UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE FINANÇAS E CONTABILIDADE
CURSO DE GRADUAÇÃO EM CIÊNCIAS CONTÁBEIS

JEAN CARLOS DA SILVA NASCIMENTO

PROTEÇÃO DE DADOS: UM ESTUDO DE CASO NO TRIBUNAL DE CONTAS DO ESTADO DA PARAÍBA

JOÃO PESSOA
2023

JEAN CARLOS DA SILVA NASCIMENTO

PROTEÇÃO DE DADOS: UM ESTUDO DE CASO NO TRIBUNAL DE CONTAS DO ESTADO DA PARAÍBA

Monografia apresentada ao Curso de Ciências Contábeis, do Centro de Ciências Sociais Aplicadas, da Universidade Federal da Paraíba, como requisito parcial para a obtenção do grau de Bacharel em Ciências Contábeis.

Orientadora: Profª. Dra. Anna Paola Fernandes Freire

JOÃO PESSOA
2023

Catalogação na publicação
Seção de Catalogação e Classificação

N244p Nascimento, Jean Carlos da Silva.
Proteção de Dados: um estudo de caso no Tribunal de Contas do Estado da Paraíba / Jean Carlos da Silva Nascimento. - João Pessoa, 2023.
61 f. : il.

Orientação: Anna Paola Fernandes Freire.
TCC (Graduação) - UFPB/CCSA.

1. Tribunal de Contas do Estado da Paraíba. 2. Lei Geral de Proteção de Dados Pessoais (LGPD). 3. Segurança de dados pessoais. 4. Segurança da informação. I. Freire, Anna Paola Fernandes. II. Título.

UFPB/CCSA CDU 657

Elaborado por ANA CLAUDIA LOPES DE ALMEIDA - CRB-15/108

JEAN CARLOS DA SILVA NASCIMENTO

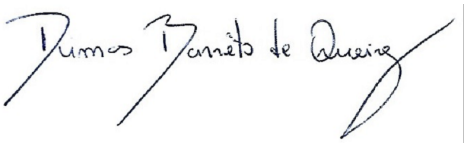
PROTEÇÃO DE DADOS: UM ESTUDO DE CASO NO TRIBUNAL DE CONTAS DO ESTADO DA PARAÍBA

Esta monografia foi julgada adequada para a obtenção do grau de Bacharel em Ciências Contábeis, e aprovada em sua forma final pela Banca Examinadora designada pela Coordenação do TCC em Ciências Contábeis da Universidade Federal da Paraíba.

BANCA EXAMINADORA

Documento assinado digitalmente
gov.br ANNA PAOLA FERNANDES FREIRE
Data: 13/06/2023 16:35:40-0300
Verifique em https://validar.iti.gov.br

Presidente(a): Profª. Dra. Anna Paola Fernandes Freire
Instituição: UFPB



Membro: Prof. Dr. Dimas Barrêto de Queiroz
Instituição: UFPB

Documento assinado digitalmente
gov.br JOSEDILTON ALVES DINIZ
Data: 15/06/2023 11:17:24-0300
Verifique em https://validar.iti.gov.br

Membro: Prof. Dr. Josedilton Alves Diniz
Instituição: UFPB

João Pessoa, 01 de junho de 2023.

DECLARAÇÃO DE AUTORIA PRÓPRIA

Eu, Jean Carlos da Silva Nascimento, matrícula n.º 20170014033, autor(a) do Trabalho de Conclusão de Curso intitulado Proteção de Dados: Um Estudo de Caso no Tribunal de Contas do Estado da Paraíba, orientado(a) pelo(a) professor(a) Anna Paola Fernandes Freire, como parte das avaliações do Curso de Ciências Contábeis no período letivo 2022.2 e requisito parcial à obtenção do grau de Bacharel(a), declaro que o trabalho em referência é de minha total autoria, não tendo sido copiado ou extraído, seja parcial ou integralmente, de forma ilícita de nenhuma fonte, além daquelas públicas consultadas e corretamente referenciadas ao longo do trabalho, obedecendo aos padrões nacionais para referências diretas e indiretas, ou daquelas cujos dados resultaram de investigações empíricas por mim realizadas para fins de produção deste trabalho. Afirmo que em hipótese alguma representa plágio de material disponível em qualquer meio, e declaro, estar ciente das penalidades previstas nos artigos 184 e 298 do Decreto-Lei n.º 2.848/1940 – Código Penal Brasileiro, como também declaro não infringir nenhum dispositivo da Lei n.º 9.610/98 – Lei dos Direitos Autorais.

Assim, se houver qualquer trecho do texto em questão que configure o crime de plágio ou violação aos direitos autorais, assumo total responsabilidade, ficando a Instituição, o orientador e os demais membros da banca examinadora isentos de qualquer ação negligente da minha parte, ou pela veracidade e originalidade desta obra, cabendo ao corpo docente responsável pela sua avaliação não aceitá-lo como Trabalho de Conclusão de Curso da Universidade Federal da Paraíba - UFPB, no Curso de Ciências Contábeis, e, por conseguinte, considerar-me reprovado no Trabalho de Conclusão de Curso.

Por ser verdade, firmo a presente.

João Pessoa, 01 de junho de 2023.

Jean Carlos da Silva Nascimento

Assinatura
do(a) discente

Documento assinado digitalmente
gov.br JEAN CARLOS DA SILVA NASCIMENTO
Data: 13/06/2023 14:57:27-0300
Verifique em https://validar.iti.gov.br

Dedico este trabalho aos meus pais José Carlos e Tânia Maria, por todo o esforço, a dedicação e o apoio em cada momento de minha vida. Agradeço também a Professora Anna Paola por todo o incentivo e orientação em prol desta pesquisa.

AGRADECIMENTOS

A Deus, pela sua bondade e infinita misericórdia e por estar sempre guiando os meus caminhos;

A mim mesmo, pela coragem extraída para concluir o presente trabalho;

Aos meus pais, por toda dedicação e amor;

Aos meus pouquíssimos amigos, sempre aptos a ajudarem.

“Só se pode alcançar um grande êxito quando nos mantemos fiéis a nós mesmos.”

Friedrich Nietzsche

RESUMO

Esta pesquisa teve por objetivo geral identificar, por meio de uma entrevista, como o Tribunal de Contas do Estado da Paraíba (TCE-PB) está se adequando às inovações proporcionadas pela Lei Geral de Proteção de Dados Pessoais (LGPD). Baseado na Lei Estadual nº 3.627 de 31 de agosto de 1970 e, segundo a Resolução Normativa TC Nº 010/2010, compete ao TCE-PB apreciar as contas prestadas anualmente pelo Governo do Estado e pelos Prefeitos Municipais, emitindo sobre elas parecer prévio, além de diversas outras competências visando o exercício das funções essenciais de controle externo. A LGPD dispõe sobre o tratamento a ser realizado quanto aos dados pessoais de pessoas físicas ou jurídicas (seja de direito público ou privado), principalmente no âmbito dos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento de cada indivíduo. No tocante à esfera pública, a LGPD estabelece em seu capítulo IV, as disposições acerca do tratamento de dados pessoais pelo poder público, determinando no caput do art. 23, que o mesmo deverá ser realizado para cumprir com a finalidade do serviço público. Após ser abordado o contexto pelo qual as entidades que integram a administração pública estão inseridas na LGPD, bem como o cenário de atuação pelo qual o TCE-PB está envolvido em nossa sociedade, merecem ser destacados os principais atos normativos publicados pelo Tribunal tendo em vista as mudanças proporcionadas pela LGPD. A Resolução Administrativa nº 07/2021 do TCE-PB, publicada no diário oficial eletrônico do tribunal no dia 22 de junho de 2021, institui a Política de Proteção de Dados Pessoais – PPDP no âmbito do órgão de contas. Ante o exposto, verifica-se, novamente, que a resolução segue em estrita observância as determinações contidas na LGPD, inclusive aquelas retromencionadas, quanto ao compartilhamento de dados pessoais pelo poder público, ser permissível somente para atender as finalidades específicas de execução de políticas públicas. Portanto, objetivando a proteção de informações sensíveis cuja titularidade pertença à pessoa natural nos termos da LGPD, o Tribunal de Contas trabalhou principalmente na camada de segurança da informação e na computação dos dados pessoais, sendo discutidas as formas de resguardar tais informações daqueles que estão inseridos em seu banco de dados.

Palavras-chave: Tribunal de Contas. LGPD. Proteção de dados.

ABSTRACT

This research had the general objective of identifying, through an interview, how the Court of Auditors of the State of Paraíba (TCE-PB) is adapting to the innovations provided by the General Law for the Protection of Personal Data (LGPD). Based on State Law No. 3627 of august 31, 1970 and, according to Normative Resolution TC No. 010/2010, it is incumbent upon the TCE-PB to assess the accounts annually by the State Government and by the Municipal Mayors, issuing a prior opinion on them, in addition to of several other competences aimed at exercising the essential functions of external control. The LGPD provides for the treatment to be carried out regarding the personal data of individuals or legal entities (whether public or private law), mainly within the scope of digital means, with the aim of protecting the fundamental rights of freedom, privacy and free development of each individual. Witch regard to the public sphere, the LGPD establishes in its chapter IV, the provisions regarding the processing of personal data by the public power, determining in the caput of art. 23, that it must be carried out to fulfill the purpose of the public service. After addressing the context in which the entities that make up the public administration are included in the LGPD, as well as the scenario in which the TCE-PB is involved in our society, it is worth highlighting the main normative acts published by the Court in view of the changes provided by the LGPD. Administrative Resolution No. 07/2021 of the TCE-PB, published in the court's official electronic journal on June 22, 2021, establishes the Personal Data Protection Policy – PPDP within the scope of the accounts body. In view of the above, it appears, again, that the resolution follows in strict compliance with the determinations contained in the LGPD, including those mentioned above, regarding the sharing of personal data by the public power, being permissible only to meet the specific purposes of implementing public policies. Therefore, aiming at the protection of sensitive information whose ownership belongs to the natural person under the terms of the LGPD, the Court of Auditors worked mainly on the information security layer and on the computation of personal data, discussing ways to safeguard such information those that are inserted in this database.

Keywords: Court of Accounts. LGPD. Data Protection.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CPF	Cadastro de Pessoa Física
DITEC	Diretoria de Tecnologia da Informação
DoS	Negação de Serviço
DDoS	Negação de Serviço Distribuída
GDPR	Regulamento Geral de Proteção de Dados
IEC	Comissão Eletrotécnica Internacional
ISO	Organização Internacional de Padronização
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
LRF	Lei de Responsabilidade Fiscal
PIMS	Sistema de Gerenciamento de Informações de Privacidade
POSICs	Políticas de Segurança da Informação e Comunicação
PPDP	Política de Proteção de Dados Pessoais
PSI	Política de Segurança da Informação
SGSP	Sistema de Gestão de Segurança Privada
TCE-PB	Tribunal de Contas do Estado da Paraíba
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
UFPB	Universidade Federal do Estado da Paraíba

SUMÁRIO

1 INTRODUÇÃO

A tecnologia da informação é um elemento indispensável para o controle e manutenção dos dados de uma organização, seja uma instituição pública ou privada. Sob essa perspectiva, Fontes (2006) afirma que a informação se constitui como algo muito maior do que um conjunto de dados. Ao transformar esses dados em informação, está transformando algo em sua forma bruta com nenhum significado, para depois de transformado, em informações vitais poderosas para a sobrevivência da organização.

Ainda segundo Fontes (2006), ao trabalhar em qualquer organização é necessário compreender que a informação é um bem valioso e precisa ser protegido.Esse bem deve ser cuidado por meio de políticas protetivas e normas, da mesma maneira que outros recursos são tratados dentro da entidade, como os recursos materiais.

Considerando esse cenário, Machado (2014) aponta que o gerenciamento desegurança inclui alguns fatores como a gestão de risco, as políticas de segurança da informação e comunicação (POSICs), assim como o treinamento de todos os funcionários envolvidos sobre a área em questão. Desse modo, seriam esses os componentes principais de qualquer programa de segurança da informação que uma entidade deveria implantar.

Além disso, existem objetivos que compõem um programa de segurança, nos quais se baseiam na identificação dos ativos de informação da entidade, desenvolvimento e implementação de políticas de segurança, tal como procedimentos, normas e diretrizes, que devem proporcionar integridade, confidencialidade e disponibilidade da informação (MACHADO, 2014).

As instituições públicas são movidas pelo objetivo primordial de prestar serviços à sociedade, portanto necessitam cada vez mais de um controle informacional mais efetivo, visando garantir a probidade das informações disponibilizadas a todos os cidadãos. Destarte, atualmente e em tempos futuros, a área da tecnologia da informação vai se constituindo cada vez mais como um dos principais pilares que sustentam a gestão do conhecimento. (KANAANE; FIEL FILHO; FERREIRA, 2010, p. 104).

