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

RAFAELA ROMANIUC BATISTA

ANÁLISE DE RISCOS EM SEGURANÇA DA INFORMAÇÃO: modelo integrado e simplificado de ações de segurança da informação para Instituições Federais de Ensino Superior (IFES)

João Pessoa
2022

RAFAELA ROMANIUC BATISTA

ANÁLISE DE RISCOS EM SEGURANÇA DA INFORMAÇÃO: modelo integrado e simplificado de ações de segurança da informação para Instituições Federais de Ensino Superior (IFES)

Tese apresentada ao Programa de Pós-Graduação em Ciência da Informação (PPGCI) da Universidade Federal da Paraíba (UFPB), como requisito final à obtenção do título de Doutora em Ciência da Informação. Linha de pesquisa: Ética, Gestão e Políticas de Informação.

Orientador: Prof. Dr. Wagner Junqueira de Araújo

João Pessoa

2022

Catalogação na publicação
Seção de Catalogação e Classificação

B333a Batista, Rafaela Romaniuc.
Análise de riscos em segurança da informação : modelo integrado e simplificado de ações de segurança da informação para Instituições Federais de Ensino Superior (IFES) / Rafaela Romaniuc Batista. - João Pessoa, 2022.
167 f. : il.

Orientação: Wagner Junqueira de Araújo.
Tese (Doutorado) - UFPB/CCSA.

1. Segurança da informação - Gestão de riscos. 2. Ensino superior - Instituições federais. 3. OCTAVE Forte. 4. IFES. I. Araújo, Wagner Junqueira de. II. Título.

UFPB/BC CDU 004.056(043)

RAFAELA ROMANIUC BATISTA

ANÁLISE DE RISCOS EM SEGURANÇA DA INFORMAÇÃO: modelo integrado e simplificado de ações de segurança da informação para Instituições Federais de Ensino Superior (IFES)

Apto em:_____/_____/_____

Tese apresentada ao Programa de Pós-Graduação em Ciência da Informação (PPGCI) da Universidade Federal da Paraíba (UFPB), como requisito final à obtenção do título de Doutora em Ciência da Informação. Linha de pesquisa: Ética, Gestão e Políticas de Informação.

BANCA EXAMINADORA

_____
Prof. Dr. Wagner Junqueira de Araújo
Orientador – PPGCI/UFPB

_____
Profª Drª Alzira Karla Araújo da Silva
Membro Examinador Interno – PPGCI/UFPB

_____
Prof. Dr. Miguel Mauricio Isoni
Membro Examinador Externo – MPGOA/UFPB

_____
Prof. Dr. Marckson Roberto Ferreira de Sousa
Membro Examinador Interno – PPGCI/UFPB

_____
Profª Drª Lucilene Klenia R. Bandeira
Membro Examinador Externo – MPGOA/UFPB

_____
Profª Drª Izabel França de Lima
Membro Suplente Interno – PPGCI/UFPB

_____
Profª Drª Sandra de Albuquerque Siebra
Membro Suplente Externo – PPGCI/UFPE

Dedico

A Deus.
À minha família.
Ao meu marido.
Ao meu filho.

AGRADECIMENTOS

A **Deus**, pois, sem Ele, nada disso seria possível.

Aos meus **pais** e minha **irmã** pela torcida ao longo da caminhada.

Ao meu **esposo**, paciente em relação aos meus estudos, suportando minhas ausências, ansiedades e nervosismos com muito amor e carinho, obrigada por sempre estar ao meu lado.

Ao meu **filho**, por me mostrar o que mais importa nesta vida: Amar.

Ao querido **Prof. Dr. Wagner Junqueira de Araújo**, por ter tido paciência e me orientado ao longo do doutorado. Obrigada pelos puxões de orelha.

Ao Superintendente **Hermes Pessoa Filho** por todo apoio profissional demonstrado.

Ao colega de trabalho **Flavio Ribeiro Córdula** pelo incentivo, apoio e anseios compartilhados.

Às minhas amigas de pesquisa, **Sueny Gomes Léda Araújo** e **Christiane Gomes dos Santos**, por todo o apoio dado na pesquisa, me ajudaram incondicionalmente, e a vocês só tenho sentimentos de gratidão e carinho. Anjos colocados por Deus em minha vida, pois não consigo imaginar meu caminhar na pesquisa sem o carinho e a ajuda prestada em todos os momentos, mesmo sem terem tempo, conseguiram me ajudar até os últimos segundos. Sempre lembrarei do amor, carinho e amizade que tiveram comigo. Muito obrigada!

Aos respondentes do questionário por terem apoiado esta pesquisa.

Aos membros titulares da banca, Prof[a] Dr[a] Alzira Karla Araújo da Silva, Prof. Dr. Marckson Roberto Ferreira De Sousa, Prof. Dr. Miguel Mauricio Isoni, e Prof[a] Dr[a] Lucilene Klenia Rodrigues, pelas contribuições dadas para a construção final desta pesquisa. Aos membros suplentes, Prof[a] Dr[a] Izabel França de Lima e Prof[a] Dr[a] Sandra de Albuquerque Siebra, pela disposição oferecida.

Por fim, finalizo os agradecimentos com uma frase: “Graças a Deus!”.

“Imaginação é mais importante que conhecimento. Pois o conhecimento é limitado a tudo o que conhecemos e compreendemos, enquanto a imaginação abrange o mundo inteiro, e tudo o que tem para ser conhecido e compreendido”.

Albert Einstein

RESUMO

A sociedade atual tem na informação o seu elemento transformador. Nas Instituições Federais de Ensino Superior (IFES) não poderia ser diferente, uma vez que o fluxo informacional tornou-se elemento estruturador de forma progressiva. Portanto, identificar e tratar os riscos de segurança que incidem nestes fluxos é um requisito para tais organizações. Contudo, observa-se que a ausência de ações de segurança da informação (SI) nessas instituições se dá, em geral, pela dificuldade de aplicação dos modelos de análise de riscos existentes, considerados o pilar desse processo. Essa dificuldade ocorre, pois modelos são propostos para fins mais genéricos que o contexto de uma universidade exige. A pesquisa propôs desenvolver um modelo integrado e simplificado de ações para análise de riscos, específico para o contexto dos setores de tecnologia das IFES. Após revisão sistemática de literatura, foi escolhido o *framework* reconhecido internacionalmente OCTAVE *Forte*, para elaboração do modelo, em conjunto com as normas e recomendações de segurança da informação do governo federal, que regem os órgão e entidades da Administração Pública Federal na temática de segurança de informação. Para alcançar esse objetivo, foi feito uma pesquisa aplicada, classificada como exploratória, em sua primeira fase, e descritiva, em sua segunda fase, fundamentada a partir de uma pesquisa de abordagem mista que combinou técnicas de pesquisa qualitativa e quantitativa. As informações foram obtidas pelos métodos de coleta utilizados: pesquisa documental e aplicação questionário on-line. Para análise dos dados, foi utilizada a análise de conteúdo e análise estatística. Assim, pretendeu-se identificar os elementos conceituais para o desenvolvimento de um modelo integrado e simplificado de ações de segurança da informação. Os elementos conceituais obtidos nesta tese permitiram a criação do modelo MISASI STI, que pode ser utilizado como guia para explorar e avaliar as ações de SI existentes e/ou necessárias aos setores de tecnologia das IFES. Esse modelo foi aplicado no questionário, utilizado como instrumento de coleta de dados, enviado para 102 IFES, ficando disponível por pouco mais de 4 meses, obtendo 101 respondentes, porém, apenas 32 finalizaram o questionário e tiveram as respostas analisadas. Pela análise dos dados coletados, foi possível concluir que a realidade das IFES em relação à SI precisa de atenção e apoio da alta administração, pois, apesar de as normas elencarem diversas ações de SI aplicáveis, as IFES aplicam ações de forma *ad hoc* em sua maioria. A tese concluiu que é possível implementar de forma integrada e simplificada ações de segurança da informação nas IFES, para isso, porém, é fundamental o apoio da alta administração, desde financeiro à promoção de cultura em SI, passando por ações de conscientização e qualificação.

Palavras-chave: gestão da segurança da informação; gestão de riscos de segurança da informação; instituições federais de ensino superior; OCTAVE *Forte*.

ABSTRACT

Today's society has information as its transforming element. In the Federal Institutions of Higher Education (IFES) it could not be different, since the information flow has progressively become a structuring element. Therefore, identifying and addressing the security risks that affect these flows is a requirement for such organizations. However, it is observed that the absence of information security (IS) actions in these institutions is, in general, due to the difficulty in applying the existing risk analysis models, considered the pillar of this process. This difficulty occurs because models are proposed for more general purposes that the context of a university requires. The research proposed to develop an integrated and simplified model of actions for risk analysis, specific to the context of the technology sectors of the IFES. After a systematic review of the literature, the internationally recognized framework OCTAVE Forte was chosen for the elaboration of the model, together with the federal government's information security standards and recommendations, which govern the bodies and entities of the Federal Public Administration on the subject of security of information. To achieve this objective, an applied research was carried out, classified as exploratory, in its first phase, and descriptive, in its second phase, based on a mixed approach research that combined qualitative and quantitative research techniques. The information was obtained by the methods of collection used: documental research and application of an online survey. For data analysis, content analysis and statistical analysis were used. Thus, it was intended to identify the conceptual elements for the development of an integrated and simplified model of information security actions. The conceptual elements obtained in this thesis allowed the creation of the MISASI STI model, which can be used as a guide to explore and evaluate existing IS actions and/or necessary for the technology sectors of the IFES. This model was applied on a survey, used as a data collection instrument, and was sent to 102 IFES, being available for just over 4 months, obtaining 101 respondents, however, only 32 completed the survey and had their responses analyzed. Through the analysis of the data collected, it was possible to conclude that the reality of the IFES in relation to the IS needs attention and support from the top management, because, although the rules list several applicable IS actions, the IFES apply actions in an ad hoc way in their majority. The research concluded that it is possible to implement information security actions in the IFES in an integrated and simplified way, for this, however, the support of the top management is essential, from financial to the promotion of culture in IS, through awareness and qualification actions.

Keywords: information security management; information security risk management; federal institutions of higher education; technology sectors; OCTAVE Forte.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
APF	Administração Pública Federal
NC	Norma Complementar
CERT.br	Centro de Estudos Respostas e Tratamento de Incidentes
CI	Ciência da Informação
CTIR GOV	Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo
E-gov	Governo Digital
ETRI	Equipe de Tratamento e Resposta a Incidentes
GSI	Gabinete de Segurança Institucional
IFES	Institutos Federais de Ensino Superior
IN	Instrução Normativa
IoT	*Internet of things* / Internet das Coisas
MISASI STI	Modelo Integrado Simplificado de Ações de Segurança da Informação para Setores de Tecnologia das IFES
NIST	Instituto Nacional de Padrões e Tecnologia
LGPD	Lei Geral de Proteção de Dados
OCTAVE *Forte*	*Operationally Critical Threat, Asset, and Vulnerability Evaluation For The Enterprises*
PDCA	*Plan-Do-Check-Act*
POSIC	Política de Segurança da Informação e Comunicações
RSL	Revisão Sistemática de Literatura
SI	Segurança da Informação
SIC	Segurança da Informação e Comunicações
STI	Setores de Tecnologia das IFES
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

Ao longo das últimas três décadas, os mercados de bens e serviços passaram por determinantes transformações, perante as exigências do atual contexto da sociedade, fundamentadas nos aspectos informacionais e tecnológicos. As organizações, com seus novos padrões administrativos, alicerçadas no planejamento interativo e liberal, estão compreendendo a informação e o conhecimento como principais componentes do planejamento estratégico, em termos da manutenção do grau da competitividade referente aos seus bens e serviços.

Com base nas novas formas de modelo administrativo, as organizações passaram a entender a importância dos documentos e informações, mediante a preocupação do processo de gerenciamento, de modo a buscar um processo eficaz de organização, armazenamento, disseminação e compartilhamento – processo caracterizado como fluxo formal de informação (DUARTE; SILVA; COSTA, 2007). Em organizações, o fluxo informacional tornou-se intenso de forma progressiva, em que as dinâmicas das demandas de informação precisam ser efetivamente atendidas conforme os meios existentes. Nesse sentido, a qualidade do desempenho organizacional encontra-se intimamente relacionada aos fluxos de recursos que percorrem todo o ambiente organizacional beneficiando os objetivos operacionais, táticos e estratégicos (GREEF; FREITAS, 2012).

Nesse contexto, como ativo essencial para o funcionamento organizacional, a informação flui de forma ininterrupta por todo o ambiente da organização instigando o seu desenvolvimento. Ou seja, ocorre a transmissão de conjunto de dados pelas unidades que compõem a organização de forma a alcançar todos os espaços que necessitam de sua atuação para a movimentação dos negócios (GREEF; FREITAS, 2012, p. 39). Considerando a atual sociedade da informação, onde os processos organizacionais quase integralmente fazem uso de suportes tecnológicos, pelos quais a informação transcorre em uma organização, é imprescindível avaliar as condições de proteção que envolvem todo esse processo, conforme a forma ou o meio pelo qual é organizada, armazenada e compartilhada, uma vez que a informação, como importante ativo social e econômico, precisa ser considerada como um patrimônio das organizações, sejam públicas ou privadas.

O tratamento dos problemas relativos à proteção informacional, em meio organizacional, está diretamente integrado ao campo da gestão da informação que compreende as ações de segurança da informação (FONTES, 2006, p. 26; SÊMOLA, 2003,

p.43). No contexto atual, cuja sociedade e a economia vivenciam o expressivo contingente informacional em seus fluxos formais contínuos, compreende-se a segurança da informação (SI) fundamentada nas transformações e inovações da tecnologia da informação – que é uma importante ferramenta de apoio das organizações, desde as atividades operacionais às estratégicas. No entanto, deve-se considerar que nessa condição, as organizações não podem se apoiar unicamente no investimento em tecnologia da informação, e estabelecer o seu alinhamento aos objetivos do negócio, mas é necessário compreender e conhecer os requisitos de segurança para os tipos de informação, em conformidade com os suportes que a sustentam, ao longo do processo de fluxo informacional.

Nesse cenário, entende-se por suportes as tecnologias que sustentam a informação organizacional durante o processo de fluxo formal, que auxiliam na tríade organização-armazenamento-compartilhamento, em referência ao meio digital nesse processo, que, no contexto do ambiente organizacional atual, compreende um dos principais meios de sustentação e transporte da informação de uma organização por atender as exigências das dinâmicas operacionais e estratégicas (SANDI, 2007). Dessa forma, considerando-se os processos de manipulação, inserção e encaminhamento em meio digital, é inerente a observação de ações de segurança perante os possíveis incidentes que as informações estão sujeitas durante esse processo.

Cada série de tarefas nesse processo representa uma dinâmica própria, cujo tema segurança da informação torna-se progressivamente recorrente, bem como uma preocupação maior nas organizações. No entanto, essa problemática não corresponde somente à eliminação de vulnerabilidades e proteção contra incidentes maliciosos, mas abrange toda a complexidade que envolve a segurança das informações de forma efetiva, e que possa garantir a compreensão dos riscos de segurança e conscientização das necessidades de controles para o processo de fluxo de informação nos suportes tecnológicos nas diferentes atividades que administram a dinâmica organizacional.

Inseridas nesse contexto, as Instituições Federais de Ensino Superior (IFES), segundo as suas necessidades informacionais para o desenvolvimento de sua missão pautada no tripé ensino, pesquisa e extensão, administram a complexidade peculiar do seu fluxo informacional, baseado em suportes tecnológicos, que, de forma sistematizada, auxiliam, em suas atividades meio e fim por intermédio de sistemas integrados. Essas instituições dependem das inovações tecnológicas para tornar os seus serviços de tecnologia da informação mais eficazes e eficientes, para a obtenção de respostas administrativas, de

pesquisas e educacionais mais ágeis e rápidas, sendo a comunidade acadêmica e, consequentemente, a sociedade, as maiores beneficiárias dessa eficiência.

Como a tecnologia da informação está em constante evolução, seja devido às inovações seja pela necessidade de melhoria contínua dos serviços organizacionais, observa-se que há diferentes formas de contribuição para que aconteça a movimentação do fluxo informacional nas instituições federais de ensino para suprir suas necessidades. No entanto, assim como as demais organizações, essas instituições precisam investir em ações que permitam uma análise dos riscos inerentes ao fluxo formal de forma a garantir a funcionalidade de sua integração sistêmica, e corresponder aos objetivos organizacionais no processo de ensino, pesquisa e extensão.

Nessa perspectiva, os aspectos que norteiam a proteção dos ativos informacionais das IFES, ao longo do processo de fluxo de informação em suportes tecnológicos, requerem a necessidade de ações integradas de segurança da informação. Que contribuem para uma maior proteção, quando houver necessidade, das informações que transitam no contexto dessas instituições. Para tanto, essa contribuição pode começar por meio de investigações que possam elaborar diagnósticos de fluxos informacionais, em suportes tecnológicos, nas distintas unidades organizacionais de universidades e institutos. Com base em *frameworks* de gerenciamento e normas internacionais e institucionais específicas para a segurança da informação, de modo a contemplar uma análise de riscos bem planejada e aplicada, que possa contribuir com um gerenciamento de riscos mais eficaz perante a natureza dessas instituições, cujo principal benefício consiste em tomar decisões e levantar ações que visam prover a proteção da informação organizacional ao longo de seu fluxo formal.

A necessidade de segurança da informação aumenta à medida da intensidade do fluxo informacional, ampliado por meios da tecnologia da informação, em que se evidencia a rapidez e eficiência nos processos de negócios organizacionais. Entretanto, a ausência de segurança pode vir a resultar em grandes prejuízos, bem como em falta de oportunidades de negócios. Nesse sentido, observa-se que há uma variedade de fatores que justificam a preocupação com um processo de segurança contínuo: a evolução dos ataques, a emergência de novas vulnerabilidades provenientes das inovações tecnológicas, o aumento da conectividade, além do aumento dos crimes digitais.

As Instituições Federais de Ensino Superior, em seu processo de fluxo informacional, precisam contemplar a problemática da ausência de ações de segurança, uma vez que seus processos de negócio passam – ou deveriam passar, se considerar a eficiência no serviço público como premissa – pelos sistemas integrativos de informação que interligam as séries

de tarefas do fluxo formal de informação, que auxiliam as universidades e institutos federais de ensino em seus processos, atividades e tarefas, com qualidade, eficiência, eficácia e segurança.

Considerando que as Instituições Federais de Ensino Superior fazem parte das organizações públicas federais, evidencia-se, quanto à necessidade de segurança da informação, que o Tribunal de Contas da União (TCU) elaborou o Relatório de Avaliação da Governança de Tecnologia da Informação no âmbito da Administração Pública Federal, o que resultou no Acórdão do TCU de nº 3117/2014, onde se esclarece que, das 355 organizações públicas federais pesquisadas, apenas 38% declararam identificar os riscos de segurança da informação, com base na tecnologia da informação nos processos críticos de negócio, sendo que apenas 21% tratam esses riscos, revelando que a maior parte da Administração Pública Federal não compreende os riscos à que estão sujeitas, sua probabilidade e impacto no negócio e, mesmo as que compreendem, não realizam o tratamento dos riscos de modo a mantê-los em níveis e custos aceitáveis (TRIBUNAL DE CONTAS DA UNIÃO, 2014, p. 4-29).

A segurança da informação tem sido objeto de preocupação constante da parte de órgãos fiscalizadores, principalmente devido à baixa conformidade das organizações em relação aos normativos e às boas práticas aplicáveis. Para o TCU, a temática sobre segurança não se limita aos aspectos tecnológicos, embora a exposição a riscos de segurança da informação possa ser decorrente também da falta de uma adequada governança de tecnologia da informação, devendo haver uma orientação para a gestão corporativa da segurança da informação nos órgãos públicos federais (TRIBUNAL DE CONTAS DA UNIÃO, 2014, p. 4-29).

Observa-se que a análise e gestão de risco é um problema recorrente em diferentes organizações, desde escritórios pequenos e familiares a grandes organizações públicas e privadas. Uma vez que as ameaças cibernéticas estão relacionadas à perda, remoção ou alteração de informações que residem ou são processadas pela tecnologia, os riscos podem surgir de dentro e de fora de uma organização, e por erro do funcionário ou ação deliberada.

Como forma de prevenção, a existência de uma comunicação interna das informações de segurança cibernética para os funcionários, de acordo com sua função, no programa de gerenciamento de riscos de segurança, deve constar na política de segurança da informação, com a devida publicidade, bem como ações devem ser avaliadas periodicamente, como: assinatura do termo de responsabilidade na entrada do funcionário na organização; e cursos de treinamento, que abrangem práticas básicas de segurança da informação que apoiam o

funcionamento de um programa eficaz de gerenciamento de riscos, projetado para ajudar os funcionários a identificar e responder a ataques de engenharia social (*phishing*, uso não autorizado) e a evitar práticas inadequadas (por exemplo, anotar senhas ou deixar material confidencial sem supervisão); e conscientização dos funcionários sobre a política corporativa. Prevendo que, se um funcionário viola as políticas da empresa, será fornecido treinamento adicional ou outras ações disciplinares a serem tomadas. Funcionários com responsabilidades de trabalho que se enquadram diretamente no programa de gerenciamento de riscos de segurança cibernética (equipe de Tecnologia da Informação (TI), gerenciamento de TI, auditoria interna e similares) têm requisitos adicionais para concluir o treinamento técnico e específico do trabalho ao longo do ano. Além disso, os funcionários que têm acesso direto aos dados de usuários e funcionários (por exemplo, vendas, atendimento ao cliente, recursos humanos, suporte técnico de TI e finanças) devem receber treinamento específico sobre gerenciamento de incidentes, manipulação de informações e proteção de dados (AICPA, 2018, p. 1, tradução nossa; MOORE, 2019, p. 16, tradução nossa).

Com essa percepção, observa-se a necessidade de conformidade das universidades e institutos federais de ensino com os normativos de segurança da informação, para que ações de prevenção sejam implementadas. Considerando-se que essas ações exigem uma análise de riscos bem fundamentada e aplicada ao contexto organizacional, a dificuldade de aplicação dos modelos existentes de análise de riscos se dá por não serem específicos ao contexto que uma universidade e/ou instituto de ensino público exige.

Esta pesquisa defende que ações de segurança da informação se fazem necessárias nas Instituições Federais de Ensino Superior. Especialmente nos suportes às tecnologias que sustentam a informação organizacional durante o processo de fluxo formal, abrangendo cada tarefa existente na dinâmica envolvendo os setores de tecnologia dessas instituições. Sejam ações relacionadas a pessoas, ambiente, infraestrutura ou tecnologias. A imagem de um cadeado fechado indicando proteção faz-se necessária não somente no acesso a sistemas, mas também envolvendo todas as ações que permeiam o sistema em si.

Na presença da problemática, envolvendo a segurança das informações organizacionais, torna-se necessário o desenvolvimento e aplicação de um modelo integrado e simplificado de ações para análise de riscos de segurança da informação específico para informações em suportes tecnológicos das IFES. Um modelo que permita abranger ações de segurança menos restritas e, ao mesmo tempo, assegurar a proteção da informação organizacional com base nos suportes tecnológicos que a sustenta. Uma vez que as universidades e institutos federais de ensino, além de estarem atualizando os meios

tecnológicos pelos quais transitam a informação, em face da demanda informacional exigida pela comunidade acadêmica e sociedade, não deixam de ser um ambiente caracterizado pela pluralidade de ideias e liberdade de expressão. Devendo os riscos informacionais nessas instituições serem controlados em benefício da sociedade, garantindo não apenas a proteção da informação exclusivamente institucional, mas também a disponibilidade da informação que precisa ser pública.

Nesse sentido, Assange (2013, p. 64) chama atenção para a interceptação estratégica da parte do Estado, que na prática consiste em interceptar a todos, independente de serem inocentes ou culpados, evidenciando um sistema de vigilância com essência de *establishment*, que, segundo o autor, sempre apresentará ausência de desejo político em expor a espionagem da parte do Estado. O uso da tecnologia, na prática secreto, não pode esperar uma supervisão democrática expressiva. Afinal quem vigia o vigilante estatal? Como é muito difícil essa ação, torna-se necessário que a análise de riscos a ser desenhada ao contexto das instituições públicas envolva ações de segurança que não permitam a criação de estruturas de vigilância, mas sim medidas de controle de segurança da informação, cujo limite proibido seja justamente essa estrutura.

Diante desse cenário, a presente pesquisa pretendeu responder ao seguinte questionamento: **como ações de segurança da informação poderiam ser implementadas (ou melhoradas) considerando a dinâmica do fluxo de informação em suportes tecnológicos das Instituições Federais de Ensino Superior, a partir de um modelo integrado e simplificado de ações de segurança da informação adequado para os setores de tecnologia dessas instituições?**

No intuito de responder a essa questão, esta tese se apoiou na revisão sistemática de literatura para conhecimento dos métodos de análise de riscos, nas normas e recomendações de segurança da informação aplicáveis à Administração Pública Federal, e na pesquisa de realidade das IFES quanto às ações advindas desse aporte teórico, para enfim estabelecer elementos conceituais para um modelo integrado e simplificado de ações de segurança da informação.

Como justificativa, observa-se que a partir da década de 2000, a Administração Pública Federal (APF) iniciou uma série de ações de governo digital, denominadas “governo eletrônico” (e-Gov), com o objetivo de priorizar o uso das tecnologias para democratizar o acesso à informação, aumentar a participação popular em políticas públicas, bem como aprimorar a qualidade e efetividades dos serviços e informações (BRASIL, 2016ª, p. 9).

Ao longo das duas últimas décadas, pôde-se observar a tendência das ações do governo eletrônico frente aos avanços da tecnologia e demandas da sociedade

Figura 1- Principais marcos de governo eletrônico na APF

Fonte: Adaptado para quadro de Estratégia de Governança Digital (BRASIL, 2016ª, p. 9).

. Entre as novidades nessa área, observa-se, em 2016, a instituição da Política de Governança Digital e Política de Dados Abertos, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. Demandando estratégias e estudo de ações integradas em segurança da informação, especialmente, após o aumento de

serviços públicos oferecidos por intermédio do e-gov, demandando serviços prestados não apenas com qualidade, mas também com segurança.

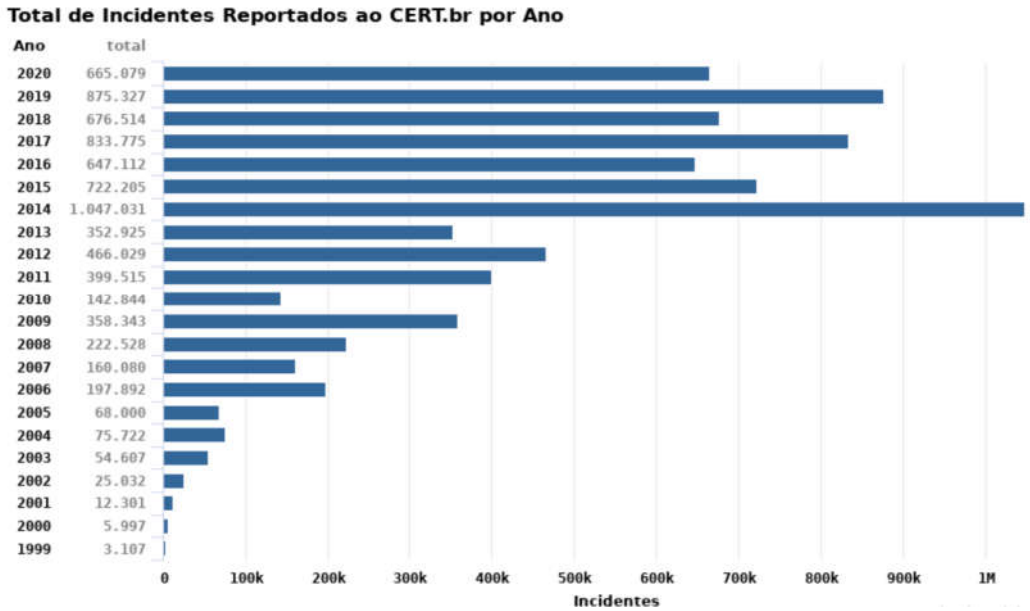
O termo segurança da informação nos remete à ideia de que a informação, como valor, deve ser guardada ou assegurada, ou seja, uma visão de ativo, o que indica que há necessidade de proteção da informação. Nesse sentido, diariamente, há notícias das mais diversas áreas que destacam os problemas relacionados aos riscos e ameaças em face da segurança da informação em suportes tecnológicos: vazamento de números de cartão de crédito, acesso às contas bancárias por hackers, acesso indevido aos sistemas organizacionais.

De acordo com Mandarino Junior e Canongia (2010, p. 13), a importância da segurança da informação no processo de comunicação entre os sistemas integrados, ou seja, em fluxos de informação em suportes tecnológicos, como função estratégica de Estado, é "essencial à manutenção das infraestruturas críticas de um país, tais como Energia, Defesa, Transporte, Telecomunicações, Finanças, da própria Informação, dentre outras", devendo as infraestruturas críticas dos países serem protegidas, entre elas a informação (MANDARINO JUNIOR; CANONGIA, 2010, p. 13).

Considera-se que existem diversas formas de ameaças de segurança da informação, que abrangem desde erros humanos e falhas de sistemas até espionagem industrial e crimes cibernéticos. Nesse entendimento, a ameaça abrange os eventos indesejados que englobam desde aspectos tecnológicos, a processos executados e, principalmente, ações humanas, que em algum momento interagem com os suportes tecnológicos, bem como com o fluxo informacional (BEZERRA, 2013, p. 3). Dessa forma, verifica-se que, apesar de ameaças e incidentes poderem ser pontuais, a segurança da informação, para ser efetiva, demanda ações integradas que incluam analisar os riscos a que as instituições estão expostas, implementar controles de segurança e mecanismos que possibilitem o monitoramento do desempenho de proteção.

No Brasil, o Centro de Estudos Respostas e Tratamento de Incidentes (CERT.br) monitora o registro de incidentes de segurança da informação no Brasil. Na Figura 2, pode-se observar que os registros aumentam a cada ano. Em 2014, houve recorde de registros no País.

Figura 2 - Estatísticas dos Incidentes Reportados ao CERT.br por ano



Fonte: Centro de Estudos e Respostas de Tratamento de Incidentes de Segurança no Brasil (COMITÊ GESTOR DE INTERNET, 2022).

Nesse caso, observa-se uma tendência crescente dos incidentes em suporte tecnológico no Brasil, especialmente nos últimos anos. Confirmando essa ideia, na Figura 3, observa-se que o Brasil se encontra em segundo lugar no mundo como alvo de incidentes cibernéticos, aparecendo com a segunda cor mais escura no mapa, o que evidencia a importância do tema segurança da informação em suporte tecnológico, para o País, também perante as instituições públicas.

Figura 3 - Países destinatários das Notificações de Incidentes

Fonte: Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR GOV, 2022) .

Nesse cenário, apesar de ser praticamente impossível projetar e desdobrar um ambiente livre de incidentes no ambiente digital, as ações de segurança da informação tornam-se salutar no intuito de possibilitar o controle dos riscos existentes em fluxos de informação institucionais, de modo que a informação seja protegida no transcurso das séries de tarefas evidenciadas em processos organizacionais abrangendo os suportes tecnológicos.

Dessa forma, observa-se que um modelo integrado e simplificado de ações de segurança da informação, se faz necessário para direcionar as ações de SI, no âmbito das universidades e institutos federais de ensino brasileiros. Devido à dinamização dos processos de fluxo informacional em suportes tecnológicos, que favorecem o ciclo informacional contínuo possibilitando a interação e integração entre atividades administrativas e acadêmicas.

A relevância desta pesquisa se justifica perante a importância da temática segurança da informação diante do contexto de inovação e dinamização tecnológica que acompanha as atividades das Instituições Federais de Ensino Superior nas últimas décadas, com processos atualizados para os suportes tecnológicos de forma integrada, implantados com o intuito de apoiar o desenvolvimento de ensino, pesquisa e extensão. A automatização de seus processos de fluxos de informação, no que se refere à organização, armazenamento e compartilhamento das informações, demandando da organização a preocupação quanto aos padrões e ações de segurança que sejam compatíveis com o valor informacional.

Observa-se que essa problemática se insere no campo da gestão da informação e do conhecimento, evidenciando que não basta conceber essa gestão como um conjunto de processos que envolvem a organização e seu ciclo informacional e do conhecimento. É necessária a proteção da informação ao longo de todo o transcurso no fluxo informacional das organizações. Necessidade essa evidenciada pela temática Segurança da Informação no campo da gestão da informação dentro da Ciência da Informação (CI). Nesse sentido, esta pesquisa visa suprir lacunas no campo teórico, pois, de acordo com a Revisão Sistemática de Literatura, capítulo 2.1, nas ciências sociais, em especial na CI, estudos em segurança da informação foram incipientes uma vez que dos 808 artigos disponibilizados nas bases de dados científicas pesquisadas, as principais bases de dados da CI, LISTA e ISTA, retornaram apenas 61 publicações na área.

No campo acadêmico, a importância da pesquisa foi evidenciada, como contribuição de impacto social, a gama de possibilidades que o estudo das ações de segurança da informação nas IFES abre para essas instituições, consolidando, em âmbito nacional, por intermédio de um modelo integrado e simplificado, as ações dos gestores responsáveis pela SI

nos setores de tecnologia, responsáveis pelo armazenamento e disponibilização da informação digital nessas instituições. Possibilitando, assim, a promoção de boas práticas de segurança e chamando atenção para as necessidades dessas instituições em SI, evidenciando o rol de possibilidades de implementação de ações de SI, desde o planejamento, perpassando pela análise de riscos, resposta a riscos e ações de monitoramento contínuo.

A contribuição científica remonta o evidenciado na Revisão Sistemática de Literatura, por ser uma temática de grande importância no meio científico, com pesquisas em crescimento contínuo, ampliada pelo contexto de pandemia, trabalho remoto e forte uso de bases tecnológicas nas organizações. A segurança das informações em suportes tecnológicos necessita das pesquisas científicas por serem a mais valia dentro das organizações na atualidade. Apesar da importância organizacional, quando a instituição investe em segurança da informação, quem ganha é a sociedade, um ganho muitas vezes invisível, porém de alto impacto, pois, quando há falhas de segurança exploradas, a perda de informação e os danos ao usuário são irreversíveis.

Como justificativa pessoal, a ideia inicial da tese consistiu em conhecer as ações de segurança da informação necessárias para garantir um nível mínimo contínuo de proteção às IFES. Esclarece-se que essa ideia surgiu ao término do mestrado em Ciência da Informação, no qual a autora desta pesquisa havia realizado a análise de riscos de segurança no sistema acadêmico da sua instituição de ensino. Posteriormente, retornando ao setor de tecnologia em que trabalha, a autora levou consigo o resultado da pesquisa de mestrado, o qual foi bem recebido pelos gestores locais que, a partir desse resultado, implementaram, dentro de suas limitações, ações específicas de segurança. Com essa implementação, foi possível perceber que as ações estabelecidas foram pontuais, condição que levou ao seguinte questionamento: quais ações de segurança da informação seriam necessárias para manter um nível mínimo de proteção nos setores de tecnologia das IFES?

Perante essa condição, fez-se necessário o desenvolvimento de um modelo integrado e simplificado de ações de segurança da informação, específico e apropriado às IFES, para proteção informacional, uma vez que, dentre o conjunto dessas instituições em âmbito nacional, algumas provavelmente possuem amadurecimento nessa área, enquanto outras estão começando a compreender essa demanda, conforme foi identificado na pesquisa de realidade das IFES, capítulo 4.2.

Em uma perspectiva prática, a relevância da pesquisa se dá pela investigação no campo das ações possíveis e necessárias de segurança da informação que possam enfrentar a

problemática existente no processo de segurança da informação para o fluxo informacional em suportes tecnológicos das IFES.

Diante do exposto, a pesquisa encontra-se justificada pela relevância do assunto, pelo aumento de incidentes de segurança em rede na Administração Pública Federal, indicando uma tendência, além da necessidade de um modelo integrado e simplificado apropriado às Instituições Federais de Ensino Superior que possibilite controle e monitoramento contínuo da segurança da informação nos fluxos de informação em suportes tecnológicos dessas instituições.

