos dos órgãos. Assim como, suspensão de atividades e de procedimentos que forem considerados inadequados.

Ademais, tanto o "programa de gestão arquivística" quanto os "documentos arquivísticos" devem cumprir algumas obrigações, conforme a Subseção 7.1. Dessarte, os documentos arquivísticos devem: refletir corretamente o que foi comunicado, decidido ou a ação implementada; conter os metadados necessários para documentar a ação; ser capaz de apoiar as atividades; prestar contas das atividades realizadas. Já o programa de gestão arquivística deve: contemplar o ciclo de vida dos documentos; garantir o acesso aos documentos; manter os documentos em ambiente seguro; reter os documentos somente pelo período estabelecido na TTDD; implementar estratégias de preservação dos documentos desde a sua produção e pelo tempo que for necessário; garantir as seguintes características do documento arquivístico (Quadro 15). Cada uma das características do documento arquivístico corresponde a um novo conjunto de exigências a serem cumpridas pelo programa de gestão.

Quadro 15 – Características dos documentos arquivísticos à luz do e-ARQ Brasil - versão 2

Relação orgânica	O documento arquivístico caracteriza-se pela relação orgânica, ou seja, pelas relações que mantém com os demais documentos do órgão ou entidade e que refletem suas funções e atividades. Os documentos arquivísticos não são coletados artificialmente, mas estão ligados uns aos outros por um elo que se materializa por meio do registro ou do CCD ou do arquivamento, que os contextualiza no conjunto ao qual pertencem. Os documentos arquivísticos apresentam um conjunto de relações que devem ser mantidas. **Exigências da relação orgânica:** os procedimentos de gestão arquivística devem registrar e manter as relações entre os documentos e a sequência das atividades realizadas, por meio da aplicação de um CCD.
Unicidade	O documento arquivístico é único no conjunto documental ao qual pertence. Podem existir cópias, mas cada cópia é única em seu lugar, porque o conjunto de suas relações com os demais documentos do grupo é sempre único. **Exigências da unicidade:** o programa de gestão arquivística deve prever a identificação de cada documento individualmente, sem perder de vista o conjunto de relações que o envolve.
Confiabilidade	Um documento arquivístico confiável é aquele que tem a capacidade de sustentar os fatos que atesta. A confiabilidade (fidedignidade, em inglês *reliability*) está relacionada ao momento em que o documento é produzido e à veracidade do seu conteúdo. Para tanto, há que ser dotado de completeza e ter seus procedimentos de produção bem controlados. A completeza dá-se pela presença de todos os elementos intrínsecos e extrínsecos exigidos pela organização produtora e pelo sistema jurídico-administrativo ao qual pertence, de maneira que esse mesmo documento possa ser capaz de gerar consequências. Dificilmente, pode-se assegurar a veracidade do conteúdo de um documento; ela é inferida da completeza e dos procedimentos de produção. A confiabilidade é uma questão de grau, ou seja, um documento pode ser mais ou menos confiável. **Exigências da confiabilidade:** para garantir a confiabilidade, o programa de gestão arquivística dos órgãos e entidades deve assegurar que os documentos arquivísticos sejam produzidos no momento em que ocorre a ação, ou imediatamente após, por pessoas diretamente envolvidas na condução das atividades e devidamente autorizadas; e com o grau de completeza requerido tanto pelo próprio órgão ou entidade como pelo sistema jurídico.
Autenticidade	Documento arquivístico autêntico é aquele que é o que diz ser, independentemente de se tratar de minuta, de original ou de cópia, e que é livre de

	adulterações ou qualquer outro tipo de corrupção. Enquanto a confiabilidade está relacionada ao momento da **produção**, a autenticidade está ligada à **transmissão** do documento e à sua preservação e custódia. Um documento autêntico é aquele que se mantém da forma como foi produzido, portanto apresenta o mesmo grau de confiabilidade que tinha no momento de sua produção. Um documento não completamente confiável, mas transmitido e preservado sem adulteração ou qualquer outro tipo de corrupção, é autêntico. **Exigência da autenticidade:** para assegurar a autenticidade dos documentos arquivísticos, o programa de gestão arquivística tem que garantir sua identidade e sua integridade. Para tanto, deve implementar e documentar políticas e procedimentos que controlem a transmissão, a manutenção, a avaliação, a destinação e a preservação dos documentos, garantindo que eles estejam protegidos contra acréscimo, supressão, alteração, uso e ocultação indevidos.
Acessibilidade	Um documento arquivístico acessível é aquele que pode ser localizado, recuperado, apresentado e interpretado. **Exigência da acessibilidade:** para assegurar o acesso, o programa de gestão arquivística deve garantir a transmissão de documentos para outros sistemas sem perda de informação e de funcionalidade. O Sigad deve ser capaz de recuperar qualquer documento, a qualquer tempo, e de apresentá-lo com a mesma forma que tinha no momento de sua produção.

Fonte: Brasil (2022, grifo nosso).

A *Metodologia do Planejamento e da Implantação de Programa de Gestão Arquivística de Documentos* da Subseção 7.2 estabelece estabelece oito passos:

1) **Levantamento preliminar**, que consiste em identificar e registrar atos normativos, legislação, regimento e regulamento.
2) **Análise das funções, das atividades desenvolvidas e dos documentos produzidos,** que consiste em identificar, documentar e classificar cada função e atividade, bem como em detectar e registrar os fluxos de trabalho e os documentos produzidos.
3) **Identificação das exigências a serem cumpridas para a produção de documentos,** consiste em identificar que os documentos devem ser produzidos, determinar a forma documental que melhor satisfaça cada função ou atividade desempenhada e definir quem está autorizado a produzir cada documento. Devem tomar por base a legislação vigente, as normas internas e os riscos decorrentes da falta de registro de uma atividade em documento arquivístico.
4) **Análise dos sistemas existentes,** serve para identificar e analisar o sistema de gestão

arquivística de documentos e outros sistemas de informação e de comunicação existentes no órgão.

5) **Identificação das estratégias para satisfazer as exigências a serem cumpridas para a produção de documentos arquivísticos,** consiste em determinar as estratégias (padrões, procedimentos, práticas e ferramentas) que levem ao cumprimento das exigências para a produção de documentos arquivísticos.
6) **Projeto do sistema de gestão arquivística de documentos,** visa projetar um sistema de gestão arquivística de documentos que incorpore as estratégias selecionadas no passo 5).
7) **Implementação do sistema de gestão arquivística de documentos,** é a execução do projeto por meio de: treinamento de pessoal; introdução do sistema de gestão arquivística de documentos ou adaptação de um já existente; integração do sistema de gestão arquivística de documentos com os procedimentos e os sistemas de informação e de comunicação existente.
8) **Monitoramento e ajustes do sistema de gestão arquivística de documentos,** consiste em recolher, de forma sistemática, informação sobre o desempenho do sistema de gestão arquivística de documentos. Verifica-se o desempenho avaliando se os documentos estão sendo produzidos e organizados de acordo com as necessidades do órgão e se estão relacionados aos processos dos quais fazem parte.

A última Subseção 7.3 – *Suspensão ou Extinção do Sigad*. Se um sistema de negócio ou um Sigad que mantém documentos arquivísticos for suspenso ou extinto, devem eles ficar acessíveis para consulta e novos documentos não devem ser incluídos. Aos documentos já inseridos, poderão ser removidos de acordo com as diretrizes de destinação ou transferidos para outros sistemas. O processo de suspensão ou de extinção deve ser documentado, inclusive os planos de conversão ou de mapeamento dos dados, pois essas informações serão necessárias à verificação de autenticidade e manutenção do acesso aos documentos inseridos no sistema suspenso ou extinto.

A Seção Oito caracteriza-se pelos *Procedimentos e Operações Técnicas do Sistema de Gestão Arquivística de Documentos Digitais e Não Digitais,* e divide-se em Seis Subseções: 8.1 *Captura* (incluindo as ações de registro, de classificação; de indexação, de atribuição de restrição de acesso e de arquivamento); 8.2 *Avaliação, temporalidade e destinação* (incluindo a eliminação, transferência e recolhimento); 8.3 *Pesquisa, localização e apresentação dos documentos*; 8.4 *Segurança: controle de acesso, trilhas de auditoria e cópias de segurança* (que além dessas ações, incluem as de uso e rastreamento e segurança da infraestrutura); 8.5

Armazenamento e 8.6 *Preservação*.

8.1 *Captura***:** declara um documento arquivístico como tal, incorporando-o ao sistema de gestão arquivística a partir de, no mínimo, as seguintes ações: registro; classificação; indexação; atribuição de restrição de acesso e arquivamento. Seu objetivo é enfatizar um documento como arquivístico ao declarar sua relação orgânica.

A captura em documento de papel é feita quando ele é registrado, classificado e arquivado. Um Sigad deve capturar e registrar todos os documentos arquivísticos que foram produzidos em outros sistemas informatizados, que pode acontecer automaticamente. Além do código de classificação, descritores, número de protocolo e número de registro, a captura pode prever a introdução de outros metadados, tais como data e hora de produção, da transmissão e do recebimento do documento; nome do autor, do originador, do redator e do destinatário, entre outros. A captura tem como pré-requisito a definição de: quais documentos (produzidos e recebidos) serão capturados pelo sistema; os critérios de acesso a eles e por quanto tempo serão retidos.

a) **Registro:** formaliza a captura dos documentos dentro do sistema de gestão arquivística por meio da atribuição de um número identificador e de uma descrição informativa. No Sigad, essa descrição corresponde à atribuição de metadados, que pode equivaler ao registro de protocolo.
b) **Classificação:** analisa e identifica o conteúdo dos documentos arquivísticos, para selecionar a classe sob a qual serão recuperados. É feita a partir de um CCD elaborado pelo órgão e pode incluir ou não a atribuição de código aos documentos.
c) **Indexação:** atribuição de termos à descrição do documento, utilizando vocabulário controlado ou lista de descritores, tesauro e o próprio CCD. A seleção dos termos pode ser feita com base em: tipo documental; título ou cabeçalho do documento; assunto do documento; datas associadas com as transações registradas no documento; documentação anexada. Tem como objetivo ampliar as possibilidades de busca e de facilitar a recuperação dos documentos, de forma manual ou automática.
d) **Atribuição de restrição de acesso:** análise dos documentos em relação à ostensividade ou à sigilosidade. No caso da sigilosidade, a legislação vigente estabelece procedimentos específicos para seu tratamento, como os graus de sigilo e de restrições de acesso.
e) **Arquivamento**: técnica de colocar e de conservar numa mesma ordem, devidamente classificados de acordo com o CCD, todos os documentos de uma instituição,

utilizando métodos adequados, de forma que fiquem protegidos e sejam facilmente localizados e manuseados.

8.2 *Avaliação, temporalidade e destinação:* avaliação é o processo de análise dos documentos arquivísticos, visando estabelecer os seus prazos de guarda e a sua destinação, de acordo com os valores primários e secundários. Os prazos de guarda e as ações de destinação deverão estar formalizados na TTDD. Já a destinação é efetivada depois da atividade de seleção, que consiste na separação dos documentos de valor permanente daqueles passíveis de eliminação, mediante critérios e técnicas estabelecidos na TTDD.

a) **Eliminação:** significa eliminar os documentos que, na avaliação, foram considerados sem valor para guarda permanente, devendo ser precedida da elaboração da listagem, do edital de ciência de eliminação e do termo de eliminação, de acordo com a legislação vigente.
b) **Transferência:** passagem de documentos do arquivo corrente para o arquivo intermediário, onde aguardarão o cumprimento dos prazos de guarda e a destinação final. Os documentos devem ser acompanhados de listagem de transferência, podendo ser realizada de duas formas: para uma área de armazenamento apropriada sob controle da entidade que produziu o documento; e para uma instituição arquivística, que ficará responsável pela custódia do documento.
c) **Recolhimento:** entrada de documentos nos arquivos permanentes de acordo com a jurisdição arquivística a que pertencem. Os documentos recolhidos devem ser acompanhados de instrumentos que permitam sua identificação e controle.

8.3 *Pesquisa, localização e apresentação dos documentos:* um sistema de gestão arquivística deve prever funções de recuperação e de acesso aos documentos e às informações neles contidas. Essa recuperação inclui pesquisa, localização e apresentação dos documentos. Num Sigad, a apresentação dos documentos faz-se pela sua exibição em um ou mais dispositivos – monitor de vídeo, impressora, caixa de som entre outros. A pesquisa é feita utilizando instrumentos de busca, como guias, inventários, catálogos, repertórios e índices. Num Sigad, tal pesquisa ocorre por meio de parâmetros predefinidos e selecionados entre as informações coletadas no momento do registro do documento e entre os metadados a ele associados. Todos os recursos de pesquisa, localização e apresentação de documentos precisam ser submetidos a

controles de acesso e de segurança.

8.4 *Segurança: controle de acesso, trilhas de auditoria e cópias de segurança:* entre esses procedimentos, tem-se o uso de controles técnicos e programáticos (diferenciando tipos de documentos), perfis de usuários e características de acesso aos dados e a manutenção de trilhas de auditoria e de rotinas de cópias de segurança.

a) **controle de acesso:** o sistema de gestão arquivística precisa limitar ou autorizar o acesso a documentos por usuário ou grupos de usuários. Deve garantir no mínimo: restrição de acesso aos documentos; exibição dos documentos, criptografados ou não, e dos metadados somente aos usuários autorizados; uso e intervenção nos documentos somente pelos usuários autorizados e registro de acesso em trilha de auditoria.

b) **Uso e rastreamento:** o uso dos documentos pelos usuários deve ser registrado pelo Sigad nos seus respectivos metadados. A gestão desse uso inclui: identificação da permissão de acesso dos usuários, do que cada um pode acessar; identificação da precaução de segurança e da categoria de sigilo dos documentos; garantia de que somente os indivíduos autorizados tenham acesso aos documentos classificados e aos originalmente sigilosos; registro de todos os acessos, tentativas de acesso e uso dos documentos (visualização, impressão, transmissão e cópia para a área de transferência), com identificação de usuário, data, hora e, se possível, estação de trabalho; revisão periódica das classificações de acesso a fim de garantir sua atualização.

c) **Trilha de auditoria:** conjunto de informações registradas que permite o rastreamento de intervenções ou tentativas de intervenção no documento arquivístico digital ou no Sigad. Serve para registrar o movimento e o uso dos documentos arquivísticos dentro de um Sigad (captura, registro, classificação, indexação, arquivamento, armazenamento, recuperação da informação, acesso e uso, preservação e destinação), informando quem operou, a data e a hora, bem como as ações realizadas. Tendo como objetivo fornecer informações sobre o cumprimento das políticas e das regras da gestão arquivística de documentos.

d) **Cópias de segurança:** o Sigad deve prover meios de realização de cópias de segurança (*backup*). O processo reverso ao *backup* é a restauração (*restore*), que consiste em recuperar as informações para o ambiente de produção do Sigad em um estado consistente. As cópias de segurança não podem ser confundidas com uma estratégia de preservação de longo prazo.

e) **Segurança da infraestrutura:** a natureza das medidas de segurança da infraestrutura de instalações do acervo digital diz respeito a requisitos operacionais não diferindo muito daquela do acervo não digital. Então: as salas reservadas a computadores, a servidores e a equipamentos de rede e ao armazenamento dos documentos digitais devem ter temperatura ambiente e umidade relativa do ar controladas, e fornecimento estável de energia elétrica; equipamentos contra incêndio devem estar presentes em toda a área de instalação e de acordo com as normas de segurança estabelecidas; o órgão ou entidade tem que prever instalações adequadas de para-raios, com procedimentos de manutenção periódica, seguindo a legislação e as normas técnicas estabelecidas; a área reservada à instalação do Sigad deve ser compartimentada, com o objetivo de controlar o acesso às informações; as salas de computadores são de uso exclusivo de pessoal autorizado e devem ter controle eletrônico de acesso; para acesso a áreas de segurança, de identificações e de credenciais de segurança têm de estar de acordo com as atribuições individuais e as regras de segurança do órgão.

8.5 *Armazenamento:* é guardar os documentos arquivísticos em local apropriado. No caso dos documentos digitais, dá-se em dispositivos de memória não voláteis, permeando todo o seu ciclo de vida. Esse armazenamento deve garantir a autenticidade e o acesso aos documentos pelo tempo estipulado na TTDD.

8.6 *Preservação:* em linhas tradicionais, a preservação concentra-se na estabilidade do suporte da informação. Contudo, nos documentos digitais, o foco da preservação é a manutenção do acesso, que pode implicar mudança de suporte e formato, bem como atualização do ambiente tecnológico. Assim, o Sigad deve utilizar da interoperabilidade com um RDC-Arq para armazenar documentos de guarda permanente.

A Nona Seção enfatiza os *Instrumentos Utilizados na Gestão Arquivística de Documentos*, dividindo-se em dois tipos: os instrumentos principais, os quais estão na redoma arquivística: o CCD, codificado ou não, baseado nas funções e nas atividades da entidade; a TTDD, o manual de gestão arquivística de documentos; o esquema de classificação referente à segurança e ao acesso aos documentos. E também os instrumentos adicionais: glossário; vocabulário controlado; tesauro. Outros instrumentos podem apoiar a gestão.

A Parte II – "Especificação de requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (Sigad)" – descreve os requisitos necessários para se desenvolver um Sigad. Divide-se em *Requisitos Funcionais* (detalham as funções que o sistema deve ser capaz de realizar sob o ponto de vista do usuário final); *Requisitos Não Funcionais* (que não

estão diretamente relacionados às funcionalidades do sistema, mas que são relevantes para a sua implementação); *Metadados; Glossário; Anexo e Referências* (estes três últimos não são objetos de análise de nossa tese). Quando da implantação de um Sigad, torna-se necessário verificar e observar o cumprimento desses requisitos.

Os *Requisitos Funcionais* têm Oito Seções com suas respectivas Subseções, e tratam de: 1. Organização dos documentos arquivísticos; 1.1 Configuração e administração do plano de classificação no Sigad; 1.2 Configuração da tabela de temporalidade e destinação de documentos; 1.3 Classificação e metadados das unidades de arquivamento; 2. Captura; 2.1 Procedimentos gerais; 2.2 Captura em lote; 2.3 Captura de mensagens de correio eletrônico; 2.4 Captura de documentos não digitais ou híbridos; 2.5 Formato de arquivo e estrutura dos documentos a serem capturados; 2.6 Estrutura dos procedimentos de gestão; 3. Avaliação: temporalidade e destinação; 3.1 Aplicação da tabela de temporalidade e destinação de documentos; 3.2 Exportação de documentos; 3.3 Eliminação; 3.4 Avaliação e destinação de documentos arquivísticos não digitais e híbridos; 4. Pesquisa, localização e apresentação dos documentos; 4.1 Aspectos gerais; 4.2 Pesquisa e localização; 4.3 Apresentação: visualização, impressão, emissão de som; 5. Elaboração de documentos; 5.1 Procedimentos gerais; 5.2 Gerenciamentos dos dossiês/processos; 5.3 Requisitos adicionais para o gerenciamento de processos; 5.4 Volumes: abertura, encerramento e metadados 5.5 Gerenciamento de documentos e processos/dossiês arquivísticos não digitais e híbridos; 6. Tramitação e fluxo de trabalho; 6.1 Controle do fluxo de trabalho; 6.2 Controle de versões e do status do documento; 7. Segurança; 7.1 Cópias de segurança; 7.2 Controle de acesso; 7.3 Classificação da informação quanto ao grau de sigilo e restrição de acesso à informação sensível; 7.4 Trilhas de auditoria; 7.5 Assinatura digital; 7.6 Carimbo digital do tempo; 7.7 Marcas d'água digitais; 7.8 Assinatura cadastrada mediante identificação do usuário e senha; 7.9 Criptografia; 7.10 Acompanhamento de mudança de suporte ou de local; 7.11 Autoproteção; 7.12 Alterar, apagar e truncar documentos arquivísticos digitais; 8. Preservação; 8.1 Aspectos físicos; 8.2 Aspectos lógicos; 8.3 Aspectos gerais.

Os requisitos imprescindíveis para um Sigad são: 1. *Organização dos documentos arquivísticos*; 2. *Captura*; 3. *Avaliação: temporalidade e destinação*; 7. *Segurança*; e 8. *Preservação*. No caso de um Sigad apoiar a produção de documentos dentro do sistema, também são considerados imprescindíveis: 5. *Elaboração de documentos* e 6. *Tramitação e fluxo de trabalho.*

Os *Requisitos Não Funcionais* têm Sete Seções, e tratam de: 9. Armazenamento; 9.1 Durabilidade; 9.2 Capacidade; 9.3 Efetividade de armazenamento; 10. Funções

administrativas; 11. Conformidade com a legislação e regulamentações; 12. Usabilidade; 13. Interoperabilidade; 14. Disponibilidade; e 15. Desempenho e escalabilidade.

A seção dos *Metadados* é dividida em Sete Partes: 1. Documento; 2. Evento de gestão; 3. Classe; 4. Evento de gerenciamento da classe; 5. Componente digital; 6. Evento de preservação; e 7 Agente.

Nas Seções dos *Requisitos Funcionais e Não Funcionais* são apresentadas tabelas correspondendo a referências (numéricas), requisitos e níveis de obrigatoriedade (Figura 0). Os níveis de obrigatoriedade seguem as seguintes classificações, de acordo com o grau maior ou menos de exigência para que um Sigad possa desempenhar suas funções: O – Obrigatório; AD – Altamente Desejável; F – Facultativo.

Assim, os requisitos são considerados: (O) obrigatórios quando indicados pela frase: "O Sigad tem que..."; (AD) altamente desejáveis quando indicados pela frase: "É altamente desejável que o Sigad..."; (F) facultativos quando indicados pela frase: "O Sigad pode...".

- **Tem**: o requisito é imprescindível.
- **Altamente Desejável**: podem existir razões válidas em circunstâncias particulares para ignorar um determinado item, mas a totalidade das implicações deve ser cuidadosamente examinada antes de se escolher uma proposta diferente.
- **Pode**: o requisito é opcional. Tanto para os requisitos considerados altamente desejáveis como para os requisitos facultativos, é preciso observar que uma implementação que não inclua determinado item altamente desejável ou facultativo deve estar preparada para interoperar com uma outra implementação que inclui o item, mesmo tendo funcionalidade reduzida. De forma inversa, uma implementação que inclua um item altamente desejável ou facultativo deve estar preparada para interoperar com uma outra implementação que não inclui o item. Abaixo, segue um exemplo de como está disposta a tabela com seus elementos a serem cumpridos por um Sigad no e-ARQ Brasil.

Figura 37 – Tabela com os elementos a serem cumpridos por um Sigad nos Requisitos Funcionais e Não Funcionais

1.1. Configuração e administração do plano de classificação no SIGAD

Os requisitos desta seção referem-se às funcionalidades do SIGAD para apoiar a configuração do plano de classificação no SIGAD, ou seja, como criar e manter um plano de classificação em um SIGAD.

Referência	Requisito	Obrig.[36]
1.1.1	Um SIGAD tem que incluir e ser compatível com o plano de classificação do órgão ou entidade, com as seguintes informações: • identificador da classe; • nome da classe; • código da classe; • subordinação da classe; • indicação de permissão de uso; • indicação de classe ativa/inativa. *O plano de classificação dos integrantes do SINAR deve estar de acordo com a legislação e ser aprovado pela instituição arquivística na esfera de competência específica.*	O
1.1.2	Um SIGAD tem que garantir a criação de classes, subclasses, grupos e subgrupos nos níveis do plano de classificação de acordo com o método de codificação adotado.	O
1.1.3	Um SIGAD tem que permitir a usuários autorizados acrescentar novas classes sempre que necessário.	O
1.1.4	Um SIGAD tem que registrar a data de abertura de uma nova classe no respectivo metadado.	O

Fonte: Brasil (2022, p. 51).

Em relação aos *Metadados*, os níveis de obrigatoriedade também são classificados de acordo com o grau maior ou menor de exigência para apoiar as funcionalidades do Sigad. Cada elemento de metadado é classificado como: (O) obrigatório; (OA) obrigatório, se aplicável; e (F) facultativo.

- **Obrigatório:** o elemento deve, obrigatoriamente, estar presente.
- **Obrigatório, se aplicável:** o elemento pode ser aplicável ou não, porém, se aplicável, sua presença é obrigatória.
- **Facultativo**: os elementos facultativos estão relacionados à implementação do Sigad e cabe à instituição decidir ou não pelo seu uso. O grau facultativo pode tornar-se obrigatório para determinada instituição, dependendo de suas necessidades específicas.

Figura 38 – Ficha com o preenchimento dos metadados na seção de Metadados do e-ARQ Brasil 2022

1.2. Número do documento

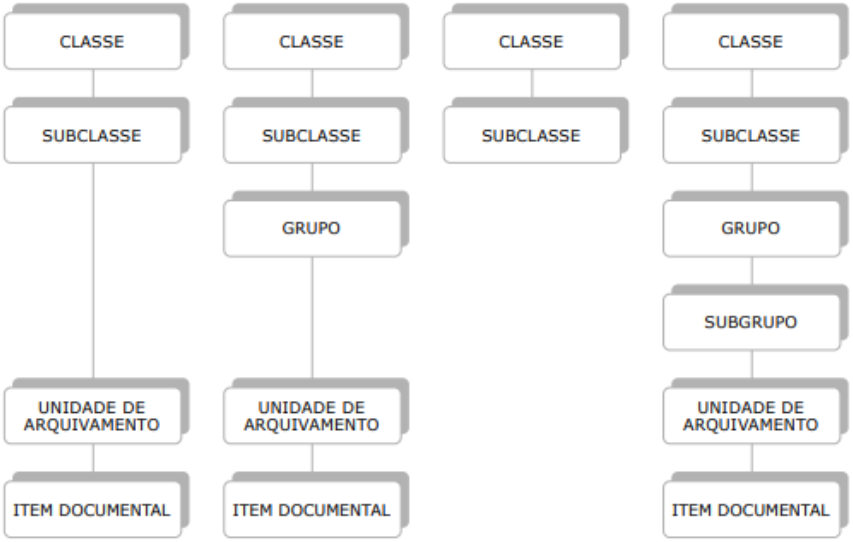
Designação	Número do documento		
Rótulo	earq.documento.numero		
Definição	Número ou código alfanumérico atribuído ao documento no ato da sua produção.		
Objetivo	Permitir a identificação precisa de um documento.		
Aplica-se a	Processo/dossiê **NA** Ver elemento 1.5 (Número de protocolo do processo)	Volume **NA** Ver elemento 1.7 (Número do volume)	Documento **OA**
Repetibilidade	-	-	Não repetível
Nota de aplicação	Em geral é uma numeração seriada correspondente a uma espécie documental, tal como memorandos, ofícios, avisos, portarias, ordens de serviço e outros. Pode ser acrescido da data de produção e da sigla do órgão produtor.		
Exemplos	*Mem.119/COAD/DIRHU;* *Ofício n. 78/2008/GABIN-AN;* *Aviso 123/2008-SCT-PR.*		
Regra de preenchimento	Deve, preferencialmente, ser gerado de forma automática pelo SIGAD. As instituições devem seguir normas específicas em seu âmbito de atuação ou esfera de competência para geração desse número.		
Requisito	2.1.9		
Equivalência	--		

Fonte: Brasil (2022, p. 123).

Entretanto, não é alçada para nossa tese expor, nem discutir, os requisitos de obrigatoriedade do e-ARQ Brasil, uma vez que torna-se necessário a quem quer avaliar um Sigad ou os seus metadados. Sendo assim, evidenciam-se sinteticamente apenas as Seções ainda não destacadas dos *Requisitos Funcionais*: 1. *Organização dos documentos arquivísticos*; 5. *Elaboração de documentos* e 6. *Tramitação e fluxo de trabalho*.

A *Organização dos documentos arquivísticos* é feita com base num CCD e constitui-se no núcleo central de qualquer Sigad. Por meio dele, são estabelecidas a hierarquia e a relação orgânica dos documentos, na forma como eles são organizados em unidades de arquivamento. Assim, os documentos são reunidos em unidades lógicas de arquivamento por metadados, como, número identificador, título e código, conforme o diagrama abaixo.

Figura 39 – Diagrama de organização dos documentos



Fonte: Brasil (2022, p. 51).

A Unidade de Arquivamento constitui o documento para fins de classificação, de arranjo, de armazenamento e de notação. Pode ser um dossiê ou um processo em que estejam reunidos documentos sob o mesmo código de classificação, como, por exemplo, as folhas de ponto de determinado ano, relatórios de atividades de um período específico ou atas de reunião.

A *Elaboração de documentos* refere-se àqueles que têm funcionalidades que apoiam à redação e à configuração dos documentos arquivísticos, bem como a formação de dossiês/processos.

Já a *Tramitação e fluxo de trabalho* tratam apenas dos casos em que o Sigad inclui recursos de automação de fluxo de trabalho (*workflow*). Seus requisitos abrangem funções para controle do fluxo de trabalho e atribuição de metadados para registro da tramitação dos documentos, incluindo-se o *status* do documento (minuta, original ou cópia).

Para os *Requisitos Não Funcionais*, o *Armazenamento* em um Sigad deve fazer parte de uma arquitetura tecnológica que permita a preservação e a recuperação de longo prazo dos documentos arquivísticos, abrigando seus metadados, os metadados do sistema (informações sobre segurança, direitos de acesso e usuários, entre outros), as trilhas de auditoria e as cópias de segurança. Do ponto de vista físico, essas informações residem em dispositivos de armazenamento eletrônicos, magnéticos e ópticos. Além disso, os equipamentos devem adequar-se às características *on-line* (realizadas somente pelo Sigad) ou *off-line (*executadas em outros sistemas computacionais, pois estão desvinculadas do funcionamento do Sigad) das operações.

As *Funções administrativas* permitem que os administradores recuperem, visualizem e

reconfigurem os parâmetros do sistema e os atributos dos usuários. Isto é, um Sigad precisa fornecer relatórios para que o administrador possa gerenciar os documentos e o seu uso. Esses relatórios devem apresentar, no mínimo: quantidade de dossiês/processos, volumes e itens a partir de parâmetros definidos (tempo, classe, unidade administrativa etc.); estatísticas de transações relativas a dossiês/processos, volumes e itens; atividades por usuário.

A *Conformidade com a legislação e regulamentações* preconiza que um Sigad tem que cumprir a legislação e as regulamentações vigentes. Setores de atividades distintos apresentam requisitos legislativos e regulamentares diferenciados. Assim, todos os requisitos desta seção são genéricos e têm que ser adaptados à realidade de cada órgão produtor de documentos arquivísticos.