Com o advento da Lei Federal nº 13.709/18, conhecida como a Lei Geral de Proteção de Dados Pessoais – LGPD, o Brasil passou a integrar o rol de países que sancionaram legislações específicas objetiva visando a proteção dos dados de seus cidadãos (SEBRAE, 2021). Observa-se em seu art.1º, que a lei supracitada abrange não somente pessoas físicas, como também quaisquer pessoas jurídicas, sejam de direito público ou privado, *ipsis litteris*:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Por fim, salienta-se que dentre as instituições públicas inseridas no cenário do Estado da Paraíba, foi escolhido o respectivo Tribunal de Contas do Estado (TCE-PB) como o local a ser estudado, visando correlacionar as determinações contidas na LGPD com as medidas implementadas pelo Tribunal, principalmente no tocante a proteção de dados pessoais.

Ante o exposto, este trabalho foi realizado por meio da construção de um estudo de caso visando identificar e descrever as principais medidas que foram implementadas pelo Tribunal de Contas do Estado da Paraíba (TCE-PB), em face da observância as determinações contidas na LGPD, objetivando, portanto, a conformidade com tais inovações que representam um marco no ordenamento jurídico brasileiro.

1.1 PROBLEMA DE PESQUISA

O presente estudo parte da necessidade de identificar e analisar a adequação do TCE-PB com relação as inovações trazidas pela Lei Geral de Proteção de Dados Pessoais (LGPD), visando a segurança das informações administradas pela organização, além de evidenciar a existência de políticas de segurança de dados implementadas no âmbito do colendo órgão.

Para analisar tais fenômenos, foi escolhido como local de pesquisa, como já fora mencionado, o TCE-PB, órgão instituído pela Lei Estadual nº 3.627 sancionada em 31 de agosto de 1970. Segundo a Resolução Normativa TC 010/2010, compete ao TCE-PB apreciar as contas prestadas anualmente pelo Governador do Estado e pelos Prefeitos Municipais, emitindo sobre elas parecer prévio, além de diversas

outras competências visando o exercício das funções essenciais de controle externo.

Desse modo, o TCE-PB, assim como qualquer outro tribunal de contas existente no país, exerce um papel crucial para a manutenção e o equilíbrio das contas públicas, sendo os auditores públicos responsáveis pela fiscalização dos gastos executados pela administração direta e indireta.

Segundo Mattos (2017), a origem da auditoria pública está relacionada as atitudes que a administração pública exerce no que se diz respeito ao controle da arrecadação de tributos e a destinação desses recursos. Diante desta situação, o papel desempenhado pelo tribunal não deve ser interferido por consequências de ataques de *hackers* ou falhas nos procedimentos de segurança.

Analisando o contexto apresentado, uma entidade de vital importância para a fiscalização da administração pública deve continuamente avaliar seus métodos de segurança e controle, de modo a garantir a produtividade e a minimização dos riscos a segurança dos dados. Dessa forma, o presente estudo de caso se propõe a reunir informações com o objetivo de responder o seguinte problema: **Como o Tribunal de Contas do Estado da Paraíba (TCE-PB) está se adequando às inovações proporcionadas pela Lei Geral de Proteção de Dados Pessoais (LGPD)?**

1.2 OBJETIVOS

1.2.1 Objetivo geral

Identificar como o Tribunal de Contas do Estado da Paraíba (TCE-PB) está se adequando às inovações proporcionadas pela Lei Geral de Proteção de Dados Pessoais (LGPD).

1.2.2 Objetivos específicos

a) Conhecer a percepção do TCE-PB sobre a importância da LGPD;

b) Descrever as políticas de segurança da informação e dados pessoais implementadas pelo TCE-PB;

c) Verificar se tais medidas em segurança da informação adotadas estão sendo observadas no cotidiano do egrégio Tribunal.

1.3 JUSTIFICATIVA

A importância da tecnologia da informação e os investimentos exercidos nessa área são fatores exponencialmente discutidos e relevantes para uma organização. Relacionando com o funcionalismo público, essa percepção está presente inclusive no Tribunal de Contas da União (TCU), que divulgou diversos manuais sobre a área. Desde o guia de boas práticas em contratação de soluções em TI, a até mesmo o manual de boas práticas em segurança da informação, percebe-se uma grande preocupação do maior órgão de auditoria pública do país em estabelecer um enfoque no aperfeiçoamento da boa conduta em gestão da informação e seus afins.

Nesta seara, para um órgão indispensável no que se diz respeito ao controle externo e fiscalização da administração pública, como o TCE-PB, um setor de TI bem como um núcleo de gestão e governança em TI, são essenciais para o controle exercido sobre os sistemas e os dados recebidos, do mesmo modo em que a manutenção das práticas e políticas de segurança da informação são desenvolvidas e aperfeiçoadas.

Dado a relevância e a atualidade do tema abordado, a segurança da informação em uma entidade consiste no conjunto de informações, normas, procedimentos técnicos e demais ações que possuem como finalidade proteger o principal recurso de uma organização que é a informação (FONTES, 2006). Ainda segundo o autor, essa segurança é de vital importância, representando um meio para que a entidade cumpra a sua missão e alcance os seus objetivos.

Outrossim, a Lei Federal nº 13.709/18 conhecida como LGPD, passou a ser um marco no ordenamento jurídico do país, proporcionando inovações acerca do tratamento de dados pessoais, preservando a privacidade dos mesmos e exigindo dos setores públicos e privados, medidas baseadas em princípios sólidos, e que de fato, protejam a privacidade dos dados dos titulares (LIMA; CRESPO; PINHEIRO, 2021).

Ainda segundo os autores, desde que a referida lei foi sancionada, surgiram inúmeros desafios às entidades públicas e privadas, sendo necessária como consequência, a adoção de medidas que visam a conformidade, devendo portanto, identificar com base na supracitada lei, seus papéis e responsabilidades, além dos meios apropriados e necessários para cumpri-la em sua totalidade.

Com os resultados do estudo de caso desenvolvido, espera-se um maior incentivo na produção de pesquisas com abordagem qualitativa, de modo a propiciar soluções de fenômenos complexos dentro de uma determinada realidade. Além do mais, a presente pesquisa agregará valor ao curso de Ciências Contábeis da Universidade Federal da Paraíba (UFPB), à medida que inspirar diversos outros estudos sobre tecnologia da informação, uma área cada vez mais atuante e necessária no contexto de organizações públicas ou privadas.

2 FUNDAMENTAÇÃO TEÓRICA

O objetivo desta seção consiste em apresentar os principais temas da pesquisa, bem como a relação teórica entre ambos os fatos abordados. Desse modo, procura-se discorrer sobre os seguintes assuntos: segurança da informação, políticas de segurança da informação, normas ISO/IEC 27000, auditoria no setor público, a ameaça proveniente dos ataques cibernéticos junto ao TCE-PB, bem como as principais medidas adotadas pelo Tribunal com vistas a adequar-se diante da LGPD.

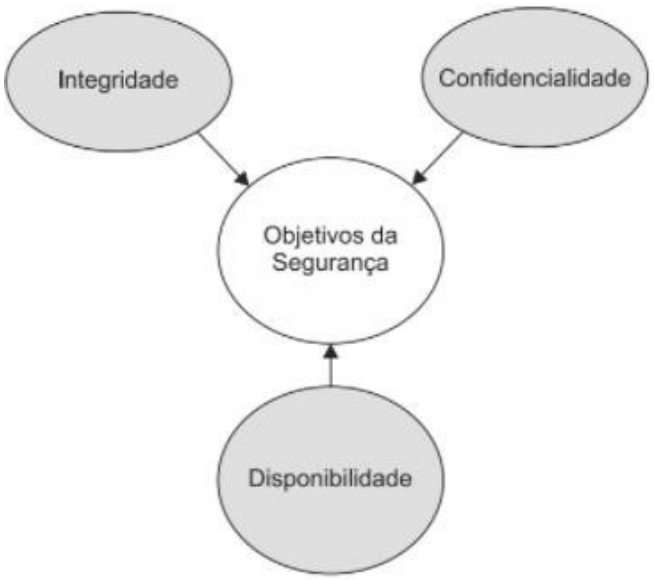
2.1 SEGURANÇA DA INFORMAÇÃO: ASPECTOS FUNDAMENTAIS

De acordo com Ramos et al. (2018), a segurança da informação consiste na proteção de um complexo de dados existentes dentro de uma entidade. Desse modo, esse conceito de segurança serve para garantir a proteção da informação contra vários tipos de ameaças, de forma a garantir a continuidade das atividades. Além disso, a segurança da informação pode ser caracterizada como um conjunto de normas, orientações, procedimentos e políticas necessárias visando proteger esse importante recurso que é a informação (FONTES, 2006).

Segundo o autor, proteger a informação significa assegurar alguns princípios essencialmente importantes, como: disponibilidade, integridade, confidencialidade, legalidade, auditabilidade e o não repúdio de autoria. O primeiro princípio representa a acessibilidade que a informação deve manter para o bom funcionamento da organização, podendo ser consultada sem mais delongas para o alcance de seus objetivos.

A integridade está relacionada a informação ser verdadeira e não corrompida ou adulterada, ou seja, sendo uma informação íntegra e correta. O terceiro princípio significa que o acesso e a utilização de uma determinada informação dever ser realizada por aqueles que necessitam unicamente dela, evitando o vazamento de algum conteúdo confidencial (FONTES, 2006). De acordo com Machado (2014), os três princípios mencionados anteriormente correspondem a chamada tríade CIA, representando pilares centrais existentes em todo e qualquer programa de segurançada informação.

Figura 1 - CIA, a tríade de segurança



Fonte: MACHADO (p. 13, 2014).

Compreendo os princípios relacionados à segurança da informação, pode-se visualizar ainda mais a importância de se proteger esse recurso tão valioso para uma organização. Nesse contexto, o TCU aponta o porquê da importância de se zelar pela segurança de informações:

> Porque a informação é um ativo muito importante para qualquer instituição, podendo ser considerada, atualmente, o recurso patrimonial mais crítico. Informações adulteradas, não disponíveis, sob conhecimento de pessoas de má-fé ou de concorrentes podem comprometer significativamente, não apenas a imagem da instituição perante terceiros, como também o andamento dos próprios processos institucionais. É possível inviabilizar a continuidade de uma instituição se não for dada a devida atenção à segurança de suas informações. (TRIBUNAL DE CONTAS DA UNIÃO, 2012, pag. 10).

Zanon (2014) aponta que a segurança da informação, segundo a Associação Brasileira de Normas Técnicas (ABNT ISO/IEC 27002:2005), consiste na proteção da informação contra vários tipos de ameaças, visando garantir a continuidade do negócio e minimizando os riscos, proporcionando a maximização do retorno sobre os investimentos e as oportunidades. Vale salientar que a referida norma menciona a relação entre a segurança dainformação e os princípios abordados anteriormente.

Para Rios, Teixeira Filho e Rios (2017), nesse processo de segurança da informação, as organizações necessitam da implementação de uma política de

segurança da informação (PSI), sendo esta utilizada para descrever os procedimentos necessários para a proteção de seus recursos informacionais, contra a divulgação indevida e outros fatores que comprometem os princípios discutidos, através da implantação de controles de segurança.

O TCU (2012) remete a definição sobre a política de segurança da informação:

> Política de segurança de informações é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações. (TRIBUNAL DE CONTAS DA UNIÃO, 2012, pag.10)

Além do mais, é recomendado pelo próprio TCU, a existência na estrutura de uma instituição, uma área responsável pela segurança das informações, sendo essa responsável por iniciar o processo de elaboração da política de segurança da informação, assim como orientar todo o processo de implantação e designando funções de segurança (TCU, 2012).

2.2 NORMAS ISO/IEC 27000

A ABNT é a única representante da Organização Internacional de Normalização, mais conhecida como ISO, aqui no Brasil, representando a posição de diversos setores brasileiros na elaboração de normas internacionais (ABNT, 2014). O próprio TCU utiliza normas da ABNT como padrão em suas auditorias de segurança da informação, conforme pode-se ver:

> Além do reconhecimento da ABNT, como instituição normalizadora brasileira, as instituições internacionais ISO e IEC (*International Eletrotechnical Commission*), autoras da norma, são mundialmente reconhecidas pela capacitação técnica. A norma ISO/IEC 27002:2005, equivalente à norma brasileira, é amplamente reconhecida e utilizada por Entidades Fiscalizadoras Superiores, órgãos de governo, empresas públicas e privadas nacionais e internacionais atentas ao tema Segurança da Informação. (TRIBUNAL DE CONTAS DA UNIÃO, 2012, pag. 38).

Ante o exposto, cabe salientar que a Organização Internacional para Padronização (ISO), consiste em uma organização não governamental e

independente, tendo como finalidade desenvolver e promover normas e padronizações que abrangem diversos segmentos da sociedade, além de facilitar as relações entre nações diferentes. (PUCPR, 2021)

Dentre tais normas, pode-se ressaltar a família ISO/IEC 27000, sendo um conjunto de normas relacionadas a segurança da informação e proteção de dados em uma organização, assim como todos os elementos envolvidos. Desse modo, as normas que compreendem esse conjunto, podem ser aplicadas tanto em entidades públicas como privadas, servindo como base para a criação e a implementação de um Sistema de Gestão em Segurança da Informação (SGSI).