1.1 HIPÓTESE GERAL DA TESE

Com base no problema de pesquisa foi possível formular a seguinte hipótese geral: Com um modelo integrado, alinhado a *frameworks* reconhecidos internacionalmente e às normas e recomendações do governo federal, para segurança da informação, é possível simplificar as ações de segurança para análise de riscos, no âmbito dos setores de tecnologia das Instituições Federais de Ensino Superior.

1.2 OBJETIVOS

No intuito de responder ao problema e testar a hipótese geral da tese, os objetivos foram delineados de modo a contemplar a construção de um modelo integrado e simplificado de ações de segurança da informação específico para os setores de tecnologia das instituições federais de ensino superior, com a contribuição de IFES, em âmbito nacional.

1.2.1 Objetivo Geral

Desenvolver um modelo simplificado de gestão de riscos para ações de segurança da informação específico para os setores de tecnologia das Instituições Federais de Ensino Superior, integrado às normas nacionais e recomendações internacionais.

1.2.2 Objetivos Específicos

a) Elaborar Revisão Sistemática de Literatura para conhecimento dos métodos de análise de riscos pesquisados pela comunidade científica;
b) Realizar pesquisa documental dos principais frameworks internacionais de gerenciamento de riscos, normas do governo federal, normas institucionais das IFES colaboradoras, e normas específicas, relacionadas à segurança da informação;
c) Conhecer a realidade das IFES quanto às ações, de processo e operacionais, de segurança da informação à luz do framework reconhecido internacionalmente OCTAVE *Forte* e das normas do governo federal para segurança da informação em setores de tecnologia;
d) Propor *checklist* de controles para subsidiar o modelo de ações de segurança da informação para os setores de tecnologia, considerando o fluxo de informação em suportes tecnológicos.

Com os objetivos delineados, o roteiro desta pesquisa encontra-se estruturado em cinco seções, que iniciou nesta introdução, seguida pela fundamentação teórica, procedimentos metodológicos, perpassando pela análise dos resultados, e, finalizando, com as considerações.

2 FUNDAMENTAÇÃO TEÓRICA

Esta seção visa apresentar a temática Análise de Riscos de Segurança da Informação com olhar voltado para a Administração Pública Federal, perpassando pelas normas, políticas e importância da análise de riscos de segurança da informação. Tendo como base a identificação de conteúdo por meio do desenvolvimento de uma Revisão Sistemática de Literatura. Para isso, a seção divide-se em três tópicos: o primeiro, relativo ao desenvolvimento da Revisão Sistemática de Literatura, que permitiu identificar como a comunidade científica vem abordando a temática da análise de riscos de segurança da informação; o segundo, aborda as normas específicas de segurança da informação aplicadas na Administração Pública Federal; e o terceiro, sobre os fluxos de informação em suportes tecnológicos em Instituições Federais de Ensino Superior.

2.1 ANÁLISE DE RISCO DE SEGURANÇA DA INFORMAÇÃO SOB A ÓTICA DA REVISÃO SISTEMÁTICA DE LITERATURA

Considera-se, em relação à revisão sistemática de literatura, que protocolos, como a colaboração Cochrane e recomendação PRISMA, foram desenvolvidos inicialmente para a área da saúde. No entanto, a abordagem de revisão sistemática de literatura é usada em diversas outras áreas, inclusive nas sociais, uma vez que, a Colaboração Cochrane conceitua a revisão sistemática de literatura como uma revisão que busca apresentar "evidências empíricas que atendem a critérios de elegibilidade, a fim de responder a uma pergunta de pesquisa específica." (HIGGINS; GREEN, 2011[1], tradução nossa).

As principais características de uma revisão sistemática, conforme Higgins e Green (2011, tradução nossa), consistem em: objetivos claramente estabelecidos, metodologia explícita e reproduzível, pesquisa sistemática que identifique os estudos elegíveis, dentre outros. Essas características da revisão sistemática auxiliam sua aplicabilidade em diversos estudos e temáticas possibilitando a coleta de evidências empíricas que preenchem os critérios de elegibilidade.

Considerando que a demanda de revisão sistemática surge com a necessidade dos pesquisadores em sumarizar toda informação existente sobre determinado fenômeno, em uma linha de definição semelhante, a recomendação PRISMA esclarece que uma revisão

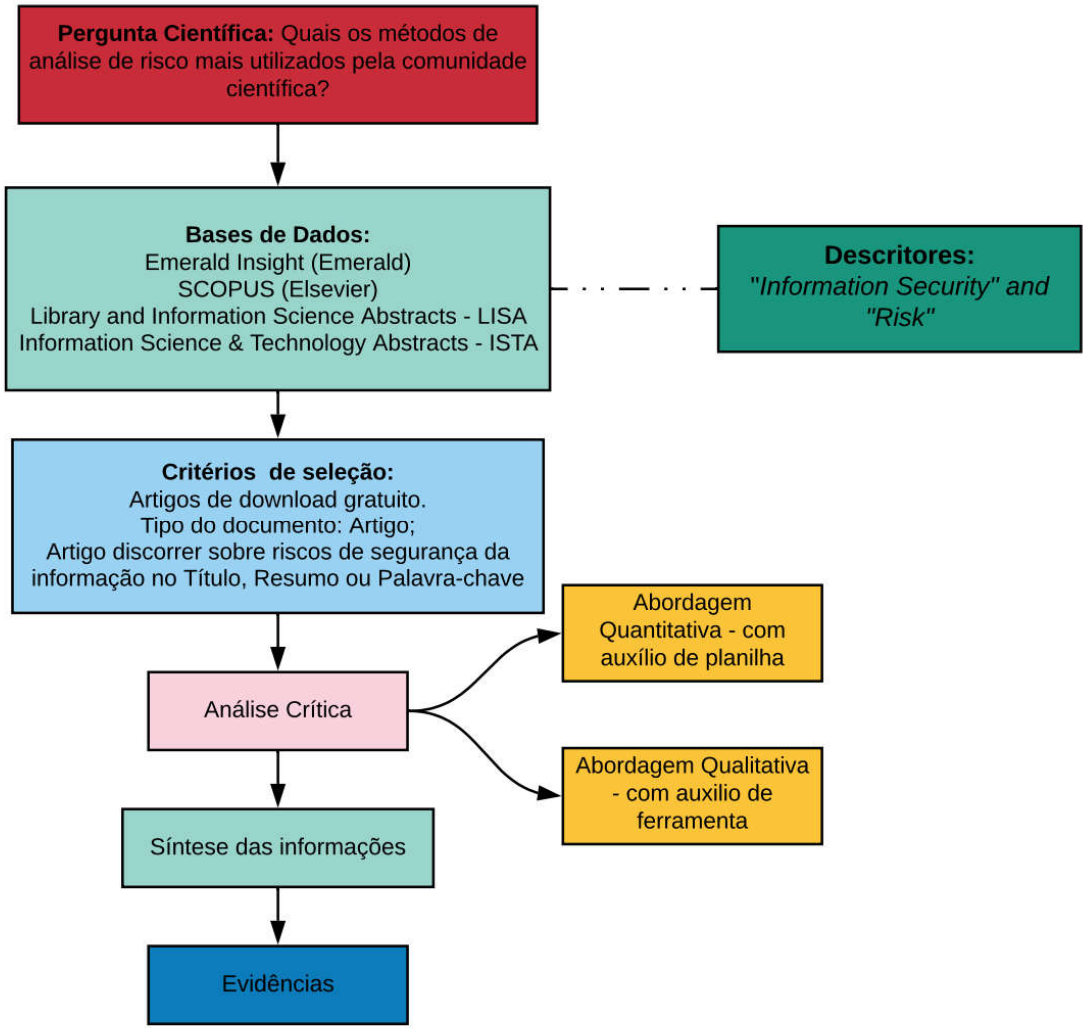
[1] Documento eletrônico não paginado.

sistemática é constituída por uma pergunta formulada de forma clara, que, por meio do uso de métodos sistemáticos e explícitos, possibilita seleção e avaliação crítica de pesquisas relevantes, coleta e análise desses estudos, bem como uso opcional de métodos estatísticos (meta-análise) para análise e resumo dos resultados (MOHER et al., 2015, tradução nossa).

Para esses autores, as revisões sistemáticas consistem em um processo interativo, o que significa que podem precisar modificar o protocolo de revisão original no decorrer da pesquisa, sendo assim, apenas 10% dos autores de revisão sistemática relatam trabalhar a partir de um protocolo. Nesse sentido, como exemplo, observa-se que Kitchenham (2004, tradução nossa) propôs um guia para revisões sistemáticas de literatura para pesquisas na área de engenharia de software.

A partir dessa observação, há de se ressaltar que a presente revisão sistemática se baseou no processo de revisão descrito por Sampaio e Mancini (2007), no intuito de se adequar à realidade da pesquisa. O critério de escolha das bases de dados se deu por serem bases de dados de referência para a Ciência da Informação, e de cobertura internacional, sendo uma delas, a Scopus, um dos maiores banco de dados de artigos científicos. Esta revisão sistemática de literatura consiste em um estudo quanti-qualitativo da produção científica na temática método de análise de riscos de segurança da informação, cuja estrutura está apresentada na Figura 4.

Figura 4 - Processo utilizado na RSL



Fonte: Elaborado pela autora (2022) a partir de Sampaio e Mancini (2007).

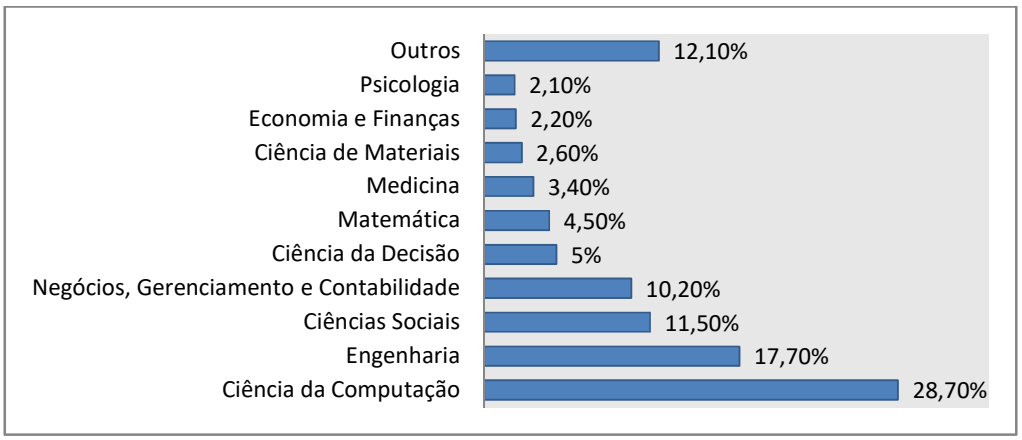
Com o processo da revisão sistemática e a pergunta científica definidos para a meta análise, procedeu-se ao levantamento dos artigos em 04 (quatro) bases de dados fortemente utilizadas na Ciência da Informação, uma delas, a Scopus, é a maior base de dados de artigos científicos. O levantamento ocorreu em julho de 2018, em uma primeira etapa de análise pré-qualificação, tendo sido atualizado em julho de 2021, em uma segunda etapa.

Com um leque amplo de bases escolhido, delimitou-se o período da publicação dos artigos para o período de 2016 a 2021. Os descritores analisados pela pesquisa, *"information security" and "risk*", foram utilizados no processo de busca em títulos, resumos e palavras-chave de artigos obtidos por download gratuito. No total, a pesquisa pôde observar um aumento da importância da temática na comunidade científica, uma vez que os pesquisadores

viram o total de artigos recuperados saltar de 146 na primeira etapa para 808 artigos recuperados das bases pesquisadas.

A Figura 5 mostra que essa temática está sendo publicada em pesquisas nas mais diversas áreas, estando a área de Ciências Sociais em terceiro lugar de publicação, estando atrás apenas de Computação e Engenharia, áreas que tradicionalmente pesquisam nessa temática.

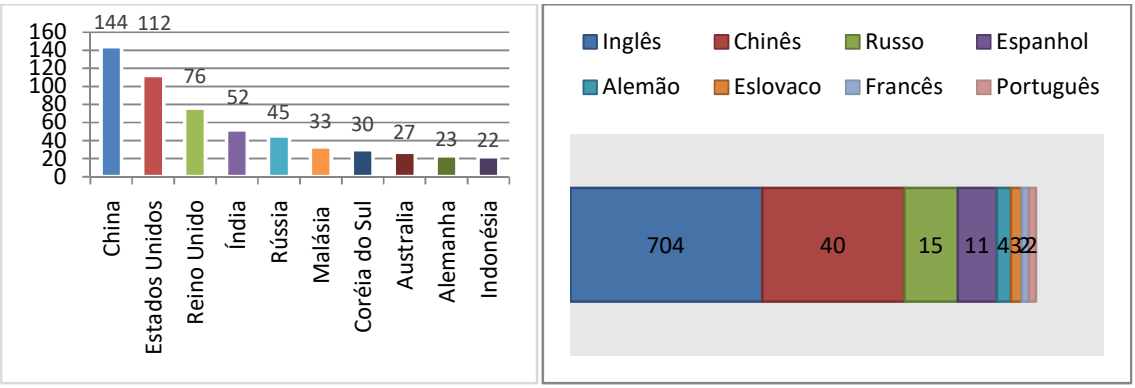
Figura 5 - Principais áreas de publicação na temática análise de riscos de segurança



Fonte: Dados da pesquisa (2022).

Do total de artigos recuperados, observa-se, na Figura 6, que o país que mais publicou na temática foi a China, com mais de 140 publicações, seguida de Estados Unidos e Reino Unido. Das publicações, a língua inglesa foi a mais utilizada, em torno de 90% dos artigos pesquisados, seguido de chinês, russo e espanhol, nessa ordem.

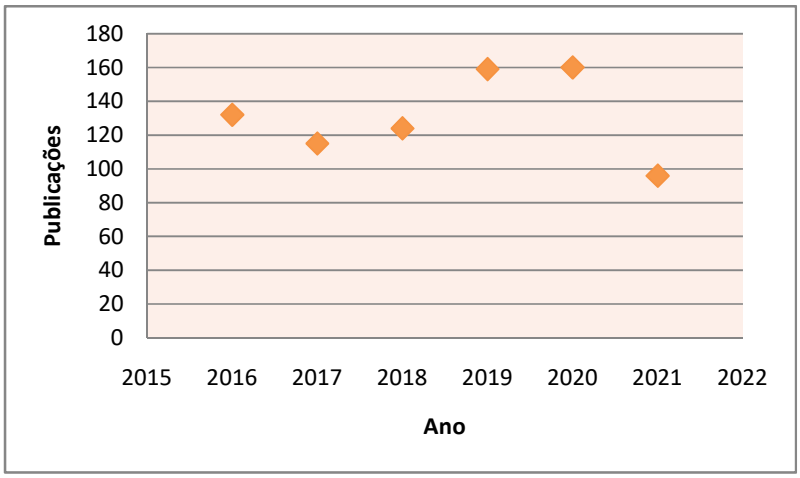
Figura 6 – 10 países que mais publicaram em análise de riscos versus línguas utilizadas



Fonte: Dados da pesquisa (2022).

Em relação ao quantitativo de publicações por ano, na Figura 7, observa-se que as publicações encontram-se em torno de 140, por ano, tendo se dado o ápice de publicações na temática por dois anos consecutivos, 2019 e 2020. No entanto, no ano de 2021, apesar de a pesquisa ter sido limitada a 01 de julho de 2021, em meados desse ano, o quantitativo de publicações já estava em quase 100, o que mostra uma tendência crescente de publicações na área pesquisada existente nos últimos anos.

Figura 7 - Quantitativo de publicações por ano



Fonte: Dados da pesquisa (2022).

Para análise dos dados obtidos, a etapa de análise crítica dos artigos fez uso das ferramentas NVivo 12[2] e Mendeley, para análise qualitativa, e planilhas eletrônicas, para análise quantitativa, que ajudaram a organizar e analisar as informações posteriormente sintetizadas no resultado da pesquisa, com 07 (sete) variáveis trabalhadas, identificadas no Quadro 1.

Quadro 1 - Variáveis trabalhadas pela RSL

1 Método de análise/avaliação de riscos utilizado	
2 Tipo de abordagem	2.1 Qualitativa 2.2 Quantitativa 2.3 Híbrida (Quanti-qualitativa)
3 Ênfase	3.1 Teórico 3.2 Empírico
4 Editoras que mais publicaram	

[2] NVivo é um software que suporta métodos qualitativos e variados de pesquisa. Projetado para organização, análise e seleção de informações não estruturadas ou qualitativas como: entrevistas, respostas abertas de pesquisa, artigos, mídia social e conteúdo web.

5 Objeto de estudo das pesquisas analisadas
6 Quantidade de pesquisadores
7 Palavras chaves envolvidas

Fonte: Dados da pesquisa (2022).

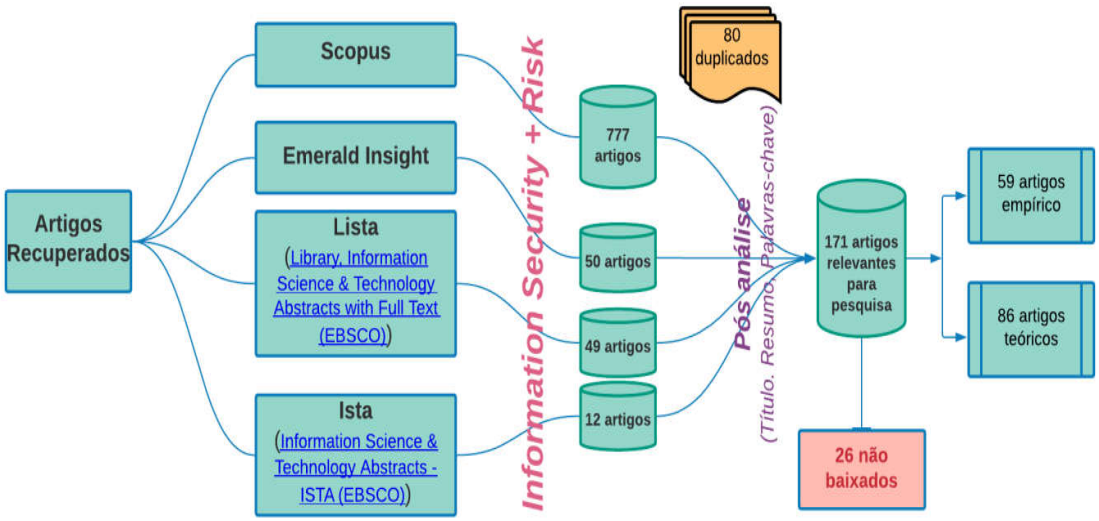
As variáveis apresentadas no quadro 1, acima, serão detalhadas durante a análise dos artigos recuperados na Revisão Sistemática de Literatura a seguir, uma vez que visam responder à pergunta científica elaborada.

2.1.1 Análise resultante da Revisão Sistemática de Literatura

Dos 808 artigos recuperados, sobre analise de riscos, das quatro bases de dados, resultantes dos critérios de seleção expostos na Figura 4, 80 artigos eram duplicados entre as bases. Em uma pré-análise do total de artigos recuperados, aplicaram-se critérios de exclusão ligados à temática, pois, foi considerado que os artigos excluídos apenas citavam os termos "risco" e "segurança da informação" em seus títulos, resumos ou palavras-chave, não fazendo referência efetiva a análise ou avaliação de riscos de segurança da informação.

Logo, nessa pré-análise buscou-se excluir artigos que não tinha por foco discorrer sobre a temática de análise/avaliação de riscos de segurança da informação. Após análise de título, resumo e palavras-chave, foram considerados 171 (cento e setenta e um) artigos relevantes para a pesquisa, dos quais 26 (vinte e seis) não estavam disponíveis ou não eram de acesso livre, 59 (cinquenta e nove) verificou-se serem empíricos e 86 (oitenta e seis) teóricos. Resultando em 145 (cento e quarenta e cinco) artigos considerados relevantes para a pesquisa, como pode ser observado na Figura 8.

Figura 8 - Quantitativo de artigos pesquisados na RSL



Fonte: Dados da pesquisa (2022).

Dos 145 artigos analisados, 27 usam, ou citam, algum método de análise de riscos, a serem detalhados mais à frente. Quanto à ênfase, conforme pôde ser visto na Figura 8, do total analisado, 86 artigos são considerados teóricos e 59 empíricos. O que demonstra predominância da abordagem teórica. No entanto, mesmo nesses artigos teóricos, observou-se preferência por validação das teorias apresentadas por intermédio de utilização de estudo de caso na quase a totalidade de artigos. Tudo isso justificável por ser uma temática em constante movimento e ligada fortemente à realidade das instituições, onde novas tecnologias são lançadas. O mundo digital se reinventa com esses lançamentos, surgem novas ameaças e vulnerabilidades, o que demanda estudos teóricos, que permitam melhorias que se adéquem à realidade mutável dos riscos. E os estudos empíricos, no intuito de serem experimentados nas diversas realidades, ajudam a confirmar as teorias existentes, bem como a formular novas teorias.

Quanto às publicações, esses artigos foram publicados em 72 periódicos científicos, pertencentes às editoras, das quais: a Elsevier foi a que mais publicou, totalizando 21 artigos, seguida das revistas IEEE e Springer, ambas com 13 (treze) artigos selecionados cada, e Emerald, com 08 publicações na temática. Todos os demais periódicos publicaram até 05 artigos no total, logo havendo média de uma publicação por ano. Mais detalhes podem ser vistos no Quadro 2

Quadro 2 – Periódicos científicos que mais publicaram

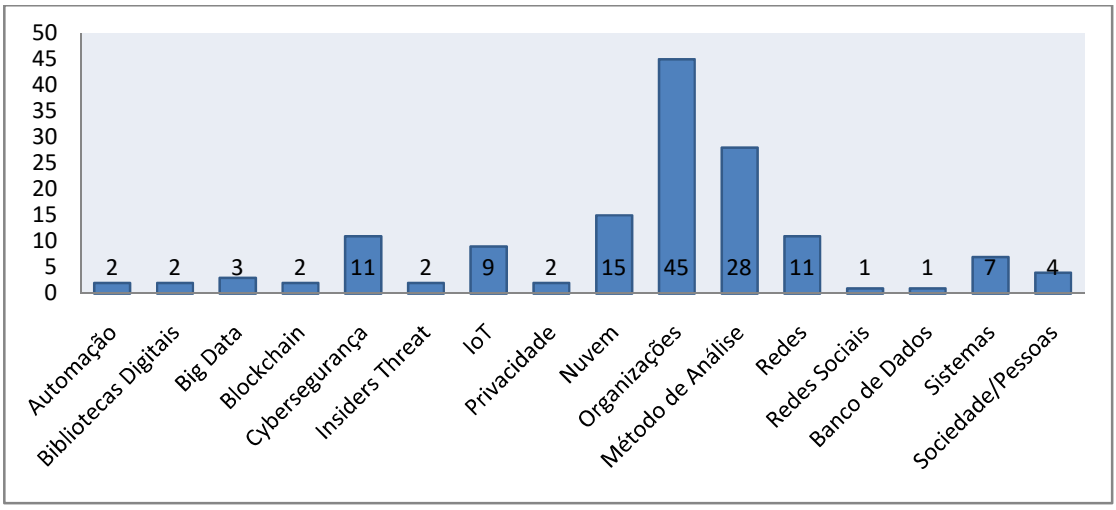
Publisher	Journal	Ano
Elsevier Ltd	*Computers and Security (8);* *Future Generation Computer Systems (2);* *Journal of Information Security and Applications (4);* *International Journal of Information Management (2);* *Computer Networks;* *Telematics and Informatics;* *Egyptian Informatics Journal;* *Government Information Quarterly;* *Heliyon;* *Technological Forecasting and Social Change*	*2021 (2)* *2020 (5)* *2019 (2)* *2018 (3)* *2017 (4)* *2016 (5)* *Total: 21*
IEEE Computer and Reliability Societies (Copublished)	*IT Professional (4);* *IEEE Latin America Transactions (2);* *IEEE Access (4)* *IEEE Photonics Journal;* *IEEE Computer;* *IEEE Security and Privacy;*	*2020 (1)* *2019 (2)* *2018 (5)* *2017 (4)* *2016 (1)* *Total: 13*
Springer	*International Journal of Information Security (2)* *Wireless Personal Communications (US);* *Automatic Control and Computer Sciences (US);* *International Journal of Systems Assurance Engineering and Management (India);* *Global Journal of Flexible Systems Management;* *Journal of Supercomputing;* *Nuclear and Radiation Safety;* *Journal of Medical Systems;* *Information Systems Frontiers(2);* *Requirements Engineering;* *Cluster Computing*	*2021 (1)* *2020(4)* *2019(3)* *2017 (3)* *2016 (2)* *Total: 13*
Emerald Group Publishing Ltd.	*Information and Computer Security (2);* *Electronic Library (2);* *Transforming Government: People, Process and Policy;* *Internet Research;* *International Journal of Supply Chain Management;* *International Business Management*	*2021 (1)* *2020 (1)* *2019 (1)* *2018 (1)* *2017 (1)* *2016 (3)* *Total: 8*

Fonte: Dados da pesquisa (2022).

Com as leituras dos artigos, foi constatada a afirmação que a grande maioria das pesquisas em análise ou avaliação de riscos são de abordagem qualitativa, e criticam-na por ser uma abordagem subjetiva. No entanto, dos 145 artigos analisados por esta revisão, 62 são qualitativos, 51 quantitativos e 32 utilizam abordagem híbrida, o que corresponde a, aproximadamente, 43%, 35% e 22%, respectivamente, demonstrando que a diferença de uso entre abordagem qualitativa e quantitativa é muito baixa, sendo a hibrida a abordagem menos utilizada.

No tocante aos objetos de estudo das pesquisas analisadas, referente à temática em risco de segurança da informação, constatou-se uma grande variedade quanto ao foco de pesquisa, conforme pode ser verificado na Figura 9. Nessa figura, evidencia-se 16 objetos de estudo elencados na linha horizontal, onde, de um total de 145 artigos analisados por inteiro, quase metade dos artigos pesquisam riscos de segurança da informação em organizações como um todo. Os demais preferiram pesquisar objetos mais específicos, como organizações, nuvens e redes, por exemplo.

Figura 9 - Objeto de estudo dos artigos



Fonte: Dados da pesquisa (2022).

Observa-se que há uma prevalência em se analisar riscos de segurança da informação em organizações, o que contou com 31% dos artigos analisados. Vale salientar que organizações envolvem como objeto de estudo pessoas, processos e tecnologias. Não obstante, o restante dos artigos analisados pesquisou objetos de estudo mais específicos ou análise de metodologias de avaliação de riscos em si, sem aplicar em um objeto específico.

Neste caso, quase 20% dos artigos preferiram estudar teorias, metodologias ou padrões existentes em análise ou avaliação de riscos. No entanto, riscos em tecnologias específicas como a de computação em nuvem, internet das coisas[3] (IoT), *bigdata*[4] *e blockchain*[5] foram

[3] Internet das Coisas (sigla em inglês "IoT") termo utilizado para a evolução tecnológica que envolve conectar os itens usados usados do dia a dia à rede mundial de computadores, como eletrodomésticos, meios de transporte, até roupas. (TECHTUDO, 2014, *online*)

[4] *Big data* é o termo utilizado para descrever o grande volume de dados que inunda uma empresa no dia a dia, onde sua análise leva a melhores decisões por meio do mapeamento de comportamentos, tendências e oportunidades de negócio. (TOTVS, 2021, *online*)

pesquisados, em menos de 10% dos artigos, com 15, 9, 3 e 2 artigos, respectivamente. Enquanto, tecnologias "antigas" como redes, sistemas e bancos de dados, na mesma proporção, estavam em 11, 7 e 1 dos artigos analisados, respectivamente. Desses dados observa-se predominância das pesquisas em organizações ou tecnologias utilizadas por elas.

No entanto, observa-se que as novas tecnologias, apesar de quantitativamente em pequeno número, têm entrado nos últimos anos no rol das pesquisas, como *Blockchain* e *Big Data*. Durante a análise foi possível evidenciar a preocupação referente a riscos ligados a *Smart Cities*[6], devido a explosão de IoT,como uma tendência; bem como o efeito *Snowden* fez aparecer pesquisas preocupadas com *Insiders Threats*, ameaças de segurança vindas de pessoal interno, na contramão de uma direção pró-sociedade; e também pôde-se observar o efeito Lei Geral de Proteção de Dados (LGPD), que fez aparecer pesquisas sobre riscos ligados especificamente ao princípio da privacidade na segurança da informação.

Quanto ao quantitativo de autores por publicação, observou-se que, das 145 publicações analisadas, houve predominância de publicações conjuntas entre dois, três e quatro autores, nessa ordem, totalizando, 28%, 26% e 21%, somando mais da metade das publicações, conforme Quadro 3.

Quadro 3 – Porcentagem de autores que publicaram em conjunto

Percentual de artigos	14%	28%	26%	21%	7%	3%	1,00%
Nº Autores	Um	Dois	Três	Quatro	Cinco	Seis	Sete

Fonte: Dados da pesquisa (2022).

Referente aos tipos de análise ou avaliação de riscos citados ou usados nos artigos investigados, pôde-se observar, durante a revisão, que, quase 40% dos artigos, (54 artigos exatamente), citam ou usam a série ISO 27000, com predominância da ISO 27005 para análise ou avaliação de risco, *National Institute of Standards and Technology* (NIST**) e** *Operationally Critical Threat, Asset, and Vulnerability Evaluation (*OCTAVE) também aparecem entre as metodologias mais correntemente citadas e/ou usadas nos artigos,

[5] Moeda virtual ou criptomoeda é um registro digital criptografado que funciona dentro de um banco de dados seguro conhecido como blockchain, que possui tecnologia que mantém as informações pessoais em local seguro e descentralizado. (FILHO, 2022, *online*)

[6] *Smart cities* traduzidas por cidades inteligentes são cidades que fazem uso de dispositivos IoT como sensores conectados, luzes e medidores conectados para coletar e analisar dados visando melhorar infrestrutura, serviços públicos e desenvolvimento sustentável.(INSIDER INTELLIGENCE, 2022, *online*)

estiveram em 29 e 19 artigos, respectivamente, sendo que cada uma delas foram elencadas juntamente com suas qualidades ou desafios.

Esses números não são mutuamente excludentes uma vez que, dos artigos analisados, vários trouxeram mais de uma metodologia, por vezes formulando comparações, além de outras que não são fortemente usadas, mas que foram objeto de estudo e serão detalhadas mais à frente. Foi feito um levantamento das palavras-chave utilizadas pelas publicações e as cem palavras que mais apareceram nos artigos publicados podem ser vistas na Figura 10.

Figura 10 - Cem palavras-chaves mais frequentes

Fonte: Dados da pesquisa (2022).

Os artigos localizados nesta revisão sistemática de literatura trataram de diversas abordagens, devido à variedade de objetos de estudos. Para melhor compreensão, esses artigos foram sintetizados nos subtópicos: Políticas de Segurança da Informação – entendimentos e conceitos, Segurança da informação aplicada às tecnologias – riscos e vulnerabilidades identificados, e Métodos de Análise/Avaliação de Riscos – escopos e abordagens.

2.1.1.1 Políticas de Segurança da Informação – entendimentos e conceitos

Segundo Valencia-Duque e Orozco-Alzate (2017, p. 81, tradução nossa), uma política de segurança da informação (PSI) é uma diretriz que ajuda a alcançar os objetivos, definidos de acordo com o escopo, e considerada como o primeiro controle da norma ISO / IEC 27002. Os autores observam que apesar de a política geral de segurança da informação ser apenas uma, dela se desprende políticas específicas, como, por exemplo, política de acesso, de uso de dispositivos móveis, de backup, entre outras. As políticas devem estabelecer, dentre outras diretrizes, os objetivos de segurança da informação, existentes no sistema de gestão de segurança da informação.

Para Dawson (2018, p. 60, tradução nossa), a política deve ser construída observando múltiplas diretivas, padrões, mandatos, leis e melhores práticas. Nos Estados Unidos, isso pode incluir políticas do Departamento de Defesa (DoD), do Instituto Nacional de Padrões e Tecnologia (NIST), normas militares e muito mais. Portanto, a política constitui a linha de base para guiar e orientar as organizações a observarem as normas gerais de segurança da informação.

Almeida, Carvalho e Cruz (2018, p. 748 tradução nossa) definem a PSI como um documento que deve conter um conjunto de padrões, métodos e procedimentos, que devem ser comunicados a todos os funcionários, bem como revistos e revisados criticamente em intervalos regulares ou quando mudanças forem necessárias. Segundo esses autores, a ABNT NBR ISO/IEC 27001 (ABNT, 2013), por ser um padrão de códigos de prática para gerenciamento de segurança da informação, deve ser considerada na construção da PSI, uma vez que tais práticas visam implementação, manutenção e melhorias para o gerenciamento da segurança das informações nas organizações.

Porém, uma política não se restringe a documentação de instruções sobre atitudes esperadas dos funcionários ao interagir com os ativos organizacionais, mas tais instruções devem nortear as práticas dos funcionários no curso de seus trabalhos. Logo, ações e práticas locais são o que fazem a diferença nos esforços de uma organização para proteger seus ativos de informação (NIEMIMAA; NIEMIMAA, 2017, p. 13–17, tradução nossa).

Niemimaa e Niemimaa (2017, tradução nossa) observam ainda que, no tocante ao desenvolvimento e implementação de uma PSI, tudo começa com a implementação das políticas sendo imposta aos profissionais de segurança da informação (SI), por meio de pressões institucionais e legais para adotarem práticas globais de segurança. Assim, uma política é escrita, mas nunca traduzida em ações, o que dificulta que os funcionários as coloquem em prática. No intuito de mudar essa realidade, esses autores sugerem que prescrições de práticas globais de SI sejam traduzidas em prática situacionais e essas

prescrições sejam traduzidas em uma política de SI organizacional e vice-versa. Tal entrosamento só será possível quando houver trabalho conjunto entre os profissionais de segurança e demais setores organizacionais.

Em geral, estudos de conformidade com políticas de segurança da informação baseiam sua teorização na suposição de que mudar o comportamento dos funcionários é difícil, porém contratar consultores externos para formular as políticas corre risco de torná-la não alinhada com a prática organizacional. Dessa maneira, faz-se necessário saber não somente como os funcionários devem trabalhar em teoria, mas também como eles funcionam na prática, logo havendo engajamento de parte dos funcionários na construção dessas políticas pode facilitar esse processo.

Assim, o estudo de Niemimaa e Niemimaa (2017, tradução nossa) analisou a implementação de política de segurança da informação como um processo de tradução de melhores práticas em uma política de segurança da informação organizacional. Para isso, foram exploradas práticas canônicas e não canônicas. As primeiras abstratas, formais, que assumem realidade previsível e sem problemas; as últimas situacionais, contingentes, improvisadas e caracterizadas por complexidades, dilemas e alto grau de ambigüidade. Ambas existentes durante o desenvolvimento e implementação de uma política de classificação da informação dentro de uma organização de tecnologia da informação.

Como resultado da observação participante feita pelos autores, houve falha na tradução de políticas em práticas, pois, da parte dos profissionais de segurança, houve compreensão insuficiente do trabalho dos funcionários e falta de envolvimento dos profissionais de SI nas práticas organizacionais; enquanto, da parte dos demais empregados, eles não assumiram as responsabilidades de segurança alegando falta de habilidade e conhecimento, acreditando ser responsabilidade do setor de segurança a implementação dessas políticas, além do fato que novas responsabilidades consomem tempo de suas funções. Havendo, portanto, um *gap* entre as práticas dos profissionais de segurança e o resto da organização (NIEMIMAA; NIEMIMAA, 2017, p. 1–16, tradução nossa).

Por outro lado, a pesquisa de Almeida, Carvalho e Cruz (2018, p. 748–761, tradução nossa), ao analisar elementos mais e menos importantes dentro da estrutura da PSI, concluiu que, dentre os elementos mais importantes, encontram-se: gestão de ativos, gerenciamento de riscos, e escopo da PSI, enquanto que, entre os elementos menos relevantes, prevaleceu: sumário executivo, contato e inspeção manual. Esse estudo observou também que o peso do elemento varia de acordo com o setor organizacional.