Na *Usabilidade*, um Sigad deve apoiar a realização de tarefas simples, diretas e objetivas, que garantam as metas de produtividade e de qualidade de trabalho do usuário. A usabilidade depende das tarefas específicas que os usuários realizam por meio do sistema, bem como do nível de conhecimento desse sistema pelos usuários envolvidos. As recomendações para boa usabilidade estão associadas ao contexto operacional do sistema, aos diferentes tipos de usuários, tarefas, ambientes físicos e organizacionais.

A *Interoperabilidade* é o intercâmbio de informações e de serviços entre sistemas. Deve possibilitar a substituição de qualquer componente ou produto usado nos pontos de interligação por outro de especificação similar, sem comprometimento das funcionalidades do Sigad. Isto se faz por meio do uso de regras e de padrões de comunicação. O governo brasileiro definiu a arquitetura dos Padrões de Interoperabilidade de Governo Eletrônico(e-PING), visando a interoperabilidade nas diversas esferas do poder público.

A *Disponibilidade*. Os requisitos de disponibilidade descreve as exigências mínimas sobre o atendimento de um sistema. Os requisitos de disponibilidade devem ser especificados pelo administrador do Sigad. O grau de disponibilidade a ser estabelecido deve levar em conta fatores como as regras de negócio da organização, a necessidade de realização de *backup*, manutenções planejadas, entre outros.

No *Desempenho e escalabilidade*, os requisitos de desempenho enfocam a eficiência no atendimento aos usuários, de acordo com suas expectativas quanto ao tempo de resposta. Os tempos de resposta são influenciados por fatores externos ao Sigad, por exemplo, infraestrutura de rede, volume de tráfego de dados e dimensionamento dos servidores e estações de trabalho. Escalabilidade em um Sigad é a capacidade de um sistema responder a um aumento do número de usuários e do volume de documentos arquivísticos, mantendo o desempenho de suas respostas. Para tanto, faz-se necessário que a cada aumento de *hardware*

corresponda um aumento de desempenho.

E por fim, a seção dos *Metadados*. O e-ARQ Brasil os define como dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e preservar documentos arquivísticos ao longo do tempo. Alguma premissas servem de norte à elaboração do esquema de metadados nesta normativa, então:

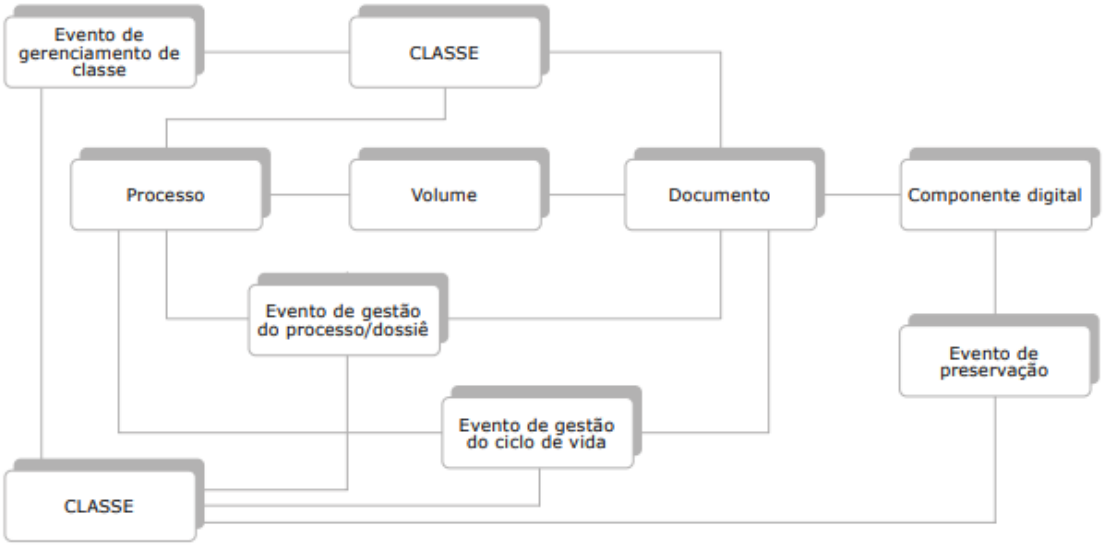
- a complementação dos requisitos do Sigad, compreendendo a identificação de documentos (documentos simples, processos ou dossiês, que podem se apresentar em formato não digital, híbrido ou digital) e as ações de gerenciamento do seu ciclo de vida; e
- o aproveitamento de elementos de metadados de esquemas similares já consagrados por organismos nacionais e internacionais, visando assegurar a interoperabilidade dos sistemas. O modelo utilizado teve como base o Grupo de Trabalho de Padrão de Metadados do Governo Eletrônico (e-PMG) e o e-PING.

Nesta nova versão do e-ARQ Brasil, os metadados de classe foram separados em "Identificação da classe" e "Eventos de gerenciamento da classe". Os primeiros dizem respeito às informações relativas a cada classe, incluindo as relacionadas a prazo de guarda e de destinação. Os segundos às alterações realizadas em cada classe, tais como, mudança de subordinação, mudança de prazo de guarda e outros tipos. Para cada grupo de eventos foram também listados os tipos de eventos previstos para registro em metadados. Essa modelagem baseou-se na proposta apresentada no dicionário de dados do *Preservation Metadata: Implementation Strategies* (Premis).

A metodologia dos *Metadados* trouxe especificação de um esquema que envolveu quatro etapas: a) identificação dos metadados referidos no e-ARQ Brasil; b) complementação dos metadados a partir de normas e de referências bibliográficas das áreas de Arquivologia e da Diplomática; c) confronto do levantamento inicial com esquemas, normas e padrões de metadados semelhantes, nacionais e internacionais; e d) análise, definição e aprovação do esquema.

A organização do esquema de metadados foi definida da seguinte forma para as entidades: documento (documento, volume e processo/dossiê), evento de gestão do ciclo de vida, evento de gestão de processos/dossiês, classe, evento de gerenciamento de classe, componente digital, evento de preservação e agente (Figura 40):

Figura 40 – Organização do esquema de metadados do e-ARQ Brasil 2022



Fonte: Brasil (2022, p. 113).

- **Documento** refere-se ao documento que foi capturado pelo Sigad, isto é, declarado como arquivístico e incorporado ao sistema por meio de registro, classificação, arquivamento entre outras especificações. Esta é a entidade mais importante de um Sigad.
- Documentos arquivísticos relacionam-se entre si, formando **processos ou dossiês.**
- **Processos/dossiês** podem ser divididos em **volumes.** Esta prática tem origem nos documentos não digitais, de forma a possibilitar que os volumes tenham tamanho e peso de fácil manejo.
- **Evento de gestão do ciclo de vida** refere-se às ações de gestão que ocorrem com os documentos arquivísticos ao longo de seu ciclo de vida, como captura, classificação, desclassificação, eliminação, transferência, recolhimento, entre outros.
- **Evento de gestão dos processos/dossiês** refere-se aos procedimentos de protocolo realizados com os processos, como abertura de volume/processo/dossiê, encerramento de volume/processo/dossiê, tramitação, juntada, desapensação, desentranhamento, desmembramento, entre outros.
- **Classe** refere-se aos diversos níveis de agregação do CCD: classes, subclasses, grupos e subgrupos, que são organizados de forma hierárquica. No contexto do e-ARQ Brasil, a entidade “classe” refere-se aos níveis citados. Assim, quando um requisito trata da classe, estão sendo considerados todos os níveis do CCD.
- **Evento de gerenciamento de classe** refere-se às ações de manutenção do CCD e

da TTDD, as quais implicam a alteração dos atributos das classes, tais como: alteração de nome da classe, alteração de subordinação, alteração de temporalidade prevista, dentre outros.

- **Componente digital** refere-se aos objetos digitais que compõem o documento arquivístico digital. De modo geral, pode-se dizer que componentes digitais são os arquivos de computador que contêm as informações de conteúdo, forma e composição necessárias à apresentação do documento arquivístico.
- **Evento de preservação** refere-se às ações de preservação realizadas nos componentes digitais, tais como migração (atualização, conversão), compressão, validação e decifração.
- **Agente** refere-se aos usuários que acessam o Sigad.
    - Agente relaciona-se com o evento de gestão do ciclo de vida pelo qual foi responsável.
    - Agente relaciona-se com o evento de gestão dos processos/dossiês pelo qual foi responsável.
    - Agente relaciona-se com o evento de preservação pelo qual foi responsável.
    - Agente relaciona-se com o evento de gerenciamento de classe pelo qual foi responsável.

Em suma, os documentos arquivísticos digitais relacionam-se formando agregações conceituais (processos e dossiês). Estes podem conter um ou mais volumes. Um volume pode conter um ou mais documentos. Cada documento é composto por um ou mais componentes digitais. E para mostrar as características do conceito de confiança extraídas do e-ARQ Brasil, temos o Quadro 16 a seguir.

Quadro 16 – Elementos do conceito de confiança extraídos do e-ARQ Brasil - versão 2

Conceitos	Definições
Armazenamento	Armazenamento num Sigad significa utilizar de uma arquitetura tecnológica que permita a preservação e a recuperação de longo prazo dos documentos arquivísticos, abrigando seus metadados, os metadados do sistema (informações sobre segurança, direitos de acesso e usuários, entre outros), as trilhas de auditoria e as cópias de segurança.
Autenticidade	Característica de documentos arquivísticos que o comprova como tal, independentemente de se tratar de minuta, de original ou de cópia, e que é livre de adulterações ou qualquer outro tipo de corrupção. A autenticidade está ligada à transmissão do documento e à sua preservação e custódia. Um documento autêntico é aquele que se mantém da forma como foi produzido, portanto apresenta o mesmo grau de confiabilidade que tinha no momento de sua produção. Um documento não completamente confiável, mas transmitido e preservado sem adulteração ou qualquer outro tipo de corrupção, é autêntico.
Captura	Declara um documento arquivístico como tal, incorporando-o ao sistema de gestão arquivística a partir de, no mínimo, as seguintes ações: registro;

	classificação; indexação; atribuição de restrição de acesso e arquivamento. Seu objetivo é enfatizar um documento como arquivístico ao declarar sua relação orgânica.
Confiabilidade	Característica de um documento arquivístico que o torna confiável. É aquele que tem a capacidade de sustentar os fatos que atesta. A confiabilidade (fidedignidade, em inglês *reliability*) está relacionada ao momento em que o documento é produzido e à veracidade do seu conteúdo. Para tanto, há que ser dotado de completeza e ter seus procedimentos de produção bem controlados.
Controle de acesso	Limitação ou autorização de acesso a documentos por usuário ou grupos de usuários. Deve-se garantir no mínimo: restrição de acesso aos documentos; exibição dos documentos, criptografados ou não, e dos metadados somente aos usuários autorizados; uso e intervenção nos documentos somente pelos usuários autorizados e registro de acesso em trilha de auditoria.
Completeza	A completeza dá-se pela presença de todos os elementos intrínsecos e extrínsecos exigidos pela organização produtora e pelo sistema jurídico-administrativo ao qual pertence, de maneira que esse mesmo documento possa ser capaz de gerar consequências. Dificilmente, pode-se assegurar a veracidade do conteúdo de um documento; ela é inferida da completeza e dos procedimentos de produção. A confiabilidade é uma questão de grau, ou seja, um documento pode ser mais ou menos confiável.
Identidade	Refere-se a atributos que caracterizam o documento arquivístico e o distinguem dos demais. Esses atributos se constituem nos elementos intrínsecos da forma documental e nas anotações.
Integridade	Refere-se ao estado dos documentos que se encontram completos e não sofreram nenhum tipo de corrupção ou alteração não autorizada nem documentada.
Interoperabilidade	intercâmbio de informações e de serviços entre sistemas. Deve possibilitar a substituição de qualquer componente ou produto usado nos pontos de interligação por outro de especificação similar, sem comprometimento das funcionalidades do Sigad. Isto se faz por meio do uso de regras e de padrões de comunicação. O governo brasileiro definiu a arquitetura dos Padrões de Interoperabilidade do e-PING, visando a interoperabilidade nas diversas esferas do poder público.
Metadados	Dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e preservar documentos arquivísticos ao longo do tempo.
Preservação	Estabilidade do suporte da informação. Nos documentos digitais, o foco da preservação é a manutenção do acesso, que pode implicar mudança de suporte e formato, bem como atualização do ambiente tecnológico. Assim, o Sigad deve utilizar da interoperabilidade com um RDC-Arq para armazenar documentos de guarda longa e os destinados à guarda permanente.
Relação orgânica	Relação que o documento arquivístico mantém com os demais documentos do órgão e que refletem suas funções e atividades. Os documentos arquivísticos apresentam um conjunto de relações que devem ser mantidas.
Restrição de acesso	Análise dos documentos em relação à ostensividade ou à sigilosidade. No caso da sigilosidade, a legislação vigente estabelece procedimentos específicos para seu tratamento, como os graus de sigilo e de restrições de acesso.

Fonte: Brasil (2022).

8.6 DIRETRIZES PARA A IMPLEMENTAÇÃO DE REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS –RDC-ARQ

Até alcançar a Resolução do Conarq de nº. 51, de 25 de agosto de 2023, as **Diretrizes para a Implementação de Repositórios Arquivísticos Digitais Confiáveis – RDC-Arq,** passaram por duas versões anteriores revogadas.

A primeira foi a Resolução do Conarq de nº. 39, de 29 de abril de 2014, que estabelecia Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis **para o arquivamento e manutenção de documentos arquivísticos digitais em suas fases corrente, intermediária e permanente,** dos órgãos e das entidades integrantes do Sistema Nacional de Arquivos (Sinar).

E a segunda, a Resolução do Conarq de nº. 43, de 04 de setembro de 2015, que alterou a redação da Resolução do Conarq de nº. 39, de 29 de abril de 2014, e estabelecia diretrizes para a implementação de repositórios digitais confiáveis para a **transferência e recolhimento de documentos arquivísticos digitais** para instituições arquivísticas dos órgãos e das entidades integrantes do Sinar.

A atualização das diretrizes e das recomendações, aprovada pela Resolução de nº. 51, tem por objetivo orientar os órgãos e as entidades integrantes do Sinar quanto à indicação de parâmetros e de requisitos para repositórios arquivísticos digitais confiáveis, de forma a garantir a autenticidade, a confidencialidade, a disponibilidade, o acesso e a preservação, tendo em vista a necessidade de manutenção dos acervos por longos períodos ou, até mesmo, permanentemente. Pontuam-se os acréscimos deste documento em relação à sua versão anterior : a Resolução de nº. 43.

As **Diretrizes para a Implementação de Repositórios Arquivísticos Digitais Confiáveis – RDC-Arq** (Resolução de nº. 51) estão divididas em Quatro Partes e os Anexos. A Parte I – Apresentação, subdivide-se em: I.1 Objetivo deste documento; I.2 Escopo; I.3 Definições. A Parte II – Repositório digital confiável de documentos arquivísticos - principais requisitos, subdivide-se em: II.1 Considerações sobre um repositório digital de documentos arquivísticos; II.2 Requisitos para um repositório digital confiável. A Parte III – Metodologia de aplicação. A Parte IV – Padrões e normas de referência; subdivide-se em: IV.1 Modelo de referência OAIS; IV.2 Metodologia de interface produtor-arquivo; IV.3 Relatório da *Research Library Group* (RLG) e da *Online Computer Library Center* (OCLC) – Repositórios digitais confiáveis: atributos e responsabilidades; IV.4 Modelo de empacotamento de dados; IV.5

Certificação e auditoria de repositórios confiáveis: critérios e *checklis*t – Trac; IV.6 Requisitos técnicos para entidades de auditoria e certificação de organizações candidatas a serem repositórios digitais confiáveis; IV.7 Metadados de preservação (Premis); IV.8 Norma Geral Internacional de Descrição Arquivística –ISAD(G); IV.9 Norma Brasileira de Descrição Arquivística (Nobrade); IV.10 Metadados do e-ARQ Brasil; IV.11 Protocolo para coleta de metadatos (OAI-PMH); IV.12 Padrão de codificação e transmissão de metadados (METS); IV.13 Descrição arquivística codificada (EAD); e os Anexos.

A Resolução de nº. 43 do Conarq está dividida em apenas Três Partes, não contemplando a Parte III e os Anexos da Resolução de nº. 51. A I e a II Parte de ambas as Resoluções tratam do mesmos assuntos, inclusive utilizando a mesma redação.

A Parte I deste documento apresenta uma visão mais conceitual dos repositórios, frisando que os documentos digitais em fase permanente dependem e necessitam de um bom sistema informatizado que apoie o seu tratamento técnico adequado, incluindo arranjo, descrição e acesso, de forma a assegurar a manutenção da autenticidade e da relação orgânica desses registros.

Dessa forma, a preservação dos documentos arquivísticos digitais arquivados nas fases corrente, intermediária e permanente deve estar associada a um repositório arquivístico digital confiável, logo, deve ocorrer em todo o ciclo vital do documento.

Em âmbito internacional, por exemplo, diversas iniciativas indicam a importância do desenvolvimento de repositórios digitais confiáveis como solução para a garantia da autenticidade, da preservação e do acesso de longo prazo. Dentre essas iniciativas, tem-se a do grupo de trabalho liderado pelo RLG e pelo OCLC, as quais advogam a necessidade de se construir, além de auxiliar no desenvolvimento, de sistemas que cada vez mais tragam segurança e preservação às informações.

Para o entendimento do conteúdo da Resolução nº. 51 do Conarq, vale destacar alguns conceitos importantes.

- **Atualização de suporte:** técnica de migração que consiste em copiar os dados de um suporte para outro, sem mudar sua codificação, para evitar perdas de dados provocadas por deterioração do suporte.
- **Autenticidade:** credibilidade de um documento enquanto documento, isto é, a qualidade de um documento ser o que diz ser e de que está livre de adulteração ou qualquer outro tipo de corrupção.
- **Confiabilidade:** credibilidade de um documento arquivístico enquanto afirmação de um fato. Existe quando um documento arquivístico pode sustentar o fato ao

qual se refere, e é estabelecida pelo exame da completeza, da forma do documento e do grau de controle exercido no seu processo de criação.

- **Confidencialidade:** propriedade de certos dados ou informações que não podem ser disponibilizadas ou divulgadas sem autorização.
- **Conversão de formato:** modificação de um formato para outro motivada, principalmente, pela normalização de formatos e para contornar a obsolescência tecnológica.
- **Disponibilidade:** propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.
- **Evidência:** documentos que comprovem o cumprimento de requisitos, de competências, de objetivos e de responsabilidades.
- **Integridade:** estado dos documentos que se encontram completos e não sofreram nenhum tipo de corrupção ou alteração não autorizada nem documentada.
- **Interoperabilidade:** capacidade de diversos sistemas e organizações trabalharem em conjunto (interoperar), de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente.
- **Metadados:** dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e preservar documentos arquivísticos ao longo do tempo.
- **Migração:** conjunto de procedimentos e técnicas para assegurar a capacidade de os objetos digitais serem acessados face às mudanças tecnológicas. A migração consiste na transferência de um objeto digital: a) de um suporte que está se tornando obsoleto, fisicamente deteriorado ou instável para um suporte mais novo; b) de um formato obsoleto para um formato mais atual ou padronizado; c) de uma plataforma computacional em vias de descontinuidade para outra mais atual. A migração pode ocorrer por conversão, atualização ou reformatação.
- **Modelo de referência:** estrutura conceitual para compreensão dos principais relacionamentos entre as entidades de um ambiente e para o desenvolvimento de padrões consistentes ou especificações que consolidam esse ambiente. Um modelo de referência é baseado em pequena quantidade de conceitos unificados e pode ser usado como base para aprendizado e explanação de padrões para não especialistas.
- **Normalização de formatos:** conversão de formatos de arquivo para um elenco gerenciável de formatos apropriados para preservação e acesso.
- **Plano de preservação:** declaração por escrito, autorizada pela gestão do

repositório, que descreve as ações a serem executadas para preservar objetos por ele custodiados de acordo com a política de preservação.

- **Política de acesso:** declaração escrita, autorizada pela gestão do repositório, que descreve a abordagem a ser adotada para a comunidade designada e usuários em geral.
- **Política de preservação digital:** declaração escrita, autorizada pela gestão do repositório, que descreve a abordagem a ser adotada pelo repositório para a preservação dos objetos por ele custodiados. A política de preservação é consistente com o plano estratégico de preservação.
- **Preservação digital:** conjunto de ações gerenciais e técnicas exigidas para superar as mudanças tecnológicas e a fragilidade dos suportes, garantindo o acesso e a interpretação dos documentos digitais pelo tempo que for necessário.
- **Preservador de documentos arquivísticos:** entidade responsável pela custódia física e legal dos documentos do produtor, bem como por sua preservação, isto é, por proteger e garantir acesso contínuo aos documentos.
- **Provedor:** pessoa ou sistema que envia um objeto digital para o repositório. O provedor pode ser o produtor.
- **Reformatação:** técnica de migração que consiste na mudança da forma de apresentação de um documento para fins de acesso ou manutenção dos dados.

A definição de evidência, de plano de preservação, de política de acesso, de prática, de procedimentos, de provedor e de reformatação não estão contemplados na Resolução de n.º 43 do Conarq.

A Parte II descreve os RDC-Arqs, bem como seus principais requisitos. Não é de hoje que a comunidade internacional olha para os repositórios com cuidado, sobretudo para apontar os requisitos necessários à sua confiabilidade.

A norma mais importante para esses tipos de sistema é o OAIS, um modelo conceitual desenvolvido pelo *Consultative Committee for Space Data Systems* (CCSDS), que resultou na norma ISO 14721:2003 (revisada em 2012). O *OAIS* descreve as funções de um repositório digital e os metadados necessários para a preservação e para o acesso aos materiais digitais gerenciados pelo repositório, que constituem um modelo funcional e um modelo de informação.

O CCSDS é formado pelas maiores agências espaciais do mundo, e tem o objetivo de oferecer um fórum para discussão de problemas comuns sobre o desenvolvimento e a operação de sistemas de dados espaciais e, consequentemente, o local onde eles estarão

armazenados.

Um repositório que segue o OAIS é constituído por pessoas e por sistemas com a responsabilidade de preservar a informação e torná-la disponível. Este modelo aborda questões fundamentais relativas à preservação de longo prazo de materiais digitais, independentemente da área de aplicação (arquivo, biblioteca, museu).

O ambiente OAIS conta com três entidades externas: o produtor, que desempenha o papel imbricado por pessoas ou por sistemas que fornecem a informação a ser preservada; o administrador, cujo papel é desempenhado por aqueles que estabelecem as políticas gerais que administram o repositório; e o consumidor, papel desempenhado por pessoas ou por sistemas que interagem com os serviços OAIS para acessar a informação preservada desejada.

O modelo também é composto de dois tipos: o modelo funcional e o de informação. O primeiro delineia as funções que precisam ser desempenhadas por um repositório OAIS. A Figura 0 apresenta os componentes funcionais, os pacotes de informação e as entidades externas de um repositório digital compatível com o OAIS.

Figura 41 – Entidades funcionais do modelo OAIS

Fonte: Brasil (2023, p. 20).

O Produtor é uma entidade externa ao repositório que se responsabiliza pela submissão do material digital. Esse material de submissão é o arquivo, traduzido como Pacote de Submissão de Informação (SIP, sigla em inglês).

No processo de Admissão, o repositório responsabiliza-se por garantir a integridade da

informação recebida. Nesta mesma fase produz-se toda a Informação descritiva que suporte a descoberta e a localização do documento depositado. Essa informação, também denominada metainformação, é armazenada e gerida pelo componente de Gestão de dados. O material a preservar é o Pacote de Informação de Arquivo (AIP, sigla em inglês) e será conservado no arquivamento ou no repositório de dados. A Admissão constitui a interface entre o arquivo OAIS e os produtores de informação

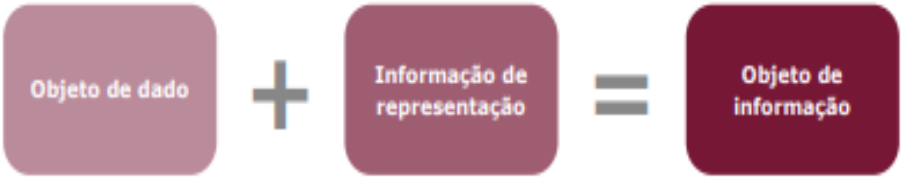
O Planejamento de preservação, encarrega-se das políticas de preservação, que é responsável por monitorar o ambiente externo ao repositório, as tendências comportamentais da sua comunidade de interesse ou de identificar formatos que se encontram obsoletos.

O componente de Acesso estabelece a comunicação entre o arquivamento ou repositório e sua comunidade de interesse, o conjunto de usuários. Este componente facilita a descoberta e localização dos objetos digitais, bem como o seu preparo para a entrega ao usuário.

Os pacotes levados ao Consumidor são denominados de Pacotes de Informação e Disseminação (DIP, sigla em inglês). O componente Administração do sistema, responsabiliza-se pelas operações cotidianas de manutenção, principalmente na monitorização dos processos no interior do arquivamento. Esse interage com todo o restante, de modo a assegurá-los o correto funcionamento.

No âmbito do OAIS, alguns conceitos são importantes elucidar: o de **informação**, sendo qualquer tipo de conhecimento que pode ser intercambiado, sempre representado por algum tipo de dado; e o de **objeto de informação,** resultante do objeto de dado, que é interpretado com o uso da informação de representação. Essa informação de representação pode ser decomposta em informação semântica e estrutural, como, por exemplo, um texto em português – informação semântica – codificado no formato ASCII – informação estrutural (Figura 42).

Figura 42 – Informação a partir dos dados

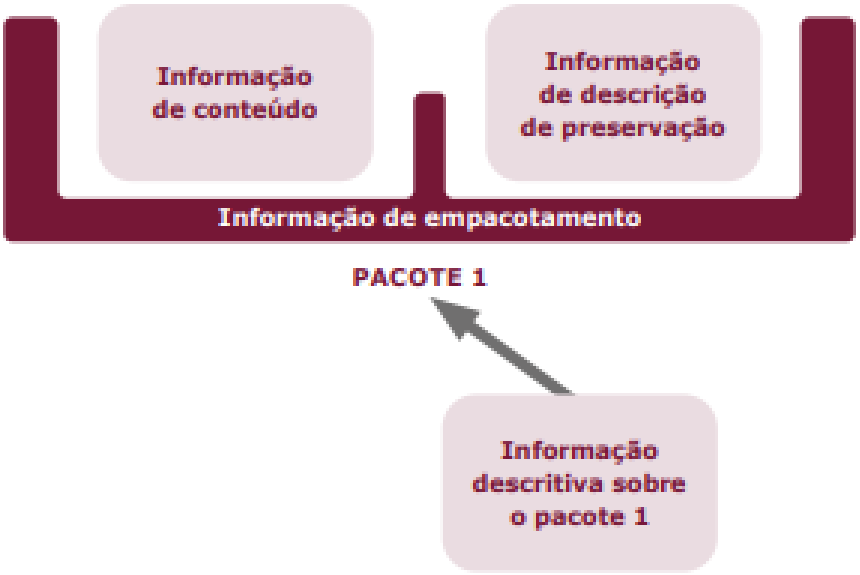


Fonte: Brasil (2023, p. 20).

O modelo de informação do OAIS propõe o conceito de pacote de informação (Figura 0), que é formado pela informação de conteúdo e pela informação de descrição de

preservação, encapsuladas e identificadas pela informação de empacotamento. A informação de conteúdo é o objeto de informação (objeto de dado + informação de representação) a ser preservado. A informação de descrição de preservação é a informação necessária para a adequada preservação da informação de conteúdo, e que pode ser categorizada como informação sobre proveniência, referência, fixidade e contexto. O pacote de informação é associado a outras informações descritivas que vão possibilitar sua localização no repositório.

Figura 43 – Conceitos e relacionamentos do pacote de informação



Fonte: Brasil (2023, p. 21).

A confiabilidade dos repositórios digitais foi evidenciada no relatório da *Task Force on Archiving of Digital Information*, uma ação cooperativa do *RLG* e da *Commission on Preservation and Access*, publicado no ano de 1996, e declarou que: um componente crítico da infraestrutura de arquivamento digital é a existência de um número suficiente de instituições confiáveis, capazes de armazenar, de migrar e de prover acesso a acervos digitais. Este relatório foi além de apontar a necessidade de um processo de certificação dos repositórios digitais para atribuir esse caráter de confiabilidade de uma forma mais isenta.

Ele estimulou também, a colaboração do RLG/OCLC, iniciada em março de 2000, no sentido de definir as bases conceituais e os principais atributos para um repositório digital confiável. O resultado disso foi a publicação, em 2002, de outro relatório: o *Trusted digital repositories: attributes and responsibilities*. Assim, em 2007, o documento Trac, foi publicado e serviu para apresentar um conjunto de critérios e um *checklist* a serem tomados como referência para a certificação de repositórios digitais confiáveis. Esse documento serviu de base à elaboração da norma ISO 16363:2012, que lista os critérios que um repositório

digital confiável deve atender. Paralelamente a essa iniciativa, desenvolveu-se a norma ISO 16919, que estabelece requisitos para entidades certificadoras de repositórios digitais confiáveis. Tais documentos apontam as diretrizes para repositórios digitais confiáveis e fundamentaram a elaboração da Resolução nº. 51 do Conarq de 2023.

Uma das contribuições indispensáveis desta Resolução é o conceito e a definição dos tipos de repositórios, são eles: repositório digital, repositório arquivístico digital, repositório digital confiável e RDC-Arq.