Conforme a PUCPR (2021), as certificações ora tratadas por esse conjunto de normas, foram desenvolvidas em parceria entre a ISO e a Comissão Eletrotécnica Internacional (IEC), outra entidade internacionalmente conhecida para fins de padronização, porém voltada às temáticas relacionadas a energia, multimídia, telecomunicações e afins.

Logo adiante, serão abordadas as normas mais conhecidas desse conjunto relacionado à seara em estudo, no qual atualmente são compostas por 45 (quarenta e cinco) normas.

2.2.1 ISO/IEC 27000:2018 - Visão geral

A primeira norma deste grupo consiste na ISO/IEC 27000:2018, atualizada no ano de 2018, que representa uma visão geral sobre o conceito de segurança da informação, assemelhando-se a algo conhecido como *framework.* Essa norma atua como uma introdução, demonstrando um glossário de termos que serão abordados nas certificações subsequentes (OSTEC, 2019).

Segundo a ABNT, existem mais de uma dúzia de normas que compreendem esse grupo, no entanto, a ISO/IEC 27000:2018 fornece uma compreensão de como os padrões se enquadram, os escopos, papéis, funções e relacionamentos uns com os outros. De acordo com essa norma, denominada Tecnologia da Informação, Técnicas de Segurança, Sistemas de Gestão de Segurança da Informação, Visão Geral e Vocabulário, tem-se que a segurança da informação consiste na preservação da confidencialidade, integridade e disponibilidade da informação, estabelecendo umaconexão com Machado (2014).

De acordo com a ISO/IEC 27000:2018, observa-se que “[...] este documento

é aplicável a todos os tipos e tamanhos de organização (por exemplo, empresas comerciais, agências governamentais, organizações sem fins lucrativos).” Com isso, tem-se a confirmação sobre a possibilidade da utilização dessa norma em diversas entidades, sejam públicas ou privadas, incluindo também as organizações que compreendem o chamado terceiro setor.

2.2.2 ISO/IEC 27001:2022

A segunda norma tratava-se da ISO/IEC 27001:2013 que dispõe sobre os requisitos necessários para que exista um sistema de gestão da segurança da informação, o SGSI. Esse sistema representa uma parte essencial para a gestão em uma organização, agindo como a principal norma que uma entidade deve utilizar para possuir a certificação em segurança da informação (OSTEC, 2019).

Não obstante, cabe ressaltar que a norma ISO/IEC 27001:2013 foi revisada recentemente, no ano de 2022, alterando sua nomenclatura para ISO/IEC 27001:2022 (publicada em outubro do referido ano). As principais alterações nessa certificação, conforme o *British Standards Institution* (2022), estão relacionadas ao Anexo A da mesma, refletindo as mudanças que foram realizadas na ISO/IEC 27002:2022:

- A estrutura foi consolidada em 04 (quatro) áreas-chaves:

  Organizacional, Pessoal, física e Tecnológica ao invés de 14 na edição anterior.

- Os controles listados diminuíram de 114 para 93:

  Alguns controles foram fundidos, outros foram removidos, novos foram introduzidos e outros atualizados.

- O conceito de atributos foi introduzido:

Alinhados com a terminologia comum utilizada dentro da segurança digital, estes 05 (cinco) atributos compreendem os seguintes: Tipos de controle, propriedades de segurança da informação, Conceitos de segurança cibernética, Capacidades operacionais e Domínios de segurança.

Outrossim, ainda segundo a *British Standards Institution* (2022), houve mudanças na norma para que ela pudesse se alinhar com a abordagem harmonizada da ISO, *in verbis*:

- Reestruturação da numeração;

- Necessidade de definir os processos necessários para a implementação do SGSI e suas interações;
- Exigência explícita de comunicar funções organizacionais relevantes para a segurança da informação dentro da organização;
- Nova cláusula 6.3 – Planejamento de mudanças;
- Nova exigência para garantir que a organização determine como se comunicar, como parte da cláusula 7.4; e
- Novos requisitos para estabelecer critérios para processos operacionais e implementar o controle dos processos.

No escopo da ISO/IEC 27001:2022, pode-se compreender que: “Esta norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação no contexto da organização.” Observa-se que o próprio escopo da norma evidencia claramente que os requisitos estabelecidos no referido documento são genéricos e a sua aplicabilidade pode ser destinada a todas as organizações, independentemente do tipo, dimensão ou natureza.

Além do mais, pode-se visualizar os requisitos para a avaliação e o tratamento dos riscos em segurança da informação que uma organização está sujeita a apresentar. Esses riscos demonstrados pela 27001 foram ajustados com base nas necessidades da organização.

Como a norma dispõe sobre os requisitos caso haja um SGSI, tem-se que um sistema de segurança da informação é amplo e compreende diversas ações de segurança operacional, física e lógica. A política de segurança e o sistema devem ser formulados em conjunto pela administração da organização e por especialistas na área de TI (ZANON, 2014).

2.2.3 Políticas de segurança da informação e a ISO/IEC 27002:2022

Retomando a discussão sobre políticas de segurança da informação (PSI) observada ao tópico 2.1 deste trabalho, o sucesso de uma PSI, conforme TCU (2012), está relacionado a participação da alta administração da organização. Quanto maior for o envolvimento e o comprometimento da alta cúpula, maior a probabilidade da política ser implementada de forma efetiva e eficaz. A participação não cabe apenas a um setor específico responsável pela questão, mas a gestão deve-se fazer presente

na elaboração e implantação de uma PSI.

Existem normas sobre a PSI na administração pública, como por exemplo o Decreto presidencial n° 9.637/2018, que revogou o até então decreto n°3.505/2000, mencionado pelo TCU em seu manual de boas práticas em segurança da informação. O Decreto n° 9.637/2018 dispõe sobre a política nacional de segurança da informação, bem como a governança em segurança da informação. Com isso, é possível perceber a preocupação do governo federal em estabelecer normas sobre um aspecto ainda pouco explorado, porém de importância imensurável para o bom funcionamento da administração pública.

O próprio TCU utiliza normas ABNT, como fora citado, para auxiliar no comprometimento a segurança da informação e a proteção necessária para os seus dados. Especificamente observa-se a utilização da norma ISO/IEC 27002:2013, que revogou a ISO/IEC 27002:2005. Segundo a versão mencionada tem-se que:

> Esta Norma Internacional fornece diretrizes para padrões de segurança da informação organizacional e práticas de gerenciamento de segurança da informação, incluindo a seleção, implementação e gerenciamento de controles, levando em consideração o (s) ambiente (s) derisco de segurança da informação da organização. (ISO/IEC 27002:2013).

Conforme a norma, esta certificação foi projetada para organizações que pretendem selecionar os controles dentro de um SGSI, baseado na anterior (27001), bem como implementar controles de segurança da informação e o desenvolvimento das próprias diretrizes organizacionais. Todos esses elementos estão inseridos na PSI, tendo em vista que a 27002:2013 funciona como um código de práticas para a gestão da segurança da informação (TCU, 2012).

No entanto, assim como a 27001 passou por um processo de revisão resultando em sua versão mais recente, publicada tão somente no mês de outubro, a 27002 também passou pelo referido processo, sendo atualizada meses antes. Dessa forma, em fevereiro de 2022 foi publicada a norma ISO/IEC 27002:2022, na qual podemos visualizar em seu *abstract*, que:

> Este documento fornece um **conjunto de referência de controles genéricos de segurança da informação, incluindo orientação de implementação**. Este documento foi concebido para ser utilizado por organizações:
> a) No contexto de um sistema de gerenciamento da informação (ISMS) baseado na ISO/IEC 27001;
> b) Pela implementação de controles de segurança da informação

> baseados nas melhores práticas reconhecidas internacionalmente;
> c) Para o desenvolvimento de diretrizes de gerenciamento de segurança da informação específicas da organização. (grifo nosso).

Nesse cenário, compreende-se que a ISO/IEC 27002:2022 funciona como um código de prática para controles de segurança da informação, detalhando as melhores formas para as organizações implementarem um SGSI.

Não obstante, cabe ressaltar as principais alterações advindas da mais recente atualização da 27002:2022, resultando na publicação da mesma do mês de fevereio de 2022. Nesse contexto, conforme a *PMGacademy* (2022), em primeiro lugar tem-se a alteração no nome da norma, na qual passou de “Tecnologia da informação, Técnicas de segurança, Código de prática para controles de segurança da informação” para “Segurança da Informação, Segurança Cibernética e Proteção à Privacidade, Controles de Segurança da Informação.”

Além do mais, por meio dessa grande atualização, observa-se que o tamanho da norma aumentou significativamente, passando de 88 páginas para 164 páginas (PMGacademy, 2022). Por fim, vale destacar a inclusão de alguns controles para casos específicos relacionados a seara em discussão (segurança da informação), sendo eles:

- Inteligência de ameaças (compreensão lógica das ameaças);
- Segurança da informação para uso de serviços em nuvem;
- Prontidão da TIC para continuidade de negócios;
- Monitoramento de segurança física;
- Gerenciamento de configurações;
- Exclusão de informações;
- Mascaramento de dados;
- Prevenção de vazamento de dados;
- Atividades de monitoramento;
- Filtragem da web;
- Codificação segura.

2.2.4 ISO/IEC 27003:2017 – Implantação de um SGSI

Por fim, outra norma bastante conhecida desse grupo trata-se da ISO/IEC 27003:2017 (atualizada no referido ano), responsável por apresentar um conjunto de

diretrizes para adoção de um SGSI. Essa certificação serve como um guia detalhado relacionado a implantação de um sistema de gestão em segurança da informação em uma organização, fornecendo orientações (OSTEC, 2019).

De acordo com esta norma, ainda vigente no ano de 2022, são dadas instruções referentes aos requisitos apresentados ainda na ISO/IEC 27001:2013, sobre a existência de um SGSI, bem como recomendações, possibilidades e permissões em relação a esses requisitos. Observando o seu escopo, percebe-se, claramente, o objetivo da norma, sendo utilizada para fornecer explicações e orientações acerca da 27001 (ISO/IEC 27003:2017).

Segundo Ramos et al. (2017), o conjunto de normas que compreendem a família ISO/IEC 27000 orientam principalmente sobre o SGSI. Esse sistema é tratado como uma forma de segurança para todos os tipos de dados em uma organização, sendo que os seus principais benefícios são:

- Estabelecimento de uma metodologia clara e concisa sobre a gestão em segurança da informação;
- Reduzir o risco ou qualquer fraude relacionada a informação;
- O acesso restrito a informação por meio das medidas de segurança;
- Confiança e regras para todos os integrantes da organização; e
- Os riscos e os controles relacionados a estes são verificados continuamente.

2.2.5 ISO/IEC 27701:2019

Segundo a PUCPR (2021), a certificação ora apresentada foi implantanda no ano de 2019 para adequar as normas à *General Data Protection Regulation* (GDPR), enquanto no Brasil, já se encontrava em vigor a Lei Federal nº 13.709/18 (LGPD).

Conforme o escopo da norma, nota-se que a 27701:2019 especifica os requisitos e fornece orientação para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gerenciamento de Informações de Privacidade (PIMS) na forma de uma extensão da ISO/IEC 27001 e ISO/IEC 27002, para gerenciamento de privacidade no contexto da organização.

Em face ao exposto, a norma ISO/IEC 27701:2019 consiste, em verdade, em uma extensão da 27001:2022, sendo que esta última, como já vimos, está

relacionada ao Sistema de Gestão em Segurança da Informação (SGSI), enquanto a primeira trata sobre o Sistema de Gestão de Segurança Privada (SGSP), ou em inglês, *Privacy Information Management System* (PIMS). Por fim, vale salientar que a ISO/IEC 27701:2019 fornece novos mecanismos de controle para a segurança da informação, visando a proteção da privacidade dos dados pessoais.

2.3 RISCOS À SEGURANÇA DA INFORMAÇÃO

Segundo Machado (2014), as ameaças estão relacionadas às falhas de segurança, que são os pontos fracos do *hardware* e *software* dos computadores, que por consequência acarretam perdas na organização. Essas ameaças exploram as fragilidades dos sistemas de informação para causar danos, assim como um assaltante fica a espreita esperando por uma oportunidade para cometer o roubo.