Ainda segundo esses autores, o setor de governo e serviços públicos possui diferenças significativas em relação aos demais setores pesquisados – financeiro, saúde, tecnologia da informação, turismo e indústria –, pois elementos como contatos, penalidades ou políticas de controle de acesso assumiram um papel mais importante para eles. Tal descoberta se justifica uma vez que esse setor é reconhecido como uma área onde as instituições assumem uma dimensão maior e aspectos relacionados aos processos e à burocracia estão bem estabelecidos. De forma diversa, a área de Tecnologia da Informação (TI) pesquisada atribuiu menos importância a resumo executivo, contatos, inspeção manual e penalidades, enquanto o gerenciamento de acesso a serviços da Web é considerado mais importante no campo de TI. Assim, o peso dos elementos, ao variar de acordo com o setor, também deve ser observado no processo de construção de uma PSI dentro da organização.

2.1.1.2 Riscos e vulnerabilidades identificados nas tecnologias

Quanto aos Sistemas Gerenciadores de Banco de Dados (SGBD), Azan Basallo, Estrada Senti e Martinez Sanchez (2018, p. 897–901, tradução nossa) desenvolveram um modelo baseado em conhecimento e lógica *fuzzy*, que utiliza técnicas de inteligência artificial para aprendizagem com base em resultados de auditorias passadas para avaliação de riscos de um SGBD. Os autores avaliaram o modelo proposto em relação aos resultados obtidos por especialistas e obtiveram 87% de exatidão.

Bharathi (2017, p. 183–186, tradução nossa) buscou analisar fatores de risco que surgem sob a ótica do *big data*, termo relativo a explosão de dados que surgiu com os milhares de dados armazenados em bancos de dados corporativos somado a internet das coisas (IoT) que aumentou de forma abrupta a quantidade de dados gerados. Segundo o autor, complexidades do modelo de implantação enxuta de Tecnologia da Informação (TI), como a nuvem, atraíram muita vulnerabilidade em segurança, privacidade e gerenciamento de dados. O artigo elencou como riscos inerentes a essa tecnologia: intermediação de dados, exposição global a dados pessoais, falta de projeto de segurança baseado em governança, vulnerabilidades de *big data* em constante evolução e complexidades de segurança na nuvem.

O *big data*, devido às complexidades de segurança na nuvem, representa uma grave ameaça de expor dados pessoais a mãos erradas, o que pode levar a distúrbios que vão desde a inundação de e-mails de spam até a eliminação de milhões de dólares. O estudo, portanto, exigiu técnicas robustas de criptografia no nível micro (nível de organização) e regulamentos aprimorados de segurança de dados no nível macro (economia) e prescreve que as

organizações devem entender que, por um lado, os usuários precisarão de um ambiente livre e flexível para realizar transações e, do outro lado, espera-se uma alta qualidade dos mecanismos de proteção para proteger seus dados pessoais.

Walterbusch, Fietz e Teuteberg (2017, tradução nossa) analisaram os riscos dos serviços de computação em nuvem combinados à *Shadow IT*[7], o que implica em situações que podem levar a duplicações indesejadas, dados inconsistentes ou perda dados. No entanto, como a tecnologia não é institucional, o departamento de tecnologia da informação nada pode fazer para dar o devido suporte. Essa combinação de tecnologias é mal vista devido à variedade de vulnerabilidades existentes, como, por exemplo, lacunas no *firewall* que surgem por meio do *download* de aplicativos não seguros ou da divulgação inadequada de dados (confidenciais) em vários dispositivos (privados, móveis). Há risco de surgir problema jurídico relativo à posse dos dados e às leis de privacidade. Na Alemanha, por exemplo, há obrigação de garantir que os dados pessoais permaneçam sob propriedade da empresa para a qual foram entregues. Logo, se um funcionário armazena dados na nuvem, ele passa a ser visto como o proprietário dos dados armazenados, embora normalmente não possa representar oficialmente a empresa.

Os autores concluem que o uso conjunto da *Shadow* IT com a tecnologia em nuvem não traz apenas riscos, mas também permite benefícios, como aumentar a efetividade dos empregados, o potencial para inovação e melhoria da qualidade no trabalho. Além do mais, esses serviços são utilizados de forma não autorizada, no intuito de melhorar a produtividade das tarefas, logo cabe à organização pesar os prós e contras de tais práticas (WALTERBUSCH; FIETZ; TEUTEBERG, 2017, p. 647, tradução nossa).

Ainda no tocante aos riscos de segurança associados à computação em nuvem, Alassafi et al. (2017, p. 999, tradução nossa) elencam como principais riscos: os relacionados a interfaces inseguras, tecnologia compartilhada, invasão de conta ou serviço, *insiders* maliciosos, falha na conformidade com regulamentos, propriedade de dados, integração serviços/dados e vazamento de dados. Assim, os autores propuseram um framework que considera esses fatores de risco, bem como fatores sociais – como confiança, cultura e privacidade –, e benefícios percebidos de segurança – como padronização de interfaces e

[7] A *Shadow* IT é definida como um processo de negócios que suporta soluções e ferramentas de tecnologia da informação (TI) que substituem ou ampliam as funcionalidades dessa tecnologia fornecidas oficialmente pelo departamento de TI. Porém, essas soluções não fazem parte da estratégia de governança dessa área e, portanto, geralmente não são conhecidas, aceitas nem suportadas pelo departamento de tecnologia da informação ou pela gestão.(WALTERBUSCH; FIETZ; TEUTEBERG, 2017, p. 644–645, tradução nossa)

concentração de recursos – como fatores críticos de sucesso a serem considerados na adoção de computação na nuvem.

Tecnologias atuais como a de *Blockchain* vem se tornando amplamente utilizadas em segurança, educação, sistemas de saúde e financeiros, e industrias, pensando nisso Zhao *et al.* (2019, p. 678–684) propuseram avaliação de riscos feita de forma descentralizada com *blockchain* aplicado a *Data Storage*, local de armazenamento de dados, provendo autenticidade às bases de dados. Iqbal e Matulevicius (2021) propuseram aplicações baseadas em *blockchain* para a indústria financeira com o objetivo de melhorar a segurança desse setor a partir de uma análise ontológica.

Como visto, os artigos que abordam tecnologias tornam-se proveitosos para análise de risco dentro das organizações uma vez que analisam riscos inerentes a tecnologias específicas ou aplicam algum modelo de análise de risco nelas próprias dentro das organizações.

Por fim, o artigo de Lowry, Dinev e Willison (2017, p. 6–7) suscita a reflexão sobre se estudos de segurança e privacidade devem se restringir somente ao mundo dos hardwares e sofwares. Os autores propõem artefatos chave adicionais, como artefatos de: processo, organizacional, pessoas, ameaças, leis, proteção, vulnerabilidade, e sociais, que podem ser detalhados conforme Quadro 4.

Quadro 4 - Exemplos não exaustivos de artefatos de SI pivôs para pesquisas em privacidade/segurança dos métodos de análise/avaliação de riscos

Artefatos	Exemplos no contexto de Privacidade / Segurança
Éticos **(decisões de segurança/privacidade de uso racional da moralidade nas organizações)**	discursos éticos, situações éticas, moralidade racional como mecanismo de dissuasão, diferenças éticas transculturais
Informacionais **(nexo entre privacidade/segurança e dados, informações, conhecimento ou comunicação)**	*big data*, manuais e políticas de SI, *phishing* emails, s*poofing* web sites, mensagens de advertência de segurança, tentativas de engenharia social, spam
Legais **(nexo entre privacidade/ segurança e leis, regulações, políticas ou melhores práticas)**	regulação de privacidade, roubo de propriedade intelectual, fluxos de dados transnacional, violações legais
Organizacionais	estratégias de governança de TI em segurança/privacidade, comportamentos extra-função, políticas de privacidade, regulações, praticas justas de informação, garantia de privacidade, padrões e melhores práticas
Pessoais **(intenções, hábitos, emoções e cognição envolvendo privacidade e segurança)**	*mindset* de hacker ou *insider* versus profissionais de segurança, cálculo de privacidade, decisões racionais e comportamentais, anonimato, sigilo, conscientização
Processo **(processo de privacidade/ segurança,**	falhas de configuração de sistema, avaliação de impacto, SGSI, gestão de riscos e governança

governança ou gerenciamento de riscos)	
Proteção (fenômeno de mensagem, treinamento e persuasão para encorajar comportamentos de proteção individual)	apelo ao medo, comportamentos de proteção, resistência a tentativas de *phishing*
Social (fenômeno social, cultural e organizacional para encorajar comportamentos de privacidade / segurança a nível coletivo)	influencias culturais em comportamentos de segurança/ privacidade, vazamento de dados em mídias sociais, senso de justiça em políticas de privacidade e segurança, reação negativa contra ameaças às políticas de segurança da informação, comportamento negativo
Tecnologia (fenômeno tangível de nexo entre privacidade/ segurança e equipamentos físicos de software, rede e interfaces)	destruição física, criptografia, roubo de equipamentos, *firewalls*, serviços locais/centralizado, perda de dispositivos com dados confidenciais
Ameaça	violações a políticas de acesso, fraude por clique, brechas de dados, invasões de privacidade, ataques DoS, ameaças internas, *malware* e *spyware*, *ransomware*, *rootkit*
Vulnerabilidade (fenômeno de fraqueza tangível ou intangível ou gap que expõe a organização a riscos a nível individual, de sistema ou organização)	Falha de hardware que revela ataque por vulnerabilidade,violação de PSI, sistemas operacionais *unpatched*, funcionários não treinados ou despreocupados, gestão de vulnerabilidade, risco de descobertas online

Fonte: Adaptado de Lowry, Dinev e Willison (2017, p. 6–7)

Por fim, os autores ressaltam que um estudo de segurança válido não precisa endereçar esses artefatos por completo, o que seria excessivo e não realístico, porém abordar um ou mais desses deve ser suficiente para um estudo fazer uma contribuição focada e significativa.

2.1.1.3 Métodos de Análise/Avaliação de Riscos – escopos e abordagens

A terminologia em análise de riscos não é unânime, pois termos como método, modelo ou *framework* foram utilizados. No entanto, em geral, os autores utilizam a nomenclatura da ABNT NBR ISO/IEC 27002 (ABNT, 2013b, p. 2–6) para distinguir entre análise e avaliação de riscos, onde: análise de riscos consiste no uso sistemático de informações para identificar fontes e estimar a magnitude dos riscos; e avaliação de riscos compara o risco estimado na análise com critérios de risco preestabelecidos, onde os resultados auxiliam no direcionamento de ações gerenciais e na implementação de controles. Deve-se considerar que, de acordo com essa norma, a análise está dentro da avaliação de riscos, evidenciando-se que a análise de riscos é a parte desafiadora da avaliação de riscos (SHAMELI-SENDI; AGHABABAEI-BARZEGAR; CHERIET, 2016).

Apesar de alguns artigos indicarem fazer avaliação de riscos, eles discorrem, em sua maioria, sobre análise de risco, como observado nos trabalhos de: Al Hadidi *et al* (2016), Bharat e Prasad (BHARAT; PRASAD, 2016), Pan e Tomlinsson (PAN; TOMLINSON, 2016), Han *et al* (HAN et al., 2016), e Basallo, Senti e Sanchez (AZAN BASALLO et al., 2018); o que é justificado, uma vez que, apesar de a análise de risco ser um subprocesso da avaliação de risco, ela constitui o pilar desse processo, servindo de base para todas as demais etapas da avaliação. Foi possível evidenciar também, durante a revisão sistemática de literatura, que os artigos, em geral, buscam fazer comparações, bem como sugerir melhorias para as metodologias de análise/avaliação de risco, algumas vezes sugerindo uma nova metodologia, como evidenciado nos trabalhos de: Shedden *et al*. (SHEDDEN et al., 2016), Pan e Tomlinson (PAN; TOMLINSON, 2016), Mansfield-Devine (MANSFIELD-DEVINE, 2017), Wangen (2017), Li *et al.*(LI et al., 2018), e Xuepeng eWei (XUEPENG; WEI, 2018).

Quanto a diversidade de métodos de análise e avaliação de riscos, Shameli-Sendi, Aghababaei-Barzegar e Cheriet (2016, p. 16, tradução nossa) afirmam que há diversidade de *frameworks* de gerenciamento de riscos de segurança da informação, cada um deles busca atender a uma necessidade específica e, por isso, possuem objetivos e etapas diferentes. Os autores usaram o NIST como base para afirmar que o gerenciamento de riscos envolve quatro processos: enquadramento de risco, avaliação de risco, resposta e monitoramento de risco.

Não obstante essa variedade de métodos, Singh e Joshi (2017, p. 129, tradução nossa) afirmam que existem inúmeros modelos de avaliação de risco, no entanto, não há mecanismo para ajudar as organizações a determinar qual modelo é o melhor a ser empregado.

A seleção de uma metodologia apropriada para avaliar o risco de segurança da informação de uma infraestrutura crítica depende, segundo Stergiopoulos, Gritzalis e Kouktzoglou (2018, p. 26, tradução nossa), de uma variedade de critérios, como: escopo e objetivos da metodologia, técnicas e padrões aplicados, cobertura de interdependências, entre outros. Alguns métodos, segundo esses autores, são projetados para serem usados como métodos independentes de avaliação de risco, enquanto outros são projetados para trabalhar em conjunto com processos de gerenciamento de riscos mais gerais. Alguns descrevem o processo de avaliação de risco de uma forma muito estruturada e com detalhes técnicos, enquanto outros simplesmente fornecem um ponto de vista abstrato e sugerem diretrizes ou melhores práticas que devem ser levadas em conta por qualquer abordagem que irá implementá-las.

Assim, *frameworks* como NIST SP 800-30, OCTAVE, IRAM, CRAMM e EBIOS são arcabouços que atuam no intuito de reduzir riscos de segurança da informação ao implementar

controles de segurança confiáveis, tais como os disponíveis em *Control Objectives for IT* (COBIT), *Sys Admin e Network Security* (SANS), ABNT NBR ISO/IEC 27005 e *Information Technology Infrastructure Library* (ITIL), por exemplo.

Esses *frameworks* definem o processo de gerenciamento de riscos, servindo como referências efetivas. Como se concentram em processos genéricos de gerenciamento de risco de organizações padrões, grupos acadêmicos e indústrias, não há diretrizes claras sobre como realizar uma avaliação de segurança aceitável dos controles (AL-SAFWANI; FAZEA; IBRAHIM, 2018). Tomando como base essa afirmação, Safwani, Fazea e Ibrahim (2018, tradução nossa) propõem um modelo de controles de segurança da informação, ao invés de modelo de avaliação de risco, mostrando assim sua visão crítica do processo de gerenciamento de riscos que, em sua visão, possui uma lacuna no tocante aos ativos vulneráveis e a avaliação de controles. Segundo os autores, controles como firewalls, roteadores, sistemas operacionais e bases de dados, consistem em soluções tecnológicas que mitigam os riscos a um nível aceitável, que consistem em dar um guia granular de passos-chave na identificação de controles tecnológicos críticos.

Nurse, Creese e de Roure (2017, p. 2–3) buscaram comparar os métodos de avaliação de riscos no que os diferencia e dois aspectos mais significantes encontrados residiram: na natureza da abordagem, onde uns, como o OCTAVE, focam nos ativos críticos e os perigos sobre eles, outros são guiados a ameaças e possibilidade de ocorrências, como o NIST; e o cálculo do risco também se diferencia muito entre os métodos, com abordagens quantitativas e qualitativas.

Tendo delineado as metodologias de análise de risco de segurança da informação que mais apareceram nos artigos durante a revisão sistemática de literatura, a listagem a seguir traz um resumo dos métodos de análise/avaliação de riscos citados pelos autores, seja para comparação de métodos ou para uso da metodologia.

- COBIT 5 – Realiza o gerenciamento de riscos usando cenários de risco. Um cenário de risco é uma descrição de um evento provável que, quando ocorrer, terá um impacto precário no alcance dos objetivos da empresa. O evento de perda é acionado por um evento de ameaça, e a frequência do evento de ameaça é influenciada por uma vulnerabilidade. Duas abordagens são oferecidas para o gerenciamento de risco: a *top-down*, de cima para baixo, aproveita as metas corporativas gerais e considera os cenários de risco mais relevantes e prováveis a afetá-las; a *bottom-up*, de baixo para cima, fornece uma lista de cenários genéricos para definir uma coleção de cenários mais relevantes e personalizados, aplicados ao empreendimento específico. Ambas as abordagens são complementares e podem ser usadas simultaneamente. (STERGIOPOULOS; GRITZALIS; KOUKTZOGLOU, 2018, p. 26, tradução nossa)

- MEHARI (*Method for Harmonized Analysis of Risk*) – Esse método avalia a probabilidade real dos riscos ao considerar a probabilidade intrínseca ou a exposição natural ao risco, a eficácia das medidas dissuasivas e preventivas. Propõe quadros de decisão baseados no tipo de cenário de ameaça (por exemplo, acidente, erro, ação humana voluntária) para avaliar a probabilidade. Uma escala qualitativa é fornecida com as potencialidades muito provável, provável, improvável ou muito improvável da aparência de risco. (STERGIOPOULOS; GRITZALIS; KOUKTZOGLOU, 2018, p. 26, tradução nossa)
- MAGERIT (*Methodology for Information Systems Risk Analysis and Management*) – Propõe ambos os modelos qualitativos e quantitativos para a avaliação da probabilidade dos riscos. A abordagem qualitativa é modelada através de uma escala nominal para descrever a potencialidade da aparência de risco com uma opção quase certa, muito alta, possível, improvável ou muito rara. Por outro lado, a probabilidade é numericamente modelada como uma taxa de ocorrência. Valores típicos são 100 para muito frequentes, 10 para frequentes, 1 para normal ou 0,1 para ocorrências não frequentes. A seleção da abordagem de avaliação de probabilidade é subjetiva e definida pelo tomador de decisão e pelas características particulares da avaliação da infraestrutura. (STERGIOPOULOS; GRITZALIS; KOUKTZOGLOU, 2018, p. 26, tradução nossa)
- FRAAP (*Facilitated Risk Analysis and Assessment Process*) – É um método qualitativo de avaliação de ameaças que tenta descobrir os perigos em termos de suas consequências nas estratégias empresariais ou no projeto da organização empresarial. Ele não tenta mais atingir números únicos para estimativas de perigo ou perda estimada. Ele se concentra na identificação de áreas com inclinação de chance e controles adequados para mitigá-los. Depende intensamente dos insumos de um profissional, sofrendo os perigos que a maioria das metodologias qualitativas tem: falta de consistência nos valores de perigo (BHARAT; PRASAD, 2016).
- FAIR (*Factor Analysis of Information Risk*) – Fornece uma estrutura para compreender, analisar e medir o risco da informação. Feito para endereçar as preocupações da segurança com fraquezas. Permite que as organizações padronizem o risco, apliquem a avaliação e visualização total dos riscos organizacionais, defendam a determinação de riscos usando análises avançadas e compreendam como tempo e dinheiro afetarão o perfil de segurança da organização. A principal falha do FAIR é a falta de informação sobre a metodologia e exemplos de como devem ser aplicadas (JOSHI; SINGH, 2017).
- TARA (*Threat Agent Risk Assessment*) – É uma estrutura de avaliação de risco criada pela Intel que ajuda as empresas a gerenciarem riscos refinando as possíveis informações sobre ataques de segurança. A principal desvantagem é ser muito caro e impraticável para defender uma possível vulnerabilidade. Uma das principais tarefas desta avaliação de risco é a varredura de vulnerabilidades (JOSHI; SINGH, 2017).
- *Ten Step procedure* – Define os dez passos para avaliação de risco. As etapas abrangem: desenvolvimento de declaração de escopo, montagem de uma equipe competente, identificação de ameaças, priorização de ameaças, efeito de priorização de perda, cálculo de perigo, identificação de salvaguardas, avaliação de ganho de valor, classificação de salvaguardas em ordem de prioridade e prática de arquivo de avaliação de perigos. Mas, esse método não carrega em mente as vulnerabilidades explicitamente (BHARAT; PRASAD, 2016).

- Ebios – É um conjunto abrangente de diretrizes para gerentes de risco do sistema de informação, originalmente lançado pelo governo francês. Produz práticas comuns e documentos de aplicações direcionados aos usuários finais. No entanto, embora sugira práticas comuns e identifique controles para formalização de objetivos de segurança, não possui diretrizes claras sobre como realizar esses objetivos de maneira estruturada. Depende do autojulgamento ou da opinião de especialistas. (AL-SAFWANI; FAZEA; IBRAHIM, 2018)
- IRAM (*Information Risk Analysis Methodology*) – é uma metodologia proprietária disponível no *Information Security Forum*, que utiliza abordagens de análise de influência de negócios para análise de risco. Voltada para avaliar a influência de possíveis violações de segurança nos negócios, avaliar ameaças e vulnerabilidades, determinar riscos de informações, identificar e analisar requisitos de controle e gerar um plano de ação para abordar os requisitos de controle identificados. A seleção de controle do IRAM é realizada por meio de entrevistas qualitativas de todas as partes interessadas e proprietários de negócios (AL-SAFWANI; FAZEA; IBRAHIM, 2018).
- CRAMM (CCTA *Risk Analysis and Management Method*) – É um método de análise de risco que requer o uso de uma ferramenta especial. A primeira versão, método e ferramenta, foi baseada nas melhores práticas das organizações governamentais britânicas. É o método de análise de risco atualmente preferido por grandes organizações, como órgãos governamentais e indústrias, no Reino Unido. A ferramenta de gerenciamento de risco está em conformidade com os padrões *International Organization for Standardization* (ISO) para fornecer orientação para o Sistema de Gestão da Segurança da Informação (SGSI). A probabilidade para cada risco identificado por ativo é avaliada através de questionários avaliados pelo pessoal de suporte, especialistas e outros. Usa planilhas e uma escala qualitativa para avaliação da probabilidade de cada ameaça que possa explorar a vulnerabilidade de cada ativo, com nenhuma (0), baixa (1-4), moderada (5-7), alta (8-9) e muito alta (10) (AL-SAFWANI; FAZEA; IBRAHIM, 2018; STERGIOPOULOS; GRITZALIS; KOUKTZOGLOU, 2018).

Como pode ser observado, os métodos possuem semelhanças e diferenças entre eles. Para uma melhor análise comparativa, por meio de pesquisa aprofundada nos métodos, foi possível comparar as metodologias e os elementos considerados para análise e avaliação de risco, sintetizados no Quadro 5.

Quadro 5 - Características dos métodos de análise/avaliação de riscos

Método	Elementos considerados	Metodologia	Proposto por	Relações ou Conformidades
Cobit 5	Cenários de risco	Qualitativa	ISACA	A ISACA cita o FAIR e seus conceitos em seu Risk IT
MEHARI	Ativos / Ameaças / Vulnerabilidades / Cenários	Qualitativa	Clube de segurança da informação francês (associação independente de profissionais)	Conformidade com ISO 27005/27001
Magerit	Ativos / Ameaças / Impacto /	Híbrida	Conselho Superior de Administração Eletrônica do	Conformidade com ISO 27001 / 2005, 15408 /

	Salvaguardas		Governo da Espanha	2005, 17799 / 2005, 13335 / 2004
FRAAP	Ameaças / Controles	Qualitativa	Thomas R. Peltier	
FAIR	Cenário / Frequência de eventos / Probabilidade de perdas	Quantitativo	Jack Jones	
TARA	Ameaças / Varredura de vulnerabilidades / Controles ou Exposição	Híbrida	Intel	
Ten Step procedure	Ameaças/Atacantes / Motivações/Método de ataque/ Impacto	Qualitativa	Thomas R. Peltier	
EBIOS	Ameaças/Objetivos de segurança / Vulnerabilidades	Qualitativa	Divisão Central de Segurança de Sistemas de Informação (Governo da França)	Conformidade com ISO 13335, ISO 15408, ISO 17799
IRAM	Ameaças / Vulnerabilidades/ Controles	Qualitativa	*Information Security Forum* (Organização Independente)	Conformidade com ISO 27014, 27001, 27002, 27005, 27036, COBIT V4, PCI DSS, Sarbanes Oxley Act
CRAMM	Negócio / Ameaças/ Vulnerabilidades / Contramedidas	Qualitativa	Agência Central de Comunicação e Telecomunicações (Governo Britânico)	
ISO 27005	Ativos / Ameaças / Controles/ Vulnerabilidades	Qualitativa	*International Organization for Standardization (organização não governamental)*	
OCTAVE	Condutores / Ativos / Ameaças	Híbrida	*Software Engineering Institute of Carnegie Mellon University*	COSO, ISO 31000, NIST CSF, NIST SP 800, CERT RMM e FAIR
NIST SP 800-37	Sistema / Ameaças / Vulnerabilidades / Controles / Probabilidade / Impacto / Risco	Híbrida	*National Institute of Standards and Technology*	ISO/IEC 27005:2011,ISO/IEC Guide 73, ISO/IEC 31000:2009,ISO/IEC 30101:2009

Fonte: Dados da pesquisa (2022).

Depreende-se do Quadro 5 que os métodos de análise e avaliação de risco são propostos por variados tipos de instituições, como organizações governamentais e não governamentais, empresas, universidades, associações de profissionais de segurança da informação e pesquisadores da área como Peltier. Alguns são construídos visando a indústria, outros focam nos sistemas de defesa dos países, bem como os que se preocupam com

instituições governamentais, mas nenhum foi feito especificamente para instituições governamentais ligadas ao ensino, apesar de haver estudos como os de Joshi e Singh (2017) que aplicaram alguns desses métodos em universidades. Como exemplo dessa diversidade de objetivos, observa-se que a ABNT NBR ISO/IEC 27005 (ABNT, 2011) teve como foco uma padronização universal, o NIST foi escrito para segurança de sistemas de informação federais dos Estados Unidos e o OCTAVE foi projetado tendo como foco sistemas de defesa.

Ao detalhar os métodos mais citados ou utilizados pelos artigos, começa-se pela ABNT NBR ISO/IEC 27005 (ABNT, 2011), que oferece um suporte especial aos requisitos especificados na ABNT NBR ISO/IEC 27001. O plano de fundo do método, ao ser estabelecido, permite avaliar os riscos por meio de um plano de tratamento de riscos, cujo objetivo consiste em implementar efetivamente os controles e as decisões recomendadas. Esse método tenta identificar as fontes reais de riscos específicos antes de decidir o que pode ser feito e quando. O objetivo principal dessa norma é reduzir os riscos a um nível aceitável e, apesar de ser uma diretriz genérica para o gerenciamento de riscos, não delineia, obviamente, uma análise adequada dos controles atuais. No entanto, o método falha em dar orientação granular sobre as principais etapas da identificação dos controles críticos, e dados qualitativos são usados para análise. Além disso, selecionar controles de práticas comuns é difícil e as organizações são deixadas a escolher os melhores controles que se ajustam às suas condições (AL-SAFWANI; FAZEA; IBRAHIM, 2018).

O *framework* de gerenciamento de riscos do *National Institute of Standards and Technology* (NIST**)** é uma estrutura de sistemas criada para gerenciamento de riscos, com abordagem baseada em risco para seleção e especificação de controles de segurança, considerando eficácia, eficiência e restrições relacionadas às leis, diretivas, ordens executivas, políticas, normas ou regulamentos aplicáveis. De acordo com Dawson (2018, p. 66, tradução nossa), existem seis etapas de categorização que servem de base para o NIST, são elas: Categorizar o sistema com base em uma análise de impacto; Selecionar, personalizar e documentar os controles de segurança, de acordo com o risco para operações e ativos organizacionais, os quais devem ser abordados no projeto e resultam de requisitos de alto nível que são decompostos em requisitos de nível inferior; Implementar os controles selecionados e implantar no sistema; Avaliar se os controles implementados estão funcionando conforme o esperado e se atendem aos requisitos de segurança do sistema; Autorizar o sistema a operar com base em uma decisão sobre o risco aceitável para o sistema; e Monitorar continuamente os controles de segurança, o que inclui verificações anuais de segurança para revisar a conformidade (DAWSON, 2018, p. 66, tradução nossa).

Para Kim, Lee e Lim (2017, p. 4591, tradução nossa), essas seis etapas se resumem a: classificação dos sistemas de informação; restrições de segurança da informação; implementação das restrições; avaliação das restrições; certificação de segurança da informação; e monitoramento das restrições de segurança da informação. Observam que o NIST dispõe de três classes de controles: controles técnicos, operacionais e de gerenciamento, fornecendo diretrizes sobre 256 controles de segurança organizados em 18 famílias. Ademais, vale salientar que o NIST nasceu como forma de o governo dos Estados Unidos estipular obediência a um conjunto mínimo de requisitos de segurança para operações do sistema de informação federal.

O *Operationally Critical Threat, Asset, and Vulnerability EvaluationSM* (OCTAVE) foi construído com foco nos sistemas de defesa, o que refletiu no extenso corpo de documentos e práticas para sua implementação. No entanto, como parte do pressuposto que toda ameaça potencial irá acontecer, o cálculo das probabilidades torna-se incompatível com as considerações feitas por outros métodos (STERGIOPOULOS; GRITZALIS; KOUKTZOGLOU, 2018, p. 25, tradução nossa).

O OCTAVE é uma metodologia de avaliação de risco autodirigida que permite que as organizações estudem e conduzam avaliações de risco para que possam capturar seus próprios conhecimentos técnicos. A metodologia pretende alavancar conhecimento de pessoas, práticas e processos organizacionais a fim de determinar o estado atual de segurança. Os riscos para os ativos críticos identificados determinam as áreas de melhoria necessárias e auxiliam o desenvolvimento de uma estratégia de segurança. O OCTAVE-S, sendo uma versão para pequenas empresas, concentra-se em riscos organizacionais e práticas relacionadas, enquanto outras metodologias se concentram em tecnologia. O método ajuda a equipe a identificar ativos de informações críticas com base em seu alinhamento com os objetivos de negócios. O OCTAVE está em conformidade com as fases típicas de avaliação de risco, incluindo estabelecimento de contexto, identificação de risco, análise de risco e controle de risco. Fornece 04 (quatro) árvores de ameaças, 02 (duas) considerando problemas técnicos e 02 (duas) considerando atores humanos, com significado técnico ou físico. Cada ramificação das 04 (quatro) árvores é percorrida usando as informações do ativo, a fim de garantir uma cobertura completa e a identificação de ameaças.

Com o objetivo de reduzir riscos de segurança, as atividades do OCTAVE estão estruturadas em 03 (três) fases, a primeira foca em conhecer as fraquezas, por meio da construção de perfis de ameaças baseados em ativos; a segunda visa compreender as áreas de maior risco, ao identificar vulnerabilidades examinando a infraestrutura de computação em

relação aos ativos críticos; e a terceira consiste em um plano de remediação, por intermédio de planos de proteção e mitigação, a serem definidos após o desenvolvimento de estratégia de segurança, resultante da identificação e análise de riscos (SHEDDEN et al., 2016; SINGH; JOSHI, 2017).

Por fim, a revisão sistemática de literatura contribuiu para uma melhor compreensão dos métodos de análise/avaliação de riscos e para conhecimento da visão dos pesquisadores sobre os diferentes tipos de abordagens de pesquisa. Contribuiu para identificar a lacuna de métodos de análise/avaliação de riscos específicos para o contexto das universidades e institutos federais de ensino, e para compreender as vantagens e desvantagens dos diversos métodos existentes e sua estrutura e comum.

2.2 NORMAS ESPECÍFICAS DE SEGURANÇA DA INFORMAÇÃO PARA APF

Para desenvolver uma cultura organizacional de segurança da informação, o governo federal lançou a Política Nacional de Segurança da Informação (PNSI), com a publicação do Decreto nº 9.637, de 26 de dezembro de 2018 (BRASIL, 2018[8]), que atualizou o Decreto nº 3.505 (BRASIL, 2000[9]). Nessa política foram revistos e atualizados os princípios e diretrizes que orientam a atuação dos gestores públicos federais e possui a educação como alicerce fundamental para o fomento da cultura em segurança da informação. Ressalta-se, entre seus objetivos, o incentivo da evolução constante da qualificação das pessoas envolvidas com a área.

Segundo a Política Nacional de Segurança da Informação, a segurança da informação (SI) abrange: a segurança cibernética; a defesa cibernética; segurança física e a proteção de dados organizacionais; e as ações destinadas a assegurar as propriedades de SI: disponibilidade, a integridade, a confidencialidade e a autenticidade da informação. Logo, para garantir uma efetiva segurança da informação, devem-se assegurar medidas protetivas para tecnologias, infraestrutura e dados organizacionais, de modo a garantir as propriedades da segurança da informação nesses ativos. Tais medidas envolvem pessoas, processos e tecnologias.

Dos princípios dessa política observa-se "respeito e promoção dos direitos humanos e das garantias fundamentais, em especial a liberdade de expressão, a proteção de dados

[8] Documento eletrônico não paginado.
[9] Documento eletrônico não paginado.

pessoais, a proteção da privacidade e o acesso à informação" (BRASIL, 2018[10]), ideia alinhada aos pilares da segurança da informação que visam não só a confidencialidade das informações pessoais, mas também a disponibilidade da informação, quando for o caso. A política traz obrigações aos órgãos e entidades da Administração Pública Federal (APF), elencadas no art.15:

> I - implementar a PNSI;
> II - elaborar sua política de segurança da informação e as normas internas de segurança da informação, observadas as normas de segurança da informação editadas pelo Gabinete de Segurança Institucional da Presidência da República;
> III - designar um gestor de segurança da informação interno, indicado pela alta administração do órgão ou da entidade;
> IV - instituir comitê de segurança da informação ou estrutura equivalente, para deliberar sobre os assuntos relativos à PNSI;
> V - destinar recursos orçamentários para ações de segurança da informação;
> VI - promover ações de capacitação e profissionalização dos recursos humanos em temas relacionados à segurança da informação;
> VII - instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais, que comporá a rede de equipes formada pelos órgãos e entidades da administração pública federal, coordenada pelo Centro de Tratamento de Incidentes de Redes do Governo do Gabinete de Segurança Institucional da Presidência da República;
> VIII - coordenar e executar as ações de segurança da informação no âmbito de sua atuação;
> IX - consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão de segurança da informação; e
> X - aplicar as ações corretivas e disciplinares cabíveis nos casos de violação da segurança da informação. (BRASIL, 2018[11]).

É possível observar que, dessas competências, o fomento do governo federal para ações de segurança da informação em seus órgãos e entidades, a instituição do comitê e elaboração de políticas e normas, são competências da alta administração. Como visto, muitas ações devem ser abordadas de forma *top-down*, começando pela alta administração e finalizando em equipes treinadas e servidores conscientes de seu papel na segurança da informação.

Para viabilizar as ações de SI, o Gabinete de Segurança Institucional (GSI), órgão ligado à Presidência da República, editou 03 (três) instruções normativas pilares das ações de segurança a serem tomadas pela Administração Pública Federal. A primeira, Instrução Normativa 01 (BRASIL, 2008a), do Gabinete de Segurança Institucional, que disciplina a Gestão de Segurança da Informação e Comunicações (GSIC) na APF, traz o cidadão como

[10] Documento eletrônico não paginado.
[11] Documento eletrônico não paginado.

principal cliente da gestão de segurança da informação, assim não é para menos que todas as ações de segurança devem ser pautadas para proteger os mesmos de roubo de informações, bem como arbitrariedades.