- **Repositório digital** é um ambiente de armazenamento e de gerenciamento de materiais digitais. E não somente uma solução informatizada (muitas vezes associada apenas a um *storage*, que é apenas um de seus componentes) em que os documentos são capturados, armazenados, preservados e acessados. Ele forma um complexo que apoia o gerenciamento dos documentos, pelo tempo que for necessário, sendo formado por elementos de *hardware*, de *software* e de metadados, bem como por uma infraestrutura organizacional e procedimentos normativos e técnicos. Tal ambiente tem sido empregado em diversas situações, tais como: arquivo corrente e intermediário (quando associação a um Sigad); arquivo permanente; biblioteca digital; acervo de obras de arte digitais; depósito legal de material digital; e curadoria de dados digitais de pesquisa.
- **Repositório arquivístico digital** é aquele que armazena e preserva esses documentos, nas fases intermediária e/ou permanente, devendo: gerenciar os documentos e metadados de acordo com as práticas e as normas da Arquivologia, especificamente relacionadas à gestão documental, à descrição arquivística multinível e à preservação; e proteger as características do documento arquivístico, em especial a autenticidade e a relação orgânica entre eles. Contudo, um repositório arquivístico digital não se destina a ser o ambiente de gestão de documentos, para isso deve-se usar um Sigad.
- **Repositório digital confiável** é aquele capaz de manter autênticos os documentos digitais, de preservá-los e de prover pelo tempo que for necessário. Para cumprir essa missão, eles devem:
  a) aceitar, em nome de seus depositantes, a responsabilidade pela manutenção dos materiais digitais;
  b) dispor de uma estrutura organizacional que apoie não somente a viabilidade de longo prazo dos próprios repositórios, mas também dos documentos digitais sob sua responsabilidade;

c) demonstrar sustentabilidade financeira e transparência administrativa;
d) projetar seus sistemas de acordo com convenções e padrões comumente aceitos, no sentido de assegurar, de forma contínua, a gestão, o acesso e a segurança dos materiais depositados;
e) estabelecer metodologias para avaliação dos sistemas que considerem as expectativas de confiabilidade esperadas pela comunidade;
f) considerar, para desempenhar suas responsabilidades de longo prazo, os depositários e os usuários de forma aberta e explícita;
g) dispor de políticas, de práticas e de desempenho que possam ser auditáveis e mensuráveis; e
h) observar os seguintes fatores relativos às responsabilidades organizacionais e de curadoria dos repositórios: escopo dos materiais depositados, gerenciamento do ciclo de vida e preservação, atuação junto a uma ampla gama de parceiros, questões legais relacionadas com a propriedade dos materiais armazenados e implicações financeiras.

Uma das formas para se atestar a confiabilidade de um repositório digital dá-se pela sua certificação por terceiros, mas para isso, tem-se a Trac.

Um **RDC-Arq** deve ser capaz de atender aos procedimentos arquivísticos em suas diferentes fases e aos requisitos de um repositório digital confiável, conforme exposto. Esse ambiente deve ter suas estratégias de preservação muito bem documentadas nas suas políticas, nos seus procedimentos, nos seus planos e nas suas práticas, descrevendo as ações que é capaz de realizar na promoção da preservação dos documentos que custodia, mas, acima de tudo, comprovar que possui capacidade de manter suas estratégias sempre funcionais e que suas decisões mais relevantes sobre essas estratégias garantem a preservação dos documentos arquivísticos digitais de forma eficaz e confiável.

Outro fator a destacar nesta Resolução, foram os requisitos e os princípios para implementação dos repositórios digitais (arquivísticos) confiáveis, para tal, seus Anexos mostram os passos a serem cumpridos por esses sistemas.[105]

Dessa forma, um repositório digital confiável deve seguir alguns princípios para ser considerado arquivístico: responsabilidade pelo repositório; tratamento arquivístico; princípios de preservação digital; independência dos repositórios; e interoperabilidade.

[105] O trabalho disponível em: R§epositório Institucional da UFPB: Características, funções e preservação digital do archivematica à luz da resolução nº 43 do conselho nacional de arquivos, mostra o cumprimento das funcionalidades *software Archivematica* avaliado à luz dos requisitos da Resolução nº. 43 do Conarq.

Assim, os requisitos para um repositório digital confiável estão definidos em nível conceitual e devem ser cumpridos no desenvolvimento desse ambiente. Tais requisitos baseiam-se baseados na norma ISO 16363:2012 e abrangem todos os tipos de documentos digitais. A listagem detalhada dos requisitos e suas possíveis evidências de validação encontram-se no Anexo III, Seção D, da Resolução nº. 51 do Conarq. Os requisitos estão organizados em três conjuntos: A. Infraestrutura organizacional; B. Gerenciamento do documento digital; e C. Tecnologia, infraestrutura técnica e segurança.

Quadro 17 – Requisitos para um repositório digital confiável

A. Infraestrutura organizacional	Aborda questões relativas a como a instituição se organiza técnica, processual e normativamente para atender sua missão como RDC-Arq. A forma como a instituição se organiza e se estrutura impacta diretamente na manutenção do repositório. Inclui, mas não se restringe a eles, os seguintes elementos: governança; estrutura organizacional; mandato ou propósito; escopo; funções e responsabilidades; arcabouço político; sistema de financiamento; questões financeiras (incluindo ativos); contratos, licenças e passivos; transparência.
A.1 Governança e viabilidade organizacional	Independentemente do tamanho, escopo ou natureza do programa de preservação, um RDC-Arq deve demonstrar um compromisso explícito, exequível e de longo prazo para a conformidade às políticas, aos padrões e melhores práticas vigentes.
A.2 Estrutura organizacional e de pessoal	Um repositório arquivístico digital confiável deve ter funcionários designados com as habilidades e treinamento necessários, além de promover o desenvolvimento contínuo desses profissionais. Deve ser capaz, também, de documentar os esforços para mapear e manter as funções, descrições de cargos, planos de desenvolvimento e habilidades necessárias.
A.3 Transparência de procedimentos e arcabouço político	Um RDC-Arq deve fornecer documentação clara e explícita de seus requisitos, decisões, desenvolvimento e ações para garantir preservação e acesso em longo prazo dos documentos sob sua custódia. Essa documentação garante à comunidade-alvo, gerentes, produtores, auditores e certificadores que o repositório está atendendo aos seus requisitos e desempenhando plenamente sua função. A certificação, o indicador mais claro da prática sólida baseada em normas e padrões, é facilitada pela responsabilidade processual que resulta de políticas, procedimentos e práticas abrangentes e atuais.
A.4 Sustentabilidade financeira	Um RDC-Arq deve ser capaz de provar sua sustentabilidade financeira. Em geral, um RDC-Arq segue todas as boas práticas de negócios e deve ter um plano de negócios sustentável – um conjunto geral de documentos que refletem o passado, o presente e o futuro do repositório e suas atividades.

	Um plano de negócios incorpora planos de gestão e implicações financeiras relacionadas ao desenvolvimento de atividades de produção, podendo observar as estratégias e/ou riscos que afetariam as operações. Os procedimentos de análise e adequação financeira devem ser revistos anualmente. Devem ser usados procedimentos contábeis aderentes a normas e procedimentos legais e administrativos (estar em *compliance*). Os ciclos de planejamento financeiro de curto e longo prazos devem demonstrar um equilíbrio contínuo de risco, benefício, investimento e despesa. Os orçamentos e reservas operacionais devem ser adequados às necessidades do negócio.
A.5 Contratos, licenças e passivos	Os contratos, licenças e passivos de um RDC-Arq devem ser explícitos e definidos de forma clara e em termos mensuráveis, delinear funções e responsabilidades, prazos e condições, e ser prontamente acessíveis ou disponíveis às partes interessadas sob demanda. Os contratos incluem aqueles entre o RDC-Arq e os produtores/depositários dos documentos arquivísticos digitais e aqueles entre o RDC-Arq e seus provedores de serviço. Independentemente do relacionamento, esses contratos e licenças devem estar disponíveis para auditorias.
B. Gerenciamento do documento digital	O gerenciamento dos documentos de um RDC-Arq deve estar de acordo com o modelo de referência OAIS, que estabelece a formação de pacotes de informação envolvendo os documentos digitais (informação de conteúdo) e seus metadados (informação de representação). Incluem-se aspectos organizacionais e técnicos relacionados a essas responsabilidades, como funções do repositório, processos e procedimentos necessários para admitir, gerenciar, preservar e fornecer acesso aos documentos arquivísticos digitais. Os requisitos desta seção são categorizados em seis grupos com base no agrupamento de funcionalidades das entidades funcionais do modelo OAIS. Estes requisitos pressupõem familiaridade com o OAIS, seus conceitos, fluxos e funcionalidades.
B.1 Admissão: captura de documentos digitais	A admissão consiste na entrada dos documentos e seus metadados no repositório digital. Os requisitos de admissão variam dependendo do tipo de material, do contexto legal e da relação entre o produtor de documentos e o repositório. Independentemente dessas variações, pode-se afirmar que a admissão se inicia com o recebimento de um SIP, que é convertido em AIP, e termina quando um AIP está seguro no repositório, incluindo a criação de cópias de segurança.
B.2 Admissão: criação do pacote de arquivamento	O RDC-Arq deve completar o processo de admissão criando um pacote de informação apropriado para arquivamento (AIP), com toda a informação recebida do produtor.

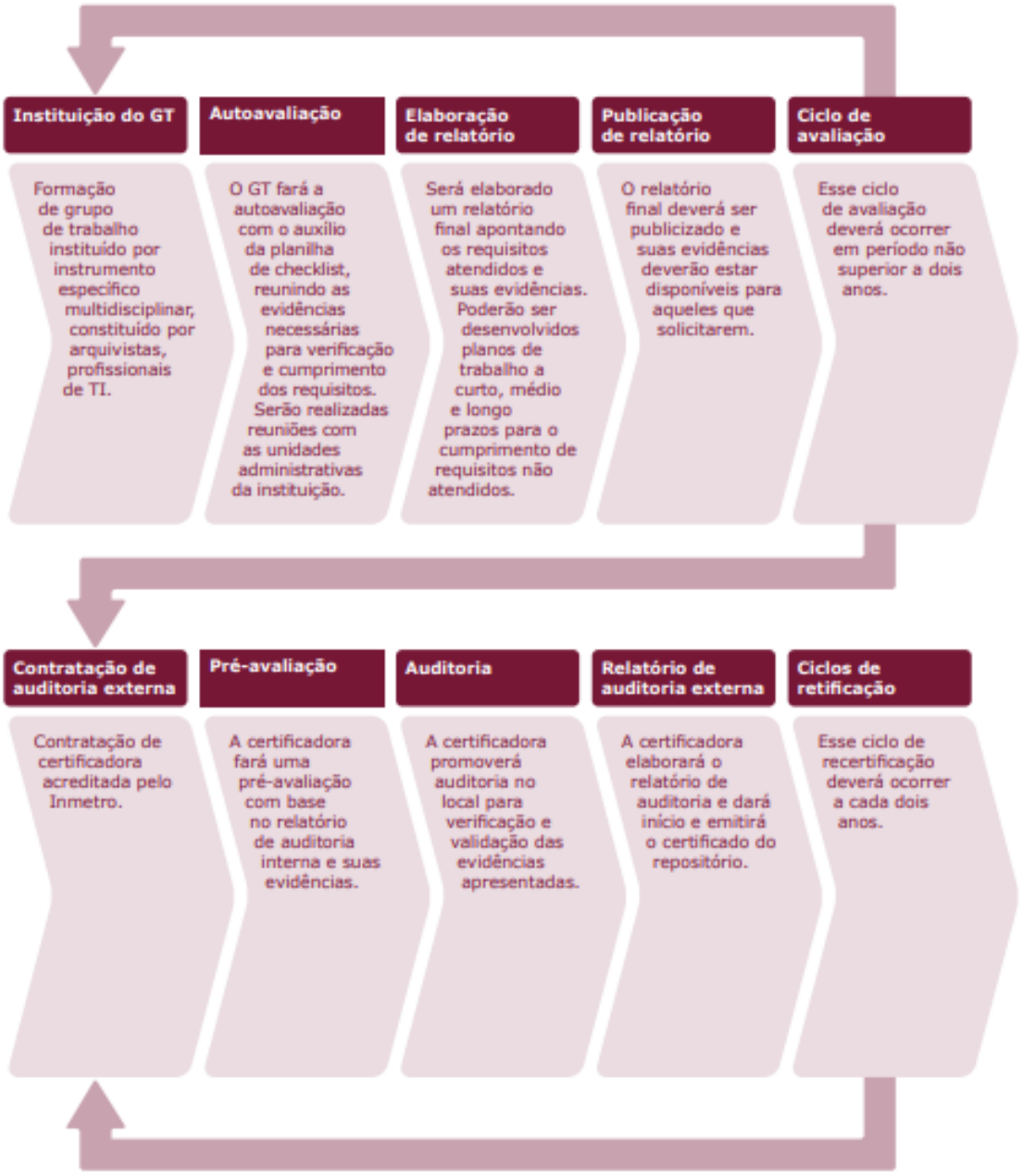
B.3 Planejamento da preservação	Um RDC-Arq deve fazer o planejamento da preservação dos documentos sob sua custódia, a fim de enfrentar os problemas trazidos pela obsolescência tecnológica e fragilidade do suporte. Esse planejamento deve ser feito a partir de uma política de preservação digital e ser bem documentado.
B.4 Armazenamento e preservação/manutenção do AIP	Um repositório deve atender a um conjunto de condições para garantir o bom desempenho da preservação de longo prazo dos AIPs.
B.5 Gerenciamento da informação	Uma funcionalidade essencial de um RDC-Arq é o gerenciamento da informação, aqui entendido como a gestão das informações descritivas (metadados) dos documentos admitidos no repositório. O principal objetivo desses metadados é apoiar o acesso e a recuperação dos documentos, e eles vão além das informações descritivas mais usuais (autor, título, data), envolvendo outras também úteis aos usuários, tais como o tamanho do arquivo disponível para download ou informação sobre a aplicação necessária para ler o arquivo.
B.6 Gerenciamento de acesso	O termo acesso possui vários sentidos diferentes, incluindo, por exemplo, acesso dos usuários ao sistema do repositório; segurança física e autenticação do usuário; e as diferentes fases de acesso aos documentos digitais (fazer uma solicitação, verificar os direitos do solicitante, preparar e enviar um pacote de informação para disseminação, DIP). Esta subseção tratará sobre o assunto.
C. Tecnologia, infraestrutura técnica e segurança	Esses requisitos não prescrevem *hardware* e *software* específicos para garantir a preservação de longo prazo dos AIPs, mas apenas descrevem as melhores práticas das áreas de gestão de dados e segurança que devem ser atendidas por um RDC-Arq. O repositório deve adotar uma tecnologia de *hardware* e *software* apropriada para os serviços que presta, procedimentos para o recebimento e monitoramento de notificações e para a avaliação da necessidade de mudanças na tecnologia utilizada. De uma forma geral, esses requisitos medem a adequação da infraestrutura técnica do repositório e sua capacidade de atender as demandas de gerenciamento e segurança. Repositórios e instituições que passaram por certificação da ISO 27002 certamente atenderão a muitos desses requisitos.
C.1 Infraestrutura de sistema	Um repositório deve possuir uma infraestrutura tecnológica robusta, de maneira a apoiar a confiabilidade dos AIPs nele mantidos.
C.2 Gestão de risco e segurança	A segurança do repositório não se limita a aspectos de tecnologia, mas abrange também instalações físicas e ações de pessoas.

Fonte: Brasil (2023, p. 14-17, grifo nosso).

Em relação ao requisito “C”, a Resolução 43 dividia-se em – Tecnologia, infraestrutura técnica e segurança: a. Infraestrutura de sistema; b. Tecnologias apropriadas e c. Segurança. Sua recomendações eram análogas às descritas no Quadro 17.

A Parte III: Metodologia de aplicação desta Resolução, recomenda seguir as diretrizes da ISO 19011:2018, ISO 17021:2016 e ISO 16919:2014, em termos de auditoria interna, externa ou de terceira parte. O fluxo a seguir é uma adaptação resumida das normas citadas para fins de referência.

Figura 44 – Fluxo de auditoria e de certificação



Fonte: Brasil (2023, p. 18).

A Parte IV: Padrões e normas de referência percorrem as mesmas informações descritas na Parte III da Resolução 43 e está dividida em 13 documentos de referências para o RDC-Arqs, duas a mais que a última Resolução.

Tais documentos destacam temáticas variadas como: os que definem modelos ou orientam a certificação de repositórios confiáveis; os que definem de metadados, que podem ser utilizados de acordo com o propósito do repositório; e os que trazem codificações, em XML, de metadados e de padrões de transmissão. São eles:

1. Modelo de referência OAIS.
2. Metodologia de interface produtor-arquivo.
3. Relatório da *Research Library Group* (*RLG*) e da *Online Computer Library Center* (*OCLC*) – Repositórios digitais confiáveis: atributos e responsabilidades.
4. Modelo de empacotamento de dados.
5. Certificação e auditoria de repositórios confiáveis: critérios e *checklist* – Trac;
6. Requisitos técnicos para entidades de auditoria e certificação de organizações candidatas a serem repositórios digitais confiáveis.
7. Metadados de preservação (Premis).
8. Norma Geral Internacional de Descrição Arquivística, ISAD(G);
9. Norma Brasileira de Descrição Arquivística (Nobrade);
10. Metadados do e-ARQ Brasil;
11. Protocolo para coleta de metadatos (OAI-PMH);
12. Padrão de codificação e transmissão de metadados (METS)
13. Descrição arquivística codificada (EAD).

Os não contemplados na Resolução nº .43 do Conarq foram: 2. Metodologia de interface produtor-arquivo e 4. Modelo de empacotamento de dados.

A **Metodologia de interface produtor-arquivo** é uma recomendação técnica criada pelo CCSDS e tem o objetivo de identificar, de definir e de estruturar as relações e as interações entre um produtor de informação e um arquivo. Traz ferramentas para que ações necessárias sejam estruturadas desde o momento do contato entre o produtor-arquivo até que os objetos de informação sejam recebidos e validados pelo arquivo. Essas ações abrangem a primeira etapa do processo de Admissão do e descreve partes das entidades funcionais da Administração do OAIS.

Já o **Modelo de empacotamento de dados conhecido como** *BagIt*, é um conjunto de esquemas hierárquicos projetado para suportar armazenamento e transferência de qualquer conteúdo digital. Um *bag* consiste em um diretório contendo os arquivos de *payload* e de

outros arquivos de metadados que os acompanham, conhecidos como arquivos *tag*. As *tags* são arquivos de metadados destinados a facilitar e documentar o armazenamento e a transferência do pacote (*bag*). O processamento de um *bag* não requer nenhuma compreensão do conteúdo do arquivo *payload* e os arquivos de *payload* podem ser acessados sem processar os metadados do *BagIt*.

De diversas formas, as partes dos Anexos foram mencionadas durante nossa explanação da Resolução n.º 51, e também não serão objeto de nossa análise aqui. Para o detalhamento deles, pode-se acessar a citada Resolução na íntegra no *site* do Conarq, nas suas Publicações Técnicas.

Quadro 18 – Elementos do conceito de confiança extraídos das Diretrizes para a Implementação de Repositórios Arquivísticos Digitais Confiáveis – RDC-Arq - versão 2

Conceitos	Definições
Autenticidade	Credibilidade de um documento enquanto documento – a qualidade deste de ser o que é, de estar livre de adulteração ou qualquer outro tipo de corrupção.
Confiabilidade	Credibilidade de um documento arquivístico enquanto afirmação de um fato. É quando ele pode sustentar o fato ao qual se refere, estabelecido pelo exame da completeza, da forma do documento e do grau de controle exercido no seu processo de criação.
Conversão de formato	Modificação de um formato para outro motivada, principalmente, pela normalização de formatos e para contornar a obsolescência tecnológica.
Evidência	Documentos que comprovem o cumprimento de requisitos, de competências, de objetivos e de responsabilidades.
Integridade	Estado dos documentos que se encontram completos e não sofreram nenhum tipo de corrupção ou de alteração não autorizada nem documentada.
Interoperabilidade	Capacidade de diversos sistemas e de organizações trabalharem em conjunto (interoperar), de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente.
Metadados	dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e preservar documentos arquivísticos ao longo do tempo.
Migração (tem a ver com o tempo)	conjunto de procedimentos e de técnicas para assegurar a capacidade de os objetos digitais serem acessados face às mudanças tecnológicas. A migração consiste na transferência de um objeto digital: a) de um suporte que está se tornando obsoleto, fisicamente deteriorado ou instável para um suporte mais novo; b) de um formato obsoleto para um formato mais atual ou padronizado; c) de uma plataforma computacional em vias de descontinuidade para outra mais atual. A migração pode ocorrer por conversão, atualização ou reformatação.
Planejamento da preservação	Um RDC-Arq deve fazer o planejamento da

	preservação dos documentos sob sua custódia, a fim de enfrentar os problemas trazidos pela obsolescência tecnológica e fragilidade do suporte. Esse planejamento deve ser feito a partir de uma política de preservação digital e ser bem documentado.
Preservação digital (tempo)	Conjunto de ações gerenciais e de técnicas exigidas para superar as mudanças tecnológicas e a fragilidade dos suportes, garantindo o acesso e a interpretação dos documentos digitais pelo tempo que for necessário.
Preservador de documentos arquivísticos	Entidade responsável pela custódia física e legal dos documentos do produtor, bem como por sua preservação, isto é, por proteger e garantir acesso contínuo aos documentos.
RDC-Arq	Deve ser capaz de atender aos procedimentos arquivísticos em suas diferentes fases e aos requisitos de um repositório digital confiável, conforme exposto.
Repositório arquivístico digital	Armazena e preserva documentos arquivísticos, nas fases intermediária e/ou permanente, devendo: gerenciar os documentos e metadados de acordo com as práticas e as normas da Arquivologia, especificamente relacionadas à gestão documental, à descrição arquivística multinível e à preservação; e proteger as características do documento arquivístico, em especial a autenticidade e a relação orgânica entre eles.
Repositório digital	Ambiente de armazenamento e de gerenciamento de materiais digitais.
Repositório digital confiável	É aquele capaz de manter autênticos os documentos digitais, de preservá-los e de prover pelo tempo que for necessário.

Fonte: Brasil (2023).

9 RESULTADOS E DISCUSSÃO

As Publicações Técnicas do Conarq como objeto desta tese, de modo orgânico, vão atribuindo novos termos, conceitos e definições a cada atualização de seus documentos, a fim de dar conta das mudanças ocorridas na sociedade e, precipuamente, por causa do avanço tecnológico.

Nesse sentido, constata-se que o campo da preservação digital cresce exponencialmente, não apenas porque se encarrega de proteger os documentos contra as adversidades desse ambiente; mas por envolver a comunicação e a cooperação, bem como investimentos de diversas áreas, sobretudo as ligadas às questões computacionais.

A Arquivologia desde os anos 1960, traz grandes contribuições para a preservação dos documentos eletrônicos e digitais, materializando suas ações em normativas, em projetos e em *software* para lidar com a obsolescência tecnológica. Uma norma será compreendida como válida se se observar o conjunto de operações do sistema jurídico, em que uma comunicação se entrelaça à outra em um processo contínuo (Pereira, 2010).

Esses produtos além de todas as suas atribuições de segurança, de proteção e de acessibilidade, permitem fornecer confiança à informação. Percebe-se que, nas Publicações Técnicas de Preservação Digital do Conarq, muito se tem falado acerca da confiança, mas pouco se tem explicado ou definido.

Para tratar dessa problemática, analisam-se as concepções dos autores que discutem o conceito de confiança, a fim de concatenar às normativas em questão, utilizando como subsídio a teoria de conceito Dahlberg. Dessa forma, identificam-se em cada diretriz: termos, conceitos, elementos, enunciados, características, categorias e definições que se relacionassem à confiança. E, para entender tais elementos, recorre-se às teorias dos autores adotados no Referencial Teórico sobre o conceito de confiança.

Em relação à sumarização neste Referencial, o Apêndice B criou um quadro elencando os autores, os enunciados acerca dos conceitos de confiança, conceitos de confiança e as características dos conceitos de confiança.

Para as seis normativas analisadas, extraíram-se conceitos e definições que estavam afinados, prioritariamente, aos postulados dos autores do nosso Referencial Teóricos, isto é, nem todos os conceitos retirados no fim das subseções das Diretrizes foram contemplados, apenas o que se encaixavam diretamente ao Referencial supra (Quadro 19). Para fins de organização do *corpus* desta pesquisa, o Anexo A referenciou essas seis Publicações Técnicas.

Quadro 19 – Síntese dos conceitos e definições de confiança extraídos das seis Publicações Técnicas do Conarq de preservação digital

Conceitos	Definições	Normas em que os conceitos e definições foram encontrados
Acessibilidade	A acessibilidade é uma categoria que engloba o elemento "Recepção" e "Saída". Nesse sentido, acessibilidade, dá-se pelo acesso aos documentos, por meio de *software* e de *hardware*, além de formatos de arquivos, que garantam a facilidade de acesso a longo prazo. Um desses elementos é a interoperabilidade que facilita o acesso, permitindo a troca de informações entre sistemas diferentes, devendo levar em consideração a responsabilidade e competência técnica e profissional do preservador na cadeia de preservação.	Diretrizes do Produtor (Brasil, 2013b). Diretrizes do Preservador (Brasil, 2013a).
Ações cooperativas	Visa incentivar programas cooperativos de preservação de documentos digitais para aplicação e compartilhamento de recursos sob a forma de acordos, de consórcios, de convênios e de parcerias.	Carta para a Preservação... (Brasil, 2005b).
Acurácia	Grau de precisão, de correção, de verdade, de ausência de erros e de distorções nas informações contidas nos documentos. Para a acurácia ser estabelecida, deve-se ter controle sobre os processos de produção, de transmissão, de manutenção e de preservação dos documentos digitais.	Diretrizes do Produtor (Brasil, 2013b). Diretrizes do Preservador (Brasil, 2013a).
Autenticidade	Qualidade de um documento ser o que diz ser, ou seja, aqueles não foram adulterados, alterados ou corrompidos de qualquer outra forma. Aos documentos arquivísticos, a autenticidade refere-se à confiabilidade enquanto tais. Para garantir a presunção de autenticidade, deve-se definir e conservar a identidade e a integridade dos documentos. A autenticidade é composta de identidade e de integridade. A autenticidade está ligada à transmissão do documento e à sua preservação e custódia. Um documento autêntico é aquele que se mantém da forma como foi produzido, portanto apresenta o mesmo grau de confiabilidade que tinha no momento de sua produção. Um documento não completamente confiável, mas transmitido e preservado sem adulteração ou qualquer outro tipo de corrupção, é autêntico.	Diretrizes do Produtor (Brasil, 2013b). Diretrizes do Preservador (Brasil, 2013a). Diretrizes para a presunção... (Brasil, 2012). e-ARQ Brasil – versão 2 (Brasil, 2022). Diretrizes para a Implementação... – versão 2 (Brasil, 2023).
Autenticação	É a declaração de autenticidade de um documento arquivístico, num determinado momento, inserindo algum elemento como acréscimo de uma pessoa investida de autoridade para tal. Um exemplo de técnica de autenticação é a criptografia e a assinatura digital.	Diretrizes do Produtor (2013b). Diretrizes para a Presunção... (Brasil, 2012).
Confiabilidade	Credibilidade do documento digital enquanto conteúdo ou declaração de um fato, estabelecida com base na sua completeza, na sua acurácia e no seu grau de controle exercido no processo de sua produção. Portando, tornando um documento arquivístico confiável. A confiabilidade é sinônimo de fidedignidade que está relacionada ao momento em que o documento é produzido e à veracidade do seu conteúdo. Para tanto, há que ser dotado de completeza e ter seus procedimentos de produção bem controlados.	Diretrizes do Produtor (Brasil, 2013b). Diretrizes do Preservador (Brasil, 2013a). Diretrizes para a presunção... (Brasil, 2012). e-ARQ Brasil – versão 2 (Brasil, 2022). Diretrizes para a Implementação... – versão 2 (Brasil, 2023).
Cadeia de custódia ininterrupta	Linha contínua de custodiadores de documentos arquivísticos (desde o seu produtor até o seu legítimo	Diretrizes para a Presunção... (Brasil, 2012).

	sucessor) pela qual se assegura que esses documentos são os mesmos desde a produção, não sofreram nenhum processo de alteração, sendo assim, autênticos.	
Completeza	A completeza dá-se pela presença de todos os elementos intrínsecos e extrínsecos exigidos pela organização produtora e pelo sistema jurídico-administrativo ao qual pertence, de maneira que esse mesmo documento possa ser capaz de gerar consequências. Dificilmente, pode-se assegurar a veracidade do conteúdo de um documento; ela é inferida da completeza e dos procedimentos de produção. A confiabilidade é uma questão de grau, ou seja, um documento pode ser mais ou menos confiável.	e-ARQ Brasil – versão 2 (Brasil, 2022).
Evidência	Documentos que comprovem o cumprimento de requisitos, de competências, de objetivos e de responsabilidades.	Diretrizes para a Implementação... – versão 2 (Brasil, 2023).
Fixidez (forma fixa e conteúdo estável)	É a qualidade de um documento arquivístico em assegurar sua forma fixa e seu conteúdo estável. A primeira ocorre quando o documento sustenta a mesma aparência ou apresentação cada vez que é recuperado. O segundo ocorre quando a informação e os dados documentos permanecem imutáveis, exigindo que eventuais mudanças sejam feitas por meio do acréscimo de atualizações ou da produção de uma nova versão. Assim, forma é a aparência ou a apresentação do documento, já conteúdo, a informação contida o documento.	Diretrizes do Produtor (Brasil, 2013b). Diretrizes para a Presunção... (Brasil, 2012).
Gestão arquivística de documentos	Tem o objetivo de garantir a produção e a manutenção de documentos fidedignos, autênticos, acessíveis, compreensíveis e preserváveis. Envolve a definição dos requisitos estruturais, bem como o desenho, a implementação e a manutenção de uma estrutura de cadeia de preservação, que inclui todos os elementos de política, de estratégia, de metodologia, entre outros necessários para o gerenciamento de documentos digitais.	Carta para a Preservação... (Brasil, 2013a). Diretrizes do Preservador (Brasil, 2013a).
Governo digital	Promove a participação de representantes das instituições arquivísticas nos projetos de governo digital, para a definição de estratégias, de padrões e de normas de gestão, de preservação e de acesso a documentos e informações, conforme orientação do Conselho Internacional de Arquivos e da Unesco.	Carta para a Preservação... (Brasil, 2005b).
Identidade	Conjunto dos atributos de um documento arquivístico que o caracterizam como único e o diferenciam de outros documentos arquivísticos (ex.: data, autor, destinatário, assunto, número identificador, número de protocolo). A identificação dos documentos digitais é chamada de metadados e esses atributos se constituem nos elementos intrínsecos da forma documental e nas anotações.	Diretrizes do Produtor (Brasil, 2013b). Diretrizes do Preservador (Brasil, 2013a). Diretrizes para a Presunção... (Brasil, 2012). e-ARQ Brasil – versão 2 (Brasil, 2022).
Integridade	Refere-se ao estado ou à qualidade dos documentos que se encontram completos e não sofreram nenhum tipo de corrupção ou alteração não autorizada nem documentada. É também um documento que não sofreu alterações de forma e de conteúdo. Junto à identidade, é um componente da autenticidade.	Diretrizes do Produtor (Brasil, 2013b). Diretrizes do Preservador (Brasil, 2013a). Diretrizes para a presunção... (Brasil, 2012). e-ARQ Brasil – versão 2 (Brasil, 2022). Diretrizes para a Implementação... – versão