De acordo com o autor, existem vários tipos de ameaças fundamentais aos sistemas de informação, comprometendo os princípios de segurança. O Quadro 1 demonstra os quatro tipos dessa classificação:

Quadro 1 – Ameaças fundamentais

VAZAMENTO DE INFORMAÇÕES	Esse vazamento pode ocorrer de forma voluntária ou involuntária. Voluntária por ser realizada a partir de pessoas mal-intencionadas e involuntária devido a falhas de hardware, software, dentre outros.
VIOLAÇÃO DE INTEGRIDADE	Representa o comprometimento da consistência dos dados ou do sistema por intermédio de alterações não autorizadas de dados.
INDISPONIBILIDADE DE SERVIÇOS DE TI	Trata-se do impedimento deliberado do acesso aos recursos computacionais por usuários autorizados ou não.
ACESSO E USO NÃO AUTORIZADO	Essa ameaça acontece quando um recurso de algum sistema, site ou rede é utilizado por uma pessoa não autorizada ou de forma não autorizada.

Fonte: Elaboração própria (2021) a partir de Machado (2014).

Relacionado à ameaça de indisponibilidade dos serviços de informática, existem os ataques *Denial of Service* (DoS), que comprometem a integridade dos sistemas de informação por meio de ataques para causar negação de serviços a um site em específico. Esses ataques são uma maneira de impedir que o usuário tenha dificuldade ou seja impedido de acessar o site em seu computador (MACHADO, 2014).

Além desses ataques DoS, existem também os ataques *Distributed Denial of Service* (DDoS), consistindo em uma ameaça de maior escala. No DDos, o *hacker* pode utilizar vários computadores infectados que atuam como zumbis, para atacar determinado servidor no qual estão as páginas do site de uma entidade (MACHADO, 2014).

Desse modo, a maior ameaça que pode comprometer o trabalho em uma instituição pública como o tribunal de contas, seria um ataque externo como o DoS ou o DDoS, impedindo que os servidores do órgão acessem os sistemas e executem as suas tarefas. Como as informações do TCE-PB são divulgadas publicamente, por se tratar de um ente público, não há risco com relação a um banco de dados de acesso restrito como seria no caso de organizações do setor privado. Sendo assim, os ataques externos provocados por *hackers* comprometem no desempenho e no cumprimento dos objetivos da instituição em questão.

2.4 LEI FEDERAL Nº 13.709/18 – LGPD

Como já fora mencionado ao longo do presente estudo, a LGPD dispõe sobre o tratamento a ser realizado quanto aos dados pessoais de pessoas físicas ou jurídicas (seja de direito público ou privado), principalmente no âmbito dos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento de cada indivíduo (BRASIL, 2018).

De acordo com Sousa, Barrancos e Maia (2019), a LGPD apresenta em seu art. 5º, a definição de dados pessoais como sendo toda a informação referente à pessoa natural identificada ou que possa ser identificável, no qual o titular da informação seria tal pessoa a quem estão relacionados os dados pessoais que são objetos de tratamento. Desse modo, qualquer pessoa natural tem garantida a titularidade de seus dados pessoais, assim como os direitos fundamentais de liberdade, intimidade e privacidade.

Ainda segundo os autores, da mesma forma que a pessoa jurídica de direito privado deve se atentar a finalidade da transparência quanto à proteção dos dados, o tratamento de dados pessoais a ser realizado pelas entidades do setor público, deve atender ao interesse público e a finalidade da coisa pública, com o objetivo de desempenhar as competências exigidas por lei e cumprir com as atribuições legais do serviço público, conforme explicitado no art. 23 da LGPD.

No tocante à esfera pública, a LGPD estabelece em seu capítulo IV, as disposições acerca do tratamento de dados pessoais pelo poder público, determinando no caput do art. 23, que o mesmo deverá ser realizado para cumprir com a finalidade do serviço público, *ipsis litteris*:

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , **deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público**, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público (...) (grifo nosso)

Nesse contexto, ressalta-se que no capítulo supracitado, a lei estabelece que os dados deverão ser mantidos em formato interoperável (capaz de se comunicar de forma transparente com outro sistema) e, ao mesmo tempo, estruturado para o uso compartilhado, visando à execução de políticas públicas, bem como à prestação de serviços públicos e à descentralização da atividade pública, juntamente com o acesso das informações pelo público em geral (BRASIL, 2018).

Outrossim, conforme o art. 26, a lei prevê que o uso compartilhado dos dados pessoais pelo poder público, deve atender estritamente ao cumprimento de finalidades específicas de execução de políticas públicas e atribuição legal pelos demais órgãos e entidades que compõem o serviço público.

Não obstante, o artigo supramencionado também dispõe sobre os casos específicos nos quais o poder público, poderá transferir a entidades do setor privado, dados pessoais constantes de base de dados a que tenha acesso, *in verbis*:

> § 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:
>
> I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) ;
>
> III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.
>
> IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou
>
> V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades (BRASIL, 2018).

Ademais, vale também mencionar a existência das figuras dos 03 (três) agentes envolvidos nos tratamentos de dados pessoais, conforme a LGPD. Segundo informações constantes no portal do TCU, a referida lei estabelece a definição de três membros relacionados com o tratamento de dados, sejam eles o controlador, o operador, e o encarregado.

Conforme o TCU, o primeiro agente (controlador), pode ser uma pessoa natural ou jurídica, seja de direito público ou privado, responsável pelo processo decisório quanto ao tratamento dos dados. O operador, no entanto, consiste no agente que realiza o tratamento de dados pessoais em nome do controlador, enquanto que o encarregado trata-se de uma pessoa encarregada pelo controlador e pelo operador para atuar como um meio de comunicação entre as figuras do controlador, dos titulares dos dados envolvidos, e da Autoridade Nacional de Proteção de Dados.

Em face aos elementos ora apresentados, observados diretamente na própria legislação regente, destaca-se a importância e a relevância da mesma para o tema do presente estudo: a Segurança da Informação, estando nela inclusa a Segurança Cibernética, ambas como fatores cruciais para a adequada proteção dos dados pessoais (LIMA; CRESPO; PINHEIRO, 2021).

Conforme os autores, observa-se que no cenário atual, a maioria dos dados pessoais estão armazenados no ambiente digital, sendo necessária a atenção especial dos controladores quanto a qualidade dos recursos em TI disponíveis para a entidade e acerca das ferramentas computacionais adequadas para reforçar a segurança a esse bem tão valioso, reduzindo as vulnerabilidades, para justamente fazer frente às ameaças que rondam o meio cibernético.

Para tanto, a Lei Federal nº 13.709/18 estabelece em seus artigos 46 ao 51, as disposições quanto à segurança e as boas práticas requisitadas para os agentes de tratamento de dados, inclusive quanto a permissividade concedida aos controladores e operadores em estabelecer regras de boas práticas e políticas que salvaguardem os dados pessoais em uma organização.

2.5 TRIBUNAL DE CONTAS DO ESTADO DA PARAÍBA

Para que se possa compreender qual o envolvimento do TCE-PB com a LGPD, primordialmente faz-se necessário a apresentação sobre o papel e a

relevância do egrégio Tribunal no contexto da fiscalização das contas públicas.

As atribuições que envolvem o TCE-PB sãodiversas, nas quais encontra-se em sua própria página institucional a dimensão do trabalho executado em serviço à sociedade.

Segundo o TCE-PB,compete a instituição acompanhar a gestão, fiscalizar e analisar os processos de prestação de contas, dentre outros relatórios, de pelo menos 59 órgãos da administração estadual; 20 secretarias; 10 autarquias; 09 fundações; 12 sociedades de economia mista; 04 empresas públicas; 15 fundos; 06 órgãos em regime especial, além é claro, das 223 prefeituras municipais que compõem o Estado da Paraíba.

Considerando o cenário apresentado, a Constituição Estadual em sua seção VIII, dispõe sobre a fiscalização contábil, financeira e orçamentária do estado, delegando as competências do TCE-PB dentre outras providências, bem como a composição dos sete conselheiros responsáveis.

Especificamente em seu art. 71, vislumbra-se que compete ao tribunal de contas apreciar as contas prestadas anualmente pelo governador do Estado, assim como julgar as contas dos administradores e demais responsáveis por dinheiro, bens e valores públicos dos três Poderes, da administração direta e indireta, incluídas as fundações e sociedades instituídas e mantidas pelo Poder Público Estadual, e as contas daqueles que derem causa a perda, extravio ou outra irregularidade de que resulte prejuízo ao erário.

Dentre outras competências, observa-se que é assegurado ao tribunal de contas autonomia administrativa e financeira, conforme disposto no art. 73 da Constituição Estadual, remetendo este à Constituição Federal:

> Art. 96. Compete privativamente:
> I - aos tribunais:
> a) eleger seus órgãos diretivos e elaborar seus regimentos internos, com observância das normas de processo e das garantias processuais das partes, dispondo sobre a competência e o funcionamento dos respectivos órgãos jurisdicionais e administrativos; (...) (CONSTITUIÇÃO, 1988)

A Lei Complementar N°101/2000, conhecida como lei de responsabilidade fiscal (LRF), também dispõe sobre o papel desempenhado pelos tribunais de contas. Ao decorrer do art. 56, temos que: “As contas prestadas pelos Chefes do Poder Executivo incluirão, além das suas próprias, as dos Presidentes dos órgãos dos

Poderes Legislativo e Judiciário e do Chefe do Ministério Público, referidosno art. 20, as quais receberão parecer prévio, separadamente, do respectivo Tribunal de Contas" (BRASIL, 2000).

2.6 RESOLUÇÃO ADMINISTRATIVA RA-TC Nº 07/2021

Após ser abordado o contexto pelo qual as entidades que compõem a administração pública estão inseridas na LGPD, bem como o cenário de atuação no qual o TCE-PB está envolvido em nossa sociedade, merecem ser destacados na presente oportunidade os principais atos normativos publicados pelo tribunal tendo em vista as mudanças proporcionadas por esta lei que representa um marco para área de segurança da informação.

A Resolução Administrativa nº 07/2021 do TCE-PB, publicada no diário oficial eletrônico do tribunal no dia 22 de junho de 2021, institui a Política de Proteção de Dados Pessoais – PPDP no âmbito do colendo órgão de contas.

Observa-se em sua primeira consideração, que a referida resolução foi elaborada tendo em vista a necessidade do tribunal em estabelecer mecanismos visando o tratamento de dados pessoais, conforme as exigências da LGPD, *ipsis litteris*:

> A imprescindibilidade de prover o Tribunal de Contas do Estado da Paraíba de mecanismos de tratamento e proteção de dados pessoais dos cidadãos e de seus jurisdicionados para manter as informações íntegras, autênticas, disponíveis e, quando for o caso, sigilosas ou com acesso restrito, nos termos da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei Nacional n.º 13.709, de 14 de agosto de 2018).

Desse modo, constata-se ao art. 1º, §1º, que a PPDP do tribunal possui como fundamento a LGPD (Lei Nacional n.º 13.709, de 14 de agosto de 2018), a Lei de Acesso à Informação – LAI (Lei Nacional n. 12.527, de 28 de novembro de 2011), o Marco Civil da Internet (Lei Nacional n. 12.965, de 23 de abril de 2014), os regramentos da ABNT NBR ISO que forem aplicáveis, o Regimento Interno do Tribunal de Contas do Estado da Paraíba (RN-TC nº 10/2010), e os demais instrumentos normativos da instituição.

Ademais, no art. 2º da resolução, observar-se a abrangência da política em destaque, na qual regula a proteção de dados pessoais nas atividades jurisdicionais e administrativas do Tribunal, alcançando todos os relacionamentos institucionais

com usuários de seus serviços, inclusive servidores, contratados, fornecedores e terceiros, abrangendo a totalidade dos dados pessoais contidos em todos os suportes físicos ou eletrônicos, ou de qualquer contratado pelo TCE-PB.

Outro ponto que merece ser destacado, está contido no art. 4, no qual dispõe sobre os dados pessoais tratados pelo tribunal, *in verbis*:

> Art. 4º. Todos os dados pessoais tratados pelo Tribunal de Contas devem ser:
>
> I. protegidos por procedimentos internos de rastreabilidade, com trilhas auditáveis que registrem autorizações, utilizações, impactos e violações;
>
> II. mantidos exatos, adequados e atualizados, devendo as neutralizações ou descartes observar as condições e períodos legais de retenção de dados;
>
> III. compartilhados somente para os exercícios das funções de políticas públicas aplicáveis, sempre com a ressalva de cumprimento da LGPD pelo recebedor.
>
> Parágrafo único. A nenhum membro ou servidor do Tribunal, no exercício de suas competências, pode ser negado o acesso a dados que entenda necessários para o desempenho dos controles interno ou externo, bem assim para as atividades administrativas (RA-TC Nº 07/2021).

Ante o exposto, verifica-se, novamente, que a resolução segue em estrita observância as determinações contidas na LGPD, inclusive aquelas retromencionadas, quanto ao compartilhamento de dados pessoais pelo poder público, ser permissível somente para atender as finalidades específicas de execução de políticas públicas:

> Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei (BRASIL, 2018).