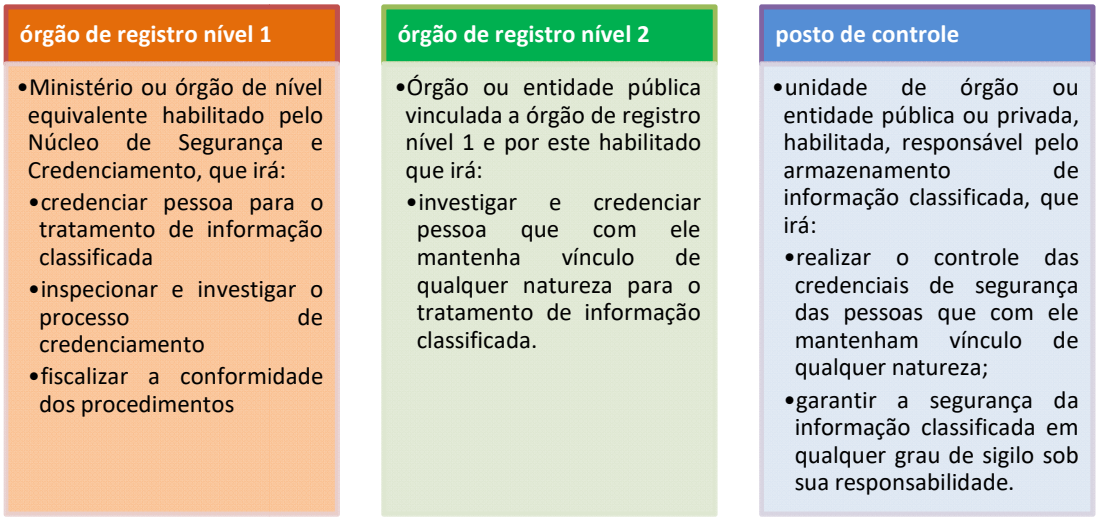
A instrução normativa GSI 02 (BRASIL, 2013a) traz a necessidade do credenciamento de segurança para acesso a informação classificada[12]. Esse acesso, bem como a divulgação e o tratamento de informação, ficaram restritos a pessoas que tenham necessidade de conhecê-la e que tenham Credencial de Segurança, segundo as normas fixadas pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR), por intermédio do Núcleo de Segurança e Credenciamento (NSC). Porém, pessoas não credenciadas também podem acessar esse tipo de informação, desde que permitido mediante assinatura de Termo de Compromisso de Manutenção de Sigilo (TCMS), conforme Anexo I do Decreto nº 7.845 (BRASIL, 2012[13]), pelo qual a pessoa se obrigará a manter o sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da Lei.

O credenciamento de segurança permite que somente pessoas devidamente autorizadas tenham acesso a informações sigilosas e sejam responsabilizadas pelo mau uso de tais informações, o limite está exatamente no que deve ser sigiloso e o que deve ser público, devendo o sigilo ser a exceção, um rol exaustivo de casos, e a regra ser a publicidade das informações nas instituições públicas. Porém, há de se analisar sobre a necessidade ou não de criação de toda a estrutura de credenciamento, a depender do órgão ou entidade, uma vez que essa estrutura inclui órgãos de registro, nível 1 e 2, além de postos de controle, como pode ser visto na Figura 11.

[12] informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, a qual é classificada como ultrassecreta, secreta ou reservada (Art. 2º, (BRASIL, 2013a))

[13] Documento eletrônico não paginado.

Figura 11 - Estrutura de credenciamento



Fonte: Adaptado de instrução normativa GSI 02 (BRASIL, 2013a).

No entanto, a partir de toda uma estrutura para controle de sigilo, somente os proprietários ou responsáveis pela informação no órgão ou entidade podem avaliar a necessidade de todo esse processo de credenciamento dentro das instituições, sob pena de engessamento do acesso à informação e/ou mau uso do sigilo. Devendo os respectivos setores de tecnologia serem informados sobre o uso de informação classificada, uma vez que o art. 38 do Decreto nº 7.845 (BRASIL, 2012[14]) salienta que os sistemas de informação e canais de comunicação devem atender um padrão mínimo de qualidade e segurança para o devido tratamento da informação classificada, devendo fazer uso da rede corporativa, através de canal seguro, para mitigar o risco da quebra de segurança. Para isso, as instituições devem atender, aos seguintes requisitos para o tratamento da informação classificada, segundo art. 38, 39 e 40 do decreto supracitado, dentre outros:

- ✓ A autenticidade da identidade do usuário da rede deverá ser garantida, no mínimo, pelo uso de certificado digital;
- ✓ Os sistemas de informação deverão ter níveis diversos de controle de acesso e utilizar recursos criptográficos adequados aos graus de sigilo.
- ✓ Os sistemas de informação deverão manter controle e registro dos acessos autorizados e não-autorizados e das transações realizadas por prazo igual ou superior ao de restrição de acesso à informação.
- ✓ Os equipamentos e sistemas utilizados para a produção de documento com informação classificada em qualquer grau de sigilo deverão estar isolados ou ligados a canais de comunicação seguros, que estejam física ou logicamente isolados de qualquer outro, e que possuam recursos criptográficos e de segurança adequados à sua proteção.

[14] Documento eletrônico não paginado.

> ✓ A cifração e a decifração de informação classificada em qualquer grau de sigilo deverão utilizar recurso criptográfico baseado em algoritmo de Estado. (BRASIL, 2012[15])

Ou seja, uma vez decidido sobre a existência de informação classificada, para o tratamento das informações, que perpassam o ambiente tecnológico, faz-se necessário implementar uma série de requisitos de segurança.

Fazendo também parte dessas medidas de segurança da informação, segundo o decreto, o controle de acesso das áreas e instalações que contenham documento com informação classificada em qualquer grau de sigilo, ou que, por sua utilização ou finalidade, demandem proteção, sendo o acesso restrito às pessoas autorizadas pelo órgão ou entidade. Observa-se assim que carece de maiores informações o estabelecimento do processo de credenciamento dentro das Instituições Federais de Ensino Superior, além do levantamento da existência de informações classificadas dentro dessas instituições, porém é possível antecipar que informações relativas a projetos de pesquisa que envolva patentes poderiam entrar nesse rol de segurança, mas desde que envolvam a segurança da sociedade ou do Estado.

Observa-se que o credenciamento se faz necessário apenas para um tipo restrito de informação sigilosa, a informação classificada, não sendo exigido para os demais tipos, como as informações pessoais e as hipóteses legais de sigilo, por exemplo. Assim, os órgãos e entidades da APF continuam tendo que manter o sigilo dessas informações, mas sem a necessidade de obedecer aos critérios engessados do credenciamento.

Outra norma de SI, a Instrução Normativa GSI 03 (BRASIL, 2013b) estabelece os parâmetros e padrões mínimos para recursos criptográficos baseados em algoritmos de Estado, que devem ser implementados pelos órgãos e entidades na criptografia da informação classificada, em qualquer grau de sigilo. Observa-se, então, que tal norma só é exigida nos casos de informação classificada e, nesse caso, compete à Alta Administração dos órgãos e entidades, sob pena de responsabilidade, assegurar a implementação e uso desses parâmetros e padrões mínimos, devendo o recurso criptográfico ser, prioritariamente, de desenvolvimento próprio desses órgãos e entidades, vedada, em regra, a participação e contratação de empresas e profissionais externos, para isso, podendo, porém, solicitar apoio técnico do GSI/PR.

Foram vistas as 03 (três) instruções normativas consideradas pilares da SI pelo governo federal, tais instruções são sucedidas de normas complementares no intuito de detalhar mais ainda as normas de SI para a APF. No Quadro 6, apresenta-se uma síntese dessas normas complementares.

[15] Documento eletrônico não paginado.

Quadro 6 - Síntese das Normas Complementares das Instruções Normativas do GSI

NORMAS COMPLEMENTARES DA IN01			
NC01	Critérios para normatização sobre GSI	**NC11**	Avaliação de conformidade em SIC
NC02	Metodologia de gestão de SIC	**NC12**	Uso de dispositivos móveis aspectos de SIC
NC03	Elaboração da POSIC	**NC13**	Gerenciamento de mudanças
NC04	Processo de Gestão de Riscos de SIC	**NC14**	SI para computação em nuvem
NC05	Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais	**NC15**	SI para redes sociais
NC06	Gestão de Continuidade de Negócios	**NC16**	Desenvolvimento de software seguro
NC07	Controle de Acesso	**NC17**	Profissionais da área de SIC
NC08 **NC21**	Gerenciamento de Incidentes em Redes de Computadores	**NC18**	Atividade de ensino em SIC
NC09	Uso de recursos criptográfico	**NC19**	Padrões mínimos de SIC em sistemas
NC10	Inventário e Mapeamento de Ativos de Informação, sob aspecto de SIC	**NC20**	Tratamento da Informação sob aspecto de SIC
NORMAS COMPLEMENTARES DA IN02			
NC01	Credenciamento de segurança		

Fonte: Dados da pesquisa (2022).

O quadro mostra as dezenas de normas que detalham as ações de segurança da informação a serem tomadas pela APF em seus órgãos e entidades. Para melhor conhecimento pretende-se elucidar, no restante deste tópico, algumas dessas normas à luz das medidas de segurança desejadas pelo governo federal para essas instituições.

As ações de SI começam pela Política de Segurança da Informação e Comunicações (POSIC), segundo a Norma Complementar 03, da instrução normativa 01 (IN01/GSI), cujo objetivo consiste em declarar o comprometimento da alta direção organizacional no intuito de estabelecer "diretrizes estratégicas, responsabilidades, competências e o apoio para implementar a gestão de segurança da informação e comunicações nos órgãos ou entidades" (BRASIL, 2009a, p. 2). Por meio dessas diretrizes, as propriedades de segurança da informação são viabilizadas, sendo recomendada a instituição de um grupo de trabalho para sua elaboração, que inclua diversos setores como, por exemplo, os de patrimônio, tecnologia, pessoal, jurídico, financeiro e planejamento. A POSIC deve estabelecer, como diretrizes gerais, considerando as normas específicas vigente, no mínimo, os temas estabelecidos no Quadro 7:

Quadro 7 - Temas a serem abordados na POSIC

Tratamento da Informação	Tratamento de Incidentes de Rede	Gestão de Risco	Gestão de Continuidade
Auditoria e Conformidade	Controles de Acesso	Uso de e-mail	Acesso a Internet

Fonte: Adaptado para quadro de (BRASIL, 2009a, p. 3)

Salienta-se que a POSIC estabelece as diretrizes, cabendo às normas específicas, dos órgãos ou entidades, uma orientação mais detalhada sobre os procedimentos a serem estabelecidos para os usuários da informação e tecnologia da informação. Ademais, cabe a POSIC trazer ainda as penalidades, competências e responsabilidades em sua estrutura.

A produção e o tratamento da informação ocupam relevância fundamental para gestão da máquina pública e o processo de tomada de decisões quanto às políticas públicas. Nesse sentido, a Norma Complementar 20, da Instrução Normativa 01, afirma que "toda informação institucional dos órgãos e entidades da APF em qualquer suporte, materiais, áreas, comunicações e sistemas de informação institucionais, é patrimônio do Estado brasileiro" (BRASIL, 2014a, p. 3).

Consequentemente, a informação deve ser tratada em todo seu ciclo de vida de modo ético, responsável e seguro, conservando as propriedades de segurança da informação. Essa norma contempla não apenas segurança da informação, mas também gestão documental e arquivística, gestão da informação, acesso à informação e sigilo da informação. Cabendo a todo agente público, sob pena de responsabilização civil, penal e/ou administrativa, "salvaguardar a informação sigilosa e a pessoal, bem como assegurar a publicidade da informação ostensiva, utilizando-as, exclusivamente, para o exercício das atribuições de cargo, emprego ou função pública" (BRASIL, 2014a, p. 4). No caso de empresa terceirizada, tal responsabilidade e as diretrizes de segurança são estabelecidas em termos contratuais.

Assim, cabe aos órgãos e entidades da APF estabelecer mecanismos de gestão dos processos e procedimentos envolvidos no tratamento da informação, ao longo do ciclo de vida, para a implementação das diretrizes de segurança da informação, sendo recomendado que a Alta Administração estabeleça metodologia de gestão de tratamento da informação, sendo as normas e procedimentos internos de tratamento da informação elaborados com participação do Gestor de Segurança da Informação e Comunicações, aprovados no âmbito do respectivo Comitê de Segurança da Informação e Comunicações. Devendo o proprietário e custodiante da informação serem identificados pelos órgãos e entidades da APF, com o proprietário da informação incumbido de, no mínimo, descrever a informação, definir as

exigências de segurança e comunicá-las aos custodiantes e usuários, assegurar o cumprimento das exigências de segurança por meio de monitoramento e indicar os riscos que podem afetar a informação; e ao custodiante aplicar os níveis de controle exigido pelo proprietário para assegurar as propriedades de segurança (BRASIL, 2014a, p. 3–10).

Em observância da relação da segurança da informação com os Agentes Públicos em geral, a Norma Complementar 18 (BRASIL, 2013c), da IN01/GSI, orienta que recebam instruções em SI no período de ambientação, formação inicial ou continuada em seus órgãos ou entidades, por meio de atividades de ensino de: **sensibilização**, orienta o que é SIC e que a perceba em sua rotina pessoal e profissional; **conscientização**, possibilita multiplicadores sobre o tema; **capacitação**, torna os participantes aptos a atuar como Gestores de SIC; e **especialização**, permite que os participantes tornem-se referências na pesquisa de novas soluções e modelos de SIC. Os conhecimentos dessas atividades de ensino são cumulativos, do menor para o maior, e a carga horária mínima está estabelecida no anexo da norma, variando de 1 hora a 360 horas.

Um dos mecanismos de segurança da informação consiste no uso de recursos criptográficos que, como dito anteriormente, influencia fortemente no controle sobre a privacidade da informação, à medida que os algoritmos sejam mais robustos e desde que seja mantida a sua privacidade sob controle de profissionais restritos a APF. Assim, segundo a Norma Complementar 09 (BRASIL, 2014b), da IN01/GSI, é de responsabilidade da Alta Administração dos órgãos e entidades da APF a utilização do uso de recursos criptográficos para a segurança das informações, principalmente as sigilosas, além de capacitar os agentes responsáveis pelo uso desses recursos.

Cabendo ao Gestor de Segurança da Informação e Comunicação desses órgãos e entidades a implementação de procedimentos para o uso desses recursos em conformidade com as orientações das normas de segurança. Evidenciando-se que é de responsabilidade de cada usuário de recurso criptográfico, a execução das normas e respectivo sigilo da informação, havendo necessidade de criptografia das informações sigilosas não classificadas, com algoritmo criptográfico registrado considerando a necessidade de proteção da informação sigilosa, possíveis ameaças e controles adequados. Como já visto na Instrução Normativa 03, há um grau de proteção ainda maior se a informação sigilosa for do tipo classificada.

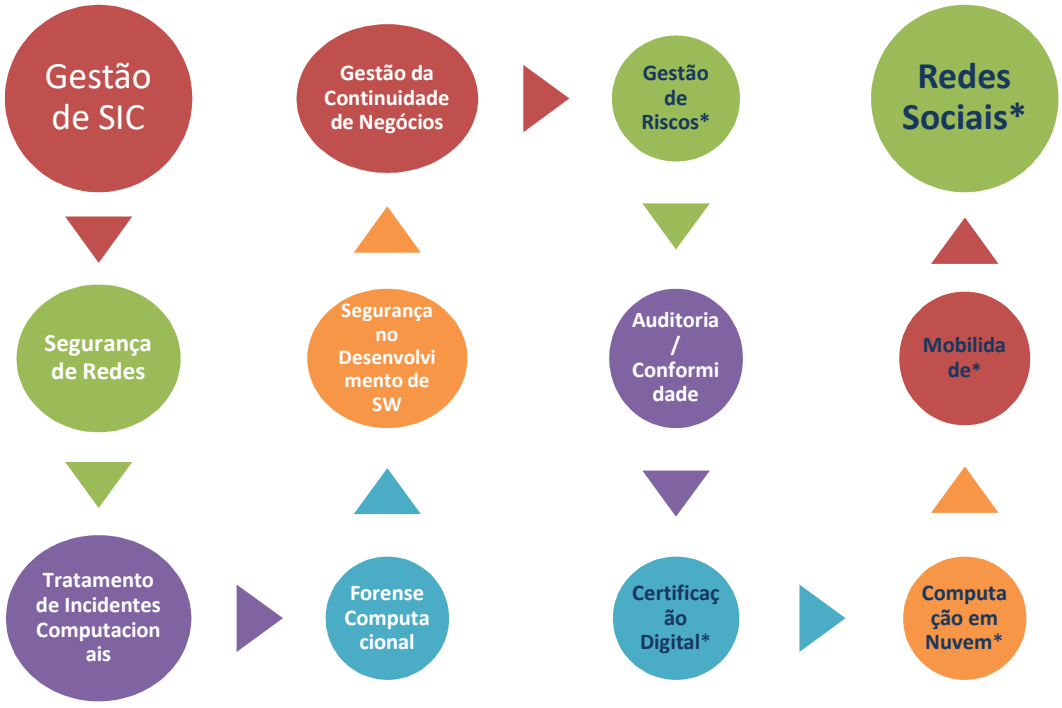
Assim, observa-se que naturalmente as ações de segurança da informação perpassam pelos profissionais da área que devem ser capazes de planejar e implementar medidas de segurança. Nesse sentido, a Norma Complementar 17 (BRASIL, 2013d), da IN01/GSI, evidencia que o intercâmbio de conhecimento entre profissionais de segurança da informação

e comunicações (SIC), especialmente entre os órgãos e entidades da APF, é altamente recomendado, de preferência entre grupos de trabalho formalmente constituídos.

Dessa forma, buscar conhecimento multidisciplinar torna-se um pré-requisito desse profissional, uma vez que a SIC abrange os âmbitos estratégico, tático e operacional das instituições. A norma recomenda ainda que profissionais de SIC participem da elaboração do planejamento estratégico e da programação orçamentária do órgão ou entidade ao qual mantenham vínculo, afinal as ações de segurança devem estar fortemente alinhadas não apenas com a legislação, mas também com o objetivo estratégico dessas instituições que devem contemplar, dentre outros aspectos, formação educacional, retenção e compartilhamento do conhecimento em SIC.

O anexo A, da Norma Complementar 17 (BRASIL, 2013d), pontua certificações recomendadas para profissionais de segurança, de acordo com o foco. E seu anexo B traz indicação de temas para capacitação e compartilhamento do conhecimento dos profissionais de SIC. A figura 12 mescla ambos os anexos mostrando certificações recomendadas versus temáticas indicadas para capacitação e compartilhamento do conhecimento dos profissionais de SIC, onde os círculos com letras na cor azul e asterisco (*) indicam que não foi recomendada certificação nessa temática:

Figura 12 - Certificações recomendadas versus temáticas para capacitação em SIC



Fonte: Anexos A e B da Norma Complementar 17 da IN01/GSI (BRASIL, 2013d)

Salienta-se que a norma não indica que deve haver um super profissional de SIC com conhecimento em todas as temáticas abordadas, mas sim que o órgão ou entidade da APF busque profissionais de SIC com conhecimento multidisciplinar, que sejam capacitados, se possível com as certificações recomendadas, e que compartilhem conhecimento com outros profissionais. Tal observação evidencia a interdisciplinaridade da área de segurança da informação, que abrange desde redes, software, tecnologia em nuvem, a redes sociais e dispositivos móveis, além de inúmeras outras disciplinas a depender do contexto.

Parte desses profissionais de SIC deve ser realocada para fazer parte da Equipe de Tratamento e Resposta a Incidentes (ETRI), pois, segundo a Norma Complementar 05 (BRASIL, 2009b), da IN01/GSI, essa equipe faz parte das estratégias de segurança a serem adotadas na APF. Assim, é de competência do Departamento de Segurança da Informação e Comunicações, do Gabinete de Segurança Institucional apoiar os órgãos nas atividades de capacitação e tratamento de incidentes, mas, para que essa equipe seja formada, o órgão ou entidade deve ser o administrador de sua infraestrutura de rede e, uma vez formada a equipe, deve informar os incidentes, de imediato, via Termo de Cooperação Técnica, ao Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal.

Essa obrigação visa permitir soluções integradas de incidentes de segurança para a APF, bem como a geração de estatísticas. Para instituir a ETRI, cada órgão ou entidade deve escolher entre os modelos, centralizado, descentralizado ou híbrido, onde no centralizado há uma equipe dedicada de forma exclusiva para tratar incidentes e no descentralizado há colaboradores espalhados. A norma também oferece a opção de utilizar os membros da equipe de tecnologia da informação, que iriam acumular função, mas essa opção seria transitória, devendo haver migração posterior para um dos demais modelos. A autonomia da ETRI, para realizar as medidas necessárias, dependerá do documento de constituição podendo ser completa, compartilhada ou sem autonomia.

Nesse sentido, cabe a ETRI, segundo a Norma Complementar 08 (BRASIL, 2010), da IN01/GSI, além de realizar o gerenciamento de incidentes, oferecer serviços opcionais que auxiliem a comunidade, como: tratamento de artefatos maliciosos; vulnerabilidades; emissão de alertas e advertências; anúncios; prospecção ou monitoração de novas tecnologias, avaliação de segurança; desenvolvimento de ferramentas de segurança; detecção de intrusão e disseminação de informações relacionadas à segurança; sem prejuízo de outros requisitados

pela comunidade. Tais serviços solidificam a implementação da estratégia de segurança no tocante ao gerenciamento de incidentes de segurança da informação.

Considerando que um incidente é um evento adverso, faz-se necessário que o processo de Gestão da Segurança da Informação e Comunicações abranja as atividades de registro de eventos, coleta e preservação de evidências de incidentes de segurança em redes computacionais. Para isso, segundo a Norma Complementar 21 (BRASIL, 2014c), da IN01/GSI, os ativos informacionais, bem como os servidores de hospedagem de página eletrônica devem manter registros históricos de eventos (*logs*) de maneira a permitir uma completa identificação dos fluxos de dados. Devendo os dados serem guardados pelo período mínimo de 06 (seis) meses, obedecendo os procedimentos estabelecidos para coleta e preservação de evidências.

Outra importante medida de ação em segurança da informação consiste na identificação e implementação de controles de acesso lógico e físico. Tal medida está condicionada a prévia aprovação da autoridade responsável do órgão ou entidade – no caso das Instituições Federais de Ensino Superior passaria pelo crivo de reitoria, conselhos consultivos e comitês de segurança. A elaboração e ampla divulgação das normas de controle de acesso, juntamente com programas de conscientização, são pré-requisitos para a eficácia da implementação desses controles (BRASIL, 2014c, p. 2). Assim, diretrizes para implementação dos controles de acesso, biométrico, lógico e físico, foram sintetizadas no Quadro 8, a partir da Norma Complementar 07 (BRASIL, 2014d).

Quadro 8 - Diretrizes para controle de acesso lógico, físico e biométrico

CONTR.		DIRETRIZES
Biometrico		- Conta de acesso biométrico vinculada a conta de acesso lógico e ambas devem ser utilizadas para atender a autenticação de multifatores. - Dados biométricos são sigilosos e devem ser criptografados na forma da legislação vigente.
Lógico	**Administração de contas de acesso**	- Existir procedimentos para criação de contas de acesso bem como credenciamento, bloqueio e exclusão de contas de acesso. - Contas de administração únicas, com acesso pessoal e intransferível, utilizadas por usuários cadastrados para execução de tarefas específicas. - Responsabilização do usuário pela quebra de segurança mediante assinatura de termo de responsabilidade e comprometimento. - Uso de autenticação multifatores (recomendado).

	Rede Corporativa	- Credenciais de acesso a rede concedidas, ou excluídas, conforme entrada ou desligamento de usuário, respectivamente. - Acesso a rede rastreável por usuário, endereços de origem e destino, bem como serviços utilizados, guardados em *logs* Informações sigilosas tratadas por meio de canal seguro. - Regras para uso de rede sem fio.
	Ativos de informação	- Usar ferramentas de proteção contra acesso não autorizado aos ativos de informação. - Credenciais ou contas devem fazer uso do princípio do menor privilégio. - Fazer registro de eventos relevantes para a segurança e fazer rastreamento de acesso às informações sigilosas. - Criar mecanismos para garantir a exatidão dos *logs*/registros de auditoria nos ativos de informação. - Regras para uso de Internet, correio Eletrônico e Mensagens instantâneas
Físico	**Áreas e instalações físicas**	- Regras para uso de credenciais físicas - Haver sistema de detecção de intrusos instalados nas áreas - Áreas e instalações são classificas de acordo com valor e criticidade. - Mapeamento das instalações críticas. - Controle de acesso físico com barreiras físicas de segurança, nos ambientes que necessitem. - Mecanismos de proteção contra vandalismos, sabotagens e ataques, especialmente aos ativos considerados críticos. - Recepção com regras claras para entrada e saída de pessoas, equipamentos e materiais. - Áreas críticas possuem maiores controles conforme legislação. - Uso de controle biométrico para acesso físico, é utilizado em conjunto com outro sistema de identificação (autenticação multifatores).
	Usuários	- Exigir o cumprimento da POSIC. - Conscientização em segurança da informação. - Aplicar controles de acesso do usuário e avaliar riscos - Fazer uso de Termo de Responsabilidade assinado individualmente por cada usuário.
	Ativos de informaçã	- Ativos de informação classificados por nível de criticidade (considerar tipo do ativo e impacto da quebra de segurança). - Ativos de informação sigilosos possuem procedimentos especiais para controle de acesso físico. - Estabelecer distância mínima para backups.
	Perímetro segurança	- Estabelecer os perímetros e regulamentar armazenamento, veiculação da imagem, vídeo ou áudio; - Quem transitar em perímetro de segurança deve estar ciente do perímetro.

Fonte: Adaptado para quadro Norma Complementar 07 da IN01/GSI (BRASIL, 2014d)

Observa-se que existem controles de diversos tipos visando diferentes finalidades, como controle de acesso físico e lógico, controle de rede, controle de ativos de informação e de usuários, mas, para a da ABNT NBR ISO/IEC 27002 (ABNT, 2013b, p. xi), a seleção de controles está sujeita a decisões da organização, além de legislações e regulamentações nacionais e internacionais, dependendo também da interação entre controles de modo a prover uma segurança efetiva. Observa-se que a identificação e implementação desses controles de acesso é resultado de um processo de gestão de riscos de segurança da informação bem

elaborado e tais controles visam não apenas prevenir incidentes, mas também auxiliar investigação no caso de sua ocorrência.

Objetivando a segurança da informação como uma estratégia de defesa, o governo federal, por intermédio do Departamento de Segurança da Informação e Comunicações, editou uma série de leis, decretos e normas para essa área. As mais relevantes para esta proposta de pesquisa, considerando a temática segurança da informação para APF, foram apresentadas nesta seção. No entanto, não de forma exaustiva, havendo diversas outras normas que se aplicam ao contexto. No Quadro 9, estão compiladas essas normas de segurança da informação que possuem utilidade para a APF, portanto devem ser conhecidas pelos Agentes Públicos.

Quadro 9 - Leis, decretos e normas técnicas de segurança da informação

NORMA	DESCRIÇÃO
Lei nº 12.965/2014 (Marco Civil da Internet)	Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
Lei nº 12.737/2012	Dispõe sobre a tipificação criminal de delitos informáticos.
Lei nº 9.983/2000	Altera o Código Penal incluindo penas para acessos indevidos aos sistemas de informação, assim como manipulação de dados indevidos.
Lei 13.709/2018 (Lei Geral de Proteção de Dados)	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.
Decreto Nº 9.637/2018	Institui a Política Nacional de Segurança da Informação - PNSI, no âmbito da administração pública federal, com a finalidade de assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação a nível nacional.
Decreto Nº 7.845/2012	Regulamenta os procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.
Decreto Nº 7.724/2012	Regulamenta a LAI, no âmbito do Poder Executivo federal, os procedimentos para a garantia do acesso à informação e para a classificação de informações, sob restrição de acesso, observados grau e prazo de sigilo
ABNT NBR ISO/IEC 27005:2011	Fornece diretrizes para o processo de gestão de riscos de segurança da informação.
ABNT NBR ISO/IEC 27004:2017	Auxilia as organizações a avaliarem o desempenho da segurança da informação e a eficácia do SGSI quanto os requisitos de segurança.
ABNT NBR ISO GUIA 73:2009	Apresenta o vocabulário da gestão de riscos.
ABNT NBR ISO/IEC 27001:2013	Especifica os requisitos para estabelecer, implementar, manter e melhorar um sistema de gestão da segurança da informação.

ABNT NBR ISO/IEC 27002:2013	Diretrizes para práticas de gestão de normas de segurança da informação para as organizações, incluindo a seleção, implementação e gerenciamento de controles.

Fonte: Dados da Pesquisa (2022).

Considerando que a segurança da informação visa prover não apenas a proteção da informação sigilosa, mas também a publicidade da informação ostensiva, normas específicas para a APF relacionadas a publicidade também devem ser levadas em consideração pelos órgãos e entidades, como as sintetizadas no Quadro 10.

Quadro 10 - Normas relacionadas a publicidade da informação

NORMAS	OBJETIVOS
Decreto n. 5.482/2005 - Portal Transparência Pública	Dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da administração pública federal, por meio da Rede Mundial de Computadores - Internet.
Portaria Interministerial n. 140/2006	Disciplina a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da rede mundial de computadores – internet – e dá outras providências.
LC n. 131/2009 - Lei da Transparência	Determina a disponibilização, em tempo real, de informações pormenorizadas sobre a execução orçamentária e financeira da União, dos Estados, do Distrito Federal e dos Municípios.
Decreto n. 7.185/2010	Dispõe sobre o padrão mínimo de qualidade do sistema integrado de administração financeira e controle, no âmbito de cada ente da Federação.
Decreto S/N de 15/09/2011	Institui o Plano de Ação Nacional sobre Governo Aberto e dá outras providências.
Lei 13.709/2018	Lei Geral de Proteção de Dados Pessoais (LGPD)
Lei n. 12.527/2011 - Lei de Acesso à Informação Pública – LAI	Regula o acesso a informações. Dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações.
Decreto n. 7.724/2012	Regulamenta a Lei n. 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.
Portaria da Controladoria Geral da União (CGU)n. 277/2013	Institui o Programa Brasil Transparente com objetivo de apoiar Estados e Municípios na implementação da Lei n. 12.527, no incremento da transparência pública e na adoção de medidas de governo aberto.
Decreto S/N de 12/03/2013	Altera o Decreto de 15 de setembro de 2011, que institui o Plano de Ação Nacional sobre Governo Aberto.
Decreto n. 8.638/2016	Institui a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.
Decreto n. 8.777/2016	Institui a Política de Dados Abertos do Poder Executivo Federal.

Fonte: Adaptado de Gama e Rodrigues (2016, p. 50) e atualizado por Rios (2019, p. 37).

Como visto, são variadas as normas e as temáticas abordadas no campo da segurança da informação, que, em conjunto, possibilitam uma efetiva segurança organizacional. Devido a sua capilaridade, as temáticas tendem a crescer, assim como normas, controles e vulnerabilidades. Todos esses instrumentos devem ser objeto da análise de riscos de segurança da informação, os quais possuem papel fundamental no gerenciamento de riscos, e irão fornecer subsídios para o efetivo tratamento dos riscos.

2.3 ANÁLISE DE RISCOS – CONCEITOS E ESPECIFICIDADES PARA APF

Toda organização, seja ela pública ou privada, possui fluxos informacionais, porém a forma como a informação é tratada dentro dessas instituições pode ampliar ou reduzir os riscos relacionados. Para Duarte, Silva e Costa (2007), há dois tipos de fluxos informacionais, os fluxos formais, objeto de estudo da gestão de informação, relacionados às etapas de organização, armazenamento, disseminação e distribuição da informação, e caracterizado pelos cuidados que os gestores devem ter quanto ao processamento da informação; e os fluxos informais, objeto de estudo da gestão do conhecimento, relacionados à aprendizagem organizacional, por meio das etapas: pessoas, estrutura e cultura organizacional.

A análise de risco objeto desta proposta de estudo tem como foco os fluxos informacionais formais relacionados ao processamento organizacional da informação – englobando organização, armazenamento, disseminação e distribuição da informação –, pela necessidade de proteção da informação ao longo de sua existência, em geral, de responsabilidade dos gestores da organização.

No campo da segurança da informação, as normas preconizam um Sistema de Gestão de Segurança da Informação que possui uma amplitude organizacional abrangente, envolvendo desde políticas de segurança, análise e avaliação de riscos, a tratamento de incidentes. Assim, a segurança da informação propõe-se a proteger os ativos informacionais relacionados ao fluxo, visando minimizar os riscos do negócio, mas tendo em mente que não é possível proteger todos esses ativos devido à escassez de recursos, principalmente ao se considerar o contexto da Administração Pública Federal.

Dessa forma, faz-se necessário adequar as ações de segurança para cada realidade. Para a ABNT NBR ISO/IEC 27005 (2011), risco de segurança da informação consiste na "possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou conjunto de ativos, desta maneira prejudicando a organização" (ABNT, 2011, p. 1). Conforme o

exposto pode-se afirmar que risco é um evento potencial, que pode ocorrer devido à existência de vulnerabilidades[16] e ameaças, ao longo do fluxo informacional, envolvendo diretamente os ativos informacionais.

As fontes das ameaças[17] podem vir do pessoal interno, por erro humano ou simplesmente insatisfação; de parceiros e fornecedores, onde uma simples pane pode impactar, direta ou indiretamente, no negócio; hackers, motivados por diversão ou metas financeiras ou pessoais, acabam por atacar os negócios, em geral, virtualmente. Ademais, evidencia-se que as ameaças ganham uma conotação e dimensão muito maior quando se trata do uso do espaço cibernético, podendo atingir mais de um ativo, estando em constante mutação, especialmente ao se considerar a velocidade da evolução tecnológica nos dias atuais. Mesmo assim, nenhuma ameaça deve ser ignorada, inclusive as não previstas (ABNT, 2011, p. 11).

Além disso, para se identificar ameaças, faz-se necessário analisar histórico de incidentes passados na organização, além de catálogos externos de ameaças. Com as ameaças e suas fontes identificadas, a análise de riscos segue para identificar controles e vulnerabilidades existentes ligados aos ativos e ameaças identificados.

O termo controle consiste em qualquer mecanismo de segurança, seja administrativo, físico, operacional, tecnológico ou humano, que possibilite o tratamento dos riscos de ocorrência de um incidente de segurança. Exemplos de controle são diversos, como: administrativos, políticas, procedimentos e estruturas organizacionais; tecnológicos, *firewall*, software detector de intrusos, antivírus, backups e *patches*[18]; físicos, fechaduras, câmeras de segurança, acesso por biometria e extintores; e lógicos, autenticação e autorização, para suprir processos de identificação de pessoas, equipamentos, sistemas, e privacidade e autenticidade das comunicações, por meio da criptografia e certificado digital (BEZERRA, 2013; SÊMOLA, 2003).

O universo de controles é amplo, podendo um controle atuar em diversas ameaças e uma ameaça precisar de diversos controles. Portanto, todos os tipos devem ser considerados para o contexto organizacional, conforme preceitua a ABNT NBR ISO/IEC 27002 (ABNT, 2013b, p. xi) ao afirmar que a seleção desses controles se sujeita a decisões da organização,

[16]Vulnerabilidade é a fraqueza em sistemas de informação, procedimentos de segurança do sistema, controles internos, ou aplicação que pode ser explorada tendo como origem uma ameaça. (2011, p. B11, tradução nossa)

[17] Ameaça é qualquer circunstância ou evento com o potencial de afetar negativamente as operações organizacionais (incluindo missão, funções, imagem ou reputação), os ativos organizacionais, os indivíduos, outras organizações, ou a Nação, por meio de um sistema de informação via acesso não autorizado, destruição, divulgação, modificação de informações, e/ou negação de serviço (NATIONAL INTITUTE OF STANDARS AND TECHNOLOGY, 2011, p. B11, tradução nossa)

[18] Quando vulnerabilidades são descobertas, certos fabricantes costumam lançar atualizações específicas, chamadas de *patches, hot fixes* ou *service packs*. (CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL, 2012)

além de legislações e regulamentações nacionais e internacionais, dependendo também da interação entre controles, de modo a prover uma segurança efetiva.