		2 (Brasil, 2023).
Interoperabilidade	Capacidade de diversos sistemas e de organizações trabalharem em conjunto, de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente. Isto se faz por meio do uso de regras e de padrões de comunicação.	e-ARQ Brasil – versão 2 (Brasil, 2022). Diretrizes para a Implementação... – versão 2 (Brasil, 2023).
Metadados	Dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e preservar documentos arquivísticos ao longo do tempo, com o propósito de gerir a preservação e a acessibilidade dos documentos digitais.	Carta para a Preservação (Brasil, 2005b). e-ARQ Brasil – versão 2 (Brasil, 2022). Diretrizes para a Implementação... – versão 2 (Brasil, 20213).
Obsolescência (tecnológica	Consciência acerca da prevenção contra a efemeridade do *software* e do *hardware*, a fim de atualizá-los. Estratégia para solucionar dependência de *hardware* e de *software*. Fator que pode desencadear nos documentos arquivísticos riscos e ameaças de autenticidade através do tempo e espaço.	Diretrizes do Produtor (Brasil, 2013b). Diretrizes para a Implementação... – versão 2 (Brasil, 2023).
Padrões e protocolos	Define e recomenda a utilização de padrões e de protocolos abertos e de aceitação ampla na criação, no uso, na transmissão e no armazenamento de documentos digitais, no intuito de desenvolver soluções em cooperação com organizações de pesquisa e a indústria de tecnologia da informação e da comunicação.	Carta para a Preservação... (Brasil, 2005b).
Planejamento da preservação	Um RDC-Arq deve fazer o planejamento da preservação dos documentos sob sua custódia, a fim de enfrentar os problemas trazidos pela obsolescência tecnológica e fragilidade do suporte. Esse planejamento deve ser feito a partir de uma política de preservação digital e ser bem documentado.	Diretrizes para a Implementação... – versão 2 (Brasil, 2023).
Preservação (digital)/Proteção	São procedimentos para garantir autenticidade em meio às mudanças tecnológicas. É a estabilidade do suporte da informação com foco na manutenção do acesso, que pode implicar mudança de suporte e formato, bem como atualização do ambiente tecnológico. Qualidade de proteger os documentos digitais de ações não autorizadas. É preciso demonstrar que seria impossível para qualquer pessoa corrompê-los ou manipulá-los sem que fosse identificada.	Diretrizes do Produtor (Brasil, 2013b). Diretrizes do Preservador (Brasil, 2013a). e-ARQ Brasil – versão 2 (Brasil, 2022). Diretrizes para a Implementação... – versão 2 (Brasil, 2023).
Preservador de documentos arquivísticos	Entidade responsável pela custódia física e legal dos documentos do produtor, bem como por sua preservação, isto é, por proteger e garantir acesso contínuo aos documentos.	Diretrizes para a Implementação... – versão 2 (Brasil, 2023).
Presunção de autenticidade	Inferência da autenticidade de um documento arquivístico. Acontece pela evidência de que eles foram mantidos com uso de tecnologias e de procedimentos administrativos que garantiram a sua autenticidade; ou que, pelo menos, minimizem os riscos de modificações dos documentos a partir do momento em que foram salvos.	Diretrizes para a Presunção... (Brasil, 2012).
RDC-Arq	Deve ser capaz de atender aos procedimentos arquivísticos em suas diferentes fases e aos requisitos de um repositório digital confiável. O RDC-Arq engloba todos os outros repositórios, por isso é o mais confiável.	Diretrizes para a Implementação... – versão 2 (Brasil, 2023).
Relação orgânica	Relação que o documento arquivístico mantém com os	Diretrizes para a

	demais documentos do órgão e que refletem suas funções e atividades. Os documentos arquivísticos apresentam um conjunto de relações que devem ser mantidas.	Implementação... – versão 2 (Brasil, 2023).
Restrição de acesso	Análise dos documentos em relação à ostensividade ou à sigilosidade. No caso da sigilosidade, a legislação vigente estabelece procedimentos específicos para seu tratamento, como os graus de sigilo e de restrições de acesso.	Diretrizes para a Implementação... – versão 2 (Brasil, 20213).
Segurança da informação digital	Define a política de segurança da informação, que considere os aspectos legais, organizacionais, humanos e tecnológicos, de modo a garantir a autenticidade dos documentos digitais e o sigilo da informação, bem como a proteção contra perdas, acidentes e intervenções não autorizadas.	Carta para a Preservação... (Brasil, 2005b).

Fonte: Elaborado pelo autor (2024).

O conceito de “acessibilidade”, conforme as Diretrizes do Produtor (Brasil, 2013b) e as Diretrizes do Preservador (Brasil, 2013a), é uma categoria que engloba outros dois conceitos, o de: recepção e saída. Recepção é uma atividade que tem como finalidade garantir a autenticidade e a acessibilidade contínua aos documentos arquivísticos digitais, a fim de que não haja erros no processo de transferência ou recolhimento de informação. A saída caracteriza-se pelo acesso a tais documentos, que envolve o grau de responsabilidade e de competência técnica e profissional do preservador na cadeia de preservação.

Logo, a acessibilidade é o acesso aos documentos, por meio de *software* e de *hardware*, além de formatos de arquivos, que garantam sua facilidade a longo prazo. Sob o entendimento do conceito de confiança ligado à acessibilidade, tem-se Rotenberg (2022), quando afirma que a confiança é uma força prevalente que conecta pessoas e garante os relacionamentos e o funcionamento das coisas. Assim também corrobora Belchior (2015), que enfatiza a confiança como uma propriedade estabelecida entre os membros da sociedade ou das redes sociais que ligam os indivíduos, promovendo normas de cooperação recíprocas.

Para Rotenberg (2022), atualmente, o acesso a informações pode ser considerado um elemento negativo, quando há falta de confiabilidade. Com a tecnologia e as redes sociais, cada ação é transmitida a milhões de pessoas, muitas vezes, sem o devido cuidado, possibilitando acesso a informações não confiáveis.

Do ponto de vista dos preceitos da preservação digital, o acesso às informações pode ocorrer de diferentes formas, desde que seu objetivo seja manter os documentos arquivísticos digitais autênticos e acessíveis a longo prazo. Esse processo pode envolver aspectos como: a identificação (tipos documentais a serem preservados); a seleção (quais informações são realmente de valor); o armazenamento (as informações que foram selecionadas em um formato resistentes à obsolescências); e o acesso (sistemas informatizados de preservação ou

outro instrumento). Numa perspectiva sistêmica, esse complexo age de forma integrada, compreendendo todo o ciclo de vida documental em uma CCDA.

Outro conceito englobante à acessibilidade é a "restrição de acesso", configurada como a análise dos documentos em relação à sua ostensividade ou à sua sigilosidade. No caso da sigilosidade, a legislação vigente estabelece procedimentos específicos para seu tratamento, como os graus de sigilo e de restrições de acesso (Brasil, 2023).

Gambetta (2008a; 2008b) diz que é necessário algum nível de confiança para haver relação entre as partes, para que elas consigam cumprir regras. Contudo, a restrição possui certos graus que acarretam uma condição para a cooperação/interação/relação entre pessoas-sistemas. Essa condição em termos de confiança significa decidir até onde se precisa ou se pode confiar nos outros, mas também para os outros decidirem até onde podem confiar em nós; isto é, confiar é importante, contudo ser confiável também (Dasgupta, 2008).

Ainda em Gambetta (2008a; 2008b), essa ocorrência dá-se por meio de um pré-compromisso, que em suas diversas formas (unilateral ou bilateral) é um dispositivo que possibilita impor restrições. Promessas e contratos representam formas mais fracas desses pré-compromissos. O contrato, por exemplo, muda o foco da confiança para a eficácia das sanções caso um acordo seja quebrado. Já as promessas usam palavras para a formalização de contrato, podendo não acarretar sanções diretas.

Locke (2012) foi um dos primeiros filósofos a utilizar o termo *trust* como confiança, tanto em um sentido político como pessoal. O sentido político de *trust* significa *fides* (fé), e tem o objetivo de reforçar um aspecto contratual, de acordo ou comercial. Já o sentido pessoal de *trust* dá-se pelo seu uso comum, atrelado à confiança pessoal: em um líder, na família.

A restrição de acesso é um elemento importante à preservação digital. São medidas que impõem limites à consulta de determinados documentos com base em critérios, em leis e em políticas. Hodiernamente, os *software* arquivísticos conseguem lidar com essas questões de forma automática, envolvendo, por exemplo, controles de acesso, como nomes de usuários e senhas, autenticação de dois fatores, criptografia, auditoria de monitoramento entre outros métodos, que formam apenas uma parte que traz confiança à informação.

Como produto e espaço da preservação digital arquivística, destaca-se os "RDC-Arqs", que devem ser capazes de atender aos procedimentos arquivísticos em suas diferentes fases e aos requisitos de um repositório digital confiável. O RDC-Arq, basicamente, engloba as funcionalidades e os requisitos de todos os outros repositórios, sendo por isso, o mais confiável (Brasil, 2023).

Nessa linha, o estudo de Giddens (1991) está centrado nos ambientes de confiança e de

risco. Para o autor, a confiança localiza-se em espaços que envolvem as relações de parentescos (familiar), religiosas e de tradições, isto é, nas relações pessoais orientadas ao futuro. Em suma, a confiança pode ser definida como crença na credibilidade de uma pessoa ou sistema; e essa crença expressa uma fé na probidade do outro, ou na correção de princípios abstratos (conhecimento técnico). Assim, confiança é uma forma de fé na qual há uma segurança adquirida em resultados prováveis. São Tomás de Aquino significa a confiança como fé (*fidúcia/fides*), e a fé significa acreditar em alguma coisa (Aquino, 2001), assim como Santo Agostinho (2017). Para Aristóteles (1997), a confiança é uma virtude e se opõe ao medo, mas antes de tudo é acreditar para viver bem.

Em relação ao ambiente RDC-Arq, o conceito de "planejamento de preservação" se faz presente, o qual deve ser feito a partir de uma política de preservação digital, a fim de enfrentar os problemas trazidos pela fragilidade do suporte e pela obsolescência tecnológica (Brasil, 2023). Essa ação torna-se confiável aos RDC-Arqs, uma vez que envolve a implementação de políticas e de procedimentos rigorosos para garantir a autenticidade, a integridade e a acessibilidade a longo prazo das informações digitais.

Outro conceito importante à composição da confiança extraídos das normativas analisadas é o de "obsolescência tecnológica", o qual tem a ver com as questões relacionadas ao tempo. A obsolescência tecnológica é definida como a consciência acerca da prevenção contra a efemeridade do *software* e do *hardware*, a fim de atualizá-los. É também, um fator que pode desencadear, nos documentos arquivísticos, riscos e ameaças de autenticidade através do tempo e espaço.

Sob essa perspectiva, Giddens (1991) diz que a confiança relaciona-se à ausência no tempo e no espaço. Não haveria necessidade de se confiar em alguém cujas atividades fossem continuamente visíveis e cujos processos de pensamento fossem transparentes, ou de se confiar em algum sistema, cujos procedimentos fossem inteiramente conhecidos e compreendidos.

Para Engelmann e Klein (2020), a confiança correlacionada às tecnologias da TD traz algo em comum, a necessidade de que seus usuários sintam a "segurança" de que a inovação perdure por muito tempo, o que a reveste de confiabilidade. Corroboram os autores, para a confiança operar o tempo é fundamental, isto é, a confiança possibilita o controle do tempo; ela encontra-se entre o passado e o futuro, para que no presente, reduza-se complexidade.

Ainda sobre as modalidades de tempo, os autores complementando dizem: confiar não é necessariamente eliminar os perigos existentes no futuro – que, por sua vez, é incerto e permanecerá sendo incerto –, mas agir como se o futuro fosse certo, ou melhor: confiável. Ela

traz o passado bem-sucedido para as expectativas de um futuro mais seguro, menos complexo.

A marca registrada da visão de Luhmann (2008) sobre a confiança é justamente concebê-la como um mecanismo de redução da complexidade que traz segurança para o futuro. Portanto, tê-la, também é sentir seus antônimos: insegurança, risco, perda, medo, falta. Não existe garantia de uma certeza das coisas por intermédio da confiança; mas um futuro incerto pode se fazer confiável; é como uma aposta feita no presente em experiências passadas. Assim também, concorda Gambetta (2008a) ao afirmar que a confiança inclina-se a ações futuras que condicionam nossas decisões presentes.

De acordo com Lundåsen (2002), a confiança é um modo de previsibilidade como expectativa para eventos futuros, em que existe a possibilidade de ocorrer algum tipo de perda se a confiança não for correspondida. Em outras palavras, há um elemento de risco envolvido.

Conforme os preceitos preservação digital, e para dar conta da obsolescência, necessita-se de estratégias, tanto no que diz respeito à manutenção documental, quanto à sua própria preservação. As estratégias de manutenção são ações que trazem requisitos mínimos para proteger e para manter a acessibilidade aos documentos arquivísticos e as suas cópias autênticas. E as estratégias de preservação incluem uma dependência tecnológica, subsidiada pela utilização de *hardware* e de *software* confiáveis a esses documentos a longo prazo (Brasil, 2013b; Brasil, 2013a).

Um dos exemplos mais praticados desta última estratégia é a migração, configurada pelo conjunto de procedimentos e de técnicas para assegurar a capacidade de os objetos digitais serem acessados face às mudanças tecnológicas. A migração consiste na transferência de um objeto digital: a) de um suporte que está se tornando obsoleto, fisicamente deteriorado ou instável para um suporte mais novo; b) de um formato obsoleto para um formato mais atual ou padronizado; c) de uma plataforma computacional em vias de descontinuidade para outra mais atual. A migração pode ocorrer por conversão, atualização ou reformatação (Brasil, 2023).

Como visto, a restrição de acesso serve como pêndulo à “segurança da informação digital”, que segundo a Carta para a Preservação... (Brasil, 2005b), deve considerar os aspectos legais, organizacionais, humanos e tecnológicos, de modo a garantir a autenticidade dos documentos digitais e o sigilo da informação, bem como a proteção contra perdas, acidentes e intervenções não autorizadas.

Para Aquino (2001), a confiança deve ser oposta ao temor, pois sua essência denota ter segurança de que se conseguirá um determinado bem. Para Machiavelli (2019), a confiança denota segurança em alguém.

Diz Pereira (2010) que a confiança substitui informações insuficientes, causando segurança para algo ou para alguém. Os meios de comunicação responsáveis pela formação de opiniões, pelas informações que veiculam, pelos produtos que vendem – ao gerar expectativas devem assegurá-las, para que a segurança seja mantida e a confiança não desapareça, sendo capaz de cumprir seu papel de crença no presente, por meio das atitudes do passado, de que o futuro prometido será assegurado. Esses mecanismos servem de ponte para a confiança existir, em que há viabilidade para o seu desenvolvimento; mas quando isso é rompido, quebra-se as expectativas e vem os sentimentos de desconfiança e de desinteresse.

Destaca Canedo (2012) que a segurança é uma consequência da confiança, significando confiabilidade, que é a capacidade de alguém ser confiável. Giddens (1991) e Engelmann e Klein (2020) também enfatizam que a segurança é uma forma de confiança e fé.

Outro conceito importante é representado pelo "governo digital", que inserido na Carta para a Preservação... (Brasil, 2005b), promove a participação de representantes de instituições arquivísticas para a definição de estratégias, de padrões e de normas de gestão, de preservação e de acesso a documentos e informações. Tal definição encontra-se registrada nos escritos de Confúcio (2001), quando dizia que a confiança se dá pelas relações entre pessoas na sociedade, traduzida como um princípio ou virtude para uma boa governança.

Essa concepção traz consigo elementos que servem à completude da confiança, isto é, a integridade, a confiabilidade e a fidelidade (representado pelo *Xin* e pelo *Zhing*), que significam conservar e preservar características originais dessas relações na sociedade de forma abstrata ou concreta. O *Xin* e o *Zhing* à preservação digital significam armazenar e disponibilizar informações confiáveis, ou seja, autênticas, dispostas em formato compatível com o de utilização.

Machiavelli (2019) vai ao encontro dessa ideia quando fala da confiança como uma forma de interação mais ampla, englobando o Estado como representante da interação entre as pessoas. A confiança para o filósofo expressa a segurança que um líder deve ter para governar. O Estado deve deter todo o poder e mérito para praticar suas ações desde que direcionada ao bem-estar das pessoas.

Para Gambetta (2008a; 2008b), essa relação entre pessoas-governo é chamada de cooperação, que é o sentido mais amplo desses agentes acordarem um contrato que seja cumprido. Putnam (1996; 2006), nesta concepção, enfatiza que o capital social é um componente básico da confiança e atribui seu alto nível à cooperação entre o governo e a comunidade; e o seu baixo nível, a baixa confiança no governo que interage menos com os cidadãos.

Essa figura (governo ou Estado), nas Publicações Técnicas por nós analisadas, pode ser representada pelo “preservador de documentos arquivísticos”, que consoante Brasil (2023), é a entidade responsável pela custódia física e legal dos documentos do produtor, bem como por sua preservação, isto é, por proteger e garantir acesso contínuo aos documentos.

Nesse sentido de cooperação, tem-se as “ações cooperativas” da Carta para a Preservação... (Brasil, 2005b), servindo para incentivar programas de preservação de documentos digitais para a aplicação e o compartilhamento de recursos sob a forma de acordos, de consórcios, de convênios e de parcerias. Em complemento a essa definição, tem-se também os “padrões e protocolos” da mesma Carta (Brasil, 2005b), os quais definem e recomendam a utilização de padrões e de protocolos abertos na criação, no uso, na transmissão e no armazenamento de documentos digitais; no sentido de desenvolver soluções em cooperação com organizações de pesquisa e a indústria de tecnologia da informação e da comunicação.

Em aditamento ao descrito acima, o conceito de “interoperabilidade” é caracterizado pela capacidade de diversos sistemas e de organizações trabalharem em conjunto, de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente. Isto se faz por meio do uso de regras e de padrões de comunicação.

Neste caso, a interação e a cooperação estão intimamente ligadas, principalmente por estarem inseridas no contexto da tecnologia da informação e da comunicação, sendo essencial para alcançar a interoperabilidade.

Acerca da cooperação, pode-se basilar nos conceitos de confiança de Gambetta (2008a; 2008b),– a forma mais básica de cooperação (humana) é a condição de uma interação benéfica, sendo preciso algum nível de confiança em que as partes consigam cumprir certas regras. Uma virtude instala-se no sentido de cooperação: a crença. Sendo assim, confiança é uma crença peculiar baseada não em evidências, mas na falta dela.

Continua Hwang e Burgers (1997), a confiança não é uma condição suficiente da cooperação, embora necessária, pois ela atenua o fator “risco”, que pode reverberar na perda de algo. Para Fukuyama (1995), a confiança é uma relação de cooperação, sendo de grande importância para o plano político, para a estabilidade das instituições. É um fator do capital social, que é a capacidade de indivíduos(s) (grupos ou organizações) trabalharem em conjunto para uma causa comum, que dependendo do grau de partilha de normas e de valores atendem aos interesses das pessoas.

De um ponto de vista mais documental, o conceito de “acurácia” destacado nas

Diretrizes do Produtor (Brasil, 2013b) e nas Diretrizes do Preservador (Brasil, 2013a) é definida como o grau de precisão, de correção, de verdade, de ausência de erros e de distorções nas informações contidas nos documentos. Para a acurácia ser estabelecida, é necessário se ter controle sobre os processos de produção, de transmissão, de manutenção e de preservação dos documentos. Processos estes identificados na "gestão arquivísticas de documentos" e na "preservação de documentos digitais"; o primeiro identificado na Carta para a Preservação... (2005b) e nas Diretrizes do Preservador (Brasil, 2013a); e o segundo, além de inseridos nessas duas normativas citadas, também no e-ARQ Brasil (Brasil, 2022) nas Diretrizes para a Implementação de RDC-Arqs (Brasil, 2023).

Em complemento a este conceito, tem-se a "confiabilidade", caracterizada como a credibilidade do documento digital enquanto conteúdo ou declaração de um fato, estabelecida com base na sua completeza, na sua acurácia e no seu grau de controle exercido no processo de sua produção. A confiabilidade é sinônimo de fidedignidade que está relacionada ao momento em que o documento é produzido e à veracidade do seu conteúdo. Para tanto, há que ser dotado de completeza e ter seus procedimentos de produção bem controlados. A confiabilidade é uma questão de grau, ou seja, um documento pode ser mais ou menos confiável.

Sobre isso, Ketzer (2015) realça que a confiança existe por meio do conceito de "confiar" (*trust*) e de "fiar-se" (*rely*). Para a autora, fiar-se ou fiabilidade (*reliability*) é o nível mais básico, que se define pelas nossas relações com o mundo, com as instituições e com desconhecidos, sendo necessária para nossa vida diária; porém *trust*, é mais profundo, no qual a confiança é explícita e pode envolver a instituição de promessas como acordos. A fiabilidade é uma relação que envolve sentimentos.

A fidedignidade (*trustworthy*), por sua vez, é uma forma especial de dependência do conhecimento e que confere ao falante obtê-lo e compartilhá-lo. Para isso, o ouvinte geralmente aceita as palavras do falante e as toma para si, assumindo o testemunho do falante autoridade. Portanto, confiar é ter a noção de dependência de algo ou de alguém e fidedignidade é a propriedade que alguém tem de ser competente e comprometida com o que lhe é confiado. Como diz Fricker (1998) – alguém que é fidedigno e competente tem autoridade racional, e retendo ambas características, possui credibilidade.

A "completeza", conceito extraído do e-ARQ Brasil, é definida pela presença de todos os elementos intrínsecos e extrínsecos exigidos de um documento arquivístico. Dificilmente, pode-se assegurar a veracidade do conteúdo de um documento; ela é inferida da completeza e dos procedimentos de produção.

Descarte (2012) e Kant (2000) enfatizam que a confiança está direcionada à busca pela verdade e pelo conhecimento, ensejando um elemento necessário para se chegar a um resultado desejado, a partir do conhecimento científico.

Canedo (2012) e Confúcio (1996) consideram que a confiabilidade se dá pelas relações pessoais, sendo a capacidade de alguém/algo ser confiável e a confiança seria sua consequência, possibilitando segurança a um objeto, além de conservar e preservar suas características originais.

O conceito de "autenticidade" está contemplado em todas as seis normativas desta tese, definido como a qualidade de um documento (arquivístico) ser o que diz ser, sendo aqueles que não foram adulterados, alterados ou corrompidos de qualquer outra forma, ligado à transmissão do documento e à sua preservação e custódia. É também composto de identidade e de integridade.

Um documento autêntico é aquele que se mantém da mesma forma como foi produzido, portanto apresenta o mesmo grau de confiabilidade que tinha no momento de sua produção. As Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais enfatizam três aspectos da autenticidade, cujos documentos podem ser expressos de forma legal, histórica ou diplomática.

Nesse sentido, a "identidade" é conjunto dos atributos de um documento arquivístico que o caracterizam como único e o diferenciam de outros documentos arquivísticos. E essa identificação é chamada de metadados e esses atributos se constituem nos elementos intrínsecos documentais (Brasil, 2013b; Brasil, 2013a; Brasil, 2022).

Já a "integridade", como definida nas seis normativas desta tese, é o estado ou a qualidade dos documentos que se encontram completos e não sofreram nenhum tipo de corrupção ou de alteração não autorizada nem documentada. Outro elemento da autenticidade é a "autenticação", que é a declaração de autenticidade de um documento arquivístico, num determinado momento, inserindo algum elemento como acréscimo de uma pessoa investida de autoridade para tal, como por exemplo, uma assinatura digital.

Os "metadados", por sua vez, são dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e preservar documentos arquivísticos ao longo do tempo, com o propósito de gerir a preservação e a acessibilidade dos documentos digitais; sendo assim, uma extensão da identidade e da integridade (Brasil, 2005b; Brasil, 2022; Brasil, 2023).

Sobre o conceito de confiança relacionado à autenticidade, pode-se também identificá-lo por meio da integridade, que neste caso se define pela coisa imaculada. Segundo Lucena

(2009), a integridade cria confiança, significando uma propriedade da crença, de um acordo e de uma promessa, que acontece, por exemplo, quando um indivíduo assume um risco e para diminuí-lo deve-se confiar, ou seja, acreditar nos nossos vínculos afetivos.

Já para Giddens (1991), a integridade está mais ligada à desconfiança do que à confiança, sobretudo numa relação que envolve sistema-indivíduo. Dessa maneira, a integridade, como corrobora o mesmo autor, é um elemento da desconfiança que significa duvidar ou desacreditar de algo que foi corrompido ou reivindicado, não mantendo sua forma original, indo à contraparte da concepção de Confúcio (1996).

Nesse sentido, e estando ligada à gestão de documentos, à preservação, ao acesso, e especialmente à autenticidade, destaca-se a "cadeia de custódia ininterrupta" registrada nas Diretrizes para a Presunção… (Brasil, 2012), que é uma linha contínua, sem quebra, de custodiadores (produtores e preservadores) de documentos arquivísticos pela qual se assegura que esses documentos são os mesmos desde a produção e não sofreram nenhum processo de alteração, sendo assim, autênticos, mantendo sua forma original. O importante aqui é manter a custódia, ou seja, os agentes que gerenciam os documentos devem gerar ações de comunicação entre os documentos e os sistemas informatizados, que de forma abstrata, segundo Aristóteles (1991), pode ser representada por uma linha traz confiança, mantendo assim, a fixidez dos documentos.

Sobre essa fixidez, as Diretrizes do Produtor (Brasil, 2013b) e as Diretrizes para a Presunção… (Brasil, 2012), a definem como a qualidade de um documento arquivístico em assegurar sua forma fixa e seu conteúdo estável. O documento tem forma fixa quando sustenta a mesma aparência ou apresentação cada vez que é recuperado. E o conteúdo estável, quando a informação e os dados dos documentos permanecem imutáveis, exigindo que eventuais mudanças sejam feitas por meio do acréscimo de atualizações ou da produção de uma nova versão.

A fixidade ou fixidez dá-se como uma característica do documento arquivístico (digital) de manter sua forma original, conforme confúcio (1996), ligando-se também à autenticidade. É também, um modo de dar estabilidade ao documento, que para Feres Júnior; Eisenberg (2006); Inglehart (1999) e Fukuyama (1995), significa confiar em instituições, sem violar preceitos da lei, como por exemplo, seguir normas.

A "evidência" Brasil (2023): dá-se quando os documentos podem comprovar o cumprimento de requisitos, de competências, de objetivos e de responsabilidades. Estando intimamente ligada à presunção de autenticidade, que é a inferência da autenticidade de um documento arquivístico, acontecida pela evidência de que eles foram mantidos com uso de

tecnologias e de procedimentos administrativos que garantiram a sua autenticidade; ou que, pelo menos, minimizem os riscos de modificações dos documentos a partir do momento em que foram salvos.

Os postulados de McKyler (2011) encontram-se aos de Ketzer (2015), a confiança está dividida em dois níveis. Um é representado pelo termo fiar-se ou fiabilidade, concebido por uma perspectiva mais individualista, tratando-se de uma espécie de dependência entre os agentes e as suas fontes de conhecimento para aceitar algo como evidências; e o outro pelo conceito de confiar (*trust*), que envolve mais do que fiar-se, pressupõe a boa vontade do outro em auxiliar alguém, mais do que simplesmente crer que a palavra do outro é verdadeira.

Para Gambetta (2008a; 2008b), a confiança é uma crença não necessariamente baseada em evidência, mas na falta dela, realçando assim, a possibilidade de desconfiança como um grau particular subjetivo de probabilidade, no qual um agente acredita que outro agente realizará uma ação sujeita a afetar a sua própria ação. Assim, tanto a confiança como a desconfiança representam predisposições lexicográficas para atribuir valores da probabilidade e mantê-los incondicionalmente acima de alguma evidência.

Outro elemento ligado à desconfiança é o risco. Diniz e Marconatto (2011) realçam duas condições para o desenvolvimento da confiança: 1. risco ou vulnerabilidade como a probabilidade de se perder algo/alguém, quando interpretada por uma das partes decisórias; 2. a interdependência, que é quando os interesses de uma das partes não podem ser atingidos sem a colaboração da outra. A confiança nesses sentidos (individual ou coletivo) está destinada a controlar e a fiscalizar a ação dos agentes em seus relacionamentos, como por exemplo, entre pessoas e sistemas. Ketzer (2015) complementa: quem confiança coloca-se numa posição vulnerável de risco de traição. Isto é, confiança é uma relação que envolve direitos e obrigações.

Dizem Luhmann (1996; 2008) e Barbosa (2017) que a confiança é representada pelo risco. Luhmann (1996; 2008), o risco substitui, em grande parte, o que antes era pensado como destino e torna-se separado das cosmologias. Já Lundåsen (2002) disserta que o risco é um mecanismo de previsibilidade como expectativa para eventos futuros, em que existe a possibilidade de ocorrer algum tipo de perda se a confiança não for correspondida.

Segundo Putnam (1996; 2006), também existem tipos diferentes de confiança, o denso e o delgado. O denso estabelece-se nas interações face a face e com o conhecimento direto, reduzindo o grau de risco. E no delgado, confiança é medida pela maior possibilidade de risco. Filgueiras (2007), o exercício da confiança acontece pelo modo como as instituições são capazes de reduzir o risco em sociedades complexas.

Em contrapartida, Giddens (1991) afirma que a confiança está vinculada à contingência e não necessariamente ao risco. A confiança sempre leva à conotação de credibilidade em face de resultados contingentes, ou melhor, às ações de indivíduos ou à operação de sistemas. Para o autor, outro conceito está intimamente relacionado ao risco – o perigo, porém, não possuem o mesmo significado, sendo assim, o risco pressupõe perigo (não necessariamente a consciência dele). Por exemplo, uma pessoa que arrisca algo flerta com o perigo, compreendido como uma ameaça aos resultados desejados.