Além dos fatos ora apresentados, salienta-se que conforme o art. 6º da RN-TC Nº 07/2021, a responsabilidade pelo tratamento de dados pessoais será exercida, em primeira instância, pela figura do encarregado, e em segunda e última, pelo controlador, demonstrando, portanto, que o Tribunal se atentou aos quesitos referentes aos agentes de tratamentos de dados pessoais, nos quais já foram discutidos anteriormente, por meio da seção 2.4.

Por fim, segundo o art. 11, a PPDP do TCE-PB, poderá especificar e

determinar a adoção de um “conjunto de medidas técnicas e administrativas de segurança contra acessos não autorizados e situações acidentais ou, ainda, incidentes culposos ou dolosos de destruição, perda, adulteração, compartilhamento indevido ou qualquer forma de tratamento inadequado ou ilícito”.

Destarte, percebe-se uma preocupação do colendo órgão quanto a minimização dos riscos para a instituição, no que diz respeito a integridade e a confidencialidade dos dados pessoais tratados no âmbito do tribunal, diante da possibilidade de compartilhamentos indevidos ou eventuais incidentes que comprometam a segurança da informação.

2.6.1 Portaria TC Nº 194/2021

O presente instrumento publicado no Diário Oficial Eletrônico do Tribunal, no dia 07 de outubro de 2021, criou o Comitê Gestor de Privacidade e Proteção de Dados Pessoais**,** responsável pela administração da PPDP do TCE-PB.

Observa-se no art. 2º da portaria em destaque que o Comitê Gestor de Privacidade e Proteção de Dados Pessoais consiste em um comitê com competência deliberativa e consultiva, a nível estratégico, ao qual compete as seguintes atribuições:

> I - Avaliar os mecanismos de tratamento e proteção de dados pessoais, as estratégias, metas e normas propostas pelo Encarregado para a conformidade do Tribunal com as disposições da LGPD;
>
> II - Supervisionar a execução dos planos, dos projetos e das ações voltadas à implantação das diretrizes previstas na LGPD;
>
> III - Prestar orientações sobre o tratamento e a proteção de dados pessoais de acordo com as diretrizes estabelecidas na LGPD, nas normas internas e na Resolução Administrativa RA-TC nº 07/2021.

Portanto, cabe ao referido Comitê analisar as estratégias do tribunal em prol do atendimento as diretrizes contidas na LGPD, fiscalizando a execução da PPDP, e avaliar os mecanismos de tratamento de dados pessoais implementados. Para tanto, o Comitê Gestor é constituído pelo Conselheiro-Presidente do Tribunal, pelo Diretor Executivo Geral, Assessor Técnico Chefe (atual Diretor de Tecnologia da Informação), Coordenador da Unidade de Gestão da Informação e o Consultor Jurídico.

3 PROCEDIMENTOS METODOLÓGICOS

Neste item, foram descritas as tipologias utilizadas para realização da pesquisa, bem como os procedimentos técnicos adotados para a coleta e o tratamento dos dados obtidos. Também foram apresentadas informações sobre a utilização da entrevista estruturada, além de evidenciar a importância da utilização dos procedimentos metodológicos adotados para a realização da pesquisa.

3.1 CLASSIFICAÇÃO DA PESQUISA

De acordo com Andrade (2010), os tipos de pesquisa científica podem ser classificados de diferentes maneiras, por critérios que variam conforme o enfoque do estudo. Desse modo, quanto aos objetivos, a presente pesquisa pode ser classificada como exploratória, possuindo como finalidades proporcionar maiores informações sobre determinado assunto, bem como facilitar a delimitação de um tema. Por meio de uma pesquisa exploratória, avalia-se a possibilidade de se desenvolver uma boa pesquisa sobre determinada área de estudo (ANDRADE, 2010).

No entanto, quanto aos procedimentos a pesquisa classifica-se como bibliográfica, distinguindo-se da pesquisa documental. Conforme Andrade (2010), a diferença entre as classificações mencionadas se dá pelo material consultado. A pesquisa documental baseia-se em documentos primários, originais, ou seja, documentos que não foram utilizados em nenhum estudo ou pesquisa. Porém, a pesquisa bibliográfica utiliza-se de fontes secundárias, materiais como livros, artigos e periódicos, que já passaram por algum tipo de tratamento.

Quanto a abordagem de pesquisa o presente estudo classifica-se como qualitativo, no qual segundo Creswell (2010), os métodos qualitativos demonstram uma abordagem diferente da investigação acadêmica, do que a abordagem utilizada pela investigação quantitativa. A investigação qualitativa emprega diferentes concepções, métodos de coleta, análise e interpretação dos dados.

Desse modo, o método utilizado para a construção da pesquisa trata-se do estudo de caso, sendo um método apropriado para a construção de uma investigação empírica que pesquisa fenômenos dentro de seu contexto real (MARTINS, 2008).

Ainda segundo o autor, de acordo com a abrangência e os propósitos da pesquisa, o estudo pode ser classificado como descritivo, exploratório ou

experimental. No entanto, mesmo que as diferenças entre as duas primeiras tipologias sejam tênues, o presente estudo de caso enquadra-se como exploratório, sendo uma pesquisa que se propõe a investigar um fenômeno atual e ainda pouco explorado.

3.2 POPULAÇÃO E AMOSTRA

A pesquisa foi direcionada ao setor competente do TCE-PB, responsável por administrar e supervisionar toda a área de tecnologia da informação no ambiente do tribunal. Desse modo, para compor a amostra, foi solicitada a participação do atual Diretor de Tecnologia da Informação do TCE-PB, o Sr. Ed Wilson Fernandes de Santana, chefe da Diretoria de Tecnologia da Informação (DITEC), que além de participar do planejamento técnico, administrativo e financeiro do órgão, também presta assistência e apoio ao Presidente e aos membros do Tribunal no exame de problemas operacionais, administrativos e financeiros, dentre outras delegações.

3.3 PROCEDIMENTOS DE COLETA DE DADOS

Nesta seção, encontram-se as informações relativas ao instrumento de coleta de dados utilizado, bem como os procedimentos metodológicos realizados para a obtenção e o tratamento dos dados obtidos.

3.3.1 O instrumento de pesquisa

De acordo com Marconi e Lakatos (2021), a entrevista trata-se de uma técnica de pesquisa que consiste em um encontro entre duas pessoas, no qual mediante conversação, se obtenha informações acerca de um assunto. Desse modo, a entrevista representa um método que proporciona coletar verbalmente a informação necessária, sendo um importante instrumento de pesquisa nos vários campos das Ciências Sociais ou de outros setores de atividades.

Diante da tipologia apresentada, optou-se por uma entrevista estruturada, com 06 (seis) perguntas abertas, e um roteiro prontamente definidos, sendoefetuada com um participante selecionado de acordo com o plano de pesquisa. Ademais, permitiu-se um espaço em aberto destinado ao entrevistado, para que o mesmo

pudesse apresentar suas considerações acerca do tema proposto, bem como proferir comentários que não foram realizados durante o momento das respostas.

Vale salientar, que a entrevista foi gravada com o total consentimento do entrevistado (ver ANEXO C) e, em seguida, transcrita integralmente. Com isso foi feito o cruzamento das informações obtidas com o estudo realizado e a referida entrevista. Assim, pode-se observar o alinhamento entre as informações adquiridas e os objetivos do presente estudo.

3.4 MÉTODOS DE ANÁLISE DOS DADOS

Inicialmente, cabe salientar que a entrevista foi realizada presencialmente no âmbito do TCE-PB, com horário acertado pelo próprio entrevistado e executada no local em que ele exerce suas funções de Diretor de Tecnologia da Informação e chefe da DITEC. Também merece ser destacada a extrema cordialidade e atenção do entrevistado em responder de forma clara e elucidativa os questionamentos que foram feitos.

A entrevista ocorreu por volta das 07:30h às 8:15h no dia 19 de maio de 2023. Por meio das respostas obtidas com a gravação, foi possível realizar uma análise acerca de todas as questões levantadas, possibilitando a compreensão dos fatos relacionados ao impacto ocasionado pela LGPD e o gradativo processo de adequação e treinamento pelo qual o TCE-PB vem enfrentando desde que a lei começou a vigorar.

4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Nesta seção do presente trabalho, procurou-se discorrer sobre a análise das respostas obtidas por meio da entrevista realizada com diretor de Tecnologia da Informação do TCE-PB, transcrita integralmente em seu inteiro teor e contida no Apêndice A. Dessa forma, a seguir encontra-se a análise dos fatos ora levantados por meio do procedimento de coleta de dados utilizado.

4.1 ANÁLISE E DISCUSSÃO DOS DADOS OBTIDOS

4.1.1 Principais impactos ocasionados pela LGPD

Por meio das respostas obtidas com a gravação da entrevista, e a partir de uma reanálise minuciosa *a posteriori* da fala do entrevistado, pode-se perceber que o processo de adaptação do TCE-PB quanto a LGPD consiste em um processo de análise contínuo e gradativo, sendo, inicialmente, trabalhadas as camadas de segurança da informação e divulgação da informação.

Também merece ser destacada a figura do Comitê Gestor de Privacidade e Proteção de Dados Pessoais do tribunal, como o principal ambiente de discussão acerca do tema em epígrafe, fato esse reforçado pelo próprio entrevistado.

Ante o exposto, com o advento da lei, o tribunal realizou um estudo aprofundado quanto às mudanças trazidas por esse marco na legislação brasileira, sendo criado o Comitê para discutir sobre diversos pontos, dentre os quais a identificação do CPF dos credores da administração pública visualizados nos sistemas do tribunal. Desse modo, por meio da LGPD, tais dados pessoais cuja titularidade pertença à pessoa natural (pessoa física), são protegidos por lei, resultando no mascaramento dessas informações nos sistemas do TCE-PB, assim como nos demais tribunais de contas.

Tal procedimento pode ser verificado no Sistema de Acompanhamento e Gerenciamentos dos Recursos da Sociedade (SAGRES), disponível publicamente na versão *on line*, os dados relativos aos CPFs de fornecedores encontram-se com os 03 (três) primeiros dígitos e os 02 (dois) últimos com um símbolo de asterisco (*), de modo a proteger a identificação integral do número do CPF.

No entanto, pelo teor da primeira resposta, o entrevistado esclareceu que na sua visão, a LGPD veio para proteger os dados pessoais sensíveis da utilização indevida por terceiros, e essa proteção perdura até o limite em que não entra em conflito com outros normativos, como a Lei de Acesso à Informação (LAI) e a Lei da Transparência. Nesse contexto, para o Diretor de TI do tribunal o processo de mascarar o CPF que era disponibilizado nas prestações de contas não seria o caminho correto, fazendo referência inclusive, sobre a Resolução TCU nº 354/23, publicada em 12 de abril de 2023.

Ao analisar o conteúdo da norma supracitada, observa-se que a recente resolução do TCU dispõe sobre o tratamento da informação relativa ao número de inscrição no Cadastro de Pessoas Físicas (CPF) dos jurisdicionados e demais interessados nos processos, nas respectivas peças e nas publicações do Tribunal, em face das disposições trazidas na Lei 12.527/2011 (LAI) e na Lei 13.709/2018 (LGPD). Desse modo, conforme o TCU (2023), o número de inscrição do CPF seria um dado imprescindível ao exercício das atribuições do órgão.

Outro ponto que merece ser destacado está relacionado diretamente ao tema objeto do presente estudo: Segurança da Informação. Para o entrevistado, a principal mudança proporcionada pela LGPD para as demais entidades que integram a administração pública, estaria relacionada tão somente no contexto da segurança da informação. Ao longo dos comentários realizados ao final da entrevista, nota-se que no setor privado havia uma desvirtuação da livre privacidade e liberdade, sendo que as empresas, como por exemplo, redes sociais e as indústrias de jogos coletavam dados de forma arbitrária do usuário, sem qualquer consentimento.

Nesse cenário, destaca-se o contexto advindo das redes sociais e dos perfis coletados por empresas influenciadoras de resultados, chegando até mesmo impactar o cenário político em outros países, como é o caso do escândalo envolvendo a empresa *Cambridge Analytica*.

De acordo com a BBC (2018), uma das redes sociais mais conhecidas do mundo, o *Facebook*, teria vazado informações de mais de 50 milhões de usuários da plataforma para a empresa americana de análise de dados *Cambridge Analytica*. Tal compartilhamento indevido teria sido utilizado pela empresa para criar um sistema, permitindo, assim, predizer e influenciar as opções de escolha dos eleitores norte-americanos (BBC, 2018).

Retomando o contexto da sociedade brasileira, a LGPD veio em um momento necessário, não somente para combater esse tipo de uso indevido de dados e informações pessoais por parte das entidades do setor privado, mas também no sentido de incluir a administração pública nessa área de segurança da informação.

Desse modo, por meio da referida lei, com base nas informações já elencadas ao longo do presente trabalho, os dados pessoais em posse do poder público devem ser utilizados com a finalidade do pleno interesse público. Outrossim, tais dados são tratados tendo em vista o cumprimento de finalidades específicas e de execução de políticas públicas, sendo vedado o uso compartilhado dessas informações constantes nas bases de dados órgãos para entidades do setor privado, exceto nos casos elencados pela lei (BRASIL, 2018).