Implantar controles de segurança envolve monitoramento e manutenção da qualidade e segurança das atividades de entrada, processamento, saída e armazenamento de informações, logo perpassando todo o fluxo informacional. Ademais, não bastam controles de segurança da informação implantados, faz-se necessário analisar periodicamente sua eficácia e eficiência, para não permanecerem estáticos, enquanto que as ameaças que eles deveriam mitigar são dinâmicas. Dessa forma, os controles, que são inicialmente muito eficazes, podem se tornar inadequados ao longo do tempo e possuir efeito adverso, aumentando ainda mais o risco por fornecer uma falsa sensação de segurança (HARKINS, 2013, p. 19, tradução nossa)

As vulnerabilidades podem ser internas, quando se questiona o comprometimento dos sistemas pelos funcionários, e externas, quando se analisa o que pode ser acessado fora da instituição que possa comprometer os ativos informacionais, podendo ser observadas em diversas áreas: organização; processos e procedimentos; rotinas de gestão e documentação; recursos humanos (incluindo terceiros e prestadores de serviços); ambientes físicos e instalações prediais; configuração dos sistemas de informação (incluindo os sistemas operacionais e aplicativos); hardware, software e equipamentos de comunicação; e dependências de entidades externas. Abrangendo diversas áreas, como: hardware, software, rede, recursos humanos, local ou instalações, e organização. Para cada uma dessas áreas é possível identificar ameaças e possíveis vulnerabilidades. Assim, antecipar as vulnerabilidades por meio da análise de riscos de segurança da informação, permitirá à organização estabelecer um nível aceitável de risco (BEZERRA, 2013, p. 11).

No entanto, a maior vulnerabilidade encontrada nas organizações atualmente é a percepção equivocada de risco. Com ela, funcionários podem postar nas redes sociais informações relacionadas ao trabalho por achá-las inofensivas, enquanto hackers podem utilizar essa informação em "*phishing emails*"[19]. Enquanto os usuários finais tendem a subestimar os riscos de uma atividade ou tecnologia, especialistas em segurança podem apresentar tendências opostas, focando obsessivamente nos riscos de informação associados a uma ameaça ou vulnerabilidade específica. Ao fazê-lo, perde-se completamente a percepção sobre riscos maiores (HARKINS, 2013, p. 18, tradução nossa).

Por consequência, a percepção de riscos de segurança da informação precisa ser trabalhada nas organizações para encontrar um meio termo, no campo da segurança, entre a

[19] "*phishing emails* são emails enviados por pessoas que se passam por pessoas conhecidas para conseguir informações, no intuito de obter acesso aos sistemas organizacionais. (HARKINS, 2013, p. 15, tradução nossa)

ausência de percepção de risco e a percepção excessiva a esse fator. Na prática, o risco depende da percepção das pessoas, especialistas de segurança e usuários; por isso a análise de riscos é de suma importância dentro da gestão de segurança da informação e, principalmente, dentro do gerenciamento de riscos de segurança da informação.

Uma vez valorados os ativos, identificadas as ameaças, vulnerabilidades e controles existentes, é possível quantificar os riscos, e possíveis consequências, de modo o mensurar o grau de riscos organizacional (ABNT, 2011, p. 10). Assim, a identificação dos ativos na APF serve de base na reunião de informações para a análise de riscos e a relevância do ativo a ser protegido por possuir relação com o risco identificado.

2.3.1 Inventário e mapeamento de Ativos na APF

Para a análise de riscos de segurança da informação, não basta listar todos os ativos existentes dentro de uma organização, como, por exemplo, ocorrem com os sistemas evidenciados em almoxarifados. Sua importância organizacional, valoração e criticidade são de extrema importância dentro da análise de risco de SI. Para isso, o governo federal publicou a Norma Complementar 10 (BRASIL, 2012b, p. 4), da IN01/GSI, abordando o processo de inventário e mapeamento de ativos, o qual leva em consideração os objetivos estratégicos, processos, requisitos legais e estrutura do órgão ou entidade. Tal processo objetiva a segurança das infraestruturas críticas de informação e subsidia a proteção dos ativos informacionais, possuindo como pré-requisitos ser: dinâmico, periódico e estruturado, devendo manter uma base de dados atualizada desses ativos informacionais. No tocante aos aspectos de segurança da informação e comunicações da APF, esse processo oferece subsídios tanto para a gestão da segurança da informação, como a gestão de riscos de SI e gestão da continuidade do negócio, pois visa prover o órgão ou entidade da APF:

> [...] de um entendimento comum, consistente e inequívoco de seus ativos de informação; da identificação clara de seu(s) responsável(eis) - proprietário(s) e custodiante(s); de um conjunto completo de informações básicas sobre os requisitos de segurança da informação e comunicações de cada ativo de informação; de uma descrição do contêiner de cada ativo de informação; e da identificação do valor que o ativo de informação representa para o negócio do órgão ou entidade da APF [...] (BRASIL, 2012b, p. 4).

Conforme o especificado, observa-se que análise de riscos bem como demais processos da gestão de segurança da informação, gestão de riscos e de continuidade tem como

base um processo de inventário e mapeamento de ativos bem feito, que visa autoconhecimento institucional do que deve ser protegido. Assim, ao fim desse processo é possível identificar os ativos primários consistentes nos principais processos e informações, tidos como sensíveis e úteis para a elaboração da política de segurança da informação ou do plano de continuidade do negócio.

Esses ativos, frequentemente, herdam os controles implementados para a proteção de processos e informações sensíveis (ABNT, 2011, p. 30-31). Porém, vale salientar que mesmo ativos primários não sensíveis podem vir a herdar controles por oferecer suporte a ativos sensíveis. Considerando que os ativos apresentam vulnerabilidades que podem ser exploradas pelas ameaças, faz-se necessário listar as ameaças existentes e vulnerabilidades relacionadas aos ativos, de modo a dar andamento à análise de risco.

2.3.2 Análise de Riscos na APF

Considerando que o nível de risco depende da percepção de segurança da informação de especialistas e usuários, alguns gestores veem erroneamente a análise de riscos como análise de sua gestão e tendem a diminuir os riscos. Mas o resultado da análise de riscos visa essencialmente mostrar a realidade da organização frente aos riscos e justificar maior proteção, portanto, maiores investimentos nessa área. No final, não há culpados pela presença ou ausência de segurança, mas sim um desenho da segurança da informação institucional e um olhar voltado para medidas de segurança, pois, apenas em cenários utópicos, a organização está completamente protegida de todos os tipos de ameaças.

Corroborando com essa ideia, a Norma Complementar 07 (BRASIL, 2014d, p. 3) conceitua a gestão de riscos de segurança da informação como o conjunto de processos para "identificar e implementar medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos", ou seja, determinar qual ativo deve-se proteger, e contra o quê. A gestão de riscos possui o olhar voltado para a segurança da informação organizacional e oferece subsídio para suportar o Sistema de Gestão de SI e a Gestão da Continuidade do Negócio.

Assim, a análise de riscos de SI na APF faz parte de um quadro mais amplo que deve ser considerado durante sua execução, onde, segundo a Norma Complementar 02 (BRASIL, 2008b), da IN01/GSI, a metodologia de gestão de segurança da informação e comunicações, a ser aplicada na APF, baseia-se no processo de melhoria contínua, denominado ciclo “PDCA”

(*Plan-Do-Check-Act*), referenciado pela norma ABNT NBR ISO/IEC 27001 (ABNT, 2013). Essa escolha deveu-se à simplicidade do modelo, compatibilidade com a cultura de gestão da segurança da informação e coerência com as práticas de qualidade e gestão adotadas pelos órgãos públicos.

O ciclo PDCA nessa norma refere-se a ações a serem tomadas pelos gestores de segurança dos respectivos órgãos ou entidades, o qual possui as fases de planejamento, onde se planejará as ações de segurança a serem implementadas; execução, onde se implementará as ações definidas na fase de planejamento; verificação, fase em que o gestor de segurança avaliará as ações de segurança implementadas na fase anterior; e ação, que possui o intuito de aperfeiçoar as ações implementadas, com base no monitoramento feito na fase anterior, e promover a melhoria continua. A síntese das ações dos gestores de segurança exigidas pela norma encontra-se no Quadro 11.

Quadro 11 - Ações a serem tomadas pelos gestores de segurança

FASE	AÇÕES
Planejamento (Plan)	• Definir o escopo e os limites onde serão desenvolvidas ações de segurança, os objetivos a serem alcançados com a implementação dessas ações e a abordagem de gestão de riscos do órgão ou entidade, sendo necessário: · definir uma metodologia de gestão de riscos adequada; · identificar os níveis de riscos aceitáveis e os critérios para sua aceitação, considerando decisões superiores e o planejamento estratégico do órgão ou entidade; • Identificar os riscos, sendo necessário identificar: os ativos e seus responsáveis, as ações de segurança da informação e comunicações; as vulnerabilidades; os impactos que perdas de disponibilidade, integridade, confidencialidade e autenticidade podem causar nestes ativos; • Analisar os riscos, sendo necessário identificar: · os impactos para a missão do órgão ou entidade que podem resultar de falhas de segurança, levando em consideração as conseqüências de uma perda de disponibilidade, integridade, confidencialidade ou autenticidade destes ativos; · a probabilidade real de ocorrência de falhas de segurança, considerando as vulnerabilidades prevalecentes, os impactos associados a estes ativos e as ações de segurança implementadas; · os níveis de riscos, são aceitáveis ou requerem tratamento utilizando os critérios de aceitação. • Identificar as opções para o tratamento de riscos, considerando a possibilidade de: · aplicar ações de segurança da informação e comunicações além das que já estão sendo executadas; · aceitar os riscos de forma consciente e objetiva, desde que satisfaçam o planejamento organizacional, bem como a diretrizes expedidas pela autoridade decisória de seu órgão ou entidade, bem como aos critérios de aceitação de riscos; evitar riscos; ou transferir os riscos a outras partes, por exemplo, seguradoras ou terceirizados; • Selecionar as ações de segurança da informação e comunicações consideradas necessárias para o tratamento de riscos. • Obter aprovação da autoridade decisória quanto aos riscos residuais propostos; • Obter autorização da autoridade decisória para implementar as ações de SIC selecionadas, mediante uma Declaração de Aplicabilidade

Execução (Do)	• Formular um plano de metas, obter autorização para cada objetivo das ações de segurança aprovadas, incluindo responsabilidades, prazos e custos estimados; • Implementar o plano e medir a eficácia das ações por meio de indicadores mensuráveis para as metas aprovadas. • Implementar programas de conscientização e treinamento, que deverão: · assegurar que todo pessoal que tem responsabilidades atribuídas no plano de metas receba o treinamento adequado para desempenhar suas tarefas; · manter registros sobre habilidades, experiências e qualificações do efetivo do órgão ou entidade relativos à segurança da informação e comunicações; · assegurar que todo efetivo do órgão ou entidade esteja consciente da relevância e importância da segurança da informação e comunicações em suas atividades e como cada pessoa pode contribuir para o alcance dos objetivos das ações de segurança da informação e comunicações; • Gerenciar a execução das ações e os recursos empenhados para seu desenvolvimento; • Implementar procedimentos capazes de permitir a pronta detecção de incidentes de segurança da informação e comunicações, bem como a resposta a incidentes de segurança da informação e comunicações.
Verificação (Check)	• Fazer avaliação e análise crítica, a fim de: · detectar erros nos resultados de processamento e incidentes de segurança; · determinar se as ações de segurança delegadas a pessoas, ou implementadas através de tecnologia, são executadas conforme planejado; · determinar a eficácia das ações, mediante o uso de indicadores; • Realizar análises críticas regulares, e atualizá-las, a intervalos planejados de pelo menos uma vez por ano; • Verificar se os requisitos ou pressupostos estabelecidos pelo planejamento organizacional, bem como as diretrizes expedidas pela autoridade decisória foram atendidos; • Conduzir auditoria interna das ações de segurança a intervalos planejados de, pelo menos, uma vez ao ano; • Atualizar os planos de segurança da informação, considerando os resultados da avaliação e análise de crítica; • Registrar e levar ao conhecimento da autoridade superior possíveis impactos na eficácia da missão de seu órgão ou entidade.
Ação (Act)	• Propor à autoridade decisória a necessidade de implementar as melhorias identificadas; • Executar ações corretivas ou preventivas, de acordo com a identificação de não conformidade real ou potencial; • Comunicar as melhorias à autoridade decisória de seu órgão ou entidade; e • Assegurar-se de que as melhorias atinjam os objetivos pretendidos.

Fonte: Adaptado para quadro de Norma Complementar 02 (BRASIL, 2008b)

Observa-se do quadro de ações dos gestores de segurança que a análise e avaliação de riscos encontram-se dentro da fase de planejamento, até porque, como evidenciado, o resultado da análise de riscos visa mostrar a realidade institucional e evidenciar a necessidade de investimentos na área. Fazendo uma leitura em conjunto com a Norma Complementar 04 (BRASIL, 2013e), observa-se que o ciclo PDCA também foi incluído dentro do processo de gestão de riscos de segurança da informação, que possui como diretrizes gerais que o processo considere, prioritariamente, objetivos estratégicos, processos, requisitos legais e a estrutura do órgão ou entidade da APF.

O Quadro 12 traz a síntese desse processo, o qual deve estar alinhado ao planejamento estratégico organizacional e ao processo de gestão de riscos corporativos, se houver, onde seu escopo se limita a ações de SI.

Quadro 12 - Síntese do processo de gestão de riscos na APF

	ETAPAS	AÇÕES
Plan	Definições preliminares	➢ Definir escopo ➢ Adotar Metodologia
	Análise e avaliação dos riscos	➢ Realizar inventário e mapeamento dos ativos de informação, Identificar os riscos associados ao escopo definido, considerando: ameaças envolvidas; vulnerabilidades existentes nos ativos de informação; e as ações de segurança da informação já adotadas. ➢ Estimar os riscos levantados, considerando valores ou níveis para a probabilidade e a consequência do risco associados à perda, nos ativos, de disponibilidade, integridade, confidencialidade e autenticidade; ➢ Avaliar os riscos, se são aceitáveis ou se requerem tratamento, ➢ Relacionar os riscos que requeiram tratamento, priorizando-os de acordo com critérios estabelecidos
	Plano de tratamento dos riscos	➢ Determinar as formas de tratamento dos riscos, considerando as opções de reduzir, evitar, transferir ou reter o risco, observando: a eficácia das ações de SI já existentes; as restrições organizacionais, técnicas e estruturais; os requisitos legais; e a análise custo/ benefício. ➢ Formular um plano de tratamento dos riscos, relacionando, no mínimo, as ações de SI, responsáveis, prioridades e prazos de execução necessários à sua implantação
	Aceitação dos riscos	➢ Verificar os resultados do processo executado, considerando o plano de tratamento, aceitando-os ou submetendo-os à nova avaliação
Do	Implementar plano de tratamento	➢ Executar as ações de SI incluídas no Plano de Tratamento dos Riscos aprovado
Check	Monitoração e análise crítica	➢ Detectar possíveis falhas nos resultados e monitorar os riscos: · Do processo de gestão: monitorar e analisar criticamente o processo de Gestão de Riscos SI de forma a mantê-lo alinhado às diretrizes gerais estabelecidas e às necessidades do órgão ou entidade; · Do risco: manter os riscos monitorados e analisados criticamente, a fim de verificar regularmente, no mínimo, mudanças nos: critérios de avaliação e aceitação dos riscos; no ambiente, ativos de informação e ações de SI, fatores do risco (ameaça, vulnerabilidade, probabilidade e impacto).
Act	Melhoria do processo de Gestão de Riscos de SI	➢ Propor à autoridade decisória a necessidade de implementar as melhorias identificadas durante a fase de monitoramento e análise crítica; ➢ Executar as ações corretivas ou preventivas aprovadas; ➢ Assegurar que as melhorias atinjam os objetivos pretendidos

Fonte: Adaptado para quadro de Norma Complementar 04 (BRASIL, 2013e)

Observa-se do quadro que a análise de riscos, consiste em uma das etapas do processo de gerenciamento de riscos e, como já dito, é considerada a base desse processo que irá alimentar as etapas seguintes. A etapa de Comunicação do Risco não está representada no quadro visto que permeia todo processo, sendo alimentada pelas demais etapas, uma vez que

objetiva informar as instâncias superiores do andamento de todas as fases da gestão de risco, compartilhando as informações entre o tomador da decisão e as demais partes envolvidas e interessadas.

2.3.2.1 Sistemas seguros na APF

Após a noção do papel da análise de riscos de segurança da informação na APF, dentro do gerenciamento de riscos e da gestão de segurança da informação, e considerando o fluxo de informação digital, seu ambiente, e suporte tecnológico, inerente ao fluxo informacional formal relacionado aos ativos de informação, evidencia-se a necessidade de uma análise de riscos mais apurada que considere os ativos inerente a esse ecossistema, como rede, suporte, desenvolvimento, tecnologias em nuvem, dentre outros.

Logo, espera-se que o mapeamento de ativos na APF, base da análise de riscos, deve se preocupar também com o meio tecnológico pelo qual perpassa a informação. As informações dos órgãos e entidades que transitam pela computação em nuvem, devem passar por um processo de gestão de riscos, que considere o tipo de informação a ser tratada nesses meios e a localização geográfica da nuvem, bem como regras de propriedade.

Nesse sentido, a Norma Complementar 14 (BRASIL, 2018b) preceitua que, no caso da computação em nuvem, quando a informação a ser tratada não possui restrição de acesso, pode ser tratada a critério do órgão ou entidade da APF, considerando a legislação vigente e os riscos envolvidos; quando a informação é sigilosa, em regra, deve evitar o uso da nuvem, mas se for do tipo classificada ou material de acesso restrito é proibido o uso de computação em nuvem.

Quanto a localização geográfica e propriedade da informação, pode-se observar que, na adoção de serviços em nuvem, deve ser assegurado que dados, metadados, informações e conhecimento, tratados pelo provedor, bem como os backups, deverão residir em território brasileiro, não podendo ser fornecidos a terceiros e/ou usados pelo provedor para fins diversos do contratado, havendo necessidade de autorização formal do órgão ou entidade da APF (BRASIL, 2018b, p. 5). Tal preocupação revela-se uma vez que o órgão ou entidade da APF é tido como proprietário ou custodiante da informação, portanto responsável pela segurança das informações tratadas em nuvem.

A análise de riscos na APF também deve considerar o desenvolvimento de software seguro, uma vez que o fluxo informacional transita precipuamente entre sistemas, que são foco de ataques a softwares e hardwares, onde concentra-se a exploração de vulnerabilidades

de segurança no suporte tecnológico, não importa se são desenvolvidos ou apenas adquiridos pelos órgãos e entidades.

Com isso, o não uso de boas práticas de codificação segura, bem como ausência de testes de segurança que validem os controles aplicados dificultam a segurança do fluxo informacional que perpassa por esses suportes. Assim, torna-se necessário definir requisitos de segurança, funcionais e não funcionais, mínimos, durante o processo de desenvolvimento e manutenção de sistemas, com o objetivo de proteger os ativos informacionais dos órgãos e entidades da APF (BRASIL, 2012c, p. 2–5). Tais requisitos devem considerar, conforme o Quadro 13:

Quadro 13 - Requisitos para desenvolvimento de software seguro

Tipo de Aquisição	• a aquisição, paga ou não, de software pronto; • o desenvolvimento e/ou manutenção de software feito por profissionais da própria organização; e • a contratação de terceiros para o desenvolvimento e/ou manutenção de software.
Tipo de análise	• Análise Dinâmica: teste de software que verifica comportamento externo em busca de anomalias ou vulnerabilidades. Ocorre por meio de interações com o software em execução; • Análise Estática: teste de software que verifica lógica interna em busca de falhas ou vulnerabilidades. Ocorre por meio da verificação do código-fonte ou dos binários;
Tipo de requisitos de segurança	• Funcionais: descrevem comportamentos que viabilizam a criação ou a manutenção da segurança e, geralmente, podem ser testados diretamente. Na maioria dos casos, remetem a mecanismos de segurança como exemplo: o Controle de acesso baseado em papéis de usuários, o Autenticação com o uso de credenciais (usuário e senha, certificados digitais,etc.) • Não funcionais: descrevem procedimentos necessários para que o software permaneça executando suas funções adequadamente mesmo quando sob uso indevido. Ex: o validação das entradas de dados, e o registro de logs de auditoria com informações suficientes para análise forense

Fonte: Adaptado para quadro de Norma Complementar 16 (BRASIL, 2012c, p. 2–5).

Observa-se do Quadro 13, que a norma preceitua a necessidade de um responsável pela definição e validação dos requisitos de software identificados – os quais devem ser definidos desde o início do projeto de desenvolvimento –, bem como controles de segurança implementados – de preferência utilizados como componentes e baseados em padrões do mercado –, que sejam catalogados e reutilizados, observando que fica a critério de cada órgão a escolha das melhores soluções de mercado.

Assim, dentre outros quesitos de segurança, o desenvolvimento de software deve considerar: controles de acesso; implementar controles de segurança em múltiplas camadas, pois dificulta a exploração de vulnerabilidades; usar arquitetura de software que privilegie alta coesão e baixo acoplamento; evitar mensagens de erro que revelem detalhes arquiteturais;

realizar análise estática ou dinâmica dos requisitos de segurança do software; e fazer limpeza dos dados de teste antes de passar para o ambiente de produção (BRASIL, 2012c, p. 5–6).

No caso de terceirização do desenvolvimento seguro, isto é, caso se pretenda obter software, recomenda-se que o órgão ou entidade da APF:

> - ✓ Estabeleça normas internas para aquisição de software seguro;
> - ✓ Estabeleça acordos de licenciamento que permitam adquirir a titularidade do software ou apenas exercer o direito de uso;
> - ✓ Ter os requisitos de segurança definidos e documentados, no caso de aquisição ou desenvolvimento externo;
> - ✓ Estabelecer definições sobre custódia do código-fonte e manutenção de software, a critério de cada órgão;
> - ✓ Definir execução de testes pela contratada e homologação feita pelo órgão ou entidade antes da instalação em ambiente de produção onde:
>   - o orienta-se análise estática caso software desenvolvido por terceiros
>   - o o tratamento das vulnerabilidade deve ser um dos critérios de aceite do sistema
> - ✓ Definir regras e procedimentos para a liberação de acesso, lógico ou físico, aos recursos tecnológicos do órgão ou entidade, caso necessário;
> - ✓ Definir regras para transferência de conhecimento sobre o software de modo a permitir sua manutenção;
> - ✓ Certificar que os procedimentos de segurança estejam previstos no instrumento contratual. (BRASIL, 2012c, p. 7–8)

Assim, observa-se do desenvolvimento seguro estipulado pela legislação para a APF que há regras a serem estabelecidas tanto para o desenvolvimento interno do órgão, como para a terceirização, todas visando a segurança da informação devendo ser consideradas durante a análise de riscos. Ademais, o Apêndice A, que traz um *checklist* de controles específicos para aplicações web proposto pela *SysAdmin, Audit, Network and Security Intitute* (SANS), é de suma importância para análise de riscos no ecossistema digital dos órgãos ou entidades.

A análise de riscos de SI nesse ambiente deverá considerar, quanto a área de redes, controles criptográficos, certificação digital, controles de acesso específicos e também parcerias entre as instituições, uma vez que, para a ABNT NBR ISO/IEC 27002 (2013b, p. 6) torna-se salutar parcerias quando o assunto é segurança da informação, como, por exemplo, a parceria, desde 2014, entre a Rede Nacional de Ensino e Pesquisa e a *Globalsign*, empresa fornecedora de certificados digitais, que permite às instituições de ensino emitir gratuitamente os próprios certificados digitais SSL[20] (GUIMARÃES, 2016)

[20] Esses certificados são mecanismos de controle que visam garantir a autenticidade da página de uma instituição, evitando mensagens nos navegadores indicando que o certificado da página institucional não é válido, oferecendo maiores garantias quanto à página pertencer verdadeiramente ao respectivo órgão, por exemplo. (GUIMARÃES, 2016)

Essas parcerias devem ser consideradas no sentido que, às vezes, uma empresa ou profissional que atue na área pode trazer um melhor custo-benefício que iniciar do zero. Não podendo se esquecer que a análise de riscos deve sempre estar alinhada ao planejamento estratégico organizacional, leis e normas aplicáveis a APF, boas práticas nacionais e recomendações internacionais, no sentido de planejar e identificar controles para mitigar os riscos, ações essas que podem ser facilitadas por meio de parcerias, e devem ser consideradas pelos gestores de segurança da informação dessas instituições.

Uma vez ciente da importância da segurança da informação para o ecossistema digital da APF, observa-se que ações nesse sentido ampliam a proteção ao fluxo informacional existente nessas organizações e a comunidade acadêmica, diretamente, bem como o governo federal, se beneficiam dos resultados que podem vir associados a ações pós análise de riscos de segurança.

Logo, deve haver um mínimo de controle e monitoramento que permita, à comunidade acadêmica e à sociedade, a proteção das informações pessoais e divulgação das informações ostensivas. Construindo-se um laço com eles que não pode ser nem apertado demais, para não sufocar suas liberdades, nem solto demais ao ponto que possibilite o roubo ou mau uso das informações por terceiros inidôneos. Há o dever do Estado de proteção das informações pessoais dos cidadãos; o que inclui a necessidade de incrementar a segurança no ecossistema digital, processos e pessoas; bem como orientar a condução de políticas de segurança da informação e comunicações pela APF.

2.3.3 Lei Geral de Proteção de Dados Pessoais

Uma área mais específica em Segurança da Informação, e tendência atual frente à alta exposição de dados em forma digital na atualidade, encontra-se na Lei Geral de Proteção de Dados Pessoais (LGPD), Lei Nº 13.709 de 2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais. A LGPD Visa proteger especialmente o direito à privacidade, que consiste em uma das propriedades da Segurança da Informação. Essa lei prevê a privacidade dos dados desde sua origem, abrangendo todo o ciclo de vida de tratamento dos dados pessoais.

Em tempos de vazamento de dados organizacionais na rede, a efetivação da LGPD possibilita exigir que as organizações, públicas e privadas, prestem atenção no tratamento dos dados pessoais e invistam em segurança da informação, de modo a prevenir vazamentos de dados. Com isso, alguns pontos elencados na lei podem ser sintetizados em:

- ✓ Orientação aos funcionários e os contratados da organização a respeito das práticas a serem tomadas para tratamento de dados pessoais;
- ✓ O tratamento de dados pessoais sensíveis ocorre, em regra, com o consentimento do titular;
- ✓ O consentimento para tratamento dos dados pessoais é feito, em regra, por escrito;
- ✓ Criação de relatório de impacto à proteção de dados;
- ✓ Confirmação da existência ou fornecimento de acesso a dados pessoais mediante requisição do titular;
- ✓ Descrição dos tipos de dados coletados e da metodologia utilizada para a sua coleta de dados;
- ✓ Avaliação de forma permanente das salvaguardas e mecanismos de mitigação de riscos adotados;
- ✓ Canal de comunicação para aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- ✓ Receber comunicações da autoridade nacional e adotar providências;
- ✓ Manter registro das operações realizadas para tratamento de dados pessoais. (BRASIL, 2018c).

Como pode ser observado, a lei elenca ações de segurança da informação, com foco na privacidade dos dados pessoais e, por isso, essa lei deve ser considerada no rol de ações de segurança da informação necessárias à Administração Pública Federal. Uma vez que, as atividades desempenhadas pelos órgãos ou entidades setoriais lidam e tratam com dados pessoais em volume considerável em seus processos, e em caso de inconformidade com normas e políticas da empresa, como a disponibilização irregular de dados pessoais, pode ser configurada como extravio de dados, acarretando em outros delitos, ensejando punições não desejadas.

Nesse sentido, não se poderia pensar em ações de segurança para as Instituições Federais de Ensino Superior sem incluir as ações fomentadas nos normativos de segurança da informação para administração pública Federal, incluída a LGPD, e nas recomendações internacionais.

3 PROCEDIMENTOS METODOLÓGICOS

Para o atendimento do objetivo da pesquisa em estabelecer elementos conceituais para o desenvolvimento de um modelo integrado e simplificado de ações de segurança para análise de riscos de segurança da informação, adequado para o contexto informacional dos setores de tecnologia das Instituições Federais de Ensino Superior (IFES), este estudo se fundamentou nos métodos e técnicas disponibilizados pela pesquisa científica.

A pesquisa científica consiste no processo formal e sistemático com base no método científico, cujo objetivo visa descobrir respostas para problemas, por meio do emprego de procedimentos específicos. Dentre os tipos de pesquisa, a pesquisa social visa obter respostas no campo da realidade da sociedade (GIL, 2012, p. 26). Com base nessa perspectiva, esta pesquisa buscou se fundamentar nos métodos e técnicas da pesquisa social, de modo a obter subsídios orientadores do processo de investigação de um estudo centrado no contexto social, para a compreensão da problemática questão voltada para a orientação direcionada à avaliação e controle de riscos de segurança nos fluxos de informações em suportes tecnológicos das IFES.

Nesta seção, serão apresentados: a caracterização da pesquisa; a contextualização do objeto de pesquisa; universo e amostra; técnicas de coleta de dados; finalizando com métodos de análise dos dados e a trajetória da análise.

3.1 CARACTERIZAÇÃO DA PESQUISA

Para poder atingir ao objetivo do estudo, foi necessário que se caracterizasse como de natureza aplicada, onde os objetivos a definiram com base em 02 (dois) tipos de pesquisa: pesquisa exploratória (primeira fase da pesquisa) e pesquisa descritiva (segunda fase da pesquisa), fundamentadas a partir de uma pesquisa de abordagem mista combinando técnicas de pesquisa qualitativa e quantitativa.

A natureza aplicada da pesquisa justifica-se devido à investigação propor um estudo de solução de natureza prática referente à orientação voltada para a análise e controle de riscos de segurança da informação existentes no contexto informacional dos setores de tecnologia das IFES.

De acordo com Fleury e Werlang (2017), a pesquisa aplicada se concentra em problemas existentes nas atividades de instituições, organizações, entre outros, com o intuito

de buscar soluções com contribuições práticas. Conforme esses autores, uma pesquisa de natureza aplicada, que se concentra em problemas práticos, pode possibilitar a descoberta de princípios científicos.

Nesse entendimento, o estudo foi realizado com base em uma investigação da realidade à luz do modelo de processo de gerenciamento de riscos OCTAVE *Forte* e às normas de SI que regem a APF, que puderam, com a metodologia aplicada, estabelecer e identificar novos parâmetros científicos para explicar e solucionar a problemática em questão.

Conforme os objetivos estabelecidos para este estudo, foi fundamental que a pesquisa fosse desenvolvida em duas fases. Na primeira fase, a pesquisa se caracterizou como pesquisa exploratória que teve como intuito facilitar a familiaridade do pesquisador com o tema em pesquisa, ou seja, aprofundar suas especulações de modo a encontrar as causas reais da ocorrência de determinado fenômeno ainda pouco conhecido, ou de uma problemática que não foi totalmente delineada, concentrando-se no levantamento de informações sobre o objeto de estudo, delimitando e mapeando o seu campo de trabalho e as suas condições de ocorrência, respectivamente. (APPOLINÁRIO, 2011; DELL-MASSO; COTTA; SANTOS, 2014; SEVERINO, 2007).

A pesquisa exploratória permitiu alcançar aos objetivos específicos de mapeamento do contexto de segurança da informação em setores tecnológicos das IFES, à luz das ações de segurança da informação; – que colaboraram com a pesquisa por meio de uma seleção racional (amostragem intencional) –, e a realização de pesquisa documental relacionadas à segurança da informação, como os frameworks de gerenciamento de riscos, normas do governo federal para segurança da informação, e trabalhos publicados nesse sentido. Foi possível estabelecer nessa fase um mapeamento das ações de segurança da informação, de processo de gerenciamento de riscos e operacionais de SI, para maior fundamentação dos estudos das etapas de construção do modelo.

A pesquisa exploratória, além de ter proporcionado à pesquisadora maior aproximação com as ações institucionais em SI que compõem os conhecimentos que auxiliaram no desenvolvimento do modelo integrado e simplificado de ações de segurança da informação, permitiu a obtenção de informações específicas referentes à sua construção, guiada pela hipótese específica, com base no levantamento da pesquisa documental e pré-teste com especialistas em segurança da informação.

A segunda parte da pesquisa foi caracterizada como pesquisa descritiva, que com base no conhecimento desenvolvido com a pesquisa exploratória – com as informações de segurança delineadas alimentando o modelo de ações de análise de riscos de segurança da

informação construído –, permitiu afinar o modelo, com a aplicação do questionário semi-estruturado (amostra probabilística), em conjunto com as IFES, em âmbito nacional, e o estabelecimento da análise e interpretação desses dados.

Nesse contexto, a pesquisa descritiva contribuiu com a obtenção dos objetivos de proposição do modelo, permitindo pesquisar a realidade das IFES quanto às ações, de processo e operacionais, de segurança da informação à luz do framework reconhecido internacionalmente OCTAVE *Forte* e das normas do governo federal para segurança da informação em setores de tecnologia, e, principalmente, afinar o modelo de ações de segurança, a partir da realidade aplicada aos setores de tecnologia no contexto das IFES.

A pesquisa descritiva é útil quando se pretende descrever o tema ou problema de pesquisa por meio da coleta de dados, cuja ideia é medir, avaliar ou coletar dados sobre variados aspectos do fenômeno a ser pesquisado. Esse tipo de pesquisa visa descrever as características de determinado fenômeno ou o relacionamento entre variáveis, sendo que sua característica mais relevante encontra-se no uso de técnicas padronizadas de coleta de dados (GIL, 2012, p. 28; SAMPIERI; COLLADO; LUCIO, 2006, p. 101). Logo, a pesquisa descritiva justificou-se pela necessidade de obter a resposta para a problemática da pesquisa, com base na adequação do modelo formulado alinhado à realidade, em contexto nacional, com ações e controles de segurança que perpassam os setores de tecnologia.

A combinação de técnicas de pesquisa qualitativa e quantitativa foi necessária, para o contexto específico do desenvolvimento do modelo integrado simplificado, devido a duas análises: a qualitativa, pertinente quanto à falta de disponibilidade de dados/informações ou quando são precários esses dados, uma vez que pode se basear em valores referenciais; e a quantitativa, devido à disponibilidade de dados confiáveis, em que a análise é elaborada com base em valores absolutos (DANTAS, 2011).

No contexto da pesquisa, a abordagem qualitativa se fez necessária para a compreensão do fenômeno social, sendo útil na identificação de questões e compreensão de sua importância. Enquanto a quantitativa foi adequada para a projeção de medidas precisas e confiáveis que permitiram uma análise estatística, podendo medir opiniões, atitudes e comportamentos. Ademais, com a necessidade de integração entre abordagens, a pesquisa qualitativa costuma ser seguida de um estudo quantitativo (MORESI, 2003; RICHARDSON, 2015).

Para Minayo (2009, p. 22), a natureza da pesquisa é o que diferencia a abordagem quantitativa da qualitativa, havendo uma oposição complementar. Nesse sentido, Araújo (2009) evidencia que apesar de ambas oferecerem resultados úteis e significativos, as suas

propriedades demonstram essa oposição complementar, pois, enquanto à quantitativa, possui cálculo complexo, demanda tempo e requer grande volume de informações, a qualitativa é subjetiva e envolve suposições, geralmente de especialistas. Portanto, a combinação de técnicas entre pesquisas quantitativas e qualitativas se fez necessária para permitir maior acurácia ao desenvolvimento do modelo integrado simplificado de ações em segurança da informação.