Confiar não é necessariamente eliminar os perigos existentes no futuro – que, por sua vez, é incerto, mas agir como se o futuro fosse certo, ou melhor: confiável. Ela traz o passado bem-sucedido para as expectativas de um futuro mais seguro, menos complexo. Coloca-se cobertas nas contingências para não as enxergar e dessa forma poder agir com menos receio. Se isto não for possível, invertem-se os polos e mostra-se toda a insatisfação através da desconfiança (Giddens 1991).

O conceito de "relação orgânica" conforme as Diretrizes para a Implementação… (Brasil, 2023), dá-se pela ligação, conexão e/ou vínculo que o documento arquivístico mantém com os demais documentos, refletindo suas funções e atividades.

Para Confúcio (1996), a confiança pode acontecer como forma de uma relação sobre um objeto de forma abstrata ou concreta. Isto é, de forma abstrata quando ela não é praticada e concreta quando ela é praticada, por exemplo, a conexão entre duas pessoas que garanta o funcionamento de alguma coisa é um exemplo disso (Rotenberg, 2022; Lucena, 2009).

Inglehart (1999) diz que deve-se existir pelo menos um grau de relacionamento entre pessoas, servindo, sobretudo, para a estabilidade da sociedade. Para Belchior (2015), a confiança existe porque tem tido relevância nas relações entre indivíduos das ordens mais diversas, desde que afetem a vida em sociedade de alguma forma. Já Diniz; Marconatto (2011), por exemplo, diz que quanto maior a confiança entre dois negociadores, menos a sua relação demandará de marcos regulatórios (como contratos formais), uma vez que há a crença de parte a parte de que um não trairá o outro, ou seja, não incorrerá em comportamentos oportunistas.

Uma das maiores representações do conceito de confiança é dada pela relação inter(pessoal); é como se ele somente existisse se começasse por esse caminho. A maioria dos autores o concebem como uma interação que envolve pelo menos duas pessoas. E a partir disso, é que se desenvolvem seus outros elementos: a cooperação, o risco, a segurança, o tempo, entre outros.

Aplicado às tecnologias digitais, tal conceito vem ganhando cada vez mais notoriedade

(mesmo que involuntariamente) entre a sociedade e o meio corporativo, haja vista as suas possibilidades de segurança, de transparência e de acesso, subsidiado por ferramentas como por exemplo, a *blockchain* e os sistemas informatizados arquivísticos; dispositivos estes, inseridas na preservação digital.

De acordo com as normativas analisadas, percebe-se uma incipiência à PDS, talvez isso se justifique por ser um conceito incipiente e ainda parco conhecido no Brasil. Mesmo as Diretrizes mais recentes como o e-ARQ Brasil e as dos RDC-Arqs, não mencionam os termos, ou o fazem alusão.

Viu-se que diversos termos, enunciados, conceitos e definições nas Publicações Técnicas do Conarq de preservação digital estão intimamente compostos ao conceito de confiança em sua essência. Logo, compreender a confiança em sentido substancial foi um elemento necessário para comprovar que as normas de preservação digital trazem, realmente, confiança à informação.

10 CONSIDERAÇÕES FINAIS

Por se dedicar a um insumo comum a todas as áreas científicas, a informação, a Ciência da Informação tem possibilidades de dialogar com diversos domínios do conhecimento e diferentes setores sociais. Surgida numa redoma imanente à tecnologia, ela conseguiu adaptar-se aos abundantes estudos incorporados ao meio digital. Nesse particular, Saracevic (1996) pondera que a máquina "computador" causou grandes impactos e transformações no uso, na descrição e nas transferências das informações devido à interação com as pessoas.

Nessa ambiência, foi a Arquivologia pioneira a tratar das práticas de preservação digital, concebendo-a como um campo direcionado ao cuidado e à longevidade da informação. Segundo Fontana *et al.* (2014), tal temática vem sendo discutida no âmbito de diferentes áreas como a Administração, a Contabilidade e o Direito, respeitando, sobretudo, suas particularidades, isto é, o contexto e a necessidade de cada uma.

Conforme Ferreira (2006), a implementação da preservação digital não se baseia apenas no armazenamento de informações; entretanto, na manutenção de suportes, de formatos, de *hardware*, de *software*, os quais envolvem processos de recuperação e de acesso aos seus materiais digitais. Por isso, torna-se imprescindível a adoção de tratamentos técnicos a esses objetos (Rodrigues, 2015)

Aditam Flores, Pradebon e Cé (2017), o acesso à informação, o advento da *Internet* e, especialmente, a preservação digital, fundamentam-se no desenvolvimento e na aplicação de procedimentos capazes de viabilizar a longevidade dos documentos. Assim, o resultado da constante e da rápida evolução tecnológica fez brotar uma série de preocupações em relação aos dos documentos digitais, principalmente à sua segurança e à autenticidade, indispensáveis ao processo de preservação, que vão além da conservação dos suportes (Gomes, 2019). Esta última concepção já não se restringe a uma perspectiva tradicional da preservação digital, que ocorria por meio de estratégias de migração de suportes para mídias subsequentes.

No intuito de trazer mais confiança e proteção à informação, a Arquivologia passou a adaptar a cadeia de custódia analógica para uma CCDA, e, consequentemente, à PDS, envolvendo, obrigatoriamente, parâmetros arquivísticos que se preocupam com o documentos desde sua gênese, em uma linha ininterrupta, até o seu acesso.

A ocorrência da PDS depende de *hardware* e de *software* considerados confiáveis, recebendo essa atribuição porque estão baseados em normas e diretrizes específicas que

acompanham o ciclo de vida dos documentos, além do processo da TD, a fim de dar conta das mudanças e da obsolescência tecnológica.

A CCDA, genericamente, é uma adaptação da teoria de Hilary Jenkinson, que deve incluir a manutenção de todo o ciclo de vida dos documentos arquivísticos inseridos no ambiente digital em uma cadeia de custódia ininterrupta, por meio de sistemas informatizados de gerenciamento, de preservação e de acesso, visando mitigar as suas vulnerabilidades. Já a PDS configura-se como a capacidade de garantir que os documentos digitais arquivísticos permaneçam acessíveis com qualidade suficiente para serem interpretados no futuro, quando recorrido a uma plataforma digital diferente da utilizada no momento de sua criação, por meio de uma comunicação correta, basilada pela imposição de elementos de confiança, como políticas e normas. Ambas são importantes para a Arquivologia, pois visam à preservação e à autenticidade dos documentos digitais pelo tempo que for necessário.

Pode haver confusão entre os conceitos de CDDA e de PDS, em que, muitas vezes, utilizam-se como sinônimos, porquanto possuem definições próximas e complementares. Dessa forma, umas das contribuições desta tese foi trazer concepções acerca desses dois conceitos, no intuito de dirimir e de elucidar suas participularidades, e, consequemente, dicomotizá-los.

Assim, retomando à definição de CCDA, define-se como: uma linha ininterrupta, ou seja, a comunicação entre os documentos arquivísticos, em suas fases corrente, intermediária e permanente, subsidiada por ambientes digitais distintos, como o de gestão (para as idades corrente e intermediário), de preservação e de acesso (para a idade permanente), por um processo sequencial, e, para isso acontecer, os documentos devem estar inseridos num Sigad ou num sistema de gestão com requisitos arquivísticos, interoperável com um RDC-Arq e, este, com uma plataforma de acesso e difusão, se necessário; perpassando a produção, a avaliação e a preservação, alcançando o acesso, bem como conservando as características dos documentos de arquivo, a fim de que permaneçam incorrompidos e sua autenticidade seja garantida. Além disso, envolve as entidades externas do modelos OAIS, participantes do ciclo de vida documental, o produtor, o preservador e o consumidor, que, no caso do espaço de preservação, é gerenciado por dois agentes, o administrador de preservação e o administrador de TI, os quais trabalham numa ação cooperada – compartilhada e distribuída – para manter o armazenamento e a manutenção confiável dos documentos digitais arquivísticos.

A PSD define-se como uma forma de preservação digital, que utiliza um conjunto de estratégias, para administrar o ciclo de vida dos documentos, perpassando os três ambiente das entidades externas do modelo OAIS, prevendo uma CCDA segura e ininterrupta, em que

os sistemas informatizados de gestão, de preservação e de acesso estejam devidamente integrados de maneira holística, da produção ao acesso à informação; todos eles baseados em políticas, em normas e em padrões, que assegurem a autenticidade e, consequentemente, a confiabilidade aos documentos pelo que tempo que for necessário.

A PDS é um campo de estudo e de práticas que transcende a mera salvaguarda de arquivos digitais, abrangendo não apenas os aspectos técnicos, mas também os contextos organizacionais, sociais e culturais. Para a sua implantação, deve-se considerar alguns elementos essenciais: que vão além da simples manutenção de arquivos digitais; que envolvem a integração de sistemas, de processos e de atores; que preconizam uma CCDA; que interconectam ambientes (produtor-administrador-consumidor); que se preocupam com a obsolescência tecnológica (de formatos, da *hardware*, de *software*, de suporte, entre outras). Em síntese, preservar sistemicamente é um desafio complexo, contudo essencial para garantir que nosso patrimônio digital seja continuado.

Nesse cenário, a TD serve como alicerce para se enxergar os impactos tecnológicos e a lidar com eles, mas, sobretudo, pela melhor utilização de tecnologias por meio do processo de incorporação da inovação nos diversos setores da sociedade. A representação da TD na área dos arquivos está materializada nos produtos que a CCDA e a PDS utilizam.

Lopez (2004) afirma que existe a necessidade de ampliar as discussões sobre a implicação das TDIC no universo arquivístico. Para exemplificar essa ratificação, o autor destaca alguns pontos importantes como a gestão eletrônica de documentos e a importância dos metadados, os quais no ambiente digital contribuem para manter a fidedignidade da informação, pois, além de garantir a autenticidade dos registros, independentemente do suporte, passam a ser um elemento que define sua organicidade.

Com efeito, foi nesse escopo que se inseriu este estudo, preocupado em compreender o conceito de confiança, identificado por elementos como termos, características e definições, sendo, portanto, um mecanismo fundamental que permeia as relações humanas desde tempos imemoriais. Na Antiguidade, foi um recurso crucial nas relações sociais, considerarada uma forma de cooperação para sobrevivência. Durante a Idade Média, confirmou o compromisso e a fidelidade entre os nobres, além de ser representada pela busca divina, que em alguns casos unia fé e razão. Ao longo do tempo, construiu-se por meio de ações e de comportamentos consistentes. Assim, na Idade Moderna e na Idade Contemporânea, desempenhou, de modo mais acentuado, fator significativo nas relações comerciais, políticas, familiares e pessoais para funcionar eficazmente.

A confiança sempre foi, então, pilar essencial para a coesão social, para a colaboração e para o progresso. Ela transcende culturas e épocas; em que atualmente molda nossas interações, conectando todo o mundo, por intermédio da *Web* e da *Internet*, gerando, agora, contratos e compromissos digitais. Objetos estes que demandam, cada vez mais, ações de intervenções de diversas ordens como de segurança, administrativa, política, de preservação e de acesso (confiáveis), que no campo arquivístico podem ser visualizadas nas suas Publicações Técnicas.

Uma das primeiras entidades, em âmbito internacional, a se preocupar com os estudos sobre a preservação digital e, consequentemente, a confiança da informação, foi o Projeto InterPARES, definindo conceitos e criando teorias, os quais serviram para disseminar importantes termos e características para os documentos, a saber, identidade, integridade, autenticidade, registro eletrônico e fidedignidade, entre outros.

Em âmbito nacional, os enfoques desses elementos estão registrados nas Publicações Técnicas do Conarq, mais precisamente as que envolvem preservação digital, e isto significa dizer que, para a informação ser considerada confiável, precisa estar de acordo com os preceitos arquivísticos das normativas analisadas nesta tese, a saber, Carta para a Preservação do Patrimônio Arquivístico Digital; Diretrizes do Produtor; Diretrizes do Presevador; Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais; Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos – e-ARQ Brasil - versão 2; e Diretrizes para a implementação de Repositórios Arquivísticos Digitais Confiáveis - RDC-Arq - versão 2.

Cada uma das Diretrizes examinadas tem sua particularidade e, à medida que sofrem atualizações ou são implantadas, mais elementos surgem para dar conta da complexidade do mundo tecnológico. Logo, essas não são as únicas a circundar a preservação digital, nem trazer elementos de confiança à informação e aos documentos de arquivo no âmbito do Conarq, mas, certamente, corresponde um importante recorte do espaço-tempo necessário às suas análises. Nessa perspectiva, espera-se que este escrito sirva de alicerce para que mais estudos sejam desenvolvidos dentro da temática e fora dela, e que o aprimoramente do entendimendo acerca da essência da confiança possa reverberar em futuras pesquisas para elucidar possíveis dúvidas, indagações e inquietações no meio tecnológico, em que, muitas vezes, parece demasiadamente tecnicista.

Isto posto, retoma-se aqui a questão-problema: “qual o significado de confiança nas Publicações Técnicas do Conarq com foco na preservação digital? Quais foram os recursos ou

os elementos utilizados nessas Diretrizes que serviram para nos fazer compreender o conceito de confiança?

A resposta para a primeira indagação tem como base a compreensão do conceito e do significado de confiança nas Publicações Técnicas do Conarq de preservação digital, que se deu por meio dos estudos advindos da Sociologia e da Filosofia. Procura-se entendê-lo em sua essência e sobre variadas concepções. Assim, identifica-se que a confiança relaciona-se com diferentes conceitos, como, por exemplo, o tempo, o risco, a (in)segurança, a cooperação, a relação, a fé e a virtude, entre outros, e, para correlacionar esses termos às Publicações em questão, utilizou-se como subsídio enunciados, definições e características que fizessem aporte aos seus conceitos. O fato é que a "obsolescência tecnológica" é um conceito que possui características e definições que retratam o "tempo" como elemento-chave. Logo, a confiança só existe porque todo um entorno de conceitos se ligam a ela.

Na resposta para a segunda indagação constatou-se que a representação do que significa confiança nas Publicações deram-se por meio de conceitos e de definições que se concatenaram aos postulados dos autores do Referencial Teórico do conceito de confiança; entendimento que se tornou possível por intermédio do método indiciário e da Teoria do conceito de Dahlberg.

Destarte, esta pesquisa teve o objetivo geral de analisar o conceito de confiança nas Publicações Técnicas do Conarq de preservação digital. E, para tanto, os objetivos específicos organizaram-se em quatro pontos, conforme os parágrafos abaixo.

O primeiro objetivo específico foi o de compreender o conceito de confiança na perspectiva da Filosofia e da Sociologia, para, assim, analisar os aspectos de confiança das Publicações Técnicas do Conarq de preservação digital.

Numa óptica filosófica, a confiança tem sido objeto de reflexão desde os primeiros filosófos, em que muitas vezes se firmava de forma contratualistas, como uma via que permite a cooperação e a estabilidade social. Além disso, a Filosofia também distingue variadas formas de confiança. Encontra-se nesta tese algumas delas, mas duas foram demasiadamente destacadas: a confiança interpessoal (*trust*) e a confiança na ordem natural (fiabilidade). A primeira envolve relações profundas e vulnerabilidade, enquanto a segunda é mais básica e relacionada ao funcionamento do mundo.

A óptica sociológica explora a confiança como uma hipótese sobre o comportamento futuro do outro. Ela está presente em todas as interações sociais e pode ser fortalecida ou enfraquecida com base nas ações das pessoas envolvidas. Por exemplo, a confiança em uma instituição arquivística ou em um Arquivo pode ser avaliada com base em sua capacidade de

manter seguro os documentos, isto é, preservados, autênticos e acesssíveis. Sinteticamente, tanto a Filosofia como a Sociologia oferecem *insights* essenciais para se entender como a confiança é construída, mantida e rompida.

Em relação às Publicações Técnicas do Conarq de preservação digital desta tese, a análise e o exame dos aspectos e dos elementos de confiança demonstrou e realçou que à sua depreensão estão "conceitos, definições e característica", assim, representados por elementos como a autenticidade, a integridade, a identidade, a acessiblidade, a confiabilidade entre outros, os quais são sistemas e subsistemas que se ligam, compõem, reforçam e complementam a confiança, a fim de garantir preservação digital aos documentos de arquivos e à informação. O segundo objetivo específico, o de examinar, nessas Publicações, os elementos de confiança foi contemplado neste paragráfo.

O terceiro objetivo específico foi o de relacionar o conceito de confiança aos elementos de confiança identificados nas Publicações Técnicas do Conarq de preservação digital. A confiança envolve uma presunção que permite enfrentar situações difíceis e desafiadoras, como por exemplo, confiar que normas, políticas e condutas serão cumpridas para o bem-estar de todos.

Tal analogia, no campo dos arquivos, está refletida nos elementos de confiança das referidas Publicações, os quais estão relacionados ao conceito de confiança numa perspectiva filosófica e sociológica, ou seja, do nosso Referencia Teórico. Por exemplo, a confiança está relacionada ao "risco", à segurança, a ambientes, ao tempo, entre outros elementos, que nas Publicações Técnicas estão respectivamente imbricados com: o "fluxo documental no tempo-espaço digital, que é *per si*, tendencioso à vunerabilidade", "a custódia distribuída e compartilhada" "os ambientes informatizados de gestão, de preservação e de acesso documental", "a preocupação com a obsolescência tecnológica".

O quarto e último objetivo específico foi o de certificar se essas Diretrizes, no âmbito da preservação digital, trazem garantia de confiança à informação e ao documento (de arquivo). Corroborou-se que as Publicações Técnicas de preservação digital do Conarq demonstraram ser prerrogativas obrigátorias quando se fala em proteção e cuidado ao documento e à informação a longo prazo.

A sua materialização é composta de recomendações, que envolvem: políticas que estabelecem princípios e procedimentos para garantir a autenticidade e a preservação dos documentos digitais; a orientação de tratamento técnicos e de acesso a esses documentos; a utilização de padrões de metadados, bem como de *backups* em sistemas informatizados arquivísticos; critérios de seleção de formatos, de preferência abertos, de segurança dos dados

e de armazenamento dos objetos digitais; a integração desses sistemas para permitir a preservação de documentos em uma linha ininterrupta ao longo do tempo, além de outras.

Partindo desses resultados, confirma-se a hipótese de que, na Arquivologia, é a preservação digital, por meio de suas Publicações Técnicas do Conarq, que concede o caráter de confiança à informação e ao documento (de arquivo) digital.

Em outras palavras, a preservação digital, conforme orientada pelas Publicações Técnicas do Conarq, que dispõem de diretrizes e de regras de boas práticas, são fundamentais para conferir confiança à informação e aos documentos de arquivos digitais no âmbito da Arquivologia. A resposta para tal resultado foi fechada mediante ao postulado do objetivo geral desta tese, dando-se pela análise do conceito de confiança nas Publicações Técnicas do Conarq de preservação digital.

Compreende-se que uma das contribuições deste estudo dar-se-á no sentido de mostrar que a preservação digital na sua perspectiva sistêmica ou passiva serve de aporte para distinguir o que é uma informação confiável no âmbito da Arquivologia, já que o ambiente digital pode se configurar como instável/infixo/inconstante, efêmero e obsolescente. E, por conseguinte, à medida que políticas, normas e leis arquivísticas vão surgindo na nossa sociedade, faz-se necessário observar as suas nuances, principalmente, aquelas propostas para fins de segurança, de proteção, de preservação e de acesso à informação. Por isso, quanto mais se entende a importância e a dinâmica do que é uma informação confiável, mais seguras, mais protegidas e mais preservadas serão elas.

Em suma, a confiança desempenha um papel fundamental na preservação digital. É a espinha dorsal de qualquer sistema, pois, sem ela, a autenticidade dos objetos digitais não pode ser garantida. Sua presença permite que os usuários tenham certeza de que as informações preservadas não foram alteradas ou corrompidas. Em úlima análise, considera-se também que esta é crucial para garantir a acessibilidade ao longo do tempo. Complementarmente, sem confiança, a preservação digital seria uma tarefa quase impossível. Assim, é essencial que continuemos a desenvolver e implementar mecanismos que aumentem e completem a confiança na preservação digital, que não é meramente uma necessidade técnica, mas também uma questão social e cultural.

É importante, por fim registrar, que este é um campo de estudo em constante evolução e há muito mais a ser explorado. Recomenda-se que futuras pesquisas continuem a investigar e aprofundar o entendimento do papel da confiança na preservação digital. Isso pode incluir o desenvolvimento de novos mecanismos para aumentar a confiança, a investigação de como a

confiança afeta a colaboração na preservação digital e a exploração de como a confiança pode ser mantida ao longo do tempo em um ambiente digital em constante mudança.

REFERÊNCIAS

ABOLHASSAN, F. **The drivers of digital transformation:** why there's no way around the cloud. Berlim: Springer, 2016.

AGÊNCIA GOV. Brasil lidera ranking de inovação na América Latina. **Agenciagov.ebc.com.br,** Brasília, 28 set. 2023. Disponível em: Brasil lidera ranking global de inovação na América Latina — Agência Gov (ebc.com.br). Acesso em: 24 out. 2023.

AKHTAR, S. M. F. **Big data architect's handbook.** Birmingham: Pack Publishing, 2018.

ALBUQUERQUE, R. O. **Uma proposta de um modelo de confiança computacional para grupos em sistemas distribuídos.** 2008. Tese (Doutorado em Engenharia Elétrica) – Faculdade de Tecnologia, Universidade de Brasília, Brasília, 2008. Disponível em: https://repositorio.unb.br/handle/10482/5674. Acesso em: 24 mar. 2022.

AQUINO, T. **Suma teológica.** São Paulo: Edições Loyola, 2001. Disponível em: sumateologica.files.wordpress.com/2017/04/suma-teolc3b3gica.pdf. Acesso em: 2023.

ARAÚJO, A. C. M.; GOUVEIA, L. B. Uma revisão sobre os princípios da teoria geral dos sistemas. **Estação Científica,** Juiz de Fora, n. 16, p. 1-14, jul./dez. 2016. Disponível em: uma-revisão-sobre-os-princípios-da-teoria-geral-dos-sistemas.pdf (estacio.br). Acesso em: 09 out. 2023.

ARAÚJO, A. C. M.; LOPES, J. R. S.; OLIVEIRA, B. V. C. Introdução à teoria geral dos sistemas. **Brazilian Journal of Development,** Curitiba, v. 8, n. 4, p.31540-31546, abr. 2022. Disponível em: Introdução à teoria geral dos sistemas / Introduction to general systems theory | Brazilian Journal of Development (brazilian journals.com.br). Acesso em: 09 out. 2023.

ARAÚJO, V. N. R. H. Sistemas de informação: nova abordagem teórico-conceitual. **Ciência da Informação,** v. 24, n. 1, 1995. Disponível em: Sistemas de informação: nova abordagem teórico-conceitual (brapci.inf.br). Acesso em: 09 out. 2023.

ARELLANO, M. A. M. **Critério para a preservação digital da informação científica.** 2008. Tese (Doutorado em Ciência da Informação) – Faculdade de Economia, Administração, Contabilidade e Ciência da Informação e Documentação, Universidade de Brasília, Brasília, 2008. Disponível em: https://repositorio.unb.br/bitstream/10482/1518/1/2008_MiguelAngelMarderoArellano.pdf. Acesso em: 25 nov. 2021.

ARELLANO, M. A. M. Preservação de documentos digitais. **Ciência da Informação,** Brasília, v. 33, n. 2, p. 15-27, maio/ago. 2004. Disponível em: http://revista.ibict.br/ciinf/article/view/1043. Acesso em: 25 mar. 2022.

ARISTÓTELES. **Ética a Nicômaco.** Tradução de Leonel Vallandro e Gerd Bornheim. 4 ed. São Paulo: Nova Cultural, 1991. Disponível em: ARISTÓTELES - Vol. II (usp.br). Acesso em: 07 dez. 2023.

ARMSTRONG, P. **Dominando as tecnologias disruptivas.** Tradução Afonso Celso da Cunha Serra. 1. ed. São Paulo: Autêntica Business, 2019.

ARQUIVO NACIONAL. Ministério da Justiça e Segurança Pública. **Série AN Digital:** projeto 2. Rio de Janeiro, 2018. Disponível em: https://www.gov.br/arquivonacional/pt-br/canais_atendimento/imprensa/noticias/serie-an-digital-projeto-2. Acesso em: 24 mar. 2022.

AZEVEDO, M. T. **Transformação digital na indústria:** indústria 4.0 e a rede de água inteligente no brasil. 2017. Tese (Doutorado em Ciências) – Escola Politécnica da Universidade de São Paulo, São Paulo, 2017. Disponível em: teses.usp.br/teses/disponiveis/3/3142/tde-28062017-110639/publico/MarceloTeixeiradeAzevedoCorr17.pdf. Acesso em: 07 nov. 2023.

BARBOSA, E. C. **A boa-fé na relação contratual e o princípio da confiança.** 2008. Dissertação (Mestrado em Direito) – Faculdade de Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2008. Disponível em: https://tede2.pucsp.br/handle/handle/8274. Acesso em: 24 mar. 2022.

BARBOSA, R. P. **Motivação das decisões:** um estudo sobre confiança e crença em Luhmann e Clifford. 2017.

BARNEY, J. B.; HANSEN, M. H. Trustworthiness as a source of competitive advantage. **Strategic Management Journal,** v. 15, p. 175-190, 1994. Disponível em: Confiabilidade como Fonte de Vantagem Competitiva no JSTOR. Acesso em: 22 dez. 2023.

BARROSO, L. R. **O direito constitucional e a efetividade de suas normas.** 8 ed. Rio de Janeiro: Renovar, 2006.

BATESON, J.; HOFFMAN, D. **Marketing de serviços.** 4. ed. Porto Alegre: Editora Bookman, 2001.

BELCHIOR, A. M. **Confiança nas instituições políticas.** Lisboa: Fundação Francisco Manuel dos Santos, 2016. Disponível em: Confiança nas Instituições Políticas - Ana Maria Belchior - Google Livros. Acesso em: 05 dez. 2023.

BELLOTTO, H. L.; CAMARGO, A. M. A. **Dicionário de terminologia arquivística.** 3 ed. São Paulo: ARQ-SP, 2012.

BERTALANFFY, L. V. **Teoria geral dos sistemas:** fundamentos, desenvolvimento e aplicações. 5. ed. Petrópolis: Vozes, 2010.

BODÊ, E. C. Documento digital e preservação digital: algumas considerações conceituais. **Revista Ibero-Americana de Ciência da Informação**, Brasília, v. 9, n. 2, p. 503-516, 2016. Disponível em: Disponível em: https://brapci.inf.br/index.php/res/v/75805. Acesso em: 24 mar. 2022.

BORKO, H. Information Science: What is it? **American Documentation,** v.19, n.1, p.3-5, jan. 1968. Disponível em: https://edisciplinas.usp.br/pluginfile.php/1992827/mod_resource/content/1/Borko.pdf. Acesso em: 24 mar. 2022.

BOULDING, K. E. The economics of the coming spaceship Earth. *In:* JARETT, H. (org.). **Environmental Quality in a Growing Economy.** Baltimore: Resources for the future/John

Hopkins University Press, 1966.

BRASIL lidera ranking de índice global de inovação na América Latina. **Poder360.com.br,** Brasília, 1 out. 2023b. Disponível em: Brasil lidera ranking de Índice Global de Inovação na América Latina (poder360.com.br). Acesso em: 24 out. 2023.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, [2023]. Disponível em: Constituição (planalto.gov.br). Acesso em: 2023.

BRASIL. Arquivo Nacional. **Dicionário brasileiro de terminologia arquivística.** Rio de Janeiro: Arquivo Nacional, 2005b. Disponível em: Dicion Term Arquiv.pmd (www.gov.br). Acesso em: 22 jul. 2023.

BRASIL. Conselho Nacional de Arquivos. Câmara Técnica de Documentos Eletrônicos. **Carta para a preservação do patrimônio arquivístico digital.** Rio de Janeiro: Arquivo Nacional, 2005a. Disponível em: www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/conarq_carta_preservacao_patrimonio_arquivistico_digital.pdf. Acesso em: 02 fev. 2024.

BRASIL. Conselho Nacional de Arquivos. Câmara Técnica de Documentos Eletrônicos. **Diretrizes do preservador,** a preservação de documentos arquivísticos digitais: diretrizes para organizações. Rio de Janeiro: Arquivo Nacional, 2013a. Disponível em: conarq_diretrizes_produtor_preservador_resolucao_38.pdf (www.gov.br). Acesso em: 02 fev. 2024.

BRASIL. Conselho Nacional de Arquivos. Câmara Técnica de Documentos Eletrônicos. **Diretrizes do produtor,** a elaboração e a manutenção de materiais digitais: diretrizes para indivíduos. Rio de Janeiro: Arquivo Nacional, 2013b. Disponível em: conarq_diretrizes_produtor_preservador_resolucao_38.pdf (www.gov.br). Acesso em: 02 fev. 2024.

BRASIL. Conselho Nacional de Arquivos. Câmara Técnica de Documentos Eletrônicos. **Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis (RDC-Arq).** Rio de Janeiro: Arquivo Nacional, 2023a. Disponível em: DIRETRIZESRDCArq12DEZ2023.pdf (www.gov.br). Acesso em: 02 fev. 2024.

BRASIL. Conselho Nacional de Arquivos. Câmara Técnica de Documentos Eletrônicos. **Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais.** Rio de Janeiro: Arquivo Nacional, 2012. Disponível em: Projeto_capa_conarq_com_logo.indd (www.gov.br). Acesso em: 02 fev. 2024.

BRASIL. Conselho Nacional de Arquivos. Câmara Técnica de Documentos Eletrônicos. **e-ARQ Brasil**: modelos de requisitos para sistemas informatizados de gestão arquivística de documentos. Versão 2. Rio de Janeiro: Arquivo Nacional, 2022. Disponível em: Resolução nº 50, de 06 de maio de 2022 — Conselho Nacional de Arquivos (www.gov.br). Acesso em: 24 jul. 2023.

BRASIL. Ministério da Economia. Secretaria Especial de Desburocratização, Gestão e Governo Digital). Secretaria de Governo Digital. **Instrução normativa n.º 1, de 19 de abril**

de 2019. Distrito Federal: Ministério da Economia, 2019. Disponível em: Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019 - versão compilada - julho/2022 — Governo Digital (www.gov.br). Acesso em: 24 jul. 2023.

CAMARGO, A. M. A.; BELLOTTO, H. L. (coord.). **Dicionário de terminologia arquivística (versão de bolso).** São Paulo: Centro de Memória e Educação FEUSP/FAPESP, 2010.