4.1.2 Principais medidas implementadas pelo TCE-PB

No tocante as ações executadas pelo TCE-PB, quanto às mudanças proporcionadas pela LGPD, têm-se a criação do próprio Comitê Gestor de Privacidade e Proteção de Dados Pessoais, mencionado pelo entrevistado e composto pelo mesmo, além das figuras do Presidente do TCE-PB, do Diretor Executivo Geral, do Coordenador da Unidade de Gestão da Informação e o Consultor Jurídico do tribunal.

Tal Comitê, responsável por discutir e administrar todas as questões referentes à LGPD no âmbito do tribunal, foi instituído pela própria PPDP em seu art. 1º, §2º, pelo qual fica evidenciado que a política de proteção de dados será administrada por esse comitê, que também designará o encarregado pela proteção de dados pessoais do órgão.

Desse modo, adentra-se no principal normativo publicado pelo TCE-PB e reforçado pelo entrevistado da presente pesquisa. A PPDP do tribunal (Resolução Administrativa RA TC nº 07/2021) constitui-se como o principal elemento norteador e balizador para todos os servidores, no tocante ao enquadramento junto a LGPD, instituindo como fora mencionado anteriormente, o comitê gestor, pelo qual são tomadas as decisões deliberativas e as orientações sobre o tratamento e a proteção dos dados de acordo com as diretrizes da LGPD.

Além do mais, de modo a deixar ainda mais evidente a relação entre o TCE-PB e as determinações da LGPD, têm-se as indicações das figuras responsáveis pelo tratamento de dados no contexto do tribunal. Dos agentes de tratamento de dados previstos no art. 5º, inciso IX da LGPD (Controlador e o Operador), assim como no capítulo VI da norma que trata especificamente desses agentes, merece ser destacado que no âmbito do TCE-PB, o controlador corresponde a figura do próprio Conselheiro Presidente, integrante do Comitê Gestor designado por meio da Portaria TC Nº 194/2021.

Em seguida, o operador de dados pessoais, representando todas as pessoas que recepcionam os dados ou trabalham diretamente com eles, a exemplo dos auditores de contas públicas que integram o corpo técnico do TCE-PB. Além desses 02 (dois) agentes, pode-se mencionar a figura do encarregado pelo tratamento de dados pessoais, previsto pela LGPD por meio do art. 41.

Dessa maneira, diante da leitura do dispositivo supracitado, cabe ao controlador indicar o encarregado pelo tratamento de dados pessoais, sendo tal ato executado em 2022, por meio da Portaria TC Nº 83/2022, publicada no Diário Oficial Eletrônico do TCE-PB em 26 de abril de 2022. Sendo assim, foi nomeado pelo Presidente do tribunal o servidor determinado para exercer a função de encarregado pelo tratamento de dados pessoais no âmbito do TCE-PB, restando evidente que o Tribunal de Contas vem seguindo as determinações contidas na lei.

Por fim, convém ressaltar as demais medidas tomadas pelo tribunal, logo após o início da vigência da lei em 2020, como, por exemplo, a iniciativa quanto a realização de cursos de capacitação. Nesse contexto, por meio da fala do entrevistado, tem-se a confirmação que foi realizado curso de capacitação pelo tribunal quanto às inovações da LGPD, não de maneira compulsória aos seus servidores, mas por adesão.

Além do mais, foi confirmada a iniciativa quanto a realização de um programa de cursos junto a Escola de Contas do TCE-PB, de caráter contínuo, para que sejam feitos cursos de capacitação no mínimo anuais, de modo a conscientizar todos os servidores sobre a importância de cada membro do tribunal nesse processo, conforme dito pelo entrevistado.

5 CONCLUSÃO

Por meio do presente estudo, procurou-se identificar como o Tribunal de Contas do Estado da Paraíba (TCE-PB) está se adequando as inovações proporcionadas pela Lei Geral de Proteção de Dados Pessoais. Para tanto, a pesquisa utilizou-se do procedimento da entrevista para a coleta dos dados necessários, de modo a obter a percepção do responsável pela área/tema no local estudado, que é o ponto de partida desse trabalho.

Desse modo, foi possível esclarecer qual a principal ferramenta elaborada pelo TCE-PB (PPDP), além de deixar evidente que o processo de adequação do tribunal está sendo feito de maneira gradativa, sempre acompanhado das decisões deliberativas do Comitê Gestor de Privacidade e Proteção de Dados Pessoais, no qual o entrevistado da pesquisa também faz parte.

Não obstante, pode-se concluir que o objetivo geral desse estudo e a consequente resposta para o problema apresentado foram devidamente alcançados e explorados com base na metodologia utilizada, bem como os demais objetivos específicos, quais sejam: I – Conhecer a percepção do TCE-PB sobre a importância da LGPD; II – Descrever as políticas de segurança da informação e dados pessoais implementadas pelo TCE-PB e; III – Verificar se tais medidas em segurança da informação adotadas estão sendo observadas no cotidiano do egrégio Tribunal.

Destarte, o primeiro objetivo específico foi atendido por meio das respostas obtidas pelo entrevistado, Sr. Ed Wilson Fernandes de Santana, no tocante a necessidade de a ver no cenário brasileiro, principalmente quanto a administração pública, uma norma capaz de regular e garantir a segurança da informação e dos dados pessoais sensíveis. Além do mais, o próprio entrevistado deixou bem claro que já trabalhava nesta área há um tempo, porém sentia a necessidade de que fosse elaborado um normativo.

O segundo objetivo específico foi alcançado ao mostrar que o TCE-PB realizou um estudo sobre a referida lei e publicou um normativo próprio, funcionando como um norte a ser seguido para todos os que trabalham com o tratamento de dados pessoais e alcançando também, como observa-se no art. 2º da PPDP, a todos os relacionamentos institucionais do Tribunal com todos os usuários de seus serviços, incluindo os servidores, além dos contratados, fornecedores e terceiros (TCE, 2021).

Quanto ao terceiro objetivo específico, este foi cumprido diante do procedimento de coleta de dados utilizado, em que ficou demonstrado a observância da LGPD e das normas promulgadas pelo TCE-PB por parte do servidor responsável do Tribunal, no qual apresentou conhecimento sobre o tema/objeto de estudo. Nesse contexto, o próprio entrevistado deixou claro a ocorrência de situações em que ele opinou pelo não recebimento de dados pessoais sensíveis, quando não era necessário se manter tais dados na base administrada pelo Tribunal, assegurando a competência e o zelo vivenciados no cotidiano do referido órgão.

Não obstante, no concernente a realização de pesquisas futuras, destaca-se as recomendações expostas na justificativa deste trabalho, no qual foi sugerida a iniciativa quanto à elaboração de mais pesquisas com abordagem qualitativa, visando a exposição dos fatos, e a utilização do método aqui empregado.

A partir do estudo de caso, foi possível explorar um determinado fenômeno dentro do contexto e do objeto de estudo aqui escolhido. Quanto às recomendações de temas, tem-se como sugestão o estudo sobre o impacto proporcionado pela LGPD nos demais órgãos da administração pública.

Para finalizar, conclui-se que o TCE-PB, desde o início da vigência da LGPD buscou de forma tempestiva adotar as devidas providências no tocante à conformidade e a observância da referida lei, demonstrando um processo contínuo de adaptação e aprimoramento, representado tanto por meio dos servidores que estão diretamente ligados a matéria em discussão, quanto pelos demais membros que realizam o tratamento de dados pessoais e os manuseiam, conforme detalhado pela lei.

Considerando o contexto apresentado, o TCE-PB por meio do Comitê criado especificamente para lidar com tais inovações desencadeadas pela norma e estabelecer a conduta necessária a ser seguida pela instituição, procurou discutir sobre as formas e as ações que deveriam ser executadas visando tal conformidade, proporcionando um enfoque no tocante a divulgação da informação constante na base de dados do tribunal, e o tratamento correto que deveria ser dado para essas informações.

A maior evidência quanto a proteção de dados pessoais dos titulares enquadrados pela Lei, estaria justamente no encobrimento dos dígitos que compõem o CPF dos credores que mantiveram ou mantém relação com os jurisdicionados fiscalizados pelo Tribunal, e que estão constantes na base de dados. Outra

evidência estaria ligada a observância do setor responsável do órgão, representado pela Diretoria de Tecnologia da Informação, em reconhecer, com base na LGPD, quais informações deveriam estar constantes na base de dados do TCE-PB e quais não seriam úteis para a instituição, e principalmente, para o controle social exercido pela população.

REFERÊNCIAS

ANDRADE, M.M. **Introdução a metodologia do trabalho científico.** 10.ed. São Paulo: Atlas, 2010.

A nova norma ISO/IEC 27001:2022. **BSIGROUP**, s.d. Disponível em: https://www.bsigroup.com/pt-BR/ISO-IEC-27001-Seguranca-da-Informacao/2022-revisao/. Acesso em: 14 nov. 2022.

ANTÔNIO, Adriano Martins. O que mudou na ISO/IEC 27002 de 2022? **PMGacademy**, 2022. Disponível em: https://www.pmgacademy.com/blog/o-que-mudou-na-iso-iec-27002-de-2022/. Acesso em: 16 nov. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ISO/IEC 27000 Norma internacional de segurança da informação é revisada. **ABNT.** Disponível em: https://www.abnt.org.br/noticias/5777-iso-iec-27000-norma-internacional-de-seguranca-da informacao-e-revisada. Acessado em: 04 jun.2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Representante oficial da ISO no Brasil. **ABNT.** Disponível em: https://www.abnt.org.br/noticias/7128-abnt-representante-oficial-da-iso-no-brasil. Acessado em: 4 jun.2021

BALDISSERA, Olívia. ISSO 27000: tudo o que você precisa saber para se destacar na segurança da informação. **PÓSPUCPRDIGITAL**, 2021. Disponível em: https://posdigital.pucpr.br/blog/iso-27000. Acesso em: 14 nov. 2022.

BRASIL. **Constituição federal.** Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 jun.2021.

BRASIL. **Decreto n°9.637, de 26 de dezembro de 2018.** Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato20152018/2018/Decreto/D9637.htm#art22. Acessado em: 08 jun.2021.

BRASIL. **Lei Nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 nov. 2022.

BRASIL, Tribunal de Contas da União. **Manual de boas práticas em segurança da informação.** Disponível em: < https://www.tcu.gov.br/>. Acessado em: 10 mar. 2021.

Conheça a LGPD. **SEBRAE**, s.d. Disponível em: https://www.sebrae.com.br/sites/PortalSebrae/canais_adicionais/conheca_lgpd. Acesso em: 14 nov. 2022.

CRESWELL, J.W. **Projeto de pesquisa: métodos qualitativo e misto.** 3.ed. Porto Alegre: Artmed, 2010.

Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. **BBC**, 2018. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de autoridades.ghtml. Acesso em: 23 maio 2023.

FONTES, Edison. **Segurança da informação**: o usuário faz a diferença. 1. ed. São Paulo: Saraiva, 2006.

INTERNACIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27000:2018. **ISO.** Disponível em: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>. Acessado em: 05 jun.2021.

INTERNACIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27001:2013. **ISO.** Disponível em: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en>. Acessado em: 05 jun.2021.

INTERNACIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27002:2013. **ISO.** Disponível em: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en>. Acessado em: 06 jun.2021.

INTERNACIONAL ORGANIZATION FOR STANDARDIZATION**.** ISO/IEC 27003:2017. **ISO.** Disponível em: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27003:ed- 2:v1:en>. Acessado em: 06 jun.2021.

ISO/IEC 27701:2019. **ISO**, 2019. Disponível em: https://www.iso.org/standard/71670.html. Acesso em: 16 nov. 2022.

KANAANE, R.; FIEL FILHO, A.; FERREIRA, M. G. **Gestão pública**: planejamento, processos, sistemas de informação e pessoas. São Paulo: Atlas, 2010.

MACHADO, Felipe Nery Rodrigues. **Segurança da informação**: princípios e controle de ameaças. 1. ed. São Paulo: Érica, 2014.

MARCONI, M.A; LAKATOS, E.M. **Fundamentos de metodologia científica.** 9.ed. São Paulo: Atlas, 2021.

MARTINS, G.A. **Estudo de caso:** uma estratégia de pesquisa. 2.ed. São Paulo: Atlas, 2008.

MATTOS, J.G. **Auditoria.** 1.ed. Porto Alegre: Sagah, 2017.

MEGASYAH, Y.; ARIFNUR, A.A. Academic information sistem security audits using COBIT 5 framework domains APO12, APO13, AND DSS05. **Journal of Applied Engineering and Technological Science.** v. 1. n. 2. 2020. Disponível em: https://www-periodicos-capes-gov-br.ezl.periodicos.capes.gov.br/index.php?. Acessado em: 20 jun.2021.