3.2 OBJETO, UNIVERSO E AMOSTRA DA PESQUISA

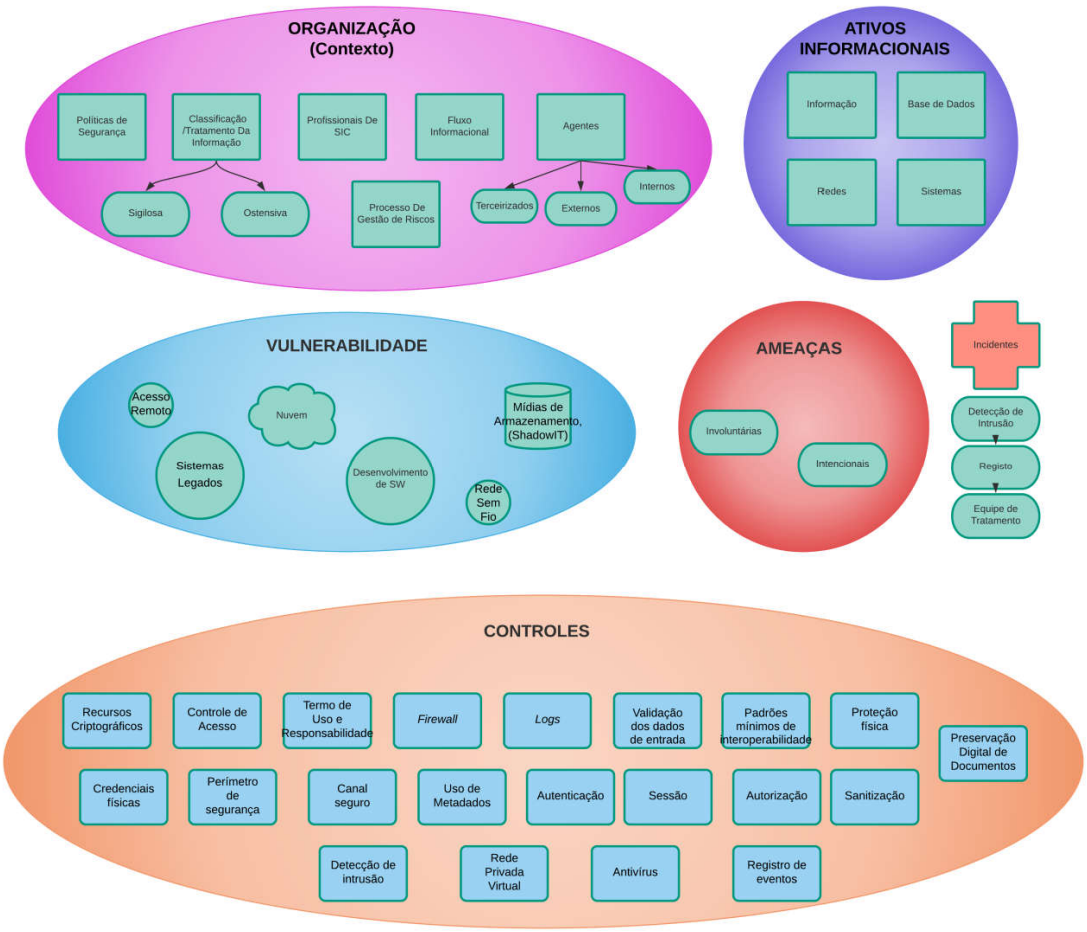
Tendo em vista que o objetivo da pesquisa consistiu em desenvolver um modelo integrado e simplificado de ações para análise de riscos de segurança da informação, específico para o contexto informacional dos setores de tecnologia das Instituições Federais de Ensino Superior. O objeto de pesquisa constituiu as ações de segurança da informação existentes ou necessárias aos setores de tecnologia das IFES.

Para alcançar o desenvolvimento dos elementos necessários ao modelo, que permitissem responder à hipótese da pesquisa, contemplando as ações de segurança, adequadas para o contexto informacional dos setores de tecnologia das Instituições Federais de Ensino Superior (IFES), fez-se necessário um pensamento em etapas, que compreende um estudo para levantar as ações necessárias e afiná-lo de acordo com a realidade dessas instituições por intermédio dos conhecimentos dos responsáveis pela segurança da informação do setores de tecnologia dessas instituições, esclarecendo as condições de avaliação e controle dos riscos à segurança da informação inerentes aos fluxos de informação que passam sob suas responsabilidades.

Sabe-se que as IFES contam com estruturas organizacionais de alta complexidade, constituídas por faculdades, centros, departamentos, escolas, institutos, coordenações de cursos e órgãos periféricos, e, na atual sociedade da informação, essas estruturas são proprietárias de informações que perpassam, em sua grande maioria, na forma digital, pelo setor de tecnologia responsável, principalmente se a instituição adota o modelo centralizador de competências tecnológicas. Essa relação de aspectos técnicos foi definitiva para a escolha do contexto de pesquisa no tocante à aglutinação informacional digital: os setores de tecnologia. Por serem setores responsáveis pela segurança da informação, a partir do momento que a informação entra nos sistemas estruturantes das instituições, em sua forma digital, para guarda, armazenamento e processamento.

Os conhecimentos evidenciados em uma visão macro do modelo de ações de segurança para análise de riscos, específico para os setores de tecnologia, permitiram observar, ao longo da pesquisa, o esboço da análise de riscos à luz das exigências das normas de SI para a administração pública federal, sintetizados na Figura 13 em: Organização, Ativos Informacionais, Vulnerabilidades, Ameaças e Controles.

Figura 13 - Esboço da análise de riscos à luz das normas de SI da APF



Fonte: Elaborado pela autora (2022).

O modelo desenvolvido levou em consideração a estrutura do modelo de processo de gerenciamento de riscos OCTAVE *Forte* e, como o modelo se dirige aos setores de tecnologia das IFES, foi adaptado e customizado com as ações de segurança da informação existentes nos controles das normas ABNT NBR ISO/IEC 27002 (2013), e nas Instruções Normativas 01, 02 e 03 do Gabinete de Segurança Institucional da Presidência da República do Brasil e da Lei Geral de Proteção de Dados, que regem a Administração Pública Federal. Ao fim o

modelo permitiu abranger as variáveis esboçadas na figura 13 acima, de forma simplificada, em constructos: Estrutura de Governança, Análise de Riscos, Resposta a Riscos e Monitoramento/Melhorias, a serem detalhados mais à frente, porém no intuito de diminuir a granularidade das ações de SI para o modelo.

O modelo partiu do desenho do contexto organizacional, local das ações de governança, com levantamento dos ativos informacionais, tolerância a risco, políticas e requisitos de continuidade, para, na análise de riscos, trazer os componentes necessários, dispostos na figura 13 - ativos, riscos, ameaças, vulnerabilidades e controles correntes – de forma simplificada. Com as ações de governança e componentes de riscos identificados na análise, as ações de resposta ao risco e monitoramento contínuo do próprio processo complementam o modelo.

Para o desenvolvimento dos elementos conceituais do modelo integrado e simplificado de ações de segurança para análise de riscos de segurança da informação, adequado para o contexto informacional dos setores de tecnologia das Instituições Federais de Ensino Superior (IFES), por se tratar de um modelo de aplicação ampla, a pesquisa precisou ser composta por um universo que contemplou a contribuição de responsáveis envolvidos com a segurança da informação nos setores de tecnologia das IFES, em âmbito nacional, que é composto por 63 Universidades e 39 Institutos Federais de Ensino Superior, totalizando 102 instituições. Devendo-se considerar que o universo, ou população, de uma pesquisa se fundamenta no total de elementos que possuem características comuns, ou seja, que atuem de forma que suas ações corresponderão às necessidades do entendimento do objeto de estudo (PARDAL; LOPES, 2011; VERGARA, 2010).

Nesse contexto, é imprescindível especificar, novamente, que a pesquisa trabalhou com base em duas fases: pesquisa exploratória e pesquisa descritiva. Nessa condição, a pesquisa precisou de dois tipos distintos de amostras. Para a pesquisa exploratória, que se deu em fase de pré-teste, foi necessária a determinação por sistema de amostra intencional, ou de seleção racional, que foi constituída por 6 (seis) especialistas em segurança da informação que foram escolhidos por conveniência de proximidade com o ambiente da pesquisadora desta pesquisa, com o objetivo de afinar o questionário à realidade da segurança da informação das IFES.

A amostra intencional "constitui um tipo de amostragem não probabilística e consiste em selecionar um subgrupo da população que, com base nas informações disponíveis, possa ser considerado representativo de toda a população." (PRODANOV; FREITAS, 2013, p. 98–99). Especifica-se ainda que, para as amostras intencionais o significado maior de seu

procedimento não está relacionado à quantidade de agentes e/ou instituições que integrarão a pesquisa, mas no modo como se conceberá a sua representatividade e qualidade das informações que serão obtidas com base em suas contribuições (FONTANELLA; RICAS; TURATO, 2008).

Nesse sentido, a amostra intencional foi definida por critérios de proximidade da pesquisadora com especialistas em segurança da informação. Nessa perspectiva, com a pesquisa exploratória, que correspondeu a fase de pré-teste da pesquisa, foi possível afinar as informações, e formulação de conhecimentos, por intermédio da amostra intencional, que alicerçaram a construção do questionário a fim de se adequar a realidade das ações de segurança da informação aplicada às IFES.

A pesquisa descritiva foi fundamentada no sistema de amostra aleatória ou probabilística, por conglomerado. (COOPER; SCHINDLER, 2016, p. 654; LAVILLE; DIONE, 1999, p. 169). Nessa condição, a escolha da amostra justificou-se por oferecer oportunidades iguais a todos os gestores responsáveis pela implementação de ações de segurança da informação nos setores de tecnologia das IFES, de modo que contribuíram com o conhecimento da realidade de segurança da informação ao contexto dos setores de tecnologia das IFES com a finalidade de moldar as ações constituintes do modelo simplificado. Assim, a amostra probabilística se referiu à totalidade de gestores responsáveis por ações de segurança da informação dos setores de tecnologia das IFES, totalizando 102 gestores.

3.3 TÉCNICAS DE COLETA DE DADOS

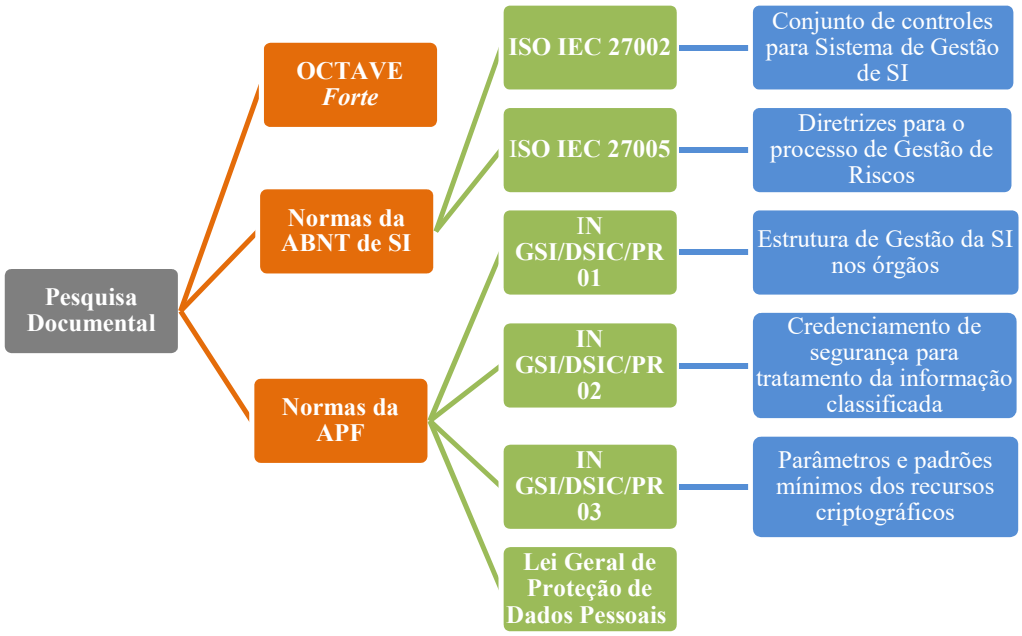
Para o procedimento de coleta de dados, a pesquisa adotou um conjunto de instrumentos específicos necessários, em virtude da interação entre as pesquisas exploratória e descritiva, para poder alcançar os objetivos propostos pela pesquisa abordada neste projeto. Nesse sentido, para a fase da pesquisa exploratória, foram adotados o procedimento de pesquisa documental e a técnica de pré-teste, e, para a fase da pesquisa descritiva, foi adotada a técnica de questionário. Ressaltamos que o questionário cumpriu todas as orientações do Ofício Circular 2/2021/CONEP/SECNS/MS, de 24 de fevereiro de 2021, que descreve os procedimentos em pesquisas com qualquer etapa em ambiente virtual.

3.3.1 Pesquisa Documental

Presente na fase da pesquisa exploratória, o procedimento da pesquisa documental estabelecido permitiu obter os documentos específicos relacionados à segurança da informação, conforme determinado nos objetivos específicos do estudo. No que concerne a esse procedimento, Carvalho (1989, p. 154) observa que a pesquisa documental se vale de documentos cientificamente autênticos, não fraudados, de amplo uso nas ciências sociais e humanas, devido à possibilidade de efetuar análises qualitativas do fenômeno pesquisado.

De acordo com Gil (2012, p. 51), apesar da semelhança com a pesquisa bibliográfica, a diferença entre ambas encontra-se na natureza das fontes, pois, enquanto a pesquisa bibliográfica baseia-se nas contribuições de diversos autores sobre um assunto específico, a pesquisa documental faz uso de materiais que não receberam tratamento analítico por completo, podendo ser reelaborados de acordo com os objetivos da pesquisa. Com isso, foi definida a estrutura da pesquisa documental na Figura 14.

Figura 14- Estrutura da pesquisa documental



Fonte: Elaborado pela autora (2022).

Foram analisados neste estudo os documentos identificados na Figura 14, colaborando com o processo de desenvolvimento dos elementos conceituais necessários ao modelo

integrado e simplificado de ações de segurança para análise de riscos de segurança da informação.

3.3.2 Questionário

O questionário, Apêndice B, foi escolhido por ser um instrumento que permite descrever características e medir variáveis de um grupo social (RICHARDSON, 2015, p. 189).

De acordo com Marconi e Lakatos (2003, p. 201–202), existem vantagens no uso da técnica de questionário, como: atingir grande número de pessoas simultaneamente (o estudo pretendeu alcanças os responsáveis pela SI dos setores de tecnologia das 102 IFES), possibilidade de abranger uma extensa área geográfica (abrangendo as Instituições Federais de Ensino Superior em âmbito nacional), não expõe o entrevistado à influência do pesquisador (os respondentes ficaram livres de contato pelo pesquisador o que poderia levar à indução direta ou indireta do pesquisado).

Nessa perspectiva, entende-se que a utilização da técnica do questionário foi importante para a pesquisa proposta no tocante à conhecer a realidade das IFES quanto às ações, de processo e operacionais, de segurança da informação, no intuito de afinar o modelo proposto baseado nessa realidade. O questionário foi on-line e enviado aos responsáveis pela segurança da informação dos setores de tecnologia das IFES

A técnica de pré-teste consiste na aplicação de questionário em sua versão preliminar, fundamental para garantir uma fácil compreensão das questões pelo público-alvo. O questionário se deu preliminarmente, em fase de pré-teste, onde 6 (seis) especialistas em segurança da informação foram consultados com o intuito de afinar as questões ao público-alvo do questionário: responsáveis pela segurança da informação dos setores de tecnologia das 102 IFES.

Após a moldagem do questionário feita com a aplicação do pré-teste, a aplicação se deu de forma on-line, com e-mails enviados indistintamente a gestores de governança, de segurança da informação, de riscos e de tecnologia da informação, possuindo o Termo de Consentimento Livre e Esclarecido estabelecido no cabeçalho do questionário, conforme Apêndice B.

No momento de envio do questionário foi fornecido e-mail e telefone para dúvidas, esclarecimentos e sugestões sobre a pesquisa. Alguns gestores entraram em contato com a pesquisadora a fim de saber se estariam expondo suas instituições, ocasião em que foi

esclarecido o nível de sigilo a ser publicado nesta tese, também pediram que fosse enviada uma cópia do resultado da pesquisa.

O questionário, composto por 50 perguntas, organizadas por constructos, baseadas nas informações e conhecimentos gerados no processo de pesquisa exploratória, com base na pesquisa, colaborou com o desenvolvimento do modelo integrado e simplificado de ações de segurança proposto, por intermédio das formulações dos constructos e variáveis da pesquisa.

O procedimento de coleta de dados na pesquisa exploratória, com a técnica do questionário, foi dividido em duas etapas. A primeira consistiu na fase do levantamento, onde foram realizados os primeiros contatos com as instituições (sensibilização quanto ao objetivo e importância da pesquisa) e o levantamento dos responsáveis envolvidos com a segurança da informação dos setores de tecnologia das IFES, com seus respectivos e-mails de contato e telefones. Na segunda etapa, fase da concretização, ocorreu o envio de um e-mail com o questionário.

3.3.2.1 Confiabilidade do instrumento de pesquisa

O questionário passou pelo processo de validação interna que evidenciou sua qualidade como instrumento de medição, apoiado nas características essenciais da confiabilidade e validade (HOSS; TEN CATEN, 2010, p. 106–109). Como forma de estimar a confiabilidade dos dados coletados relativos à realidade das IFES que permitiram afinar o modelo, foi utilizado o coeficiente α (alfa) de Cronbach, desenvolvido em 1951 por Lee J. Cronbach, que permite avaliar o grau de consistência entre múltiplas medidas de uma variável (HAIR *et al.*, 2005).

O coeficiente foi calculado por constructo do questionário. Dado que a maioria dos itens do questionário utilizou a mesma escala de medição, escala de Likert, foi possível utilizar o coeficiente α de Cronbach, com α entre 0 e 1, calculado a partir da variância dos itens individuais e das covariâncias entre eles. Com valor mínimo aceitável para confiabilidade em torno de 0,70, pois a consistência é considerada baixa com valores abaixo desse limite (STREINER, 2003; HAIR et al., 2005; GASPAR, SHIMOYA, 2017).

Segundo Tavakol e Dennick (2011, p. 54, tradução nossa), “o alfa deve ser calculado para cada um dos construtos e não para o teste ou escala inteiro”. A Tabela 3, então, apresenta o valor dos alfas de Cronbach para os quatro constructos do modelo.

Tabela 1 – Confiabilidade do instrumento de pesquisa por α de Cronbach

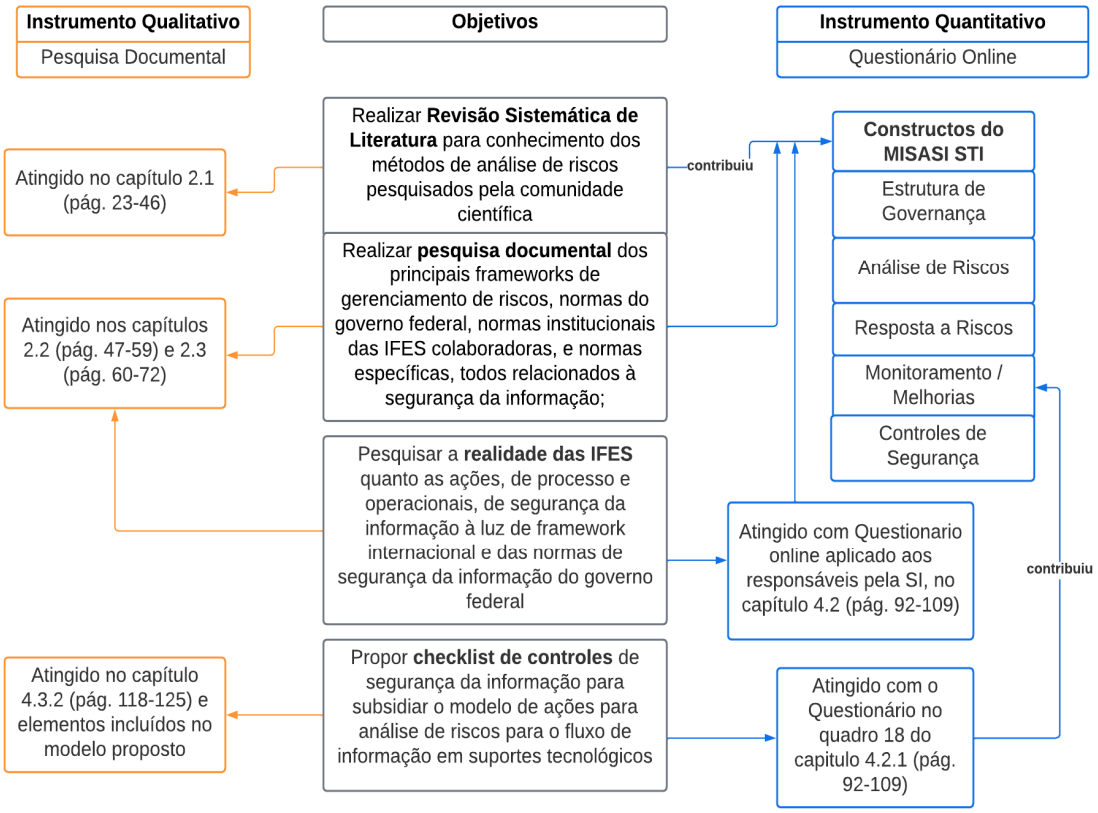
Constructos	Coeficiente Alfa De Cronbach
Estrutura de Governo	0,883
Analise de Risco	0,914
Resposta a risco	0,864
Monitoramento/Melhorias	0,678

Fonte: Dados da pesquisa (2022).

Como podem ser observados na Tabela 3, os constructos do questionário alcançaram, em geral, satisfatória consistência interna, com o valor dos alfas acima do mínimo sugerido. No capítulo seguinte será feita a análise dos resultados.

A Figura 15 demonstra as técnicas de coletas de dados em relação aos objetivos específicos para melhor visualização.

Figura 15 - Relação dos objetivos específicos com as técnicas de coleta de dados



Fonte: Elaborado pela autora (2022).

Os constructos quantitativos serviram de base para delinear o modelo, a partir dos quais foi possível realizar medições estatísticas acerca da realidade das IFES.

3.4 PROCEDIMENTOS DE ANÁLISE DOS DADOS

De acordo com as necessidades metodológicas deste estudo, os procedimentos de análise dos dados foram estabelecidos segundo observâncias das pesquisas, exploratória e descritiva. Conforme a primeira parte do estudo, referente à pesquisa exploratória, os dados obtidos com o procedimento da pesquisa documental e pré-teste, passaram pelo processo de análise de conteúdo, com evidência na análise qualitativa. Quanto à segunda parte, concernente à pesquisa descritiva, os dados foram coletados por meio da técnica de questionários, passaram pela análise estatística de dados quantitativos e qualitativos.

Segundo Bardin (2010, p. 37), a análise de conteúdo corresponde a um conjunto de técnicas de análise de comunicações que, por meio de procedimentos sistemáticos e objetivos de descrição, procura examinar em conteúdo de mensagens, indicadores que possibilitam estabelecer inferência de conhecimento relacionado às condições de produção/recepção das mensagens. Ou seja, entende-se que o método de análise de conteúdo procura obter, com base nos indicadores, inferências a partir da análise da ausência ou presença de características determinantes nos textos analisados.

Na análise de conteúdo, a ação de produzir inferência significa, entre diversas concepções, embasar determinada mensagem com pressupostos teóricos e com situações concretas que visualizam o contexto da produção e recepção das mensagens (CAMPOS, 2004, p. 613). Conforme sua natureza científica, a análise de conteúdo permite a compreensão das mensagens, de forma a se aprofundar em suas características e destacar os aspectos mais importantes fundamentado em teorias consistentes que possam servir de explicação para os questionamentos de pesquisas (LAVILLE; DIONNE, 1999; RICHARDSON, 2015).

Nessa perspectiva, em concordância com Laville e Dione (1999) e Richardson (2015) em relação à análise de conteúdo, a parte referente à análise dos dados que serão obtidos ao longo da pesquisa exploratória, prosseguirá por três etapas específicas: pré-análise, análise do material e tratamento dos resultados, inferência e interpretação.

Na fase de pré-análise, que tem por objetivo operacionalizar e sistematizar as ideias, ocorreu o processo de organização de todo o material obtido que compreendeu desde a Revisão Sistemática de Literatura, contribuindo para a escolha do framework OCTAVE *Forte,* até a pesquisa documental, com os documentos específicos alusivos à segurança da

informação, desde normas internacionais às normas federais de segurança da informação para as IFES –colaboraram com o desenvolvimento do modelo de análise de riscos. Esses documentos passaram por classificação de acordo com suas particularidades e aplicação.

Na fase relativa à análise do material, pesquisa documental e pré-teste foram feitos e permitiram a categorização em constructos para o modelo integrado e simplificado de ações de segurança da informação para os setores de tecnologia das IFES (MISASI STI), com base nos parâmetros teóricos da pesquisa. Os constructos possuem relação direta com a hipótese da pesquisa, sendo eles: qualitativos, framework de riscos, normas de segurança, controles; quantitativos, estrutura de governança, análise de riscos, resposta a riscos, e monitoramento/melhorias. Com isso, foi possível obter as ações relacionadas aos constructos e variáveis, necessárias para a construção do MISASI STI específico para as ações de segurança da informação em setores de tecnologia das IFES.

3.5 TRATAMENTO DOS DADOS COLETADOS

Conforme explanado acima, foi escolhida amostra intencional para o pré-teste onde seis especialistas em segurança da informação foram consultados de modo a afinar o questionário. Bem como amostra aleatória foi escolhida para aplicação do questionário, por oferecer oportunidades iguais a todos os gestores responsáveis pela implementação e/ou aplicação de ações de segurança da informação nos setores de tecnologia das IFES.

Nesse sentido, foram enviados emails e/ou chamados para 150 contas referentes a gestores ou responsáveis pela SI nas 102 instituições federais de ensino superior, no período de 24 de novembro de 2021 a 29 de março de 2022, em 4 rodadas de envio, totalizando pouco mais de 500 emails enviados. Os emails foram enviados para o email institucional do gestor ou email relativo à função, também foi enviado email para o sistema de chamados da instituição, quando não havia a informação sobre email disposta no site institucional.

Do universo de 102 instituições federais de ensino superior foi possível obter 33 questionários com respostas finalizadas, condição para análise dos dados, porém com total de 101 respondentes, indicando que os gestores acessaram o questionário, começaram a responder, mas não finalizaram, alguns inclusive entraram em contanto afirmando ser um questionário “grande”, porém possuía apenas 50 questões e o tempo médio para completar as questões, analisado na fase de pré-teste, ficou em torno de 18 minutos.

As respostas foram retiradas da ferramenta de criação de formulários SurveyMonkey e transmitidas diretamente para uma base de dados do *Statistical Package for the Social Sciences* (SPSS), versão 22, software utilizado nas análises estatísticas desta tese.

Na maioria das questões, houve a atribuição de valores numéricos à escala de Likert original: 1 para "Nunca", 2 para "Raramente", 3 para "Ocasionalmente", 4 para "Quase sempre" e 5 para "Sempre", outras questões exigiram respostas mais específicas.

A primeira análise realizada, que levou em consideração a completude e integridade das respostas, sem divisão ou distinção de constructos, identificou que 69 respondentes, em torno de 68,31%, não finalizaram seus questionários, os respondentes não ultrapassaram a segunda metade do questionário, conforme pode ser visto no Apêndice B, não responderam além do constructo Análise de Riscos, logo as respostas não foram contabilizadas para análise dos dados.

Considerando o total de respostas completas e válidas, o perfil dos respondentes foi identificado por região, com respectiva taxa de respostas, na Tabela 1. Observou-se que as regiões que, proporcionalmente ao quantitativo de instituições, mais responderam foram a Norte e Nordeste, seguidas de Sul, Sudeste e Centro-oeste respectivamente.

Tabela 2 – Perfil dos respondentes por região

Região	**Total de Instituições**	**Taxa de resposta por região**
Norte	17	41%
Nordeste	28	36%
Centro-oeste	12	17%
Sudeste	28	25%
Sul	17	35%
	102	32,35%

Fonte: Dados da pesquisa (2022)

Também foi mapeado o perfil do respondente dentro da instituição, função exercida, dados dispostos na Tabela 2, tendo a maioria dos respondentes função de diretor de TI ou de Segurança da Informação. Vale à pena observar que, inicialmente, os emails foram enviados apenas aos gestores de SI e diretores de TI quando inexistentes os primeiros, mas como a taxa de resposta estava muito pequena, foi ampliado para área de governança e de redes, sistemas ou infraestrutura dentro do setor de tecnologia.

Tabela 3 – Perfil dos respondentes por função

Função	Respondentes	Porcentagem
Diretor ou gestor de TI	10	31,25
Gestor de Riscos ou SI	10	31,25
Área de Governança	4	12,5
Área de Redes, Sistemas ou Infraestrutura	9	28,125

Fonte: Dados da pesquisa (2022)

Como visto, apesar de 101 das 102 instituições terem começado a responder ao questionário, e 68,31% dos respondentes não terem finalizado o questionário, o perfil dos respondentes é de pessoas especializadas, conhecedoras das ações de Segurança da Informação, abrangendo todas as regiões do Brasil, que forneceram informações válidas sobre a realidade de suas instituições respectivas.

4 ANÁLISE DOS RESULTADOS

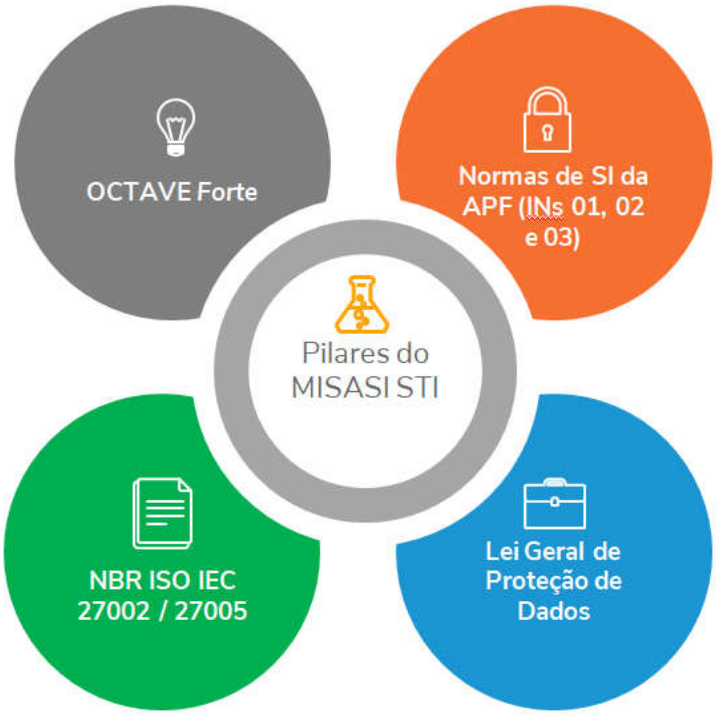
Partindo da combinação entre as técnicas pesquisa documental e questionário, com o propósito de construção do modelo integrado simplificado de ações de segurança da informação para setores de tecNologias das IFES (MISASI STI), esta seção apresenta o processo de definição do modelo, seus componentes, e os resultados obtidos com a pesquisa da realidade das IFES.

4.1 VISÃO GERAL DO MODELO MISASI STI

O modelo consiste em um conjunto de ações de segurança da informação vindas das normas nacionais e framework internacional. O modelo permitiu identificar ações próprias de segurança da informação, a serem estabelecidas no contexto dos setores de tecnologia das IFES, de implementação independente de papéis, podendo ser implementadas, preferencialmente, por gestores de riscos institucionais ou gerentes de segurança da informação, ou de implementação específica de gerentes de sistemas, redes, bases de dados, suporte e outros responsáveis pela segurança da informação em setores de tecnologia das IFES, de acordo com a realidade de cada instituição.

Na revisão sistemática de literatura feita, observaram-se estudos de métodos de análise de risco orientados a ameaças, vulnerabilidade, controles ou ativos, como os estudos de Nurse, Creese e de Roure (2017), Al-safwani, Fazea e Ibrahim (2018) e os de Bharat e Prasad (2016). O MISASI STI foi construído orientado a ações de segurança da informação aplicáveis aos setores de tecnologia, elaboradas para mitigar ameaças, de origem natural, humana, tecnológica ou ambiental, que possam afetar as propriedades básicas de segurança da informação (confidencialidade, integridade e disponibilidade). Nesse cenário, a figura 16 traz os pilares do modelo.

Figura 16- Pilares do modelo



Fonte: Elaborado pela autora (2022).

Observa-se que esses pilares foram escolhidos alinhados com o referencial teórico e permitiram construir a arquitetura do modelo, disposta na figura 17, que, como evidenciado na metodologia, possui a estrutura do processo de gerenciamento de riscos adaptada do *framework* reconhecido internacionalmente OCTAVE *Forte* e seus componentes consistem nas ações de segurança. A arquitetura permite identificar as ações de SI a serem estabelecidas no contexto dos Setores de Tecnologia das IFES, tendo como público-alvo: Gestores de riscos, de SI, de Governança, gerentes de sistemas, redes, bases de dados e outros responsáveis pela SI

Figura 17 - Arquitetura do MISASI STI

<table>
<tr><th colspan="6">Matriz do Modelo de Ações de Segurança da Informação</th></tr>
<tr><td>Etapas</td><td>Ações de Governança (Passos 1,2,3 e 4 do FORTE) CONTEXTO</td><td>Ações de Análise de Riscos (Passo 5 e 6 do FORTE)</td><td>Ações de Resposta aos Riscos (Passos 7 e 8 do FORTE)</td><td>Ações de Monitoramento e Melhorias do</td><td>Checklist de Controles de SI</td></tr>
<tr><td>Meta</td><td>Compreender Estrutura de Governança, Ativos e Capacidades, formular e documentar olerância a risco, documentando , tudo em consonância com os objetivos Institucionais.</td><td>GR reconhecida como vantagem, com processo estabelecido e alinhado à estrutura de governança, riscos analisados em relação às capacidades atuais e proteção de dados pessoais</td><td>Até aqui, a organização se concentrou em identificar riscos, vulnerabilidades e ameaças a seus ativos e serviços críticos e formou planos de resposta aos riscos identificados.</td><td>Avaliação de todo o programa de gerenciamento de risco</td><td>Ações de segurança possíveis dispostas em um checklist de controles</td></tr>
<tr><td rowspan="3">Passos Finais</td><td>3.3 Capacidades correntes medidas</td><td rowspan="3">3.4 Mapeamento de riscos</td><td rowspan="3">3.5 Equipe de Tratamento e Resposta a Incidentes</td><td rowspan="3">3.6 Comunicações</td><td rowspan="3">Controles tecnológicos (Redes, Sistemas, Base de Dados)</td></tr>
<tr><td>3.2 Requisitos de continuidade dos ativos identificados (GCN)</td></tr>
<tr><td>3.1 Ativos e Serviços críticos identificados e Classificação da Informação estabelecida</td></tr>
<tr><td rowspan="2">Passos Intermediários</td><td>2.2 Tolerância a Risco estabelecida</td><td>2.4 Analisar riscos em relação à Proteção de Dados Pessoais</td><td rowspan="2">2.5 Gestão da Continuidade do Negócio - GCN</td><td rowspan="2">2.6 Gestão de Mudanças</td><td rowspan="2">Controles Ambientais</td></tr>
<tr><td>2.1 Política de Gestão de Riscos</td><td>2.3 Analisar riscos em relação às capacidades atuais.</td></tr>
<tr><td rowspan="2">Passos Iniciais</td><td>1.2 Cultura/Conscientização em SI</td><td rowspan="2">1.2 Componentes da Análise de Riscos (lista de riscos, ameaças e vulnerabilidades por ativo)</td><td rowspan="2">1.3 Plano de Resposta</td><td>1.5 Revisar, atualizar e repetir</td><td rowspan="2">Controles Sociais (Conscientização e treinamento, Gestão de uso dos recursos)</td></tr>
<tr><td>1.1 Estrutura de governança em SI</td><td>1.4 Monitorar e medir a eficácia</td></tr>
<tr><td>Passo 0 – Ad Hoc</td><td colspan="5">Ad hoc não estruturada; NENHUMA ABORDAGEM FORMAL DE ESTRUTURAÇÃO DO PROCESSO DE ANÁLISE DE RISCOS, AÇÕES EM SI DEPENDEM DE HABILIDADES ESPECÍFICAS DE GERENTES, AUSÊNCIA DE PRÁTICAS ESSENCIAIS</td></tr>
</table>

Fonte: Dados da pesquisa (2022).

A arquitetura do modelo foi elaborada em forma de matriz para melhor evidenciar as metas de cada etapa do modelo integrado e simplificado de gerenciamento de riscos, os passos necessários para que a meta seja atingida, e, para completar o processo, o modelo trouxe *checklists* de controles de segurança categorizados por dimensões sociais, ambientais e tecnológicas.