CAMPOS, S. L. B. **As provas da existência de Deus em Tomás de Arquivo.** Campos: Editora Fi, 2016. Disponível em: As Provas da Existência de Deus em Tomás de Aquino - Sávio Laet de Barros Campos (filosofante.org). Acesso em: 11 dez. 2023.

CANEDO, E. D. **Modelo de confiança para a troca de arquivos em uma nuvem privada.** 2012. Tese (Doutorado em Engenharia Elétrica) – Faculdade de Tecnologia, Universidade de Brasília, Brasília, 2012. Disponível em: https://repositorio.unb.br/bitstream/10482/22388/1/2016_AlexandrePinheiro.pdf. Acesso em: 24 mar. 2022.

CANHETTI, B. A. P.; FERREIRA, T. C. Princípio da confiança. ETIC - ENCONTRO DE INICIAÇÃO CIENTÍFICA, 2011, São Paulo. **Anais [**...]. São Paulo: Centro Universitário Antônio Eufrásio de Toledo de Presidente Prudente, 2011. Disponível em: http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/4017. Acesso em: 24 mar. 2022.

CAPURRO, R.; HJORLAND, B. O conceito de informação. **Perspectiva em Ciência da Informação,** v. 12, n. 1, p. 148-207, jan./abr. 2007. Disponível em: https://www.scielo.br/j/pci/a/j7936SHkZJkpHGH5ZNYQXnC/?format=pdf. Acesso em: 24 mar. 2022.

CASSARES, N. C. **Como fazer conservação preventiva em arquivos e bibliotecas**. São Paulo: Arquivo do Estado e Imprensa Oficial, 2000. Disponível em: https://www.arqsp.org.br/arquivos/oficinas_colecao_como_fazer/cf5.pdf. Acesso em: 25 nov. 2021.

CASTELLS, M. **A Sociedade em rede.** Tradução Roneide Venancio Majer. 6. ed. São Paulo: Paz e Terra, 1999. Disponível em: https://globalizacaoeintegracaoregionalufabc.files.wordpress.com/2014/10/castells-m-a-sociedade-em-rede.pdf. Acesso em: 24 mar. 2022.

CHIAVENATO, I. **Introdução à teoria geral da administração.** 7. ed. Rio de Janeiro: Elsevier, 2003. Disponível em: profeltonorris.files.wordpress.com/2014/02/livro-teoria-geral-da-administrac3a7c3a3o.pdf. Acesso em: 09 out. 2023.

CHRISTENSEN, C. M. **O dilema da inovação:** quando as tecnologias levam empresas ao fracasso. São Paulo: M. Books, 2011.

CHRISTENSEN; C. M.; HORN; M. B.; STAKER, H. **Ensino híbrido:** Inovação disruptiva? uma introdução à teoria dos híbridos. Tradução Fundação Lemann e Instituto Península. 2013. Disponível: ensino-hibrido_uma-inovacao-disruptiva.pdf (pucpr.br). Acesso em: 14 out. 2023.

CHURCHMAN, C.W. **The systems approach.** New York: Dell Publishing, 1968.

COLOSSI; N.; BAADE, J. H. Interdisciplinaridade e a teoria geral dos sistemas. **Visão,** Caçador, v. 4, n. 1, p. 7-21, jan./jun. 2016. Disponível em: INTERDISCIPLINARIDADE E A TEORIA GERAL DOS SISTEMAS | Revista Visão: Gestão Organizacional (uniarp.edu.br). Acesso em: 09 out. 2023.

CONFÚCIO. **O Lun Yü em Português.** Confucius Publishing Co. Ltd., 1996. Disponível em: The Lun Yu in Portuguese (confucius.org). Acesso em: 05 dez. 2023.

CONSELHO NACIONAL DE ARQUIVOS. Câmara Técnica de Documentos Eletrônicos. **Orientação Técnica n.º3.** Cenários de uso de RDC-Arq em conjunto com o Sigad. Rio de Janeiro: Arquivo Nacional, nov. 2015. Disponível em: (Microsoft Word - Orienta\347\343o_t\351cnica_RDCarq2015_v8) (www.gov.br). Acesso em: 24 jul. 2023.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução Nº 324 de 30/06/2020.** Institui diretrizes e normas de Gestão de Memória e de Gestão Documental e dispõe sobre o Programa Nacional de Gestão Documental e Memória do Poder Judiciário – Proname. Brasília, 2020. Disponível em: atos.cnj.jus.br/atos/detalhar/3376. Acesso em: 11 nov. 2023.

CONSELHO NACIONAL DE JUSTIÇA. Resolução **Nº 408 de 18/08/2021.** Dispõe sobre o recebimento, o armazenamento e o acesso a documentos digitais relativos a autos de processos administrativos e judiciais. Brasília, 2021b. Disponível em: atos.cnj.jus.br/atos/detalhar/4065. Acesso em: 11 nov. 2023.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução Nº 469 de 31/08/2022.** Estabelece diretrizes e normas sobre a digitalização de documentos judiciais e administrativos e de gestão de documentos digitalizados do Poder Judiciário. Brasília, 2022. Disponível em: atos.cnj.jus.br/atos/detalhar/4719. Acesso em: 11 nov. 2023.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução Nº 522 de 18/09/2023.** Institui o Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário e disciplina a obrigatoriedade da sua utilização no desenvolvimento e na manutenção de sistemas informatizados para as atividades judiciárias e administrativas no âmbito do Poder Judiciário. Brasília, 2023. Disponível em: atos.cnj.jus.br/atos/detalhar/5266. Acesso em: 11 nov. 2023.

CONSELHO NACIONAL DE JUSTIÇA. Tecnologia da Informação e Comunicação. Justiça 4.0. **Balcão Virtual.** Brasília, [202-]. Disponível em: Balcão Virtual - Portal CNJ. Acesso em: 08 nov. 2023.

CONSELHO NACIONAL DE JUSTIÇA. Tecnologia da Informação e Comunicação. Justiça 4.0. **Núcleos de Justiça 4.0.** Brasília, 2021a. Disponível em: Núcleos de Justiça 4.0 - Portal CNJ. Acesso em: 08 nov. 2023.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Portaria CNMP-SG nº 105 de 10 de março de 2022.** Institui a Política de Gestão de Documentos e Informação do Conselho Nacional do Ministério Público. Brasília, 2022. Disponível em: Atos e Normas - Conselho Nacional do Ministério Público (cnmp.mp.br). Acesso em: 11 nov. 2023.

COSTA, A. A. Redução de desigualdades, governança judicial e justiça 4.0 no Brasil. *In:* MOREIRA, V. *et al.* (org.).; CONGRESSO INTERNACIONAL DE DIREITOS HUMANOS DE COIMBRA: UMA VISÃO TRANSDISCIPLINAR, 6., 2021. Jundiaí. **Anais** [...]. Campinas: Editora Brasília, 2022, p. 38-46. Disponível em: cidhcoimbra.com/_files/ugd/8f3de9_03d72525ba754f49b8a12de1a1c5e0bb.pdf#page=38. Acesso em: 08 nov. 2023.

COUCH, L.; JONES, W. Measuring Levels of Trust. **Journal of Research in Personality,** v. 31, n. 3, p. 317-336, 1997. Disponível em: Medindo Níveis de Confiança - ScienceDirect. Acesso em: 03 fev. 2024.

CRUZ, R. P. **A transformação digital nos arquivos: o processo de uso de tecnologias digitais nos estados brasileiros.** 2023. Tese (Doutorado em Ciência da Informação) – Universidade Federal Fluminense, Niterói, 2023. Disponível em: A transformação digital nos arquivos: o processo de uso de tecnologias digitais nos estados brasileiros (uff.br). Acesso em: 07 nov. 2023.

CUNHA, L. A. G. Confiança, capital social e desenvolvimento territorial. **RA'EGA,** Curitiba, v. 4, p. 49-60, 2000. Disponível em: Open Journal Systems (ufpr.br). Acesso em: 03 fev. 2024.

DAHLBERG, I. Brief Communication: concepts and terms – ISKO´s major challenge. **Knowl. Org.** v. 36, n. 2, p. 169-177. 2009. Disponível em: Comunicação Breve: Conceitos e Termos - O Grande Desafio da ISKO (researchgate.net). Acesso em: 02 fev. 2024.
DAHLBERG, I. Teoria do conceito. **Ciência da Informação,** Rio de Janeiro, v. 7, n. 2. p. 101-107, 1978. Disponível em: Teoria do conceito | Ciência da Informação (ibict.br). Acesso em: 02 fev. 2024.

DASGUPTA, P. Trust as a commodity. *In*: GAMBETTA, D. (org.) **Trust:** making and breaking cooperative relations, electronic editions. Brasil Blackwell: University of Oxford, 2008, p. 49-72. Disponível em: https://www.nuffield.ox.ac.uk/users/gambetta/Trust_making%20and%20breaking%20cooperative%20relations.pdf. Acesso em: 24 mar. 2022.

DELMAS, B. **Arquivos para quê?** Tradução de Danielle Ardaillon. São Paulo: Instituto Fernando Henrique Cardoso, 2010.

DESCARTES, R. **Discurso do método.** Tradução Maria Emantina Galvão. 3 ed. São Paulo: Martins Fontes, 2001. Disponível em: edisciplinas.usp.br/pluginfile.php/363690/mod_resource/content/1/DESCARTES_Discurso_do_método_Completo.pdf. Acesso em: 13 dez. 2023.

DESLANDES, S. F. O projeto de pesquisa como exercício científico e artesanato intelectual. *In*: DESLANDES, S. F.; NETO CRUZ, O.; GOMES, R.; MINAYO, M. C. S. (org.). **Pesquisa social:** teoria, método e criatividade. 21. ed. São Paulo: Vozes, 2002, p. 31-50. Disponível em: https://wp.ufpel.edu.br/franciscovargas/files/2012/11/pesquisa-social.pdf. Acesso em: 24 mar. 2022.

DINIZ, B. A.; MARCONATTO, D. A. Confiança: um construto universal. **Revista de Administração FACES Journal**, Belo Horizonte, v. 10, n. 1, p. 35-55, jan./mar. 2011.

Disponível em: CONFIANÇA: UM CONSTRUTO UNIVERSAL | Revista de Administração FACES Journal (fumec.br). Acesso em: 24 mar. 2022.

DIOGO, R. A.; KOLBE JUNIOR, A.; SANTOS, N. A transformação digital e a gestão do conhecimento: contribuições para a melhoria dos processos produtivos e organizacionais. **P2P & INOVAÇÃO,** Rio de Janeiro, v. 5 n. 2, p.154-175, mar./ago. 2019. Disponível em: A TRANSFORMAÇÃO DIGITAL E A GESTÃO DO CONHECIMENTO: CONTRIBUIÇÕES PARA A MELHORIA DOS PROCESSOS PRODUTIVOS E ORGANIZACIONAIS | P2P E INOVAÇÃO (ibict.br). Acesso em: 07 nov. 2023.

DURANTI, L. **An infrastructure for truthEntrusting digital facts to archival theory.** *In:* ALA-ICA CONFERENCE, México, 27 nov. 2017. Apresentação em Power Point. Disponível em: Trust & Authenticity (alaarchivos.org). Acesso em: 24 jul. 2023.

DURANTI, L. *et al.* **Strategy Task Force Report.** InterPARES 1 Project: Canadá, 2001. Disponível em: Strategy Task Force Report. Acesso em: 24 mar. 2022.

ENGELMANN, W.; KLEIN, A. H. Ressignificando a confiança no contexto do blockchain e dos smart contracts. **Revista Duc In Altum -** Cadernos de Direito, v. 12, n. 26, p. 87-119, jan./abr. 2020. Disponível em: RESSIGNIFICANDO A CONFIANÇA NO CONTEXTO DO BLOCKCHAIN E DOS SMART CONTRACTS
RESIGNIFYING TRUST IN THE CONTEXT OF BLOCKCHAIN AND SMART CONTRACTS | Duc In Altum - Cadernos de Direito (faculdadedamas.edu.br). Acesso em: 04 fev. 2024.

ENGINEBR. Já ouviu falar sobre sociedade 5.0? descubra o que é. São Paulo: ENGINE – Soluções para gestão na nuvem, 2018. Disponível em: Já ouviu falar sobre Sociedade 5.0? Descubra o que é - Engine Br. Acesso em: 08 nov. 2023.

ESTRATÉGIA BRASILEIRA PARA A TRANSFORMAÇÃO DIGITAL (E-DIGITAL). Brasília, 2018. Disponível em: eDigital.pdf — Governo Digital (www.gov.br). Acesso em: 08 nov. 2023.

ESTRATÉGIA BRASILEIRA PARA A TRANSFORMAÇÃO DIGITAL (E-DIGITAL). Ciclo 2022-2023. Brasília, 2022. Disponível: e-digital_ciclo_2022-2026.pdf (www.gov.br). Acesso em: 08 nov. 2023.

ESTRATÉGIA DE GOVERNO DIGITAL DA PARAÍBA 2021/2026. Paraíba, 2021. Disponível em: VGA-0009-21-Estratégia-de-Gov. Digital da Paraíba_A4-27-09-21.indd (paraiba.pb.gov.br). Acesso em: 14 nov. 2023.

FAULKNER, P. **Knowledge on Trust.** Oxford University Press: Oxford, 2011.

FERES JÚNIOR; J. EISENBERG, J. Dormindo com o inimigo: uma crítica ao conceito de confiança. **DADOS** – Revista de Ciências Sociais, Rio de Janeiro, v. 49, n. 3, 2006, p. 457-481. Disponível em: SciELO - Brasil - Dormindo com o inimigo: uma crítica ao conceito de confiança Dormindo com o inimigo: uma crítica ao conceito de confiança. Acesso em: 16 dez. 2023.

FERREIRA, A. A. M. B. C. Proteção do consumidor no comércio eletrônico sob a ótica da teoria da confiança. **Revista da EMERJ,** Rio de Janeiro, v. 11, n. 42, p. 160-175. 2008.

Disponível em: Proteção do Consumidor no Comércio Eletrônico sob a Ótica da Teoria da Confiança. Acesso em: 25 mar. 2022.

FERREIRA, M. **Introdução à preservação digital:** conceitos, estratégias e actuais consensos. Guimarães, Portugal: Escola de Engenharia da Universidade do Minho, 2006. Disponível em: https://repositorium.sdum.uminho.pt/bitstream/1822/5820/1/livro.pdf. Acesso em: 24 mar. 2022.

FILGUEIRAS, F. República, confiança e sociedade. **DADOS –** Revista de Ciência Sociais, Rio de Janeiro, b. 50, n. 4, p. 863-897, 2007. Disponível em: SciELO - Brasil - República, Confiança e Sociedade República, Confiança e Sociedade. Acesso em: 03 fev. 2024.

FLORES, D. A transformação digital compulsória que vem acometendo os arquivos, os documentos e arquivistas. Quais subsídios temos para uma toda de decisão: disruptiva ou inovação sustentada? **ARKHÉ:** boletín digital de la asociación latinoamericana de archivos, Lima, n. 65, 2022. Disponível em: (63) A TRANSFORMAÇÃO DIGITAL COMPULSÓRIA QUE VEM ACOMETENDO OS ARQUIVOS, OS DOCUMENTOS E ARQUIVISTAS. QUAIS SUBSÍDIOS TEMOS PARA UMA TOMADA DE DECISÃO: DISRUPTIVA OU INOVAÇÃO SUSTENTADA? (Por Daniel Flores, Representante de Brasil en el GE RIBEAU ALA) | Daniel Flores - Academia.edu. Acesso em: 17 out. 2023.

FLORES, D.; PRADEBON, D. S.; CÉ, G. Análise do conhecimento teórico- metodológico da preservação digital sob a ótica da OAIS, SAAI, ISO 14721 e NBR 15472. **Brazilian Journal of Information Science: Research Trends**, v. 11, n. 4, p. 72–80, 2017. Disponível em: Análise do conhecimento teórico-metodológico da preservação digital sob a ótica da OAIS, SAAI, ISO 14721 e NBR 15472 | Brazilian Journal of Information Science: research trends. Acesso em: 24 mar. 2022.

FLORES, D.; ROCCO, B. C. B.; SANTOS, H. M. D. Cadeia de custódia para documentos arquivísticos digitais. **Acervo** - Revista do Arquivo Nacional, v. 29, n. 2, p. 117-132, 2016. Disponível em: https://brapci.inf.br/index.php/res/v/40511. Acesso em: 22 jul. 2023.

FONTANA, F. F. *et al*. Archivematica como ferramenta para acesso e preservação digital à longo prazo. **Ágora**, Florianópolis, v. 24, n. 48, p. 62-82, 2014. Disponível: Archivematica como ferramenta para acesso e preservação digital à longo prazo | ÁGORA: Arquivologia em debate (emnuvens.com.br). Acesso em: 24 mar. 2022.

FORMENTON, D.; GRACIOSO, L. S.; CASTRO, FABIANO, F. F. Revisitando a preservação digital na perspectiva da ciência da informação: aproximações conceituais. **Revista Digital de Biblioteconomia e Ciência da Informação,** Campinas, v. 13, n. 1, p. 170-191, jan./abr. 2015. Disponível em: Revisitando a preservação digital na perspectiva da ciência da informação: aproximações conceituais. Acesso em: 24 mar. 2022.

FREIRE, G. H. A.; FREIRE, I. M. **Introdução à ciência da informação.** João Pessoa: Editora Universitária da UFPB, 2009.

FRICKER, M. Rational Authority and Social Power: Towards a Truly Social Epistemology. Proceedings of the Aristotelian Society, v. 19, n. 2, p. 159-77, 1998. Disponível em: Miranda Fricker, Autoridade racional e poder social: rumo a uma epistemologia verdadeiramente social - PhilPapers. Acesso em: 03 fev. 2024.

FUKUYAMA, F. **Trust:** the social virtue and creation of prosperity. Nova York: Free Press, 1995.

GAMBETTA, D. Can we trust Trust? *In*: GAMBETTA, D. (org.) **Trust:** making and breaking cooperative relations, electronic editions. Brasil Blackwell: University of Oxford, 2008a, p. 213-237. Disponível em: Trust : making and breaking cooperative relations. Acesso em: 24 mar. 2022.

GAMBETTA, D. Mafia: the price of distrust. *In*: GAMBETTA, D. (org.) **Trust:** making and breaking cooperative relations, electronic editions. Brasil Blackwell: University of Oxford, 2008b, p. 158-175. Disponível em: Trust : making and breaking cooperative relations. Acesso em: 24 mar. 2022.

GAVA, T. B. S.; FLORES, D. Auditoria e certificação ao longo da cadeia de custódia digital arquivística. **Informação & Informação,** v. 26, n. 4, p. 424-449, 2021a. Disponível em: Auditoria e certificação ao longo da cadeia de custódia digital arquivística (brapci.inf.br). Acesso em: 24 jul. 2023.

GAVA, T. B. S.; FLORES, D. O papel do Archivematica no RDC-Arq e possíveis cenários de uso. **Ágora:** Arquivologia em debate, Florianópolis, v. 31, n. 63, p. 1-21, jul./dez. 2021b. Disponível em: Vista do O papel do Archivematica no RDC-Arq e possíveis cenários de uso (emnuvens.com.br). Acesso em: 24 jul. 2023.

GAVA, T. B. S.; FLORES, D. Políticas de preservação digital: o caso do brasil em relação à colômbia e austrália. **Em Questão,** Porto Alegre, v. 28, n. 3, p. 1-26, jul./set. 2022b. Disponível em: https://brapci.inf.br/index.php/res/v/197141. Acesso em: 24 jul. 2023.

GAVA, T. B. S.; FLORES, D. Problematizando a pós-custódia com a contemporaneidade da cadeia de custódia digital arquivística compartilhada e distribuída na preservação digital sistêmica. **InCID:** Revista de Ciência da Informação e Documentação, v. 13, n. 2, p. 222-243, 2022a. Disponível em: Problematizando a Pós-Custódia com a contemporaneidade da Cadeia de Custódia Digital Arquivística compartilhada e distribuída na Preservação Digital Sistêmica (brapci.inf.br). Acesso em: 24 jul. 2023.

GAVA, T. B. S.; FLORES, D. Repositórios arquivísticos digitais confiáveis (RDC-Arq) como plataforma de preservação digital em um ambiente de gestão arquivística. **Informação & Informação,** v. 25, n. 2, p. 74-99, abr./jun. 2020a. Disponível em: Repositórios arquivísticos digitais confiáveis (RDC-Arq) como plataforma de preservação digital em um ambiente de gestão arquivística | Informação & Informação (uel.br). Acesso em: 22 jul. 2023.

GAVA; T. B. S.; FLORES, S. Cadeia de custódia digital arquivística – CCDA. *In:* SIMPÓSIO INTERNACIONAL DE ARQUIVOS. 2020b, São Paulo. **Anais** [...]. São Paulo: Associação dos Arquivistas de São Paulo, 2020. p. 1-11. Disponível em: Simpósio Internacional de Arquivos – ARQUIVÍSTICA (unb.br). Acesso em: 22 jul. 2023.

GAVA; T. B. S.; FLORES, S. Preservação digital sistêmica. *In:* SIMPÓSIO INTERNACIONAL DE ARQUIVOS. 2020c, São Paulo. **Anais** [...]. São Paulo: Associação dos Arquivistas de São Paulo, 2021. p. 1-11. Disponível em: (PDF) PRESERVAÇÃO DIGITAL SISTÊMICA (researchgate.net). Acesso em: 24 jul. 2023.

GIDDENS, A. **As consequências da modernidade.** Tradução Raul Fiker. São Paulo: UNESP, 1991. Disponível em: ANTHONY GIDDENS - As Consequencias da Modernidade. Acesso em: 25 mar. 2022.

GIL, A. C. **Métodos e técnicas de pesquisa social.** 6. ed. São Paulo: Atlas, 2008. Disponível em: Métodos e Técnicas de Pesquisa Social. Acesso em: 24 mar. 2022.

GINZBURG, C. **Mitos, emblemas, sinais:** morfologia e história. Tradução de Federico Carotti. 2. ed. São Paulo: Companhia das Letras, 1989. Disponível em: mitos, emblemas, sinais - morfologia e história. Acesso em: 24 mar. 2022.

GOMES, R. Análise de dados de pesquisa qualitativa. *In*: DESLANDES, S. F.; NETO CRUZ, O.; GOMES, R.; MINAYO, M. C. S. (org.). **Pesquisa social:** teoria, Método e Criatividade. 21. ed. São Paulo: Petrópolis: Vozes, 2002. p. 67-80. Disponível em: https://wp.ufpel.edu.br/franciscovargas/files/2012/11/pesquisa-social.pdf. Acesso em: 24 mar. 2022.

GOMES, W. S. **Características, funções e preservação digital do *archivematica* à luz da resolução nº 43 do conselho nacional de arquivos**. 2019. Dissertação (Mestrado em Ciência da Informação) – Universidade Federal da Paraíba, João Pessoa, 2019. Disponível em: https://repositorio.ufpb.br/jspui/handle/123456789/16319. Acesso em: 24 mar. 2022.

GONÇALVES, N. C. S.; RODRIGUES, F. A. Arquivologia e blockchain: discussão teórica sobre oportunidades e barreiras. **Ciência da Informação em Revista,** Maceió, v. 7, n. 3, p. 21-28, 2020. Disponível em: Arquivologia e blockchain: discussão teórica sobre oportunidades e barreiras (brapci.inf.br). Acesso em: 11 out. 2023.

HARDIN, R. **Trust and trustworthiness.** New York: Russell Sage Foundation, 2002.

HAZEN, D. *et al.* **Planejamento de preservação e gerenciamento de programas.** 2. ed. Tradução José Luiz Pedersoli Junior. Rio de Janeiro: Arquivo Nacional, 2001. Disponível em: https://www.arqsp.org.br/wp-content/uploads/2017/08/33_36.pdf. Acesso em: 25 nov. 2021.

HIRTLE. P. B. The history and current state of digital preservation in the United States. **Metadata and digital collections:** a festschrift in honor of Thomas P. Turner, Nova York, p. 121-140, 2008. Disponível em: https://ecommons.cornell.edu/bitstream/handle/1813/45862/7the_history_and_current_state_p_hirtle.pdf?sequence=3&isAllowed=y. Acesso em: 25 nov. 2021.

HWANG P.; BURGERS, W. Properties of Trust: an analytical view. **Organizational behavior and human decision processes,** v. 69, n. 1, p. 67-73, jan. 1997. Disponível em: Propriedades de confiança: uma visão analítica - ScienceDirect. Acesso em: 26 dez. 2023.
INGLEHART, R. Trust, well-being and democracy. *In:* WARREN. M. E (org.). **Democracy and trust.** Cambridge: Cambridge University, 1999, p. 88-120.

INNARELLI, H. C. **Gestão da preservação de documentos arquivísticos digitais:** proposta de um modelo conceitual. 2015. Tese (Doutorado em Ciência da Informação) – Escola de Comunicações e Artes, Universidade de São Paulo, São Paulo, 2015. Disponível em:

https://www.teses.usp.br/teses/disponiveis/27/27151/tde-27052015-101628/pt-br.php. Acesso em: 25 mar. 2022.

INTERPARES 1 PROJECT. International Research on Permanent Authentic Records in Eletronic Systems. **Objetivos e Metodologias.** Canadá, 1999. Disponível em: http://www.interpares.org/ip1/ip1_goals&methodologies.cfm. Acesso em: 24 mar. 2022.

INTERPARES 2 PROJECT. International Research on Permanent Authentic Records in Eletronic Systems. **Princípios Metodológicos.** Canadá, 2002. Disponível em: http://www.interpares.org/ip2/ip2_methodological_principles.cfm. Acesso em: 25 mar. 2022.

INTERPARES 3 PROJECT. International Research on Permanent Authentic Records in Eletronic Systems. **Visão Geral do Projeto.** Canadá, 2007. Disponível em: http://www.interpares.org/ip3/ip3_overview.cfm. Acesso em: 25 mar. 2022.

JENKINSON, H. **A Manual of archive administration including the problems of war archives and archive making.** Oxford: Oxford University, 1922. Disponível em: A manual of archive administration including the problems of war archives and archive making : Jenkinson, Hilary, Sir : Free Download, Borrow, and Streaming : Internet Archive. Acesso em: 22 jul. 2023.

JOBIM. C. L. G.; GALVÃO, L. V. Programa "justiça 4.0" e a razoável duração do processo. *In*: CANEN, D. (org.). **Inteligência artificial e aplicabilidade prática no direito.** Brasília: Conselho Nacional de Justiça, 2022. p. 31-46. Disponível em: 212c00_d35929a913c741a191814de41a7c2143.pdf (cyberleviathan.com.br). Acesso em: 08 nov. 2023.

JOHNSON, A. G. **Dicionário de Sociologia:** guia prático da linguagem sociológica. Tradução de Ruy Jungmann. Rio de Janeiro: Zahar, 1997.

JUÍZO 100% DIGITAL: TUDO O QUE VOCÊ PRECISA SABER. Conselho Nacional de Justiça. Brasília, 2020. Disponível em: arte cartilha Juízo 100 digital v3.indd (cnj.jus.br). Acesso em: 08 nov. 2023.

JUSTIÇA 4.0. Conselho Nacional de Justiça, Brasília, 2021. Disponível em: Cartilha_Justiça 4.0_20082021_VS_ML_DN_FP (cnj.jus.br). Acesso em: 08 nov. 2023.

KAGERMANN, H.; WAHLSTER, W.; HELBIG. **Recommendations for implementing the strategic initiative Industrie 4.0.** German: National Academy of Science and Engineering 2013. Disponível em: recommendations-for-implementing-industry-4-0-data.pdf (din.de). Acesso em: 07 nov. 2023.

KANT, I. **A crítica da razão pura.** Tradução de Manuela Pinto dos Santos e Alexandre Fradique Morujão. 5. ed. Lisboa: Fundação Calouste Gulbenkian, 2001. Disponível em: 3970 - CRÍTICA DA RAZÃO PURA (wordpress.com). Acesso em: 13 dez. 2023.

KETZER. P. **O conceito de confiança em epistemologia do testemunho:** distinguindo confiar de fiar-se. 2015. Tese (Doutorado em Filosofia) – Faculdade de Filosofia da Pontifícia, Universidade Católica do Rio Grande do Sul, Porto Alegre, 2015. Disponível em: http://tede2.pucrs.br/tede2/handle/tede/6382. Acesso em: 24 mar. 2022.

KINCHELOE, J, L.; BERRY, K. S. **Pesquisa em educação:** conceituando bricolagem. Porto Alegre: Artmed, 2007.

KUHN, T. S. **A estrutura das revoluções científicas.** Tradução de Beatriz Vianna Boeira e Nelson Boeira. 13. ed. São Paulo: Perspectiva, 2017.

KUNY, T. A digital dark ages? challenges in the preservation of eletronic information. 1997. **Trabalho apresentado a 63 Conferência Geral da IFLA,** Copenhage, 1997. Disponível em: https://archive.ifla.org/IV/ifla63/63kuny1.pdf. Acesso em: 25 nov. 2021.

LANEY, D. **3D data management:** data volume, velocity and variety. Stanford: Application Delivery Strategies by META Group Inc., 2001. Disponível em: 3D Data Management: Controlling Data Volume, Velocity, and Variety (studylib.net). Acesso em: 10 out. 2023.

LIEBER, R. R. **Teoria de Sistemas.** Guaratinguetá: UNESP, 2001. Disponível em: (PDF) TEORIA DE SISTEMAS (researchgate.net). Acesso em: 10 out. 2023.

LOCKE, J. **Ensaio sobre o entendimento humano.** Tradução de Pedro Paulo Garrido Pimenta. São Paulo: Martins Fontes, 2012. Disponível em: locke-ensaio-acerca-do-entendimento-humano.pdf (wordpress.com). Acesso em: 13 dez. 2023.

LOCKE, J. **Segundo tratado sobre o governo:** ensaio sobre a origem, os limites e os fins verdadeiros do governo civil. Tradução de Magda Lopes e Marisa Lobo da Costa. Petrópolis: Vozes, 1994. Disponível em: Locke00.vp (wordpress.com). Acesso em: 16 dez. 2023.

LONGUINI, R. C. F.; DENARDI, E. O uso da inteligência artificial como instrumento de promoção da sustentabilidade no poder judiciário brasileiro: os impactos da justiça 4.0. **RJLB,** Lisboa, ano 7, n. 5, p. 2037-2061, 2021. Disponível em: Microsoft Word - 2021_05_2037_2061 (cidp.pt). Acesso em: 08 nov. 2023.