OSTEC. **ISO 27000: as vantagens da certificação de segurança da informação para o seu negócio.** Disponível em: https://ostec.blog/geral/iso-27000-vantagens-certificacao-seguranca/. Acesso em: 02 jun.2021

MACHADO, Felipe Nery Rodrigues. **Segurança da informação**: princípios e controle de ameaças. 1. ed. São Paulo: Érica, 2014.

PARAÍBA, Tribunal de Contas do Estado. Empenhos. **Sagresonline**. Disponível em: https://sagresonline.tce.pb.gov.br/#/municipal/execucao-orcamentaria/empenhos. Acesso em: 22 maio 2023.

PARAÍBA, Tribunal de Contas do Estado. História do TCE-PB. **TCE-PB.** Disponível em: https://tce.pb.gov.br/institucional/breve-historia. Acessado em: 10 mar. 2021.

PARAÍBA, Tribunal de Contas do Estado. Membros e Diretores. **TCE-PB.** Disponível em: https://tce.pb.gov.br/institucional/autoridades-e-diretores. Acesso em: 21 maio 2023.

PARAÍBA, Tribunal de Contas do Estado. Portaria TC Nº. 083/2022. **Diário Oficial Eletrônico do TCE-PB**. João Pessoa, 26, abr. 2022. Disponível em: https://publicacao.tce.pb.gov.br/bd0cefac1bd9ca49df48eaf51b724abd. Acessado em: 18 maio 2023.

PARAÍBA, Tribunal de Contas do Estado. Portaria TC Nº. 194/2021. **Diário Oficial Eletrônico do TCE-PB**. João Pessoa, 07, out. 2021. Disponível em: https://publicacao.tce.pb.gov.br/8c89b59316b0cd4676f0238c18a38450. Acessado em: 15 dez. 2021.

PARAÍBA, Tribunal de Contas do Estado. Regimento Interno. **TCE-PB.** Disponível em: https://tce.pb.gov.br/legislacao/leis/regimento-interno-tce-pb.pdf. Acessado em: 10 mar.2021.

PARAÍBA, Tribunal de Contas do Estado. Resolução Administrativa RA-TC Nº 07/2021. **Diário Oficial Eletrônico do TCE-PB**. João Pessoa, 22, jun. 2021. Disponível em: https://tce.pb.gov.br/diario-oficial-eletronico#. Acessado em: 15 dez. 2021.

RAMOS, Kellen da Silva *et al*. Gestão de segurança da informação em uma empresa do setor de saúde. **Colloquium Exactarum,** v. 9, n.4, out-dez. 2017. Disponível em: https://doaj.org/article/faa397fe2f21455b82ccf75ebcbf35cb. Acesso em: 15 mar. 2021.

RIOS, O.K.L; FILHO, J.G.A.T; RIOS, V.P.S. Gestão de segurança da informação: práticas utilizadas pelas instituições federais de ensino superior para implantação de política de segurança da informação. **Navus Revista de Gestão e Tecnologia,** Florianópolis, v.7, n.2, p. 49-65, abr.-jun. 2017. Disponível em: https://www-periodicos-capes-gov-br.ezl.periodicos.capes.gov.br/index.php?. Acessado em: 20 mar. 2021.

SILVA, M.M. **Controle externo das contas públicas:** o processo dos tribunais de contas do brasil. São Paulo: Atlas, 2014.

SOUSA, R. P. M. de; BARRANCOS, J. E.; MAIA, M. E. **Acesso a informação e ao tratamento de dados pessoais pelo poder público**. 2019. Disponível em: https://repositorio.ufpb.br/jspui/handle/123456789/25232. Acesso em: 14 maio 2023.

TCU e a Lei Geral de Proteção de Dados Pessoais. **Tribunal de Contas da União**, s.d. Disponível em: https://portal.tcu.gov.br/lgpd/. Acesso em: 22 nov. 2022.

UNIÃO, Tribunal de Contas. Resolução – TCU Nº 354, de 12 de abril de 2023. **Diário Oficial da União**, 2023. Disponível em: https: //www.in.gov.br/en/web/dou/-/resolucao-tcu-n-354-de-12-de-abril-de-2023-477406572. Acesso em: 22 maio 2023.

ZANON, Sandra Buth. Gestão e segurança da informação eletrônica: exigências para uma gestão documental eficaz no Brasil. **Biblios.** n. 56. 2014. Disponível em: https://www-periodicos-capes-gov-br.ezl.periodicos.capes.gov.br/index.php?. Acessado em: 20 mar.2021.

APÊNDICE A – Entrevista

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE GRADUAÇÃO EM CIÊNCIAS CONTÁBEIS

"Bom dia. Sou o aluno Jean Carlos da Silva Nascimento, concluinte do curso de graduação em Ciências Contábeis. Entrevistarei a partir de agora o Sr. Ed Wilson Fernandes de Santana, Diretor de Tecnologia da Informação do tribunal."

1. Qual foi o impacto proporcionado pelo advento da Lei Federal nº 13.709/18 (LGPD) para o Tribunal de Contas?

"Bom dia Jean, a gente recepcionou a LGPD de maneira muito positiva na nossa situação. O tribunal fez um estudo, criou uma comissão para elaborar um normativo próprio e aí tem algumas questões específicas da lei referente a dados pessoais e dados pessoais sensíveis, e a gente fez uma discussão interna a respeito disso, estamos fazendo porque a implementação da lei ela não é uma coisa com começo, meio e fim, ela um processo contínuo de aprimoramento. É nós trabalhamos a camada de segurança da informação, e, é trabalhamos também a divulgação da informação, "pra" efeito de debate, digamos assim, mais acalorado que a gente teve foi com relação aos dados, computação dos dados pessoais, mas especificamente o CPF, que com o advento da lei, o tribunal de contas do estado e todos os tribunais, inclusive o TCU, encaminhou na direção de mascarar o CPF que era disponibilizado nas prestações de contas, e a gente fez também esse procedimento, mas internamente a gente dentro do Comitê ficou discutindo se esse era o caminho correto a seguir. Eu era um defensor de que não, meu argumento era de que a lei veio para proteger os dados pessoais sensíveis, "né" da utilização indevida e com relação aos dados pessoais, essa proteção ela vai até o limite em que não impacta em outros normativos que tem ser harmonizado com ela, a exemplo da Lei de Acesso a Informação, da Lei da Transparência, o que é determina que quem transaciona com a administração pública tem que ser identificado e "pra" minha felicidade "né" porque assim "tava" muito acalorado essa discussão aqui interno, o TCU esse ano baixou um normativo exatamente nessa linha de que o CPF é uma

informação que deve ser disponibilizada em todos os processos do tribunal por ser uma informação que identifica quem tá transacionando com a administração pública, e aí o direito da teoria do agente, "né" do principal e do acessório, não é o direito do principal na administração pública e na sociedade em conhecer quem tá realizando essa transação."

2. Como o TCE-PB se atentava no tocante a proteção de dados pessoais em seu ambiente administrativo antes da LGPD? Havia algum regulamento anterior a Lei nº 13.709/18?

"Bom. É, o tribunal ele tem dois grandes sistemas de trabalho que é o TRAMITA e o SAGRES. Todos os sistemas eles são, a parte de uso da auditoria, ela é com o login e senha que é uma identificação e aí como é o normal do sistema, ele tem um log que registra todos os acessos, e a pessoa adentrar no tribunal, toma conhecimento do Código de Ética e da forma de trabalhar no tribunal para que todas as informações que ele tenha em decorrência do seu trabalho seja usado para a finalidade processual que "tá" vinculada. Essa é a regra geral e saindo disso a gente tem como identificar através do log se houve algum acesso indevido ou algum uso indevido de alguma informação processual do tribunal. Isso porque a gente tem a parte sem login e senha que é "pra" uso da sociedade e aí tem todos os dados. A parte da auditoria tem um detalhamento maior sobre remuneração e informações de caráter mais pessoal dos nossos jurisdicionados e tem esse cuidado, mas os processos em si depois de julgados eles são públicos e aí não há nenhum óbice a consulta externa. Essa é a regra geral referente a esse procedimento e é anterior a Lei Geral de Proteção de Dados."

3. Atualmente a Política de Proteção de Dados Pessoais do Tribunal (Resolução Administrativa RA TC Nº 07/2021), publicada em 22 de junho de 2021, é a norma principal que adequa o TCE-PB a LGPD?

"Sim. É a principal norma de o norte digamos assim, é para o Tribunal e, é tomando as decisões referentes à LGPD. Se observar esse normativo ele cria um comitê, e esse comitê vem fazendo reuniões e deliberando sobre as questões da LGPD."

4. Houve alguma espécie de capacitação ou curso direcionado aos servidores do TCE-PB quanto às inovações trazidas pela LGPD?

“Sim, a gente fez na época assim que a lei saiu a gente de um conjunto de capacitações e o comitê já deliberou de que fosse feito um programa junto à Escola de Contas de capacitação contínua, anualmente ter um reforço, digamos assim, para que todos tomem ciência da importância de cada um nesse processo. Na verdade, isso é uma mudança de cultura, esse cuidado, a gente já tinha muito esse cuidado com relação ao Código de Ética, mas a LGPD ela transpassa isso porque envolve todos os colaboradores, não só os servidores, mas todos os colaboradores do tribunal têm que tomar ciência da importância de cada um nesse processo.”

5. Como se deu esse processo de adequação do TCE-PB às determinações da LGPD? Foi algo de imediato ou foi uma mudança gradativa?

“Ele “tá” acontecendo na verdade, a pergunta como se deu como se fosse um processo de começo, meio e fim, ele tá acontecendo, é uma mudança gradativa e ela tá sendo implementada a cada decisão, isso faz parte de colocar dentro da rotina do tribunal as decisões. “Né” eu posso dar como exemplo, a gente teve, recentemente, um pedido do governo em enviar determinada informação “pro” tribunal, e eu fui chamado a opinar nessa situação, e eu pedi para não receber essa informação porque essa informação não ia ser útil para os processos do tribunal e era uma informação de caráter pessoal que não fazia sentido eu ter na minha base de dados se eu não ia fazer uso. Então isso já é um norte em decorrência, eu me baseei inclusive na LGPD da gente pedir exatamente é aquilo que vai ser útil para a instrução dos processos “né”, não pedi nada além disso, principalmente tratando-se de dado pessoal sensível que era o caso nessa situação.”

6. Relate sua experiência quanto às mudanças proporcionadas pela LGPD, bem como sobre o processo de adaptação do Tribunal nesse meio tempo.

“É, acho que a principal mudança ao meu sentir da LGPD para as administrações públicas de um modo geral, ela não se reside muito na questão de dado pessoal, acho que os órgãos públicos de um modo geral já têm normativos tratando do