O modelo parte do pressuposto que, para que as ações de segurança da informação sejam eficazes, o processo de gerenciamento de riscos parta de uma estratégia *top-down*, iniciando por ações de governança, políticas e estratégias organizacionais de risco, necessidade essa evidenciada pelo OCTAVE Forte. No entanto, as normas de segurança e a revisão sistemática de literatura evidenciaram a necessidade de implementação de controles *bottom-up*, fazendo-se necessário que os setores de tecnologia das IFES implementem os controles em suas dimensões sociais, ambientais e tecnológicas, de acordo com suas

possibilidades e, sempre que possível, alinhados às estratégias organizacionais, porém não totalmente dependentes delas.

Ou seja, uma IFES pode não ter estratégia de governança ou políticas de segurança totalmente estabelecidas, o que não impede seus setores de tecnologia respectivos de terem processos definidos com controles sociais, tecnológicos e ambientais e de infraestrutura. Porém, sempre que a estratégia organizacional é definida, os controles dos setores de tecnologia devem estar alinhados às demandas institucionais de segurança. Essa premissa possibilita a existência de ações mesmo na ausência normativa institucional.

Considerando a idéia inicial da tese, explicitada na introdução, que questionou quanto às ações necessárias para manter a segurança da informação contínua nos setores de tecnologia das IFES, o modelo construído trouxe essas ações evidenciando que, apesar de a análise de riscos ser a pedra angular das ações de segurança da informação nessas instituições, para manter a continuidade da segurança da informação, faz-se necessário adotar um modelo de segurança com ações que permitam um processo cíclico contínuo de segurança da informação. Porém, como todo modelo a ser adotado, precisa ser mantido e atualizado continuamente, pois tanto a realidade das instituições muda, bem como as normas e as ações de segurança necessárias. Logo, para uma melhor visualização da dinâmica do modelo, a Figura 18 mostra como seus elementos se encaixam nessa idéia de continuidade e atualização:

Figura 18 - Dinâmica do MISASI STI

Fonte: Elaborado pela autora (2022).

Tendo o aspecto cíclico de continuidade como premissa do modelo e sua arquitetura estabelecida, houve a necessidade de afinar o modelo à realidade das IFES, análise essa feita por meio de estudo de caso aplicado na forma de questionário.

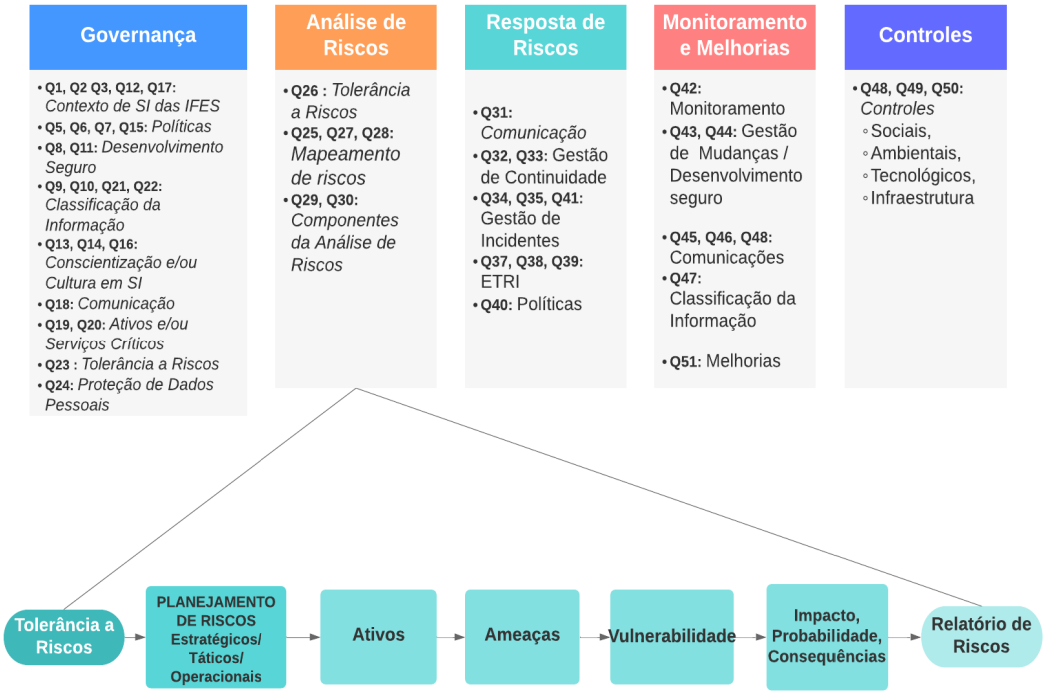
4.2 QUESTIONÁRIO

De posse do modelo, sua arquitetura e dinâmica, os gestores dos Setores de Tecnologia das IFES podem criar estruturas para manter ações contínuas de segurança da informação e moldá-las às suas realidades. De forma a conhecer a realidade das IFES quanto a essa estrutura proposta, e, também, retroalimentar o modelo para essa realidade, foi elaborado um questionário para conhecimento das ações de segurança da informação nas diferentes regiões do Brasil, enviado para as 102 IFES existentes.

O modelo MISASI STI permitiu elaborar um questionário semi-estruturado, Apêndice B, para mensurar, de forma integrada e simplificada, o quão perto de uma realidade em segurança da informação as IFES se encontram, e, ao mesmo tempo, o questionário permitiu retroalimentar o modelo de forma a afiná-lo com a realidade dessas instituições.

Os constructos e as variáveis trabalhadas no questionário, conforme podem ser vistos na figura 19, advém do modelo, que, por sua vez, foram trazidos das normas e do *framework* internacional OCTAVE Forte.

Figura 19 - Constructos e variáveis do questionário com detalhamento do pilar do modelo



Fonte: Elaborado pela autora (2022).

Além dos constructos e variáveis do questionário, retirados do modelo, a Figura 19 mostra detalhes dos componentes da análise de riscos, corroborando a Figura 14, seção 3.1, que trouxe o esboço da análise de riscos à luz das normas de SI da APF, sendo possível visualizar a diferença de granularidade trazida pelo modelo à luz das normas, realidade essa inerente ao fato de ser modelo. Dessa forma, podem-se visualizadas as etapas que se fazem necessárias às ações centrais de segurança da informação, segundo o modelo MISASI STI, e sua posição em relação aos constructos e variáveis. Ou seja, as variáveis trabalharam em cima de todo o processo de gerenciamento de riscos, abrangendo, mas não se limitando, a análise de riscos.

Por ser um modelo integrado e simplificado, fez-se necessário que o questionário acompanhasse e abordasse os constructos e variáveis desse modelo, sem entrar em detalhes, conforme explanado anteriormente, identificando as ações de segurança da informação existentes no processo de gerenciamento de riscos das IFES, mas não detalhando as ações específicas, pois ficaria demasiadamente cansativo aos respondentes e desfiguraria o propósito do modelo.

Antes da aplicação do questionário nas IFES do Brasil foi feito, conforme mencionado na seção 3.4.2, pré-teste do questionário com 6 (seis) especialistas em segurança da

informação e/ou tecnologia da informação, no intuito de melhorar o questionário e afinar o modelo, que foi de válida contribuição para melhorias, desde disposição das questões, contribuições para agrupar as questões na ordem de apresentar primeiro as que possuem escala de Likert e, posteriormente, as questões em outro formato, por exemplo; duplicidade de questões; bem como melhoria dos termos utilizados, pois alguns termos apesar de utilizados internacionalmente ficam estranhos e fora da cultura em segurança da informação no Brasil, como o termo "apetite a risco" que possui tradução mais comum para "tolerância a risco", dentre outras excelentes contribuições que afetaram não apenas o questionário como o modelo em si.

Quanto ao questionário, foram mapeadas questões referentes às ações de segurança da informação necessárias para essas instituições, considerando-se que para a não identificação dos respondentes, conforme a necessidade, essa identificação foi realizada por região do Brasil, uma vez que, nenhum gestor de segurança da informação tem o interesse de divulgar suas ações de segurança específicas, o que poderia mostrar a vulnerabilidade institucional. Sendo esse, também, um dos pontos de dificuldades da pesquisa em obter respostas aos questionários.

4.2.1 Análise descritiva dos dados coletados por constructos

As medidas estatísticas utilizadas na análise descritiva consistiram em: média aritmética, desvio-padrão e porcentagem cumulativa, consistindo em distribuições de posição, dispersão e frequência, respectivamente. A média aritmética corresponde à totalidade das respostas dividida pelo número total de respondentes, ou seja, consiste em uma medida de posição.

Segundo Crespo (2009), para qualificar os valores de uma variável, destacando a maior ou a menor variabilidade entre esses valores e a sua medida de posição, recorre-se às medidas de dispersão. Logo, o desvio-padrão foi utilizado para mostrar o grau de dispersão dos dados, ou seja, ou quão distantes encontram-se em relação à média.

As Tabelas 4, 5, 6, 7, referenciadas por constructo, dispostas a seguir, exibem a média aritmética, desvio-padrão e porcentagem acumulativa das respectivas questões, seguindo a numeração apresentada no questionário.

Considerando que a estrutura de governança permite à instituição saber por onde começar para estabelecer ações de segurança da informação direcionadas para seu gerenciamento de riscos, observa-se, na Tabela 4, que o constructo Estrutura de Governança

obteve baixos valores de média para as questões 5, 6 e 7, indicando não haver alinhamento entre a gestão de riscos e/ou segurança da informação e o planejamento estratégico da instituição, por meio da missão e objetivos estabelecidos no PDI, além de haver políticas desatualizadas cujo cumprimento, em geral, não é exigido.

Tabela 4 – Média, desvio padrão e porcentagem acumulativa para o constructo Estrutura de Governança

Questões	Média	Desvio padrão	Porcentagem acumulativa % (Nunca, Raramente, Ocasionalmente, Quase Sempre, Sempre)				
5 Há alinhamento entre a gestão de riscos e/ou gestão de segurança da informação e a missão e objetivos estratégicos da instituição presentes no PDI.	2,55	1,402	26,3	39,5	73,7	94,7	100
6 As políticas de segurança da informação são revisadas.	2,61	1,223	24,2	45,5	75,8	93,9	100
7 A sua instituição difunde e exige o cumprimento da política de segurança da informação, das normas de segurança e da legislação vigente acerca do tema.	2,73	1,206	21,2	42,4	66,7	97,0	100
8 Quando há demanda de atualização tecnológica, os setores de tecnologia fazem acompanhamento para estudos de novas tecnologias quanto a possíveis impactos na segurança da informação.	3,18	1,236	9,1	30,3	60,6	81,8	100
9 A correta manipulação de informações, classificadas como Sigilosa, Pessoal ou Ostensiva, é difundida e exigida na sua instituição.	3,03	1,212	15,2	30,3	60,6	90,9	100
10 O setor de tecnologia verifica se a informação por ele produzida, recebida ou custodiada se enquadra em quaisquer hipóteses de sigilo, a fim de adotar as medidas de segurança cabíveis quanto ao tratamento de informação. (Ex: Observância da não divulgação de dados de informação sigilosa a terceiros)	3,24	1,300	15,2	27,3	48,5	84,8	100

11 Os sistemas de informação estruturantes da Universidade possuem seu desenvolvimento e manutenção regidos pela política de segurança ou por normativo específico que disciplinam seu uso, controles e perfis de acesso.	3,09	1,466	21,2	33,3	60,6	75,8	100

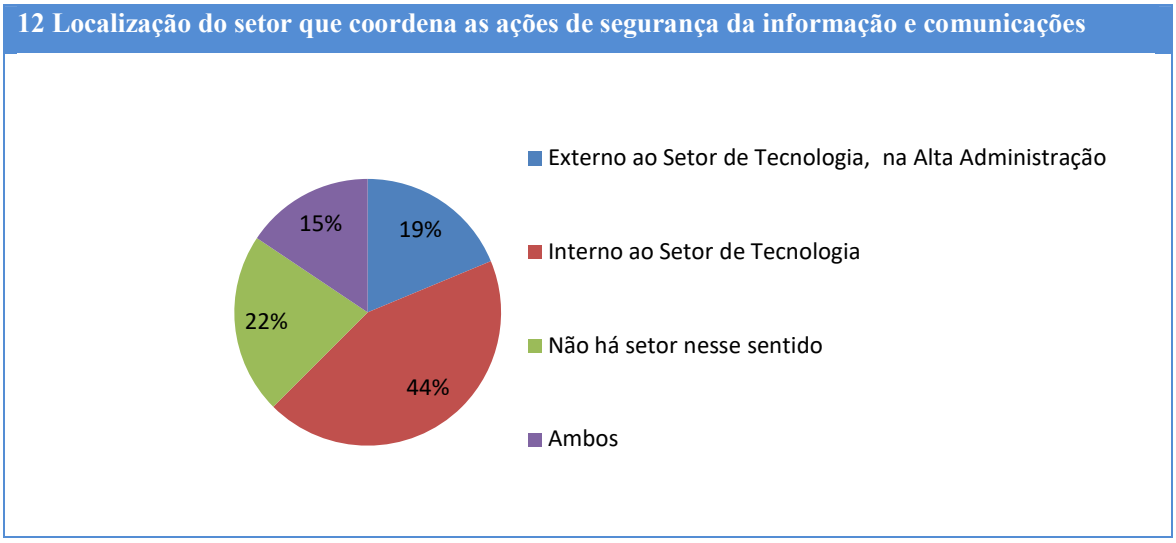
Fonte: Dados da pesquisa (2022).

Evidenciando, na Tabela 4, a necessidade de comprometimento da alta administração com ações promotoras de SI, como as ações elencadas no capítulo 2.2, trazidas da política de segurança nacional, artigo 15, abrangendo desde políticas, capacitações equipes designadas, promoção do adequado tratamento da informação sigilos e estabelecimento de ações corretivas e disciplinares.

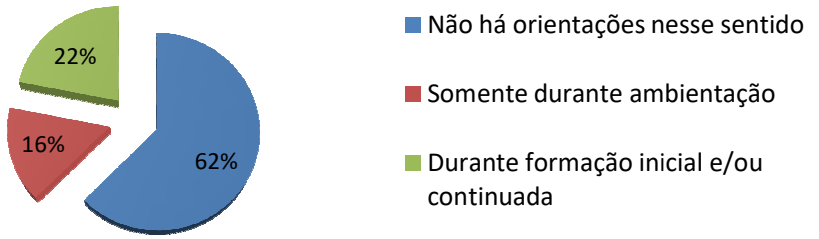
Ainda na tabela 4 pôde-se observar que as questões 8, 9, 10 e 11 obtiveram média acima de 3, indicando, conforme pode ser observado na porcentagem acumulativa, que em torno de 40% dos respondentes afirmaram positivamente com "quase sempre" ou "sempre", logo, possuindo ações de segurança no sentido de difundir a política de classificação, adotarem medidas de segurança para o tratamento da informação sigilosa e possuírem desenvolvimento de sistemas regido por normas de segurança quanto ao uso, perfis e controle de acesso. Todas as questões desse constructo tiveram baixo desvio-padrão, variando de 1,206 a 1,466, sendo que apenas as questões 5 e 11 tiveram desvio-padrão superior a 1,400.

As respostas das questões referentes a esse constructo, não baseadas em escala de likert, foram dispostas na Figura 20.

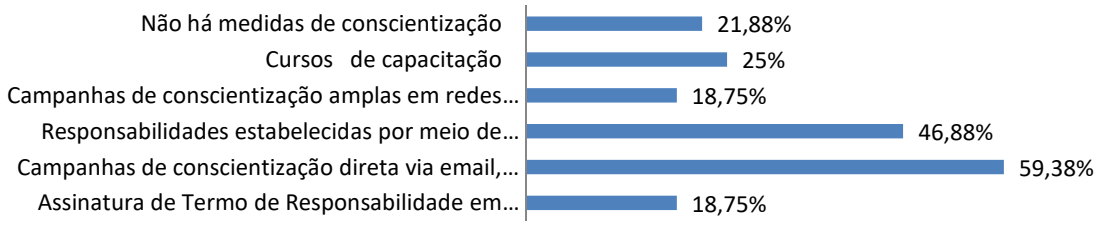
Figura 20 – Respostas amplas para constructo Estrutura de Governança



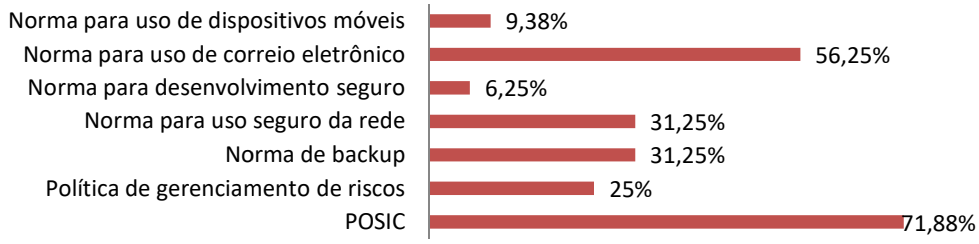
13 Momento das orientações em segurança da informação para servidores e estagiários?



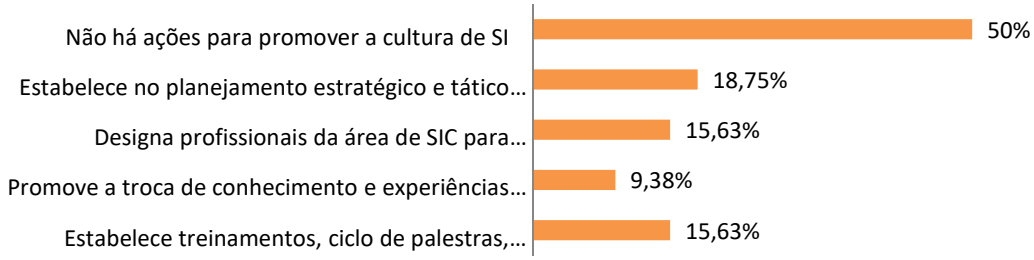
14 Medidas de conscientização em segurança da informação na instituição



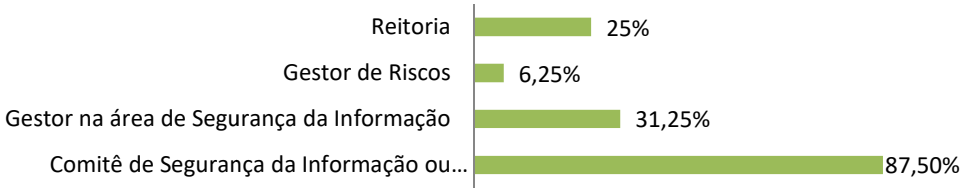
15 Políticas de segurança da informação existentes na instituição?



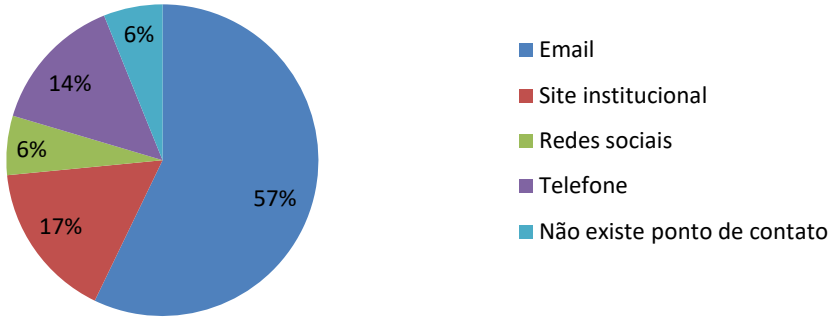
16 Promoção da cultura de segurança da informação e comunicações (SIC) na instituição



17 Quem ou que comissão/comitê toma decisão sobre riscos de SIC



18 Canais de comunicação para averiguar sugestões de melhorias ou denuncias de quebra de segurança pela comunidade acadêmica?



Fonte: Dados da pesquisa (2022).

Nesse quadro, questão 12, é possível observar que 44% dos respondentes afirmaram que os setores que coordenam a segurança da informação estão internos nos setores de tecnologia, enquanto 22% das instituições respondentes não possuem setor nesse sentido. Na questão 13, observa-se que 62% das instituições não possuem orientações em SI para os servidores e estagiários da instituição. Salienta-se que as normas trabalhadas no referencial teórico, capítulo 2.2, indicaram a necessidade dos órgãos ou entidades da APF buscar profissionais de SIC, não necessariamente alocados nos setores de tecnologia, porém com conhecimento multidisciplinar, que sejam capacitados, se possível com as certificações recomendadas pelas próprias normas, e que compartilhem conhecimento com outros profissionais.

Ainda no Quadro 14, observa-se, questão 14, que as medidas de conscientização em sua maioria consistem em campanhas de conscientização via email e responsabilidades estabelecidas por meio de políticas de segurança, com 59,38% e 46,88%, respectivamente.

A questão 15 indicou que 71,88% dos respondentes possuem política de segurança das informações e comunicações (POSIC) e 56,25% possuem normas para uso de correio eletrônico, no entanto, política de gerenciamento de riscos e normas de desenvolvimento seguro são quase inexistentes nos setores de tecnologia das IFES respondentes, contrariando as orientações normativas nesse sentido, como as normas complementares nº 03/IN01/DSIC/GSIPR (2009b) e nº 16/IN01/DSIC/GSIPR (2012c).

A questão 17 mostra que, em geral, a responsabilidade pela SI na instituição é do Comitê de Segurança da Informação ou de Governança da instituição, assinalado por 87,5% dos respondentes e, em menor proporção, apenas 31,25% afirmaram ser responsabilidade também do gestor de segurança e 25% da reitoria.

Com isso evidencia-se a tendência a uma responsabilidade coletiva em grande parte do comitê responsável. Apesar da tendência normativa para haver maior comunicação em SI por redes sociais e site institucional - segundo a Norma Complementar Nº 15/IN01/DSIC/GSIPR (2012b), por exemplo, que afirma serem as redes sociais "uma ferramenta para aproximarem-se ainda mais do cidadão brasileiro e prestar atendimento e serviços públicos de forma mais ágil e transparente".

As questões 16 e 18 mostram que a comunidade acadêmica é afetada tanto pela ausência de cultura em SI, 50% dos respondentes, como pela fraqueza da comunicação em SI que, em geral, se dá por email e mesmo assim os respondentes afirmaram não ser nem um e-mail específico para ações nesse sentido. Fato esse crítico, pois um processo bem definido de comunicação segura com educação relevante, lembretes e cursos de atualização aumentam os sentimentos de responsabilidade e propriedade dos funcionários nas decisões sobre segurança e, levam a uma atitude mais positiva sobre segurança em toda a organização. (HADLINGTON *et al*., 2019).

O constructo Estrutura de Governança - que visa permitir à instituição saber por onde começar para estabelecer ações de segurança da informação direcionadas para seu gerenciamento de riscos- teve os resultados sintetizados na Figura 21.

Figura 21 – Síntese dos resultados para o constructo Estrutura de Governança

Fonte: Elaborado pela autora (2022).

Quanto ao constructo Análise de Riscos, na Tabela 5 podem-se observar os baixos valores da média, valor até 3,00, indicando que mais de 60% dos respondentes marcaram no máximo "ocasionalmente" para ações nesse constructo, assim, apesar de a análise de riscos ser o pilar das ações de SI - conforme visto no referencial, na Revisão Sistemática de

Literatura, capítulo 2.1.1.3, página 39, último parágrafo-, esse constructo não faz parte da realidade dos setores de tecnologia das IFES.

Tabela 5 – Média, desvio padrão e porcentagem acumulativa para o constructo Análise de Riscos

Questões	Média	Desvio padrão	Porcentagem acumulativa (Nunca, Raramente, Ocasionalmente, Quase Sempre, Sempre)				
19 A instituição registra os principais ativos da instituição em um catálogo de ativos informacionais.	3,00	1,369	21,2	33,3	60,6	84,8	100
20 É possível identificar no catálogo os ativos informacionais críticos que auxiliam nos serviços considerados críticos.	2,82	1,424	24,2	45,5	63,6	84,8	100
21 Os ativos informacionais, quando classificados como sigilosos, possuem procedimentos especiais de controle de acesso físico/lógico.	3,21	1,341	18,2	27,3	48,5	84,8	100
22 Quanto à devida classificação da informação, a instituição estabelece rótulos relativos ao proprietário/custodiante da informação, estabelecendo responsabilidades quando há necessidade de sigilo.	2,67	1,362	27,3	48,5	66,7	90,9	100
25 Sua instituição faz algum tipo de gestão de riscos de segurança da informação.	3,00	1,225	15,2	30,3	66,7	87,9	100
26 Os critérios de aceite dos riscos estão definidos e registrados em documento.	2,82	1,489	27,3	45,5	63,6	81,8	100

Fonte: Dados da pesquisa (2022).

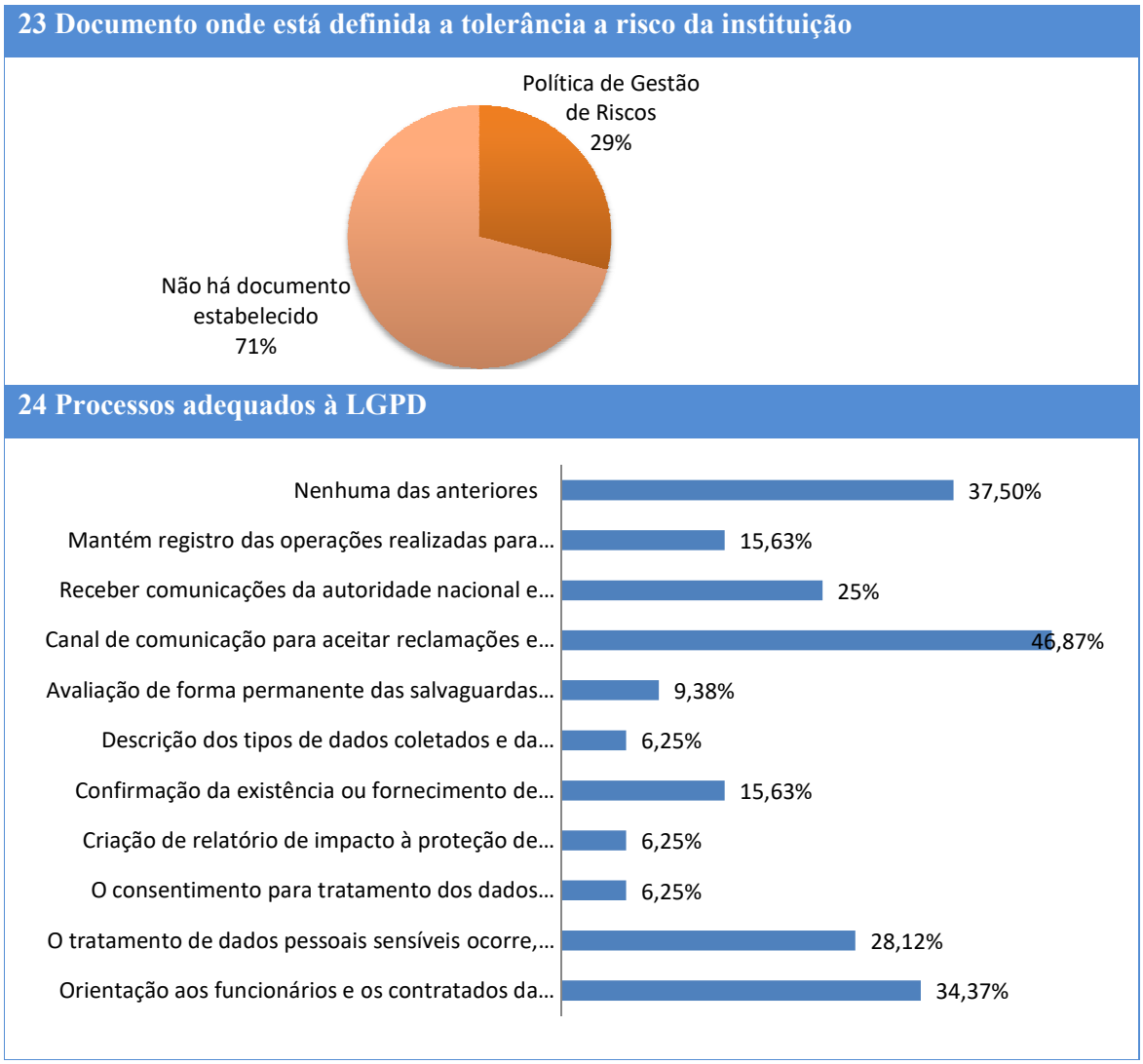
Com exceção da questão 21, que apresentou média 3,21, mostrando haver procedimentos especiais de controle de acesso físico e lógico para ativos classificados, mas se a instituição não cataloga seus ativos, classifica a informação ou identifica seus serviços

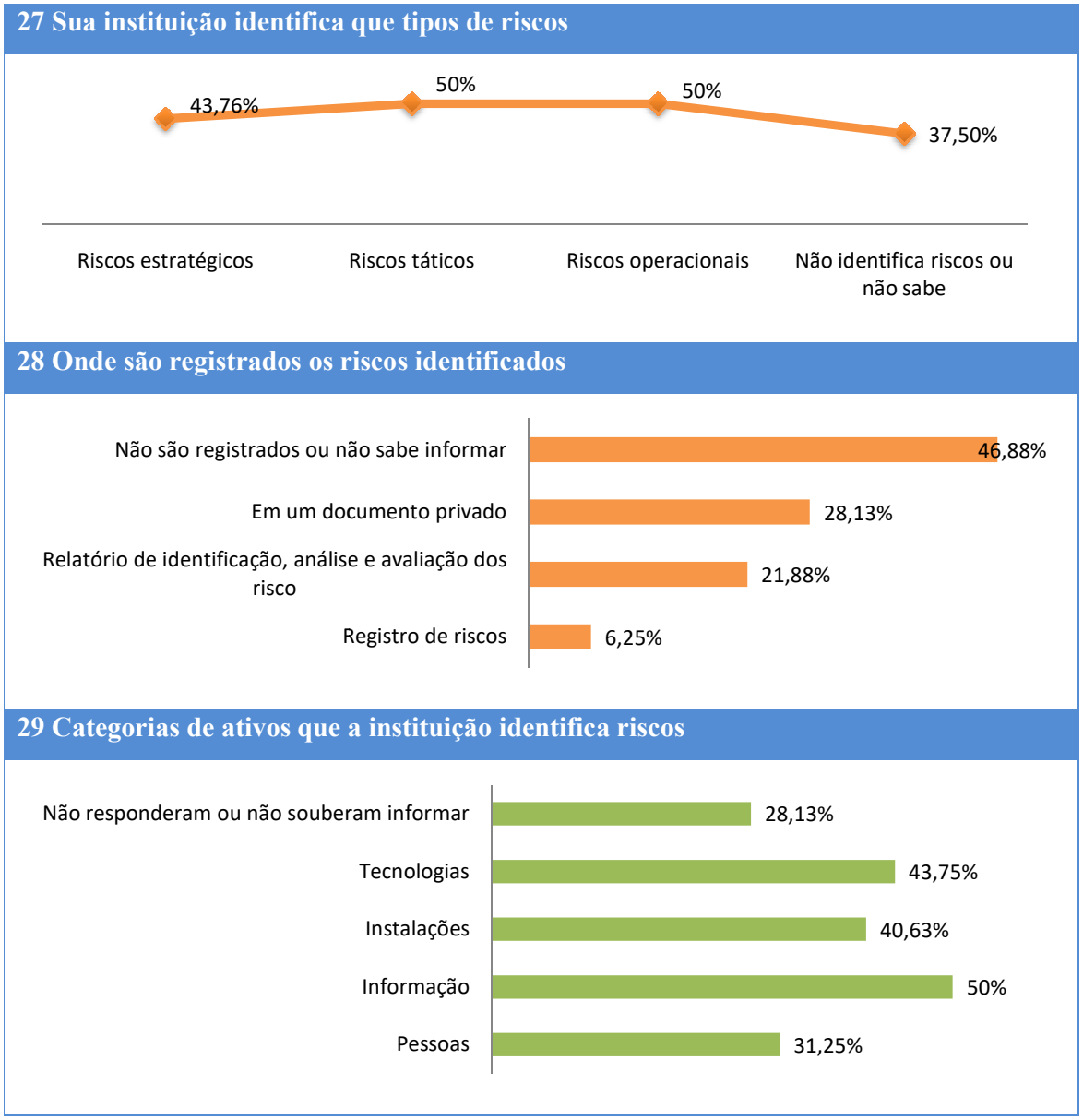
críticos, como identificados nas questões 19, 20, 22, 25 e 26, com média abaixo de 3,00, dificilmente se faz uso dos procedimentos de controle existentes.

Ainda de acordo com a Tabela 5, questão 26, pouquíssimas instituições fazem gestão de riscos, média 3,00, até 66,7% dos respondentes marcaram no máximo "ocasionalmente"; ou não possuem critérios de aceite definidos para os riscos, 63,6% marcaram no máximo "ocasionalmente".

As questões referentes a esse constructo, não baseadas em escala de likert, podem ser vistas na figura 22. Corroborando a análise quantitativa evidencia-se, questão 23, que 71% das instituições não possuem tolerância a risco estabelecida e, em torno de apenas 50% das instituições identificam algum tipo de risco, questão 27.

Figura 22 – Respostas amplas para constructo Análise de Risco





Fonte: Dados da pesquisa (2022).

A questão 28 evidencia que apenas 21,88% das instituições registram riscos, conforme recomendação normativa, em um relatório de identificação, análise e avaliação, observa-se que 28,13% o fazem em um documento privado. Se não há tolerância a riscos estabelecida, como medir o grau de aceite dos riscos, o que indica a falta de planejamento em SI, corroborado pela falta de registro de riscos, logo, em relação às normas de SI, as IFES encontram-se navegando em modo *ad hoc* dentro de um barco repleto de vulnerabilidades em um mar cheio de ameaças.

Na figura 22, os gestores informaram sobre adequação à Lei Geral de Proteção de Dados, questão 24, onde 46,87% dos respondentes instituíram canal de comunicação para

providências relativas à proteção de dados, 34,37% orientam os funcionários a respeito das práticas de tratamento de dados pessoais e 28,12% pedem consentimento do titular dos dados para tratamento dos dados sensíveis, porém apenas 6,25% o pedem por escrito. Essas são as ações predominantes em relação à proteção de dados pessoais e, mesmo assim, não obtiveram nem 50% de respostas positivas, indicando que o assunto encontra-se incipiente ainda nas IFES.

Essa figura 22 é muito esclarecedora quanto a realidades das IFES, para o constructo Análise de Riscos, evidencia-se que no máximo 50% das instituições identificam algum tipo de riscos, questão 27, e da categoria dos ativos que mais se identifica riscos, a categoria pessoas, é a que as instituições menos se preocupam. No entanto, consiste no ponto mais vulnerável da corrente de segurança, logo, na metáfora no mar supracitada, equivale a deixar o capitão e seus tripulantes sem conscientização das necessidades de segurança.

Ainda em relação às questões, uma precisou ser mostrada à parte pela valia da informação coletada, a de número 30, por mostrar os elementos utilizados na análise de riscos das IFES cujas respostas estão dispostas em forma de matriz no quadro 14, com as cores das linhas indicando a região do respondente, a quantidade de elementos utilizada na análise de riscos, última coluna, e a quantidade de instituições que fazem análise de riscos considerando o elemento respectivo, penúltima linha.