LOPEZ, A. P. A. Princípios Arquivísticos e documento digitais. **Arquivo Rio Claro,** n. 2, p. 70-85. 2004. Disponível em: https://repositorio.unb.br/handle/10482/1428. Acesso em: 24 mar. 2022.

LUCENA, M. Z. **"Quem acreditou no amor, no sorriso, na flor":** a confiança nas relações amorosas. 2009. Tese (Doutorado em Sociologia) – Centro de Filosofia e Ciência Humanas, Universidade Federal de Pernambuco, Recife, 2009. Disponível em: https://repositorio.ufpe.br/handle/123456789/9380#:~:text=Citation%3A,a%20confian%C3%A7a%20nas%20rela%C3%A7%C3%B5es%20amorosas.. Acesso em: 24 mar. 2022.

LUHMANN, N. **Confianza.** Tradução Amanda Flores. Barcelona: Anthropos, 1996.

LUHMANN, N. Familiarity, confidence, trust: problems and alternatives. *In*: GAMBETTA, D. (org.) **Trust:** making and breaking cooperative relations, electronic editions. Brasil Blackwell: University of Oxford, 2008, p. 94-108. Disponível em: https://www.nuffield.ox.ac.uk/users/gambetta/Trust_making%20and%20breaking%20cooperative%20relations.pdf. Acesso em: 24 mar. 2023.

LUNDÅSEN, S. Podemos confiar nas medidas de confiança? **OPINIÃO PÚBLICA,** Campinas, v. 8, n. 2, p. 304-327, 2002. Disponível em: SciELO - Brasil - Podemos confiar nas medidas de confiança? Podemos confiar nas medidas de confiança?. Acesso em: 23 dez. 2023.

LUZ, C.; FLORES, F. Cadeia de custódia e de preservação: autenticidade nas plataformas de gestão e preservação de documentos arquivísticos. **ResearchGate,** 2017. Disponível em: (PDF) Cadeia de custódia e de preservação: autenticidade nas plataformas de gestão e preservação de documentos arquivísticos (researchgate.net). Acesso em: 22 jul. 2023.

LYDON, B. Industry 4.0: Intelligent and flexible production. **ISA,** Boston, maio/jun. 2016 Disponível em: Indústria 4.0: Produção inteligente e flexível - ISA. Acesso em: 07 nov. 2023.

MACHIAVELLI, Nicolò. **O príncipe.** Tradução de Mário e Celestino da Silva. Brasília: Senado Federal, 2019. Disponível em: 001143485_O_principe.pdf (senado.leg.br). Acesso em: 06 dez. 2023.

MACNEIL, H. *et al.* **Authenticity Task Force Report.** InterPARES 1 Project: Canadá, 2001. Disponível em: http://www.interpares.org/display_file.cfm?doc=ip1_atf_report.pdf. Acesso em: 24 mar. 2022.

MACULAN, B. C. M. S.; LIMA, G. A. B. O. Buscando uma definição para o conceito de "conceito". Perspectivas em Ciência da Informação, v. 22, n. 2, p. 54-87, abr./jun. 2017. Disponível em: Gestão do conhecimento ou gestão de organizações da era do conhecimento (scielo.br). Acesso em: 02 fev. 2024.

MAHRAZ, M.-I.; BENABBOU, L.; BERRADO, A. A systematic literature review of digital transformation. In: INTERNATIONAL CONFERENCE ON INDUSTRIAL ENGINEERING AND OPERATIONS MANAGEMENT, 1., 2019, Toronto. Proceedings [...]. Southfield: IEOM Society International, 2019. p. 917-931. Disponível em: (PDF) A Systematic literature review of Digital Transformation (researchgate.net). Acesso em: 07 nov. 2023.

MAIOLI, M. L. **Jurisprudência e confiança.** 2012. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade Federal do rio Grande do Sul, Porto Alegre, 2012. Disponível em: https://lume.ufrgs.br/bitstream/handle/10183/194330/000861094.pdf?sequence=1&isAllowed=y. Acesso em: 25 mar. 2022.

MANYIKA, J. *et al.* **Big data:** The next frontier for innovation, competition, and productivity. Mckinsey e Company: EUA, 2011. Disponível em: Manyika, James; Chui, Michael; Brown, Brad; Bughin, Jacques; Dobbs, Richard; Roxburgh, Charles Byers, Angela Hung (2011). Big data: The next frontier for innovation, competition, and productivity (2011). https://bigdatawg.nist.gov/pdf/MGI_big_data_full_report.pdf (2018-07-28). - Pesquisa Google. Acesso em: 10 out. 2023.

MARQUES, C. L. **Contratos no Código de Defesa do Consumidor. 4**. ed. São Paulo: ed. Revista dos Tribunais, 2002.

MARTINS, R. M. O princípio da confiança legítima e o enunciando n. 362 da IV jornada de direito Civil. **Revista CEJ,** Brasília, v. 12, n. 40, p. 11-19, jan./mar. 2008. Disponível em: https://revistacej.cjf.jus.br/cej/index.php/revcej/article/view/956. Acesso em: 25 mar. 2022.

MARTINS-COSTA, J. Princípio da confiança legítima e princípio da boa-fé objetiva - Termo de compromisso de cessação (TCC) ajustado com o CADE - Critérios da interpretação contratual: os 'sistemas de referência extracontratuais' ('circunstâncias do caso') e sua função no quadro semântico da conduta devida - Princípio da unidade ou coerência hermenêutica e 'usos do tráfego' - Adimplemento contratual. **Revista dos Tribunais,** São Paulo, v. 95, n. 852, p. 87-126, out. 2006. Disponível em: https://dspace.almg.gov.br/handle/11037/29218. Acesso em: 24 mar. 2022.

MCMYLER, B. **Testimony, Trust and Authority.** Oxford University Press: Oxford, 2011.

MINISTÉRIO DA EDUCAÇÃO. **Portaria nº 613, de 18 de agosto de 2023.** Regulamenta o art. 4º da Portaria MEC nº 360, de 18 de maio de 2022. Brasília, 2022. Disponível em: PORTARIA Nº 613, DE 18 DE AGOSTO DE 2022 - PORTARIA Nº 613, DE 18 DE AGOSTO DE 2022 - DOU - Imprensa Nacional (in.gov.br). Acesso em: 11 nov. 2023.

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. Governo Digital. **Estratégia de Governo Digital 2020-2022.** Brasília, 2023c. Disponível em: Estratégia de Governo Digital 2020-2022 — Governo Digital (www.gov.br). Acesso em: 24 out. 2023.

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. Governo Digital. Estratégia de Governança Digital. **Do Eletrônico ao Digital.** Brasília, 2023a. Disponível em: Linha do tempo — Governo Digital (www.gov.br). Acesso em: 24 out. 2023.

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. Governo Digital. Estratégia de Governo Digital 2020-2022. **Um governo eficiente.** Brasília, 2023b. Disponível em: Um Governo Eficiente — Governo Digital (www.gov.br). Acesso em: 24 out. 2023.

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. Governo Digital. **Gestão debate objetivos da nova Estratégia de Governo Digital.** Brasília, 2023d. Disponível em: Gestão debate objetivos da nova Estratégia de Governo Digital — Governo Digital (www.gov.br). Acesso em: 30 out. 2023.

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. Governo Digital. Transformação Digital. **Trajetória da transformação digital.** Brasília, 2023e. Disponível em: Trajetória da transformação digital — Governo Digital (www.gov.br). Acesso em: 08 nov. 2023.

MORI, A. *et al.* Análise comparativa entre os requisitos da RDC-Arq e a tecnologia Blockchain: uma perspectiva de profissionais arquivistas. **Ibersid:** revista de sistemas de información y documentación, v. 14, n. 1, p. 29-40, 2020. Disponível em: Análise comparativa entre os requisitos da RDC-Arq e a tecnologia Blockchain: uma perspectiva de profissionais arquivistas - Dialnet (unirioja.es). Acesso em: 11 out. 2023.

MOTA, R. Confiança e complexidade social em Niklas Luhmann. **PLURAL,** Revista do Programa de Pós-Graduação em Sociologia da USP, São Paulo, v. 23, n. 2, p. 182-197, 2016. Disponível em: Confiança e complexidade social em Niklas Luhmann | Plural (usp.br). Acesso em: 03 fev. 2024.

NAKAMOTO, S. **Bitcoin:** a peer-to-peer electronic cash system. 2009. Disponível em: bitcoin.pdf. Acesso em: 11 out. 2023.

NUNES, M. P.; MALAGRI, C. A. N. O estado da arte sobre transformação digital e blended education. **Educ. Soc.,** Campinas, v. 44, p. 1-19, 2023. Disponível em: SciELO - Brasil - O ESTADO DA ARTE SOBRE TRANSFORMAÇÃO DIGITAL E BLENDED EDUCATION O ESTADO DA ARTE SOBRE TRANSFORMAÇÃO DIGITAL E BLENDED EDUCATION. Acesso em: 08 nov. 2023.

OLIVEIRA, I. Brasil é vice-líder mundial em tempo de uso de internet; veja o ranking. **Gizmodo.uol.com.br**, São Paulo, 22 set. 2023. Disponível em: Brasil é vice-líder mundial em tempo de uso de internet; veja o ranking - Giz Brasil (uol.com.br). Acesso em: 15 out. 2023.

PACÍFICO, J. V. Tecnologia permite ao tribunal de justiça ampliar atendimento e estabelecer novos fluxos processuais. **Tjpb.jus.br**, João Pessoa, 25 maio 2023. Disponível em: Tecnologia permite ao Tribunal de Justiça ampliar atendimento e estabelecer novos fluxos processuais | Tribunal de Justiça da Paraíba (tjpb.jus.br). Acesso em: 08 nov. 2023.

PAGDEN, A. The Destruction of trust and its economic consequences in the case of eighteenth-century naples. *In*: GAMBETTA, D. (org.) **Trust:** making and breaking cooperative relations, electronic editions. Brasil Blackwell: University of Oxford, 2008, p. 127-141. Disponível em: Microsoft Word - Document2 (ox.ac.uk). Acesso em: 26 dez. 2023.

PAIXÃO, S. A. *et al.* Proposta de um modelo para transformação digital. In: SIMPÓSIO DE ENGENHARIA, GESTÃO E INOVAÇÃO, 3., 2020, São Paulo. **Anais** [...]. São Paulo: USP, 2020. Disponível em: Proposta De Um Modelo Para Transformação Digital | Even3 Publicações. Acesso em: 07 nov. 2023.

PEREIRA, F. S. Teoria da aparência e confiança na pós-modernidade: a tutela dos consumidores. **Revista da Faculdade de Uberlândia,** Uberlândia, v. 38, n. 2, p. 489-504, dez. 2010. Disponível em: https://seer.ufu.br/index.php/revistafadir/article/view/18409. Acesso em: 25 mar. 2022.

PEYREFITTE, A. **A Sociedade de confiança:** ensaio sobre as origens e a natureza do desenvolvimento. Rio de Janeiro: Topbooks, 1999.

PINHO, L. O.; MONTEIRO, L. P. Plataforma digital do poder judiciário e acesso à justiça 5.0: o futuro do processo eletrônico judicial. **Revista CNJ**, Brasília, v. 6, n. 1, p. 95-110, jan. /jun. 2022. Disponível em: Plataforma Digital do Poder Judiciário e Acesso à Justiça 5.0: o futuro do processo eletrônico judicial | Revista CNJ. Acesso em: 08 nov. 2023.

PRODANOV, C. C.; FREITAS, E. C. **Metodologia do trabalho científico:** métodos e técnicas da pesquisa do trabalho acadêmico. 2 ed. Novo Hamburgo: Feevale, 2013. Disponível em: https://aedmoodle.ufpa.br/pluginfile.php/291348/mod_resource/content/3/2.1-E-book-Metodologia-do-Trabalho-Cientifico-2.pdf. Acesso em: 24 mar. 2022.

PUTNAM, R. D. **Comunidade e democracia:** a experiência da Itália moderna. Tradução de Luiz Alberto Monjardim. 5 ed. Rio de Janeiro: Fundação Getúlio Vargas, 2006. Disponível em: PUTNAM-Robert-1993-Comunidade-e-Democracia-A-Experiência-da-Itália-Moderna.pdf (humana.social). Acesso em: 23 dez. 2023.

RÁO, V. **Ato jurídico:** noção, pressupostos, elementos essenciais e acidentais, o problema do conflito entre os elementos volitivos e a declaração. 3. ed. São Paulo: Revista dos Tribunais, 1994.

RAUTENBERG, S.; CARMO, P. R. V. Big data e ciência de dados. **Brazilian Journal of Information Science,** v. 13, n. 1, p. 56-67, 2019. Disponível em: Big data e ciência de dados (brapci.inf.br). Acesso em: 10 out. 2023.

RECK, J, R,; HÜBNER, B. H. A transformação digital do estado: digitalização do governo e dos serviços públicos no brasil. **Revista Eletrônica Direito e Política,** Itajaí, v. 16, n. 3, p. 1075-1096, 2021. Disponível em: A TRANSFORMAÇÃO DIGITAL DO ESTADO: DIGITALIZAÇÃO DO GOVERNO E DOS SERVIÇOS PÚBLICOS NO BRASIL | Revista Eletrônica Direito e Política (univali.br). Acesso em: 24 out. 2023.

REIS, B. P. W. Capital social e confiança: questões de teoria e método. **Rev. Socio. Polít.,** Curitiba, p. 35-49, nov. 2003. Disponível em: SciELO - Brasil - Capital social e confiança: questões de teoria e método Capital social e confiança: questões de teoria e método. Acesso em: 03 fev. 2024.

ROCHA, L. C. B. F.; DINIZ, M. A. V. **A administração pública e o princípio da confiança legítima.** [20--]. Disponível em: http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/salvador/ludiana_carla_braga_facanha_rocha.pdf. Acesso em: 25 mar. 2022.

ROCHA, L. S.; BARRETO, R. M. **Confiança e ciberespaço:** uma observação do direito dos contratos eletrônicos. [200-], p. 5044-5065. Disponível em: leonel_severo_rocha.pdf (publicadireito.com.br). Acesso em: 03 mar. 2024.

RODRIGUES, M. A. S.; WATKINS, C. Núcleos de justiça 4.0: o declínio da territorialidade e os novos horizontes da especialização. **Revista CNJ,** Brasília, v. 6, n. 2, p. 107–116, 2022. Disponível em: Núcleos de Justiça 4.0: o declínio da territorialidade e os novos horizontes da especialização | Revista CNJ. Acesso em: 08 nov. 2023.

RODRIGUES, M. M. **Repositório arquivístico digital confiável para o patrimônio documental oriundo do processo judicial eletrônico.** 2015. Dissertação (Mestrado em Patrimônio Cultural) – Universidade Federal de Santa Maria, Rio Grande do Sul, 2015. Disponível em: https://repositorio.ufsm.br/handle/1/11050. Acesso em: 24 mar. 2022.

ROGERS, D. L. **Transformação digital:** repensando o seu negócio para a era digital. Tradução Afonso Celso da Cunha Serra. São Paulo: Autêntica Business, 2017.

ROTENBERG, K. J. **A psicologia da confiança.** Tradução de Sonia Augusto. São Paulo: Blucher, 2022. Disponível em: A psicologia da confiança - Ken J. Rotenberg - Google Livros. Acesso em: 05 dez. 2023.

SANTO AGOSTINHO. **Confissões.** Tradução de Lorenzo Mammì. São Paulo: Companhia das Letras, 2017. Disponível em: Microsoft Word - CONFISSOES - Sto Agostinho.rtf (cancaonova.com). Acesso em: 10 dez. 2023.

SANTOS, H. M. D.; FLORES, D. Preservação sistêmica para repositórios arquivísticos. **Revista Eletrônica de Comunicação, Informação e Inovação em Saúde,** v. 14, n. 3, p. 764-781, 2020. Disponível em: Preservação sistêmica para repositórios arquivísticos (brapci.inf.br). Acesso em: 22 jul. 2023.

SANTOS, H. M.; FLORES, D. Políticas de preservação digital para documentos arquivísticos. **Perspectivas em Ciência da Informação,** Belo Horizonte, v. 20, n. 4, p. 197-217, out./dez. 2015. Disponível em: https://brapci.inf.br/index.php/res/v/37577. Acesso em: 24 mar. 2022.

SANTOS, H. M.; MAZUCO, F. C.; FLORES, D. Preservação sistêmica de documentos arquivísticos digitais: uma perspectiva holística. **PerCursos,** Florianópolis, v. 21, n.46, p. 244-271, maio/ago. 2020. Disponível em: Preservação sistêmica de documentos arquivísticos digitais: uma perspectiva holística | PerCursos (udesc.br). Acesso em: 22 jul. 2023.

SANTOS, W. **Dicionário jurídico brasileiro.** Belo Horizonte: Del Rey, 2001. Disponível em: Dicionário Jurídico (integrawebsites.com.br). Acesso em: 21 jul. 2023.

SARACEVIC, T. Ciência da Informação: origem, evolução e relações. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 1, n. 1, p. 41-62, jan./jun. 1996. Disponível em: http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/235. Acesso em: 25 mar. 2022.

SCHÄFER, M. B.; CONSTANTE, S. E. Políticas e estratégias para a preservação da informação digital. **PontodeAcesso,** Salvador, v. 6, n. 3, p. 108-140, dez. 2012. Disponível em: https://brapci.inf.br/index.php/res/v/67073. Acesso em: 24 mar. 2022.

SCHELLENBERG, T. R. **Arquivos modernos:** princípios e técnicas. Tradução Nilza Teixeira Soares. 6. ed. Rio de Janeiro: FGV, 2006.

SCHMIDT, C. M. S. **Arquivologia e a construção do seu objeto científico:** concepções, trajetórias, contextualizações. 2012. Tese (Doutorado em Ciência da Informação) - Escola de Comunicações e Artes, Universidade de São Paulo, São Paulo, 2012. Disponível em: https://www.teses.usp.br/teses/disponiveis/27/27151/tde-02072013-170328/publico/ClarissaMSSchmidt_revisada.pdf. Acesso em: 22 jul. 2023.

SCHWAB, K. **A quarta revolução industrial.** Tradução Daniel Moreira Miranda. São Paulo; Edipro, 2016.

SILVA, A. M. *et al.* **Arquivística:** teoria e prática de uma ciência da informação. 3. ed. Porto: Afrontamento, 2009.

SILVA, A. M.; RIBEIRO, F. **Das ciências documentais à ciência da informação:** ensaio epistemológico para um novo modelo curricular. 2. ed. Porto: Afrontamento, 2008.

SILVA, K. Y. C.; MORAES, C. M. A justiça 4.0 e o acesso sob a lente da agenda 2030 da ONU. **Rev. do Trib. Reg. Trab. 10ª Região,** Brasília, v. 26, n. 2, p. 42-52, 2022. Disponível em: Vista do A Justiça 4.0 e o acesso sob a lente da agenda 2030 da ONU (trt10.jus.br). Acesso em: 08 nov. 2023.

SILVA, L. C. S.; MATOS, Y. S. A. A justiça 4.0: uma análise do acesso à justiça no juízo 100% digital. *In:* MOREIRA, V. *et al.* (org.).; CONGRESSO INTERNACIONAL DE DIREITOS HUMANOS DE COIMBRA: UMA VISÃO TRANSDISCIPLINAR, 6., 2021. Jundiaí. **Anais** [...]. Campinas: Editora Brasília, 2022, p. 47-57. Disponível em: cidhcoimbra.com/_files/ugd/8f3de9_03d72525ba754f49b8a12de1a1c5e0bb.pdf#page=38. Acesso em: 08 nov. 2023.

SILVA, M. Custódia, cadeia de preservação e custodiante confiável: conceitos para a preservação de documentos digitais autênticos. **Revista Conhecimento em Ação,** v. 4, n. 2, p. 46-64, 2019. Disponível em: Custódia, cadeia de preservação e custodiante confiável: conceitos para a preservação de documentos digitais autênticos (brapci.inf.br). Acesso em: 22 jul. 2023.

SILVA, M. **O arquivo e o lugar:** a custódia arquivística como responsabilidade pela proteção aos arquivos. 2015. Tese (Doutorado em História Social) – Faculdade de Filosofia, Letras e Ciências Humanas, Universidade de São Paulo, São Paulo, 2015. Disponível em: https://www.teses.usp.br/teses/disponiveis/8/8138/tde-22122015-093801/publico/2015_MargarethDaSilva_VCorr.pdf. Acesso em: 22 jul. 2023.

SOUSA, G. C. A responsabilidade civil do estado e o princípio da confiança legítima. **Revista de Direito Administrativo**, Rio de Janeiro, v. 258, p. 115-140, set./dez. 2011. Disponível em: https://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/8611. Acesso em: 24 mar. 2022.

SOUZA, F. L. **Transformação digital no contexto da inteligência de estado:** análise e mitigação das vulnerabilidades do documento digital. 2022. Dissertação (Mestrado em Engenharia Elétrica) – Faculdade de Tecnologia, Universidade de Brasília, Brasília, 2022. Disponível em: Repositório Institucional da UnB: Transformação digital no contexo da inteligência de Estado : análise e mitigação das vulnerabilidades do documento digital. Acesso em: 07 nov. 2023.

SOUZA, G. Qual a rede social mais usada em 2023? a resposta vai te surpreender. **techtudo.com.br,** São Paulo, 21 jul. 2023. Disponível em: Qual a rede social mais usada em 2023? A resposta vai te surpreender (techtudo.com.br). Acesso em: 25 out. 2023.

SOUZA, N. C. M.; NUNES, A. A evolução da transformação digital no setor público no Brasil, no período de 2000 a 2020. **Universitas,** ano 15, n. 29, p. 11-28, jun./dez. 2021. Disponível em: A evolução da transformação digital no setor público no Brasil, no período de 2000 a 2020 | Souza | UNIVERSITAS (revistauniversitas.inf.br). Acesso em: 24 out. 2023.

SPINELLI JUNIOR, J. **A conservação de acervos bibliográficos e documentais.** Rio de Janeiro: Fundação Biblioteca Nacional, Departamento de Processos Técnicos, 1997.

SPINELLI, J.; BRANDÃO, E.; FRANÇA, C. **Manual técnico de preservação e conservação:** documentos extrajudiciais CNJ. Rio de Janeiro: Arquivo Nacional, 2011.

Disponível em: https://folivm.files.wordpress.com/2011/04/manual-an-bn-cnj-2011-c3baltima-versc3a3o-2p-f olha.pdf. Acesso em: 25 nov. 2021.

TESSARINI JUNIOR, G.; SALTORATO, P. Impactos da indústria 4.0 na organização do trabalho: uma revisão sistemática da literatura. **Revista Produção Online,** Florianópolis, v. 18, n. 2, p. 743-769, 2018. Disponível em: Impactos da indústria 4.0 na organização do trabalho: uma revisão sistemática da literatura | Revista Produção Online (producaoonline.org.br). Acesso em: 07 nov. 2023.

THIBODEAU, K. *et al*. **Preservation Task Force Report.** InterPARES 1 Project: Canadá, 2001. Disponível em: http://www.interpares.org/display_file.cfm?doc=ip1_ptf_report.pdf. Acesso em: 24 mar. 2022.

UOL. Brasil sobe 5 posições e fica em 49º lugar em ranking global de inovação. **Economia.uol.com.br,** São Paulo, 27 set. 2023. Disponível em: IGI: Brasil sobe para 49º lugar em ranking global de inovação (uol.com.br). Acesso em: 24 out. 2023.

VIANA, A. C. A. Transformação digital na administração pública: do governo eletrônico ao governo digital. **Revista Eurolatinoamericana de Derecho Administrativo,** Santa Fe, v. 8, n. 1, p. 115-136, 2021. Disponível em: Transformação digital na administração pública: do governo eletrônico ao governo digital (redalyc.org). Acesso em: 24 out. 2023.

XAVIER, A. C. C.; GOTTSCHALG-DUQUE, C. Prontuário eletrônico do paciente: qual a contribuição da arquivística e do smart contracts para a sua gestão na era da saúde 4.0? **AtoZ:** novas práticas em informação e conhecimento, Curitiba, v. 10, n. 3, p. 1-10, 2021. Disponível em: Open Journal Systems (ufpr.br). Acesso em: 11 out. 2023.

YAMAGISHI, T. **Trust and Social Intelligence:** the evolutionary game of mind and society. Tóquio: Tokyo University Press, 1998.

APÊNDICE A – PUBLICAÇÕES TÉCNICAS DO CONARQ SOBRE PRESERVAÇÃO DIGITAL

BRASIL. Conselho Nacional de Arquivos. Câmara Técnica de Documentos Eletrônicos. **Carta para a preservação do patrimônio arquivístico digital.** Rio de Janeiro: Arquivo Nacional, 2005a. Disponível em: www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/conarq_carta_preservacao_patrimonio_arquivistico_digital.pdf. Acesso em: 02 fev. 2024.

BRASIL. Conselho Nacional de Arquivos. Câmara Técnica de Documentos Eletrônicos. **Diretrizes do preservador,** a preservação de documentos arquivísticos digitais: diretrizes para organizações. Rio de Janeiro: Arquivo Nacional, 2013a. Disponível em: conarq_diretrizes_produtor_preservador_resolucao_38.pdf (www.gov.br). Acesso em: 02 fev. 2024.

BRASIL. Conselho Nacional de Arquivos. Câmara Técnica de Documentos Eletrônicos. **Diretrizes do produtor,** a elaboração e a manutenção de materiais digitais: diretrizes para indivíduos. Rio de Janeiro: Arquivo Nacional, 2013b. Disponível em: conarq_diretrizes_produtor_preservador_resolucao_38.pdf (www.gov.br). Acesso em: 02 fev. 2024.

BRASIL. Conselho Nacional de Arquivos. Câmara Técnica de Documentos Eletrônicos. **Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis (RDC-Arq).** Rio de Janeiro: Arquivo Nacional, 2023a. Disponível em: DIRETRIZESRDCArq12DEZ2023.pdf (www.gov.br). Acesso em: 02 fev. 2024.

BRASIL. Conselho Nacional de Arquivos. Câmara Técnica de Documentos Eletrônicos. **Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais.** Rio de Janeiro: Arquivo Nacional, 2012. Disponível em: Projeto_capa_conarq_com_logo.indd (www.gov.br). Acesso em: 02 fev. 2024.

BRASIL. Conselho Nacional de Arquivos. Câmara Técnica de Documentos Eletrônicos. **e-ARQ Brasil**: modelos de requisitos para sistemas informatizados de gestão arquivística de documentos. Versão 2. Rio de Janeiro: Arquivo Nacional, 2022. Disponível em: Resolução nº 50, de 06 de maio de 2022 — Conselho Nacional de Arquivos (www.gov.br). Acesso em: 24 jul. 2023.