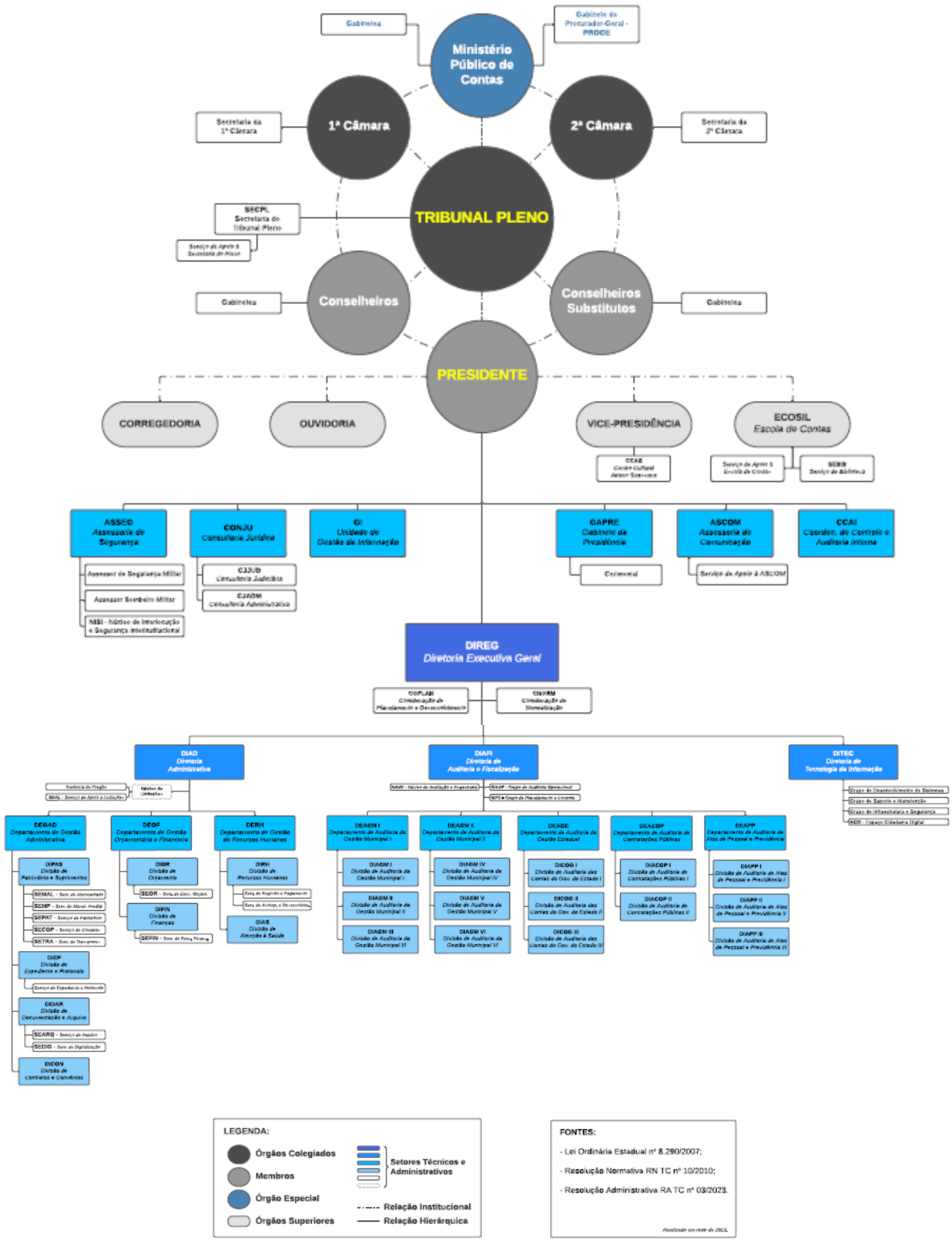
recebimento e do tratamento de dados pessoais. Os órgãos públicos que recebem dados pessoais sensíveis como a parte de saúde, segurança e educação referente ao menor, que a LGPD também dá um tratamento especial pra o menor, já tem, já tinham na realidade o cuidado em trabalhar e tratar essa informação. Eu senti um grande ganho da LGPD pra área pública, porque na área privada realmente "tava" existindo uma desvirtuação desses dados pessoais sensíveis, a utilização desses dados pessoais sensíveis, e aí eu abro parênteses pra exemplificar as redes sociais que usam você, entra de graça na rede social, mas entenda que você tá sendo um usuário da rede social, mas você também é o produto da rede social, ela vende os seus gostos, o que você navega, então toda essa informação pessoal ela usa pra negociar no mercado, "é essas informações" sem o seu consentimento, então essa é na área privada, tinha realmente essa situação e aí em boa hora a LGPD veio, mas na área pública, e aí eu fecho parênteses, na área pública o que eu entendo de grande ganho veio em segurança, na área pública olhar esse momento que estamos vivenciando, de grande exposição desses big dates, no mundo virtual que é um caminho sem volta, e a proteção dessa, desse ambiente de dados, de ataque de utilização digamos assim pra sequestro da informação e aí a administração ficar sem poder utilizar, sem poder realizar as suas ações. A LGPD deu um olhar para que as administrações públicas criassem procedimentos e rotinas de melhorar essa questão da proteção dos seus ambientes virtuais."

7- Comentários abertos para o entrevistado.

"Eu acho o tema bastante relevante assim, já trabalho nessa área há algum tempo e a gente sentia a necessidade de que isso fosse normatizando. Você tá trabalhando com a LGPD então você fez esse histórico de porquê a lei nasceu, a gente vai entender de que nesse mundo pós-moderno que a gente "tá" vivendo em que a informação é poder, a gente não "tava" dando tanto valor aos dados que estavam sendo coletados, principalmente em redes sociais e em games que a sempre acha que é de graça e aí de graça a gente bota next, next e aceita todas as políticas e que os games e as redes sociais colocam, e a LGPD ela é no mundo todo, veio nesse sentido, de alertar a população de modo geral de que isso já "tava" influenciando já decisões políticas. Isso aconteceu com o Cambridge Analytica, uma empresa que pegou esses dados pessoais e direcionou propaganda política pra favorecer um ou

outro candidato, e esse direcionamento foi muito eficaz porque, porque tinha-se qual era o gosto, o que é que aquela pessoa queria ouvir para poder ir para este ou aquele candidato então era uma propaganda muito direcionada através desses meta dados de navegação que por trás tem muito dado pessoal, do que a pessoa gosta, do que a pessoa crê, do que a pessoa acredita, então essa era uma informação muito valiosa que "tava" sendo deixada e essas redes sociais e esses games viram nesses dados uma forma de ganhar dinheiro. A lei geral veio "pra" isso, e aí no caso brasileiro a gente incluiu a administração pública, que no meu sentido em boa hora, é para essa parte de segurança. Então é como tinha comentado anteriormente, acho que isso foi o ganho, digamos assim, da LGPD para a administração pública, e se tinha algum órgão que ainda não tinha o zelo adequado com o dado, veio esse normativo "pra" trazer esse cuidado."

ANEXO A – Organograma do TCE-PB



Fonte: TCE-PB.
Disponível em https://tce.pb.gov.br/institucional/organograma. Acesso em: 22 de maio de 2023.

ANEXO B – Ofício ao TCE-PB

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DA PARAÍBA

OFÍCIO Nº 1 / 2021 ▪ CCSA ▪ CC (11.01.13.31)

Nº do Protocolo: 23074.057540/2021-39

João Pessoa-PB, 11 de Junho de 2021

A Sua Excelência o Senhor

Fernando Rodrigues Catão

Presidente do Tribunal de Contas do Estado da Paraíba

Rua Professor Geraldo Von Sohsten, nº 147

CEP: 58.015-190 - João Pessoa. PB

Assunto: Realização de pesquisa para conclusão de curso de graduação

Excelentíssimo Senhor Presidente,

1. Com os mais cordiais cumprimentos, informamos que o discente Jean Carlos da Silva Nascimento, inscrito nesta instituição sob a matrícula n.º 20170014033, está atualmente matriculado no componente curricular TRABALHO DE CONCLUSÃO DE CURSO I, deste Curso de Ciências Contábeis, desenvolvendo o trabalho intitulado "Segurança da Informação e Auditoria Pública: Um estudo de caso no Tribunal de Contas do Estado da Paraíba", sob a orientação da Professora M.Sc. Ionara Stefani Viana de Oliveira.

2. O estudo tem como objetivo geral identificar a existência de políticas e medidas relacionadas à segurança da informação no Tribunal de Contas do Estado da Paraíba - TCE/PB, visando a segurança dos dados recebidos pelo Tribunal e utilizados pelos auditores de contas públicas na fiscalização dos entes da administração pública. E os objetivos específicos são os seguintes: 1) Conhecer a percepção dos funcionários envolvidos com a área de estudo em questão sobre as normas de controle e políticas de segurança da informação – PSI; 2) Conhecer as estratégias para o aperfeiçoamento da gestão em tecnologia da informação - TI, executadas pelo Tribunal; e, 3) Verificar se as normas em segurança da informação adotadas estão sendo seguidas com conformidade pelo(s) setor(es) responsável (eis).

3. Solicita-se autorização para a aplicação de questionários de pesquisa junto aos servidores do TCE/PB por parte do discente, com o fim de possibilitar a concretização do Trabalho de Conclusão de Curso, e o discente se compromete a utilizar as informações obtidas estritamente para o objetivo proposto, de maneira que não haverá compartilhamento indevido de informações nem quebra de confidencialidade.

Com votos de estima, antecipadamente agradecemos.

Respeitosamente,

(Assinado digitalmente em 17/06/2021 16:33)
MOISES ARAUJO ALMEIDA
COORDENADOR DE CURSO
Matrícula: 1610122

ANEXO C – Termo de consentimento livre e esclarecido

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE FINANÇAS E CONTABILIDADE
CURSO DE GRADUAÇÃO EM CIÊNCIAS CONTÁBEIS

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO(TCLE)

Prezado(a) **PARTICIPANTE DE PESQUISA,**

O pesquisador Jean Carlos da Silva Nascimento convida você a participar da pesquisa intitulada "Segurança da Informação: Um Estudo de Caso no Tribunal de Contas do Estado da Paraíba". Para tanto você precisará assinar o TCLE que visa assegurar a proteção, a autonomia e o respeito aos participantes de pesquisa em todas as suas dimensões: física, psíquica, moral, intelectual, social, cultural e/ou espiritual – e que a estruturação, o conteúdo e forma de obtenção dele observam as diretrizes e normas regulamentadoras de pesquisas envolvendo seres humanos preconizadas pela **Resolução 466/2012 e/ou Resolução 510/2016**, do Conselho Nacional de Saúde e Ministério da Saúde.

Sua decisão de participar neste estudo deve ser voluntária e que ela não resultará em nenhum custo ou ônus financeiro para você (ou para o seu empregador, quando for este o caso) e que você não sofrerá nenhum tipo de prejuízo ou punição caso decida não participar desta pesquisa. Todos os dados e informações fornecidos por você serão tratados de forma anônima/sigilosa, não permitindo a sua identificação.

Objetivo da Pesquisa – Esta pesquisa tem como objetivo identificar como o Tribunal de Contas do Estado da Paraíba (TCE-PB) está se adequando às inovações proporcionadas pela Lei Geral de Proteção de Dados Pessoais (LGPD).

Descrever a metodologia: - Realização de entrevista estruturada com perguntas e um roteiro prontamente definido para a coleta dos dados e informações necessárias.

Benefícios ao(à) Participante da Pesquisa

Contribuir para a conclusão do curso de graduação de um futuro profissional contábil.

Informação de Contato do Responsável Principal e de Demais Membros da Equipe de Pesquisa

Jean Carlos da Silva Nascimento

Graduando do curso de Ciências Contábeis e Técnico em Auditoria (RWR Consultoria)
jeancarlos77br@gmail.com
(83) 98706-0198

Endereco e Informacões de Contato da UFPB

Universidade Federal da Paraíba – UFPB (Campus I)
Lot. Cidade Universitária, PB, 58051-900
(83) 3216-7200
Curso de Ciências Contábeis (CCC UFPB)
E-mail: contabeis@academico.ufpb.br
Telefone: (83) 3216-7457

Endereco e Informacões de Contato do Comitê de Ética em Pesquisa (CEP)/CCS/UFPB

Comitê de Ética em Pesquisa (CEP)
Centro de Ciências da Saúde (1° andar) da Universidade Federal da Paraíba
Campus I – Cidade Universitária / CEP: 58.051-900 – João Pessoa-PB
Telefone: +55 (83) 3216-7791
E-mail: comitedeetica@ccs.ufpb.br
Horário de Funcionamento: de 07h às 12h e de 13h às 16h.
Homepage: http://www.ccs.ufpb.br/eticaccsufpb

CONSENTIMENTO LIVRE E ESCLARECIDO

Ao colocar sua assinatura ao final deste documento, **VOCÊ**, de forma voluntária, na qualidade de **PARTICIPANTE** da pesquisa, expressa o seu **consentimento livre e esclarecido** para participar deste estudo e declara que está suficientemente informado(a), de maneira clara e objetiva, acerca da presente investigação. E receberá uma cópia deste **Termo de Consentimento Livre e Esclarecido (TCLE),** assinada pelo(a) Pesquisador(a) Responsável.

João Pessoa – PB, 19 de Maio de 2023.

Assinatura, por extenso, do(a) Participante da Pesquisa
Ed Wilson Fernandes de Santana

Jean Carlos da Silva Nascimento
Assinatura, por extenso, do(a) Pesquisador(a) Responsável pela pesquisa

ANEXO D – Autorização do TCE-PB (DOC. 44254/21)

Tribunal de Contas do Estado da Paraíba

Documento Nº

44254/21

EXERCÍCIO:	2021
SUBCATEGORIA:	Requerimento
JURISDICIONADO:	Terceiros
DATA DE ENTRADA:	22/06/2021
ASSUNTO:	Ofício nº 1/2021 - CCSA-CC(11.01.13.31) - Solicita autorização para aplicação de questionário de pesquisa, com o fim de concretizar TCC - Processo 23074.057540/2021-39 UFPB. Jean Carlos da Silva.
INTERESSADOS:	

Tribunal de Contas do Estado da Paraíba

TRAMITA - Sistema de Tramitação de Processos e Documentos
Emitido em 15/07/2021

DOCUMENTO: 44254/21
SUBCATEGORIA: Requerimento
JURISDICIONADO: Terceiros
ASSUNTO: Ofício nº 1/2021 - CCSA-CC(11.01.13.31) - Solicita autorização para aplicação de questionário de pesquisa, com o fim de concretizar TCC - Processo 23074.057540/2021-39 UFPB. Jean Carlos da Silva.

DESPACHO

De ordem, DEFIRO o requerimento.

À DIEP,

Para informar o interessado.

DIREG

Assinado em: 15/07/2021

Assinado Eletronicamente
conforme LC 18/93, alterada pela LC 91/2009 e pelo Regimento Interno, alterado pela RA TC 18/2009

Károly de Tatrai Hiluey Agra
Diretor Executivo Geral
Matrícula 3706478