APÊNDICE B – SÍNTESE DOS ELEMENTOS DO CONCEITO DE CONFIANÇA

Autores	*Enunciados acerca dos conceitos de confiança*	*Conceitos de confiança*	*Características dos conceitos de confiança*
Confúcio (1996)	*5) Dá-se por meio das relações entre pessoas.* *6) É um princípio ou uma virtude.* *7) Pressupõe integridade, confiabilidade e fidelidade.* *8) Tem como antítese a desconfiança.*	*A confiança está afinada às relações pessoais na sociedade, traduzida em princípios e virtudes para um bom governo. Estes podem ser representados pela integridade, pela confiabilidade e pela fidelidade, significando conservar e preservar suas características originais, isto é, a confiança na relação entre indivíduos ou entre indivíduos e objeto de forma abstrata ou concreta. O filósofo mencionou a desconfiança como um sentimento desvirtuoso da boa conduta humana.*	*Relação/princípio/virtude/integridade/confiabilidade/fidelidade/desconfiança/conservar/preservar*
Aristóteles (1991)	*1) É uma virtude.* *2) Traz esperança, felicidade e bem-estar.* *3) Relaciona-se à crença.* *4) Relaciona-se ao medo e à coragem.*	*A confiança é um sentido de virtude moral e ética, que traz esperança. Para o pensador um dos objetivos da vida humana é a felicidade e o bem-estar, que acontece, a partir do momento em que confiamos/acreditamos nas pessoas para viver bem. Porém, existe um meio-termo entre a confiança e o medo: a coragem, que é a linha medial entre perder o temor e iniciar a confiança.*	*Virtude/moral/ética/esperança/felicidade/bem-estar/crença/medo/coragem*
Santo Agostinho (2017)	*1) Está direcionada à crença e à esperança.* *2) É confiar em uma força divina.*	*A confiança direcionada a crer que Cristo é o provedor de todas as coisas boas e do bem no mundo, sendo a única esperança para a salvação. O ser humano não pode confiar em si mesmo sozinho, necessita de uma força divina para dar confiança em viver uma vida melhor.*	*Crença/esperança/religião/*
São Tomás de Aquino (2001)	*1) Significa ter fé.* *2) Significa crer.* *3) É ter segurança e esperança.* *4) É esperar no divino.* *5) É o oposta ao medo.*	*A confiança significava ter fé (fidúcia/fides), e a fé significa crer em alguma coisa ou alguém sem vê-lo (Cristo). A confiança é oposta ao medo/temor, significando ter segurança que conseguiremos determinado bem. Logo, confiança é o mesmo que esperança, pois quem*	*Fé(fidúcia/fides)/crença/segurança/esperança/medo/Religião*

		confia, espera.	
Machiavelli (2019)	*1) Denota segurança* *2) É uma cooperação proveitosa.* *3) É uma ação que causa bem-estar.*	*A confiança denota a segurança que um líder deve ter para governar. O Estado deve deter todo o poder e mérito para praticar suas ações desde que direcionada ao bem-estar dos cidadãos, dicotomizando da doutrina cristã medieval. Portanto, os cidadãos devem depositar sua confiança no "príncipe". Em complemento, enfatiza que um líder deve ser cauteloso e sem excesso de confiança, não desconfiando de tudo e de todos e ser intransigente. A desconfiança impede qualquer cooperação proveitosa.*	*Segurança/cooperação/bem-estar/desconfiança*
René Descartes (2001)	*1) Relaciona-se com a verdade.*	*O pensamento de Descarte sobre a questão da confiança está direcionado à busca da verdade e do conhecimento científico para se chegar a um resultado confiável. O instrumento que permite isso é o método.*	*Verdade*
John Locke (1996; 2012)	*1) Significa crer* *2) Tem um sentido político (trust/fides)* *3) Tem um aspecto contratual* *4) Tem um sentido pessoal (trust)*	*Conforme Locke, a confiança significa crer/acreditar. Para ele o ser humano é uma folha em branco e para se ter confiança é preciso experienciá-la. O filósofo foi um dos primeiros a utilizar o termo trust como confiança, tanto em um sentido político como pessoal. O sentido político de trust significa fides, e tem o objetivo de reforçar um aspecto contratual, de acordo ou comercial. Já o sentido pessoal de trust dá-se pelo seu uso comum, atrelado à confiança pessoal: em um líder, na família. Para aquele que não prova o que diz é digno de desconfiança.*	
Kant (2001)	*1) Está na razão e na fé.* *2) Significa o que é verdadeiro.* *3) É um elemento da moral.*	*A confiança está na razão e na palavra fé, que significa algo verdadeiro. Assim, a confiança não é só uma autoconfiança, é um elemento necessário para a moral, a fim de moderar e direcionar nossas inclinações para fins*	*Razão/fé/verdade/moral*

		universais.	
Feres Júnior; Eisenberg (2006)	*1) A confiança é uma relação interpessoal.* *2) Serve para estabilidade de regimes democráticos.* *3) É uma maneira de cooperação.*	*A noção de confiança interpessoal é inadequada a uma teoria democrática moderna, a confiança em instituições é uma categoria central à compreensão da estabilidade e legitimidade de regimes democráticos. Para prosseguir com este exercício de diferenciação conceitual, precisamos, entretanto, definir estas duas categorias em questão. Uma definição de confiança interpessoal sintetizada a partir de pistas fornecidas pelo texto de Inglehart assumiria a seguinte forma: é a expectativa depositada em um estranho de que este aja de maneira cooperativa, ou, pelo menos, não danosa, em relação ao depositante. Uma definição sucinta da confiança em instituições pode ser expressa da seguinte forma: é a expectativa de ação reparatória ou punitiva por parte dos poderes estabelecidos contra todos aqueles que violarem os preceitos da lei. É claro que a confiança institucional pode ser estendida para aspectos relacionados a direitos positivos de participação e deliberação política, direitos econômicos redistributivos, direitos de preservação cultural e do meio ambiente etc.*	*Relação/estabilidade/expectativa/cooperação/*
Rotenberg (2022)	*1) A confiança pressupõe a falta dela.* *2) Essa falta pode ser representada pela corrupção e a pela falta de confiabilidade.* *3) É uma força que conecta pessoas.* *4) Garante relacionamento e o funcionamento social.*	*A confiança existe pela possibilidade de sua falta e de corrupção. Desse modo, a confiança é uma força prevalente, muitas vezes silenciosa, conectando as pessoas e garantindo os relacionamentos e o funcionamento das coisas; sem isso, nosso "universo" social não existiria. Hodiernamente, o acesso a informações que revelam a falta de confiabilidade das pessoas é maior do que em qualquer momento da história humana. Com a*	*Desconfiança/corrupção/relação/confiabilidade*

		tecnologia e as redes sociais, cada ação é transmitida a milhões de pessoas conservada para escrutínio público. Essa mudança resultou em uma oportunidade sem igual para avaliação crítica do comportamento das pessoas, detecção de não confiabilidade e expressão de falta de confiança nos outros – especialmente em relação aos indivíduos expostos à opinião pública.	
Inglehart (199)	*1) Significa relação interpessoal.* *2) Que é determinada pela sociedade.* *3) É direcionada à estabilidade democrática e às tradições culturais-religiosas.* *4) Democracias estáveis promovem um alto grau de confiança interpessoal.* *5) O protestantismo promove um alto grau de confiança interpessoal.* *6) Instabilidade democrática produzem pessoas desconfiadas.* *7) Catolicismo produzem pessoas desconfiadas.*	*Está relacionada ao grau de relação entre as pessoas (relação interpessoal) de uma determinada sociedade direcionada direcionado à estabilidade democrática e às tradições culturais-religiosas. Democracias estáveis e protestantismo e os confucionistas promovem um alto grau de confiança interpessoal e instabilidade democrática e catolicismo produzem baixo grau de confiança interpessoal e, consequentemente, pessoas desconfiadas.*	*Relação/estabilidade/desconfiança/ religião/desconfiança*
Pereira (2010)	*1) Dá-se por relacionamentos entre organizações, entre indivíduos; entre sistemas; entre humanos.* *2) Sem confiança não é possível assegurar um convívio harmônico.* *3) Garante segurança do tempo futuro.* *4) Traz crença para o tempo presente.* *5) Quando a confiança é quebrada gera-se*	*A confiança dá-se pelos relacionamentos entre organizações; entre indivíduos; entre sistemas; e sobretudo, pelas relações humanas. Ausente a confiança, não há formação de expectativas e uma sociedade e sem expectativas torna-se incapaz assegurar um convívio harmônico. A confiança substitui informações insuficientes, causando segurança para algo ou para alguém. Os meios de comunicação responsáveis pela formação de opiniões, pelas*	*Relação/segurança/crença/tempo/expectativa/expectativa//desconfiança*

	desconfiança.	*informações que veiculam, pelos produtos que vendem – ao gerar expectativas devem honrá-las, para que a segurança seja mantida e a confiança não desapareça, sendo capaz de cumprir seu papel de crença no presente, por meio das atitudes do passado, de que o futuro prometido será assegurado. Esses mecanismos servem de ponte para a confiança existir, em que há viabilidade para o seu desenvolvimento; mas quando isso é rompido, quebra-se as expectativas e vem os sentimentos de desconfiança e desinteresse, por exemplo: antônimos à confiança.*	
Belchior (2015)	*1) É dada pela relação entre indivíduos.* *2) A confiança pode ser social e interpessoal.* *3) A confiança elevada entre indivíduo gera cooperação entre eles.*	*A confiança tem tido relevância pela relação entre os indivíduos, sobretudo com a confiança social e interpessoal, e a forma como estas afetam a vida em sociedade. Os níveis elevados de confiança levam a uma maior integração social dos indivíduos e a uma maior predisposição para a cooperação. Sob esta perspectiva, a confiança interpessoal é usualmente associada à satisfação dos indivíduos com a sua vida pessoal, ao otimismo, ou ao bom estado de saúde e longevidade.*	*Cooperação/relação/interação/satisfação/bem-estar*
Diniz; Marconatto (2011)	*1) A condição da confiança pressupõe risco ou vulnerabilidade interdependência.* *2) Pode ser individual ou coletiva.*	*Há duas condições para o desenvolvimento da confiança: o risco ou vulnerabilidade (a probabilidade de se perder algo/alguém, quando interpretada por uma das partes decisórias) e a interdependência (quando os interesses de uma das partes não podem ser atingidos sem a colaboração da outra). A confiança nesses sentidos (individual ou coletivo) se parece destina-se a controlar e a fiscalizar a ação dos agentes em seus relacionamentos, seja ele do tipo patrão-empregado,*	*Risco/vulnerabilidade/interdependência//relação/contrato/marco regulatório/crença*

		pessoas-sistemas, pessoas-pessoas. Por exemplo, quanto maior a confiança entre dois negociadores, menos a sua relação demandará de marcos regulatórios (como contratos formais), uma vez que há a crença de parte a parte de que um não trairá o outro, ou seja, não incorrerá em comportamentos oportunistas.	
Gambetta (2008a; 2008b)	*1) É a cooperação entre agentes.* *2) É um conjunto de regra.* *3) É um contrato, um acordo, uma interação.* *4) Pode envolver grau de restrição, de risco e de falha.* *5) Pode ser uma pré-condição.* *6) É uma virtude.* *7) Uma crença.* *8) Expectativas nos outros.* *9) Não é baseada em evidências, mas na falta dela.* *10) Essa ação realça a possibilidade de desconfiança.* *11) A confiança é relevante em condições de ignorância ou de incerteza em relação a ações desconhecidas ou incognoscíveis de outros, dando-se por meio da fé, que se traduz em "acreditar".* *12) A liberdade não é por si só suficiente para caracterizar as questões da confiança. Nossa relação com pessoas é um tipo de liberdade, na qual escolhemos manter uma relação potencialmente arriscada.*	*Cooperação é o sentido amplo de agentes (indivíduos, empresas e governos) acordarem qualquer contrato dentro de suas interações. A forma mais básica de cooperação humana é a condição de uma interação benéfica, sendo preciso algum nível de confiança (a confiança mútua) em que as partes consigam cumprir certas regras. Contudo, dependendo do grau de restrição, de risco e de interesse envolvido, a confiança atua como uma pré-condição de cooperação.* *Uma virtude instala-se no sentido de cooperação: a crença. Sendo assim, confiança é uma crença peculiar baseada não em evidências, mas na falta dela. Em contrapartida, essa ação realça a possibilidade de desconfiança. Nesse sentido, a confiança é simetricamente à desconfiança, como um grau particular subjetivo de probabilidade, no qual um agente acredita que outro agente ou grupo realizará uma ação sujeita a afetar a sua própria ação. Em primeiro espa, "confiar" pode ser visto como um limiar localizado em uma distribuição probabilística de expectativas gerais, que podem levar a uma série de valores entre a completa desconfiança (0) e confiança total (1), e que está centrada*	*Cooperação/contrato/acordo//interação/risco/crença/desconfiança/evidência/fé/tempo/ liberdade/família/amizade/moral/religião.*

	13) *É baseada nas relação familiares e de amizade.*	*em torno um ponto médio (0.50) de incerteza. Assim, tanto a confiança como a desconfiança representam predisposições lexicográficas para atribuir valores da probabilidade e mantê-los incondicionalmente acima de alguma evidência. Em segundo lugar, a confiança é relevante em condições de ignorância ou de incerteza em relação a ações desconhecidas ou incognoscíveis de outros, dando-se por meio da fé, que se traduz em "acreditar". A este respeito, a confiança inclina-se a ações futuras que condicionam nossas decisões presentes. Em terceiro lugar, postulando que nossas próprias ações são baseadas nessa probabilidade, podemos excluir os casos em que a confiança em alguém não tem influência nas nossas decisões. Por fim, a confiança aqui está limitada entre os agentes, excluindo aquela entre agentes e eventos naturais. Neste nível de abstração, a definição de confiança poderia refletir-se nas intenções dos outros de não nos enganar. A liberdade não é por si só suficiente para caracterizar as questões da confiança. Nossa relação com pessoas é um tipo de liberdade, na qual escolhemos manter uma relação potencialmente arriscada. Laconicamente, confiar em uma pessoa significa crer que ela não o prejudicará. Há ainda, casos em que a família (ou a familiaridade) e a amizade são subprodutos da confiança, acontecendo quando as partes envolvidas se conhecem e apresentam respeito e bem-estar um pelo outro. Logo, "a confiança pode emergir aí como subproduto de valores morais e religiosos.*	

Luhmann (1996; 2008)	*1) Pode ser uma condição de ignorância ou de incerteza.* *2) Pode ter grau de liberdade positiva ou negativa.* *3) Um elemento de relação entre pessoas.* *4) É um mecanismo de redução de complexidade;* *5) Pressupõe risco, insegurança, medo e falta.* *6) É uma noção de tempo: passado, presente e futuro.* *7) Relaciona-se à crença, à familiaridade à cooperação.* *8) Pode se caracterizar como confiança sistêmica.* *9) Relaciona-se à verdade.*	*A condição de ignorância ou de incerteza sobre o comportamento de outras pessoas é central à noção de confiança, assim como o grau de liberdade, o qual pode ser de cunho positivo ou negativo (esta última, traição e decepção). A condição de liberdade positiva está relacionada ao limite de nossa capacidade de alcançar um conhecimento pleno sobre os outros, prevendo suas ações para antecipar qualquer liberdade negativa. Sumariamente, essa liberdade traz a responsabilidade das pessoas sobre as suas escolhas, sobre os seus atos. A confiança interpessoal pode ser dividida em dois momentos. No primeiro, o indivíduo pode confiar em sua própria confiança em outra pessoa, atribuindo à sua confiança a habilidade para motivar terceiros. No segundo momento, pode o indivíduo confiar na confiança que outros têm nele. Nesses dois momentos (podendo-se falar então em duas dimensões), a confiança apresenta-se como confiança reflexiva. Essas virtudes se complementam, mas há distinções A confiança deve ser entendida, especificamente, em relação ao risco. Risco substitui em grande parte o que antes era pensado como destino e torna-se separado das cosmologias. Sendo assim, ter confiança, também é sentir seus antônimos: insegurança, risco, perda, medo, falta. A visão de Luhmann sobre os sistemas sociais possui marca registrada como um elemento de redução da complexidade. Não existe garantia de uma certeza absoluta das coisas por intermédio da confiança;*	*Ignorância/incerteza/liberdade/ reflexão/relação/cooperação/virtude/risco/insegurança/medo/perda/tempo/redução da complexidade/crença/família/sistêmica/verdade/dinheiro/poder*

		mas permite que um futuro incerto se faça confiável; ou seja, é uma aposta feita no presente em experiências passadas. Dessa forma, a redução da complexidade traz segurança para o futuro. Outro sentido de confiança é a crença, sendo uma atitude certa de que as coisas familiares permanecerão estáveis. Familiaridade e confiança são, portanto, meios complementares de absorção de complexidade, e, como passado e futuro, atados um ao outro. Entre duas pessoas a confiança só se mantém pelo desejo de ambos em continuar o relacionamento. Nesse sentido, existe uma outra dimensão de confiança mostrada por Luhmann, conhecida como "confiança sistêmica", que para operar depende dos meios de comunicação simbolicamente generalizados. A confiança sistêmica é mecanismo adicional à linguagem cotidiana, sendo: a verdade, o poder, o amor e o dinheiro. Eles possibilitam a formação de estruturas, diminuindo a contingência existente na sociedade. A verdade, por exemplo, desempenha um papel fundamental, pois estabelece uma relação de confiança sistêmica concomitantemente com outros meios, isto é, com o dinheiro ou o poder. Desse modo, a verdade e o dinheiro são os meios presentes em uma relação contratual.	
Dasgputa (2008)	*1) É uma virtude* *2) Direciona-se à restrição.* *3) Pode ser um pré-compromisso.* *4) São promessas e contratos.*	*A confiança é uma virtude direcionada à restrição, relevante não apenas para decidirmos até onde precisamos confiar nos outros, mas também para os outros decidirem até onde podem confiar em nós; isto é, confiar é importante,*	*Virtude/restrição/condição/relação/pré-compromisso/promessa/contrato*

		contudo ser confiável também. Essa ocorrência dá-se por meio de um "pré-compromisso", que em suas diversas formas (unilateral ou bilateral) é um dispositivo que possibilita impor restrições. Promessas e contratos representam formas mais fracas desses pré-compromissos. O contrato, por exemplo, muda o foco da confiança para a eficácia das sanções caso um acordo seja quebrado. As promessas são interessantes na medida que usa palavras para formalização de contrato, portanto, podendo não acarretar sanções.	
Canedo (2012)	*1) Capacidade de alguém ser confiável* *2) Segurança*	*Confiabilidade é a capacidade de alguém ser confiável e a confiança seria sua consequência, trazendo segurança à pessoa.*	*Confiabilidade*
Lundåsen (2002)	*1) É um mecanismo de fé.* *2) É representada pela previsibilidade.* *3) Traz o elemento risco.* *4) Pode ser dividida em 3 tipos: relacional, generalizada e na rede.*	*A fé é um mecanismo de confiança ligada ao fato de que alguém manterá sua palavra. Também se liga à previsibilidade como expectativa para eventos futuros, em que existe a possibilidade de ocorrer algum tipo de perda se a confiança não for correspondida. Em outras palavras, há um elemento de risco envolvido. A confiança interpessoal foi associada, à priori, a traços de personalidade como misantropia, contudo muitas teorias também trouxeram diversas definições e aspectos sobre confiança, mas segundo a autora, apesar dessa diversificação, a maneira mais comum de operacionalizar a confiança generalizada é por meio de surveys, como Inglehart fez. Desse modo, a confiança está ramificada em três níveis: a confiança relacional (ligada com pessoas conhecidas e específicas); a confiança na rede (ligada às redes sociais ou familiares) e a confiança*	*Fé/previsibilidade/tempo/risco/relaciona/na rede/generalizada/interpessoal*

		generalizada (na natureza humana). A confiança generalizada está relacionada a pessoas que se conhecem pessoalmente e a segunda não necessariamente – as pessoas não precisam ser conhecidas. A confiança generalizada aumentaria a probabilidade de conseguir uma reciprocidade geral e, portanto, facilitaria a ação coletiva.	
Hwang e Burgers (1997)	*1) Correlaciona-se à cobiça, o medo e a cooperação.*	*Dois elementos correlacionam-se à confiança: a cobiça (ganhar um benefício obtido pela não-cooperação unilateral em vez de mútua) e o medo (ansiedade, por exemplo), agindo como agentes influenciadores da confiança. A confiança não é uma condição suficiente da cooperação, embora necessária, ela atenua dois tipos diferentes de risco: de ser vitimado e de perder um parceiro confiável.*	*Cobiça/medo/cooperação/risco*
Fukuyama (1995)	*1) Cooperação entre indivíduos de naturezas diferentes.* *2) É um fator do capital social.*	*A confiança é uma relação de cooperação entre indivíduos de diferentes naturezas (interpessoal), sendo de grande importância para o plano político, para a estabilidade das instituições (no plano econômico) e para o funcionamento de sistemas de produção complexos de larga escala. É um fator do capital social, como a capacidade de indivíduo(s) (grupos ou organizações) trabalharem em conjunto para uma causa comum, que dependendo do grau de partilha de normas e de valores atendem aos interesses individuais e coletivos.*	*Relação/cooperação/capital social*
Putnam (1993; 2006)	*1) Serve para o desempenho das instituições políticas.* *2) Pressupõe redes de interação.* *3) Pode ser social, mas também e*	*O desempenho das instituições políticas e da própria democracia seriam afetadas pelo ambiente social, econômico e cultural, isto é, por características da organização social, como a confiança, as normas sociais*	*Interação/cooperação/coletividade/reciprocidade/capital social/densa/delgada/generalizada*

	interpessoal. *4) Pressupõe cooperação.* *5) É um componente básico do capital social.*	*ou as redes de interação, que melhorariam a eficiência do sistema político ao facilitar o desenvolvimento de ações coletivas coordenadas. A confiança social (comportamento ou interação das pessoas com outras pessoas ou instituições na sociedade) sempre foi um elemento fundamental que sustentou o dinamismo econômico e o desempenho governamental. E para isso acontecer, é necessário haver cooperação entre as partes. Assim, pertencendo a associações, os indivíduos desenvolveriam competências de relacionamento – de confiança mútua, de cooperação, de solidariedade, de tolerância e de reciprocidade – que potenciaria a eficácia governativa, ao estimular a ação coletiva para o alcance de interesses comuns ou públicos. A confiança é o componente básico do capital social, mas não o único e quanto mais alto o nível de confiança numa comunidade, maior a probabilidade de cooperação; e quanto maior a cooperação, mais alto o nível de confiança. Em contrapartida, a baixa do capital social é causada pelo aumento das taxas de infelicidade e da falta de confiança; alguns exemplos deste tipo de capital são: baixa confiança no governo, baixa eficiência política, ou seja, confiança na própria influência; menor participação dos cidadãos nas votações, menos cooperação para se resolver problemas sociais (dilemas de ação coletiva); em suma, a não participação e cooperação da sociedade em questões políticas. Para Putnam há dois tipos de*	

		confiança: o denso e o delgado. No denso estabelece-se nas interações face a face e com o conhecimento direto, reduzindo o grau de risco. E o no delgado, a confiança se mede pela maior possibilidade de risco. A confiança tratada por Putnam também pode ser chamada de confiança generalizada.	
Lucena (2009)	*1) É uma categoria do conhecimento.* *2) É criada por meio da integridade.* *3) Vem das pessoas.*	*A confiança é uma categoria do conhecimento e o confiante na confiança é uma categoria de ação. A integridade cria confiança, como um potencial de se manter uma promessa e ser digno dela. Existem dois tipos de confiança: a em si mesmo (pessoal) e a depositada nas outras pessoas (social). A confiança em si mesmo serve para que o indivíduo possa assumir riscos, acreditar em julgamento, e não no de outrem, e estabelecer vínculo afetivo.*	*Conhecimento/ação/integridade /promessa/risco*
Filgueira (2007)	*1) Pressupõe uma comunicação pessoal.* *2) Diminui o risco.*	*A confiança ganhou padrões de interação social (interpessoal) na sociedade atual. O baixo nível de confiança interpessoal está associado a interações de caráter autoritário, em que resulta na existência de corrupção como forma de mediação social; já o alto nível liga-se a interações democráticas e a uma maior prosperidade econômica, esta, gerando estabilização e eficácia das instituições políticas. O exercício da confiança não se dá meramente por raízes religiosas de determinada cultura, mas pelo modo como as instituições são capazes de reduzir o risco em sociedades complexas. A confiança interpessoal, portanto, é inadequada a uma teoria democrática moderna, porque em sociedades complexas os padrões de interação são*	*Interação/estabilização/risco/re dução de complexidade*

		mediados por instituições.	
Ketzer (2015)	*1) É dividida em dois níveis: fiar-se; fiabilidade (reliability), confiança (trust)* *2) Significa fidedignidade.* *3) Relaciona-se ao o risco e à traição.* *4) Envolve direitos e obrigações.* *5) É um tipo de laço social.* *6) Envolve a relação de boa vontade.*	*Quem confiança coloca-se numa posição vulnerável de risco de traição. Isto é, confiança é uma relação que envolve direitos e obrigações; é o tipo de laço social indicador de sucesso nas relações interpessoais. Existe a confiança por meio do conceito de "confiar" (trust) e de "fiar-se" (rely). Fiar-se é o nível mais básico, o qual também chamamos de fiabilidade (reliability), que se define pelas nossas relações com o mundo, com as instituições e com desconhecidos, sendo necessária para nossa vida diária; já o outro nível, trust, é mais profundo, no qual a confiança é explícita e pode envolver a instituição de promessas como acordos. A fiabilidade é um tipo de relação que envolve sentimentos como desapontamento. No entanto, confiança (trust) está para as relações morais, pressupondo boa vontade das partes, como a promessa daquele que é confiado em corresponder ao sentimento de confiança que lhe foi depositado, corroborando uma relação explícita. A fidedignidade (trustworthy) é uma forma especial de dependência do conhecimento e que conferem ao falante obtê-lo e compartilhá-lo. Para isso, o ouvinte geralmente aceita as palavras do falante e as toma para si, assumindo o testemunho do falante autoridade. Portanto, confiar é ter a noção de dependência de algo ou de alguém e fidedignidade é a propriedade que alguém tem de ser competente e comprometida com o que lhe é confiado.*	*Vulnerabilidade/risco/relação/confiar(trust)/fiar(rely)/promessa/acordo/boa vontade/fidedignidade*
McKyler (2011)	*1) Diferencia confiar (trust) e fiar-se.*	*Também divide a confiança em dois níveis. 1. Confiar (trust): envolve mais do que fiar-se, pressupõe a boa*	*Confiar (trust)/fiar (fiabilidade)/boa vontade/crença/evidência/dependência*

		vontade do outro em auxiliar alguém, mais do que simplesmente crer que a palavra do outro é verdadeira. *2. fiar-se (fiabilidade): concebido por uma perspectiva mais individualista, tratando-se de uma espécie de dependência entre os agentes e as suas fontes de conhecimento para aceitar algo como evidências.*	
Fricker (1998)	*1) A confiança é ligada à fidedignidade.* *2) É um mecanismo de credibilidade*	*Alguém que é fidedigno (posição de prestígio numa sociedade) e competente tem autoridade racional, e retendo ambas características, possui credibilidade. Contudo, "mera credibilidade" significa dizer que o indivíduo nem é confiável, nem competente, mas por algum motivo lhe estão concedendo autoridade.*	*Fidedignidade/credibilidade/autoridade*
Faulkner (2011)	*1) Pode ser uma ação ou atitude.* *2) Pode ser preditiva que envolva a crença, espelho da fiabilidade.* *3) Pode ser afetiva, que envolve sentimentos e atitudes de boa vontade ao depender de outra pessoa.*	*A confiança pode ser uma ação ou uma atitude. A primeira dá-se quando dependemos de outra pessoa para algo e a segunda quando criamos expectativa que algo irá ser realizado conforme esperamos. E a confiança como atitude subdivide-se em dois tipos: a "confiança preditiva" que envolve a crença, espelho da fiabilidade; e a "confiança afetiva", que envolve esperar que a confiança motive o confiado, isto é, envolvem sentimentos e atitudes como o de boa vontade ao depender de outra pessoa.*	*Ação/atitude/sentimento/crença/fiabilidade/afetiva/boa vontade.*
Giddens (1991)	*1) É localizada em ambientes parentescos. familiar, religioso e de tradições;* *2) Localiza-se na crença e na credibilidade.* *3) É uma forma de fé* *4) A confiança relaciona-se à ausência no tempo*	*Está centrada nos "ambientes de confiança e de risco". A confiança é localizada em ambientes como as relações de parentescos (familiar), religiosas e de tradições, nas relações pessoais orientadas ao futuro. A confiança pode ser definida como crença na credibilidade de uma pessoa*	*Risco/relações/família/religiosidade/fé/crença/credibilidade/segurança/risco/perigo/liberdade/contigência/credibilidade/desconfiança*

	e no espaço. *5) É um dispositivo para lidar com a liberdade.* *6) Está vinculada à contingência e não necessariamente ao risco.* *7) Não é o mesmo que fé.* *8) Relaciona-se ao perigo.*	*ou sistema. Essa crença expressa uma fé na probidade ou amor de um outro, ou na correção de princípios abstratos (conhecimento técnico). Para o autor, a confiança é uma forma de fé na qual há uma segurança adquirida em resultados prováveis. Nesse sentido, o autor sugere conceituar a confiança e suas noções, em dez pontos, alguns deles:* • *a confiança relaciona-se à ausência no tempo e no espaço. Não haveria necessidade de se confiar em alguém cujas atividades fossem continuamente visíveis e cujos processos de pensamento fossem transparentes, ou de se confiar em algum sistema cujos procedimentos fossem inteiramente conhecidos e compreendidos;* • *a confiança é um dispositivo para lidar com a liberdade dos outros, contudo a principal condição à confiança não é a falta de poder, mas a falta de informação plena.* • *a confiança está vinculada à contingência e não necessariamente ao risco. A confiança sempre leva à conotação de credibilidade em face de resultados contingentes, ou melhor, às ações de indivíduos ou à operação de sistemas.* • *a confiança não é o*	

		mesmo que fé na credibilidade de uma pessoa ou sistema; ela é o que deriva desta fé. A confiança é o elo entre fé e crença, e é isto o que a distingue do conhecimento indutivo fraco. • *Existe também, a confiança em fichas simbólicas (meios de intercâmbio sem ter em vista as características específicas dos indivíduos ou grupos que lidam com eles em qualquer conjuntura particular, por exemplo, o dinheiro) ou em sistemas peritos.* • *A definição de confiança é a crença na credibilidade de uma pessoa ou de um sistema, tendo em vista um dado conjunto de resultados ou de eventos, em que essa crença expressa uma fé na probidade ou no amor de uma pessoa, ou na correção de princípios abstratos (conhecimento técnico).* • *A confiança existe no contexto de: a) a consciência geral de que a atividade humana, incluindo nesta expressão o impacto da tecnologia sobre o mundo material, é criada socialmente, e não dada pela natureza das coisas ou por influência divina; (b) o escopo*	

		transformativo amplamente aumentado da ação humana, levado a cabo pelo caráter dinâmico das instituições sociais modernas. • *perigo e risco estão intimamente relacionados, entretanto não são a mesma coisa. O risco pressupõe perigo (não necessariamente a consciência do perigo). Uma pessoa que arrisca algo flerta com o perigo, compreendido como uma ameaça aos resultados desejados. Qualquer um que assume um "risco calculado" está consciente da ameaça que isso pode acarretar.* *O termo desconfiança, aplica-se mais facilmente quando falamos na relação de um agente com um sistema, ou entre indivíduos. Direcionada a pessoas, a desconfiança significa duvidar ou desacreditar das reivindicações de integridade que suas ações personificam ou demonstram.*	
Barbosa (2017)	*1) Representa risco* *2) Relaciona-se à confidência.*	*Confiança representa um risco. Ela diferencia-se da familiaridade, do algo comum, e também de uma simples confidência. A confidência baseia-se em questões que não envolvem decisões, como estar confidente (confiante) que o dinheiro ainda existirá amanhã.*	*Risco/confidência*
Engelmann e Klein (2020)	*1) Pressupõe aos usuários se sentir seguro sentido nas tecnologias.* *2) Relaciona-se com o tempo.*	*A confiança correlacionada às tecnologias da TD traz algo em comum, principalmente no diz que a necessidade de que seus usuários sintam a*	*Tecnologia/segurança/p/confiabilidade/redução da complexidade/perigo/contingência*

	3) *Serve para controlar o tempo.* 4) *Reduz a complexidade.*	*"segurança" de que a inovação utilizada perdure por muito tempo, o que a reveste de confiabilidade tanto no que tange à sua segurança de utilização quanto à sua efetiva garantia de prosperidade social. Por intermédio da confiança, um sistema ganha tempo. Para a confiança operar necessita-se de tempo, isto é, a confiança é uma forma que possibilita o controle do tempo; ela encontra-se entre o passado e o futuro, possibilitando que, no presente, reduza-se complexidade. Confiar não é necessariamente eliminar os perigos existentes no futuro – que, por sua vez, é incerto e permanecerá sendo incerto –, mas agir como se o futuro fosse certo, ou melhor: confiável. Ela traz o passado bem-sucedido para as expectativas de um futuro mais seguro, menos complexo, fazendo, normalmente, com que esta profecia se autorrealize, mas tendo sempre presente a possibilidade de que o contrário ocorra. Colocamos cobertas nas contingências para não as enxergar e dessa forma podermos agir com menos receio. Se isto não for possível, invertemos os polos e mostramos toda nossa insatisfação através da desconfiança.*	
Mota (2016)	1) *Relaciona-se à desconfiança.* 2) *Reduz a complexidade social*	*A confiança e a desconfiança são dois lados da mesma moeda; são equivalentes funcionais, ambos reduzem a complexidade social, só que enquanto a confiança o faz mirando expectativas positivas no seu objeto, a desconfiança observa essas expectativas como negativas. Nas relações pessoais, por exemplo, a desconfiança é transformada em comportamento desconfiado, podendo*	*Desconfiança/redução da complexidade*

		ensejar insatisfação.	