Quadro 14– Q30 - Quais categorias abaixo fazem parte da análise de riscos em sua instituição

Cálculo dos Riscos	Ameaças	Vulnerabilidades	Impacto	Probabilidade	Consequências	Qtd.
R	A	V	I	P	C	6
R				P		2
	A	V	I		C	3
	A	V	I			3
R		V			C	3
	A	V				2
	A	V	I			3
	A	V	I	P		4
R	A		I	P		4
R			I	P	C	4
			I	P		2
R	A	V	I	P	C	6
	A	V	I		C	4
R	A	V	I	P	C	6
R	A		I	P	C	5
R	A		I	P		4
R	A		I	P		4

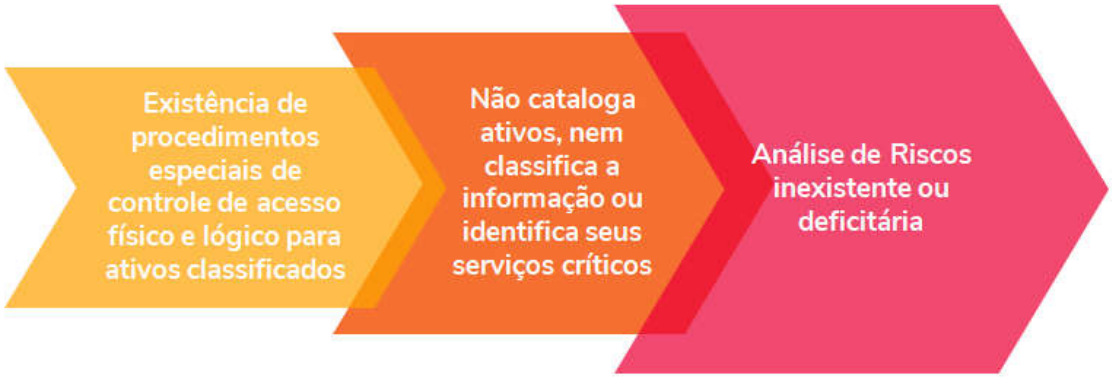
	A	V				2
		V	I		C	3
R	A	V	I	P	C	6
11	15	13	16	12	10	

Fonte: Dados da pesquisa (2022).

Essa matriz indica que 20 instituições fazem análise de riscos com pelo menos uma das categorias de análise de riscos dispostas nas colunas. Apenas 3 (três) instituições fazem cálculo de risco com todos os elementos elencados e uma instituição do nordeste observou ainda que faz análise de riscos com um sétimo elemento: os mecanismos de controle que vão informar como evitar o risco. Uma instituição observou também que a análise de riscos feita em seu setor de tecnologia é relativa apenas a riscos de TI.

O constructo Análise de Riscos - que visa compreender os riscos institucionais ao identificar riscos, ameaças e vulnerabilidades dos ativos - teve os resultados sintetizados na figura 23.

Figura 23 – Síntese dos resultados para o constructo Análise de Riscos



Fonte: Elaborado pela autora (2022).

A Tabela 6 exibe as estatísticas das questões relativas ao constructo Resposta a Riscos, possuindo desvio-padrão entre 1,324 e 1,581, valores considerados baixos como medida de dispersão, em alinhamento com os demais constructos.

Tabela 6 – Média, desvio padrão e porcentagem acumulativa para o constructo Resposta a Riscos

Questões	Média	Desvio padrão	Porcentagem acumulativa (Nunca, Raramente, Ocasionalmente, Quase Sempre, Sempre)				
31 Gerente de risco e/ou segurança da informação são notificados quando um risco se realiza (incidente ocorre)	3,15	1,564	27,3	36,4	42,4	78,8	100
32 A instituição documenta requisitos de continuidade do negócio pelo menos quanto aos ativos críticos.	2,48	1,417	33,3	57,6	72,7	87,9	100
34 Os danos decorrentes de quebras de segurança são investigados e avaliados.	3,58	1,437	9,1	30,3	42,4	60,6	100
35 Quando ocorre casos de quebra de segurança da informação, a instituição aplica ações corretivas e disciplinares.	3,58	1,324	9,1	21,2	45,5	66,7	100
36 O usuário é responsabilizado pela quebra de segurança ocorrida com a utilização de sua respectiva conta de acesso.	2,67	1,339	18,2	57,6	72,7	84,8	100
37 A instituição possui uma equipe para tratamento e resposta a incidentes em redes computacionais (ETRI) que atua quando para reparar os danos e tomar as providências necessárias.	2,94	1,560	30,3	39,4	57,6	78,8	100
38 A ETRI trabalha de forma coordenada com a gestão de segurança da informação.	2,88	1,581	31,3	43,8	59,4	78,1	100

Fonte: Dados da pesquisa (2022).

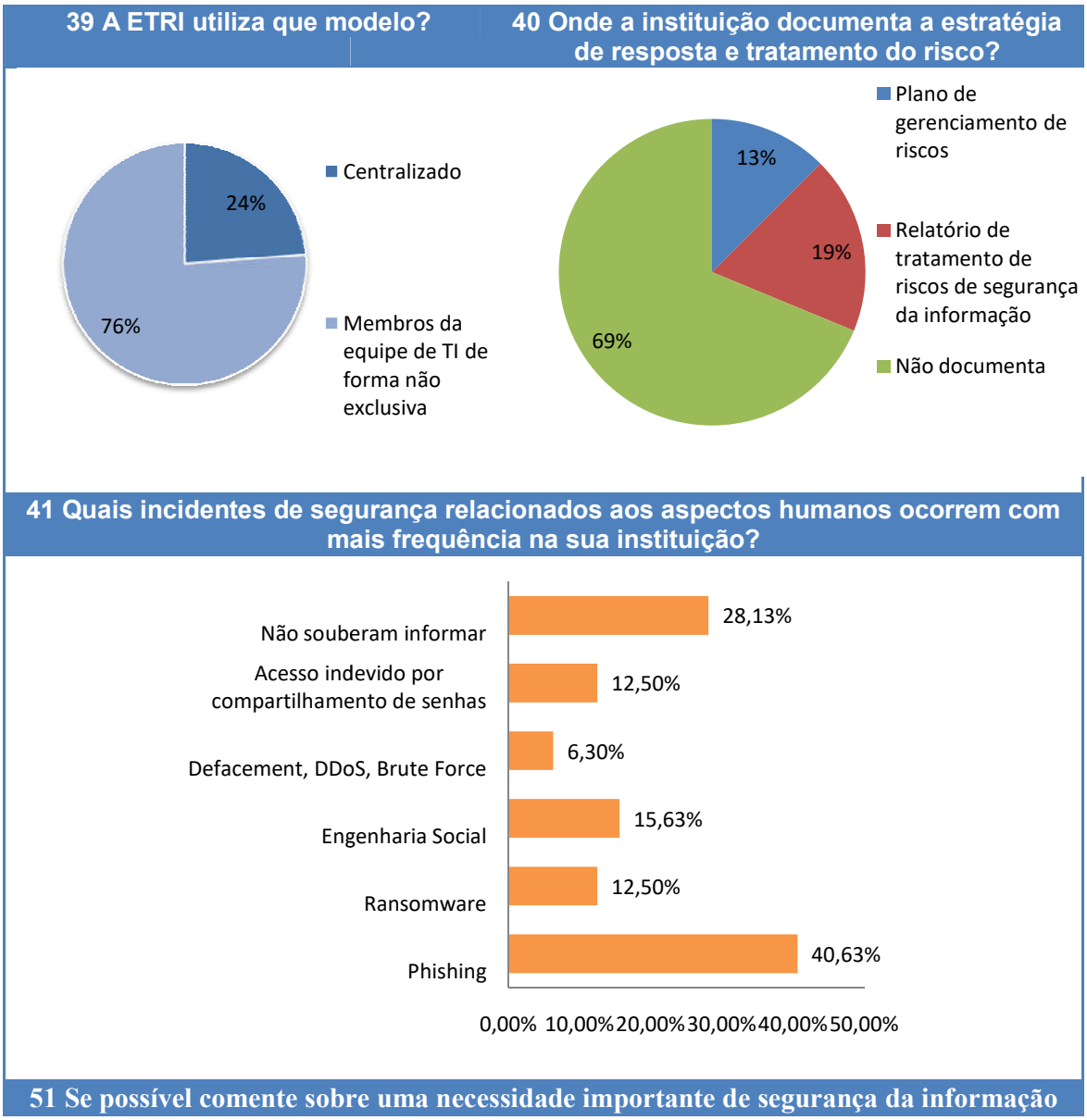
Nessa tabela é possível observar que as questões 32, 36, 37 e 38, possuem média abaixo de 3,00, indicando respostas tendendo para, no máximo, “ocasionalmente”, conforme dito anteriormente, logo, ações envolvendo existência de documentação de requisitos de continuidade, responsabilização pela quebra de segurança, existência e integração de Equipe de Tratamento e Resposta a Incidentes são incipientes nas IFES, indicando que quando da existência de incidentes deve ser um “salve o que puder” dos ativos.

As questões 31, 34, e 35 obtiveram média entre 3,15 e 3,58, indicando que em torno de quase 60% das respostas tenderam para “sempre” ou “quase sempre”, as questões abrangeram notificação dos gestores de risco ou de SI quando um incidente ocorre, sendo possível inferir que esses gestores têm pleno conhecimento dos incidentes que ocorrem em suas instituições e que os danos decorrentes de quebras de segurança são investigados havendo aplicação das medidas corretivas e disciplinares, apesar disso os gestores informaram

no campo “Outro”, que a maioria dos incidentes é investigada, porém como são de ameaças externas, a instituição pouco pode fazer.

As questões, referentes ao constructo Resposta a Riscos, dispostas na Figura 24, identificaram que, das IFES que possuem ETRI, apenas 24% trabalham com modelo centralizado, ou seja, equipes dedicadas, enquanto 76% possui membros da equipe de TI alocados de forma não exclusiva. Nesse sentido, quase 70% das IFES não documentam estratégia de resposta e tratamento de riscos, 19% documentam a estratégia no relatório de tratamento de riscos e 12% o fazem no plano de gerenciamento de riscos.

Figura 24 – Respostas amplas para constructo Resposta a Riscos



para sua instituição, mas que há fortes limitações para aquisição ou manutenção.
Respondente 3 (SE): Compras De Equipamentos Para Melhorar A Segurança
Respondente 7 (NE): Entendemos a importância e estamos implementando todas as necessidade do Sistema de Gestão de Segurança da Informação na Instituição.
Respondente 10 (S): Acredito que hoje passamos por uma péssima experiência devido ao descaso cultural pela Segurança de Informação. Cerca de 10% das pessoas da TIC se interessam e aplicam, incluindo os gestores, as boas práticas no ambiente da Instituição.
Respondente 13 (SE): Estamos precarizados em todas as frentes de sua pesquisa, seja em questão financeira/orçamentária, como também em relação ao quantitativo de pessoas para atender todas as demandas da legislação vigente.
Respondente 14 (SE): Devido a falta de pessoal, sente-se falta de uma melhor estrutura em relação as questões de Segurança da Informação e Comunicação.
Respondente 17 (NE): Um setor dedicado. Não há interesse da alta gestão por segurança.
Respondente 18(N): A maior das limitações é que não dispomos de recursos humanos para se concentrar exclusivamente no trato de segurança da informação e comunicação.
Respondente 19(N): Limitação de pessoal.
Respondente 20 (NE): O gestor foi recém nomeado e o comitê está em formação, mas é esperado que as lacunas nos processos sejam preenchidas.
Respondente 28 (S): Sistema mais atual de segurança digital, porém temos deficiências de recursos humanos e também financeiros.
Respondente 30 (NE): Mão de obra humana.
Respondente 33 (NE): Acredito que a nossa principal necessidade cujo impacto direto é a limitação das ações que podemos tomar para garantir a execução de todos os procedimentos necessários para uma boa gestão da segurança da Informação na instituição é a necessidade de criação de setor com pessoas dedicadas ao trabalho de segurança da informação, mas como existem poucas pessoas trabalhando na STI e não é tão fácil contratar novos funcionários no setor público, isso se torna inviável neste momento.

Fonte: Dados da pesquisa (2022).

Na questão 41 foi possível identificar o *phishing* como incidentes de segurança relacionados aos aspectos humanos que ocorrem com mais frequência, em torno de 40% das respostas, porém quase 30% dos respondentes não souberam identificar.A última questão, aberta, procurou saber dos respondentes sobre as necessidades em SI da sua instituição, as respostas, dispostas na questão 51 da figura 24, reportaram dificuldades enfrentadas como necessidade de pessoal, seguidas por dificuldade financeira e falta de comprometimento da alta administração.

O constructo Resposta a Riscos - que determina previamente como as instituições pretendem reduzir riscos e responder quando se tornam realidade, gerenciando incidentes, os

quais consistem na materialização do risco, determinando a resiliência organizacional - teve os resultados sintetizados na figura 25.

Figura 25 – Síntese dos resultados para o constructo Resposta a Riscos

Fonte: Elaborado pela autora (2022).

Para o constructo Monitoramento/Melhorias, a Tabela 7 traz as questões 47 e 48 com as melhores média, 3,27 e 3,97, respectivamente. Indica que, pouco mais de 40% das instituições marcaram positivamente, "quase sempre" ou "sempre", para ações envolvendo o devido cuidado com a disponibilização da informação à comunidade. A questão 47, e, na questão 48, que foi abordado o uso preferencial de canais oficiais para disponibilização da informação solicitada pela comunidade acadêmica, quase 80% das instituições, assinalaram "quase sempre" ou "sempre", obtendo a maior média das questões, 3,91.

Tabela 7 – Média, desvio padrão e porcentagem acumulativa para o constructo Monitoramento/ Melhorias

Questões	Média	Desvio padrão	Porcentagem acumulativa (Nunca, Raramente, Ocasionalmente, Quase Sempre, Sempre)				
42 Há métricas definidas para monitoramento de risco.	2,27	1,398	42,4	60,6	81,8	87,9	100,0
43 Quando há mudanças solicitadas em sistemas, é feito um controle de mudanças nos aspectos relacionados à Segurança da Informação.	2,48	1,278	30,3	48,5	81,8	90,9	100,0
45 Há contato direto com o Departamento de Segurança da Informação e Comunicações (DSIC) para o trato de assuntos relativos à segurança da informação.	2,88	1,495	24,2	45,5	63,6	78,8	100,0
46 Os incidentes são informados ao Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR GOV).	2,48	1,278	30,3	51,5	75,8	93,9	100,0

47 A informação a ser disponibilizada pelo setor de tecnologia à comunidade acadêmica é objeto de prévia análise a fim de que se identifiquem parcelas da informação com restrição de acesso.	3,27	1,232	12,1	21,2	57,6	81,8	100,0
48 A publicação de informação institucional é realizada prioritariamente por meio dos canais oficiais do órgão e entidade da APF.	3,91	1,259	12,1	0,0	21,2	63,6	100,0

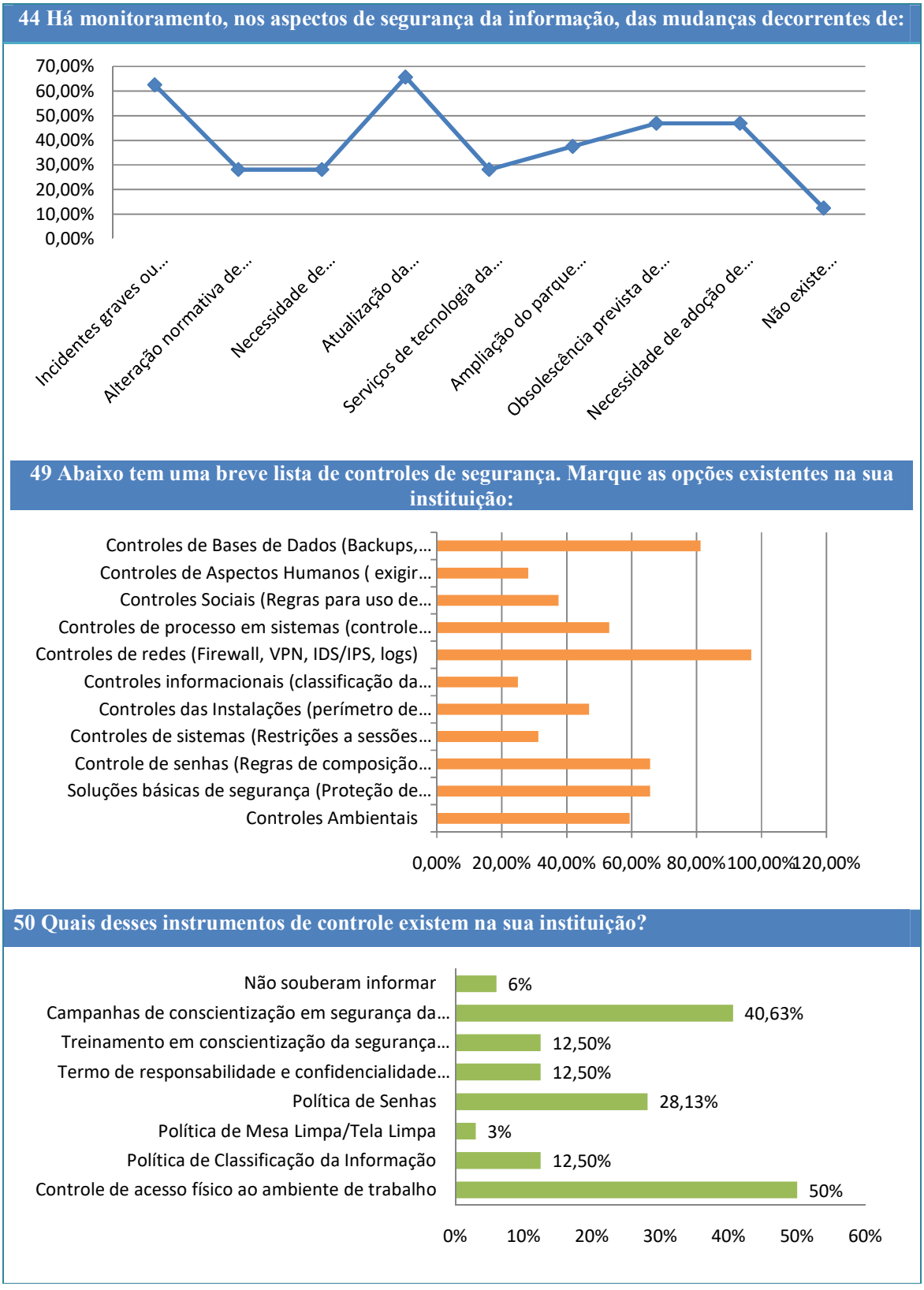
Fonte: Dados da pesquisa (2022).

Referente às últimas questões analisadas, quatro questões, dentre as seis da Tabela 7, obtiveram média de respostas abaixo de 3,00, com valores variando de 2,27 a 2,88, mostrando tendências das respostas a no máximo "ocasionalmente", como podemos observar nas questões 42 e 43, por exemplo. Nelas, de acordo com a porcentagem acumulativa delas, evidenciou-se que 81,8% das respostas de ambas tenderam a no máximo "ocasionalmente", mostrando não haver métricas definidas para riscos nem controles de mudanças nos aspectos de segurança, enquanto a porcentagem de "nunca" da primeira questão dessa tabela, foi a mais alta de todas as questões, 42,4%, indicando não haver métricas para monitoramento da SI.

Esses dados, possivelmente, podem justificar o fato de o índice de Cronbach desse constructo ter sido o mais baixo dentre os calculados. No entanto, as questões trabalhadas nesse constructo possuem respostas condizentes com a realidade identificada nos demais constructos, onde, dado que em torno de no máximo 50% dos respondentes chegam a fazer análise de riscos, era de se esperar poucas IFES com ações tendendo para a otimização do processo, propósito do constructo em análise.

As questões, não escala de likert, relativas a esse constructo, Figura 26, evidenciaram que mais de 60% das instituições, questão 44, monitoram incidentes graves e atualização de infraestrutura nos aspectos de SI. Porém, apenas 28% dos respondentes monitoram os serviços de TI nos aspectos de SI quando há mudanças, e, estranhamente, quando há obsolescência ou necessidade de adoção de novas tecnologias. Dois opostos, onde quase 50% das IFES monitoram quanto aos aspectos de SI, indicando que quanto ao novo e o velho verifica-se a segurança, mas os serviços de TI que estão no dia a dia não se preocupam com esse aspecto.

Figura 26 – Respostas amplas para constructo Monitoramento/Melhorias



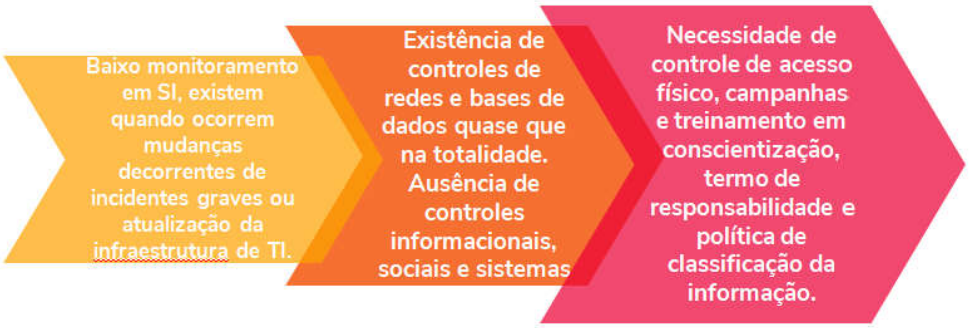
Fonte: Dados da pesquisa (2022).

Observa-se, na questão 49, que controles de redes e bases de dados existem quase que na totalidade das IFES, o que é inerente ao setor de tecnologia, evidenciando o olhar voltado para os riscos de TI. Porém, controles informacionais, de aspectos humanos, sociais e até de sistemas são incipientes aos setores de tecnologia dessas instituições, evidenciando a necessidade de apoio da alta administração para mudar essa realidade.

Por outro lado, a questão 50 aborda os instrumentos de controle existentes nas instituições dos respondentes, tendo sido mais referenciados os controles de acesso físico e campanhas de conscientização, ainda assim no máximo 50% dos respondentes os têm, enquanto há falta de políticas especificas, como a de classificação da informação e a política de senhas, e termo de responsabilidades, onde pouco mais de 10% das instituições os tem.

O constructo Monitoramento e Melhorias - que objetiva ações de monitoramento do programa de gerenciamento de riscos da instituição, fazendo análise de sua eficácia, bem como monitoramento das mudanças nos aspectos de segurança da informação. - teve os resultados sintetizados na Figura 27.

Figura 27 – Síntese dos resultados para o constructo Monitoramento e Melhorias



Fonte: Elaborado pela autora (2022).

Como evidenciado nos resultados da pesquisa de realidade das IFES, essas instituições têm necessidades de ações voltadas para a SI. Porém, a pesquisa permitiu identificar IFES que estão conseguindo manter um certo nível de segurança desejado, daí a necessidade de maior conversa entre os gestores dos setores de tecnologia das IFES, no intuito de troca de experiências e práticas de SI, mas, também, pôde-se evidenciar, nessa pesquisa, principalmente, a necessidade de comprometimento vindo da alta administração que, conforme evidenciado na fundamentação teórica, torna-se essencial para o sucesso das ações de segurança.

Logo, porque o modelo é específico aos setores de tecnologia das IFES? Porque foi construído para equipes abrangidas pelos setores de tecnologia das IFES, de desenvolvimento e manutenção de sistemas, equipes de redes, base de dados e suporte, sem deixar de lado o ambiente intrínseco que se insere esse aparato tecnológico, o ambiente das IFES, lugar de conhecimento efervescente, autônomo, mantenedor das liberdades de pensamento e constitucionais. Nesse sentido, analisaremos os elementos do modelo na próxima seção.

4.3 ELEMENTOS DO MISASI STI

Tendo a visão geral do modelo sido estabelecida, afinado pelos constructos e variáveis trabalhados no questionário, fez-se necessário conhecer seus elementos que consistem em ações de segurança da informação dispostas em passos e metas no modelo, complementadas por *checklists* de controles de segurança da informação, que levam em consideração o contexto dos setores de tecnologia e a realidade das IFES mapeadas nesta seção.

4.3.1 Ações de segurança da informação no MISASI STI

Como visto, os elementos do modelo consistem em ações de segurança da informação advindas nas normas e do framework internacional OCTAVE *Forte*, tendo o modelo disposto as ações em metas de: governança, análise de riscos, resposta a riscos, e monitoramento e melhorias, sintetizados na Figura 28 e detalhados neste capítulo.

Figura 28 – Síntese dos elementos do modelo

Fonte: Elaborado pela autora (2022).

As ações de Governança possuem como meta compreender a estrutura de governança, ativos e capacidades, para formular e documentar a tolerância a risco, tudo em consonância com os objetivos institucionais. Essa estrutura, em geral, consiste em corpo executivo, comitês e subcomitês responsáveis pelo direcionamento estratégico, políticas e planos que refletem a necessidade da organização em SI.

Compreender essa estrutura de governança alinhada ao programa de gestão de riscos auxilia no entendimento do contexto aplicado à segurança da informação e, nesse sentido, o modelo trabalhou as variáveis: contexto (estrutura de governança de SI), cultura e conscientização em SI, tolerância a riscos, comunicação, ativos e serviços críticos identificados e classificação da informação estabelecida, requisitos de continuidade dos ativos e capacidades correntes medidas, conforme podem ser vistas em detalhes no Quadro 15.

Quadro 15 – Ações de SI por variáveis no constructo Estrutura de Governança do MISASI STI

Estrutura de Governança	
Contexto	➢ Função de Gestor de Riscos ou Gestor de Segurança da Informação estabelecida ➢ Comitê Gestor de Segurança da Informação e/ou de Governança estabelecido ➢ Comitê Multidisciplinar de Proteção de Dados pessoais ou correlato estabelecido ➢ Alinhamento entre a gestão de riscos e/ou gestão de SI e a missão/objetivos estratégicos da instituição ➢ Alinhamento entre segurança da informação e proteção de dados pessoais.
Cultura/Conscientização em SI	➢ Estabelecer estratégias para promoção da cultura de segurança da informação e comunicações nos setores de tecnologia das IFES ▪ Ciclo de palestras, seminários, reuniões e outros eventos que contribuam para o constante processo de compartilhamento e absorção do conhecimento nos domínios da SIC. ▪ Promoção de troca de conhecimento e experiências no contexto e domínios de SIC por meio de grupos de trabalho formalmente instituídos com presença de profissionais da área de SIC ▪ Profissionais da área de SIC designados para participarem da elaboração do planejamento estratégico e da programação orçamentária do órgão ou entidade a qual mantenham vínculo. ▪ Planejamento estratégico e tático com ações que contemplem os aspectos de formação educacional, retenção e compartilhamento do conhecimento em SIC. ▪ Publicidade periódica da Política de Segurança da Informação e demais normas correlatas ▪ Funcionários e estagiários lotados no setor de tecnologia da instituição recebendo orientações em segurança da informação durante ambientação, formação inicial ou continuada ➢ Medidas de conscientização do usuário em segurança da informação para acesso aos sistemas: ▪ Assinatura de termo de responsabilidade ▪ Campanhas de conscientização direta via email, sistemas e etc ▪ Responsabilidades estabelecidas por meio de políticas ▪ Campanhas de conscientização amplas em redes sociais ▪ Cursos de capacitação específicos
Políticas	➢ Políticas de SI e riscos estabelecidas e revisadas periodicamente ou quando há mudanças nos objetivos estratégicos e normas de segurança ➢ Política de Gestão de Riscos definindo tolerância a riscos da instituição e normas de segurança específicas do setor e tecnologia ➢ Prescrever nas políticas métricas que indicam saúde e eficácia do programa de Gestão de Riscos. ➢ Sistemas estruturantes, de responsabilidade do setor de tecnologia, com políticas ou normativos específico que disciplinam seu uso, controles e perfis de acesso. ➢ Política de desenvolvimento seguro definida que conscientiza os desenvolvedores a prevenir e corrigir vulnerabilidades.
Tolerância a Riscos	➢ Se organização iniciante, desenvolver a declaração de tolerância a riscos ao consultar os objetivos estratégicos para compreender serviços críticos/ ativos necessários para o suporte a esses objetivos. Se organização madura, desenvolver a declaração de tolerância a riscos ao entrevistar *stakeholders* em busca dos objetivos estratégicos e de conhecer tolerâncias a riscos já estabelecidas. ➢ Plano de Gestão de Riscos estabelecido com critérios de aceite dos riscos . ➢ Alinhar, em um documento (declaração, política etc), tolerância a riscos com objetivos estratégicos organizacionais.

	➢ Quantificar tolerâncias a risco (intolerável, baixa tolerância, tolerável) para cada categoria de risco identificada durante mapeamento de riscos.
Comunicação	➢ Canal de comunicação para averiguar sugestões de melhorias ou denuncias de quebra de segurança da parte da comunidade acadêmica (email, site institucional , redes sociais, telefone...) . ➢ Assegurar que as políticas de segurança da informação e de gestão de riscos são de fácil compreensão e os usuários respectivos as compreendem. ➢ Manter contato direto com o DSIC para o trato de assuntos relativos à segurança da informação e comunicações ➢ Incidentes informados ao CTIR GOV ➢ A informação a ser disponibilizada pelo setor de tecnologia à comunidade acadêmica é objeto de prévia análise a fim de que se identifiquem parcelas da informação com restrição de acesso ➢ Publicação de informação institucional realizada prioritariamente por meio dos canais oficiais do órgão e entidade da APF
Ativos e Serviços críticos identificados e Classificação da Informação estabelecida	➢ Catalogo de ativos identificando os ativos relacionados aos serviços considerados críticos ➢ Os ativos de informação classificados como sigilosos possuem procedimentos especiais de controles de acesso. ➢ Rótulos relativos ao proprietário/custodiante da informação e/ou a responsabilização deles quanto a devida classificação da informação. ➢ Classificação da informação considerando o tipo da informação: ▪ **Sigilosa classificada em grau de sigilo** (reservada, secreta e ultrassecreta) - informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade ou do Estado. ▪ **Sigilosa protegida por legislação específica** (informações bancária, fiscal e contábil; processo administrativo disciplinar em curso; acesso a documento preparatório, inquérito policial etc.) ▪ **Pessoal** (informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem). ▪ **Ostensiva** (pode ser mostrada, sem restrição). ➢ Termo de Classificação de Informação – TCI definindo a manipulação de informação classificada ➢ Medidas de segurança estabelecidas para o tratamento da informação classificada

Requisitos de continuidade dos Ativos	➢ Ativos Críticos com requisitos de resiliência definidos. ➢ O plano de continuidade de negócios deverá ser testado regularmente, com intuito de que seus resultados sejam documentados e possam garantir a sua efetividade em caso de necessidade de ativação. ➢ O plano de continuidade de negócios em segurança da informação deverá conter, no mínimo: I - o objetivo; II - as atividades críticas de negócio a serem contempladas no plano; III - os requisitos para ativação do plano, em especial, o tempo máximo aceitável de permanência da falha; IV - o(s) responsável(is) pela ativação do plano, com seus respectivos dados de contato; V - o(s) responsável(is) por aplicar as medidas de contingência definidas, tendo cada servidor responsabilidades formalmente definidas e nominalmente atribuídas, incluindo seus respectivos dados de contato; e VI - a definição: ▪ das ações necessárias para operacionalização das medidas cuja implementação dependa da aquisição de recursos físicos e/ou humanos; ▪ dos limites de decisão para os responsáveis pela aplicação das medidas de contingência perante situações inesperadas; ▪ dos parâmetros para encerramento do plano e para a volta à normalidade; ▪ dos responsáveis por essas ações, incluindo seus dados de contato; ▪ da forma de monitoramento desse processo; e ▪ de um roteiro de simulação de teste de funcionamento e da sua forma de aplicação.
Capacidades correntes medidas	➢ Identificar controles existentes e documentar em uma lista priorizada de controles (onde os recursos devem ser investidos primeiro?) ➢ Comparar controles existentes versus requisitos de resiliência ➢ O gerente de riscos, por meio de consultas às partes interessadas - *stakeholder*s, avalia efetividade dos controles, com as seguintes questões: ▪ Os controles existentes estão atendendo aos objetivos estabelecidos? ▪ Todos os requisitos de conformidade aplicáveis são tratados suficientemente pelos controles? Se não, podem os controles atuais serem modificados para atender aos requisitos de conformidade? ▪ Os controles atuais satisfazem os objetivos cruciais da organização? Se não, a tolerância a risco da organização justifica ignorar a lacuna? ▪ Existem lacunas nas quais um objetivo de serviço não é atendido de forma adequada por um controle? Se sim, pode os controles atuais serem modificados? ▪ Qual é a opção mais econômica para satisfazer os objetivos da organização?

Fonte: Dados da pesquisa (2022).

O conhecimento da estrutura de governança institucional permitirá às IFES alinharem objetivos institucionais e segurança da informação. As variáveis no Quadro 15 permitem guiar as ações de segurança para esse alinhamento, por meio de políticas de segurança da informação, planejando a tolerância a riscos da instituição, classificando a informação e gerenciando ativos nesse sentido, especialmente os ativos relacionados a serviços críticos, analisando as capacidades correntes que nada mais é que comparar os controles existentes com os requisitos de resiliência estabelecidos, sem deixar de lado ações que promovam cultura e conscientização em SI, bem como planejar a comunicação dos setores de tecnologia com a comunidade acadêmica - de forma que não haja vazamento de informações sensíveis

nem ocultação de informações ostensivas-, e com órgãos responsáveis pela SI institucional, Em resumo, esse quadro representa um "conhece-te a ti mesmo" institucional.

De posse da estrutura de governança, a próxima etapa do modelo compreende ações que visam obter uma gestão de riscos reconhecida como vantagem, com processo de análise de riscos estabelecido e alinhado à estrutura de governança, com riscos analisados em relação às capacidades atuais e proteção de dados pessoais, para, de posse dessas informações, ser possível um mapeamento de riscos institucional.

Para isso, o Quadro 16 trabalhou a etapa da análise de riscos fazendo uso das variáveis: componentes da análise de riscos, análise de riscos em relação às capacidades atuais e proteção de dados pessoais e mapeamento de riscos.

Quadro 16 – Ações de SI por variáveis no constructo Análise de Riscos do MISASI STI

Análise de Riscos	
Componentes da Análise de Riscos	Lista de riscos, ameaças e vulnerabilidades relacionadas a cada ativo ou categoria de ativo e criação de relatório de identificação, análise e avaliação dos riscos de SI. Ações: ➢ Desenvolvimento de catálogo de **ativos** examinando seus ativos críticos e documentando seus **riscos**, **ameaças** e **vulnerabilidades** associados. ➢ **Relatório de identificação, análise e avaliação dos riscos de segurança da informação** com base em modelo estabelecido no plano de gestão de riscos de segurança da informação, contendo, **no mínimo**: ▪ Os **riscos** associados a cada ativo de informação, considerando as ameaças envolvidas, as vulnerabilidades existentes e as ações de segurança das informações já implementadas; ▪ o **grau de severidade** dos riscos identificados, considerando os valores ou os níveis de probabilidade de ocorrência do risco e as consequências da ocorrência do risco (perda da integridade, disponibilidade, confiabilidade ou autenticidade nos ativos envolvidos); ➢ os **eventos de segurança** da informação ocorridos, com a descrição das ações de segurança, e de eventuais consequências do evento para o órgão ou a entidade; as alterações nos fatores de risco; e as mudanças em relação a critérios de avaliação e análise.

Análise de riscos em relação às capacidades atuais e à proteção de dados pessoais	➢ Analisar riscos em relação às capacidades atuais: ▪ Comparar dados de controles organizacionais existentes à declaração de tolerância a risco para analisar soluções que estão funcionando e quais precisam de melhorias. As partes interessadas de toda a organização devem estar envolvidas para maximizar a eficácia do processo. ➢ Analisar riscos em relação à proteção de dados, ações no sentido de: ▪ Orientação aos funcionários e aos contratados da organização a respeito das práticas a serem tomadas para tratamento de dados pessoais. ▪ Tratamento de dados pessoais sensíveis, em regra, com o consentimento do titular. ▪ Consentimento para tratamento dos dados pessoais, em regra, feito por escrito. ▪ Criação de relatório de impacto à proteção de dados. ▪ Confirmação da existência ou fornecimento de acesso a dados pessoais mediante requisição do titular. ▪ Descrição dos tipos de dados coletados e da metodologia utilizada para a sua coleta de dados. ▪ Avaliação de forma permanente das salvaguardas e mecanismos de mitigação de riscos adotados. ▪ Canal de comunicação para aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências ▪ Receber comunicações da autoridade nacional e adotar providências. ▪ Manutenção de registro das operações realizadas para tratamento de dados pessoais.
Mapeamento de Riscos	➢ Riscos **estratégicos** (ligados aos objetivos/missões), **táticos** (ligados a processo) e **operacionais** (ligado as operações/sistemas) identificados e registrados no relatório de identificação, análise e avaliação dos risco ou documento correlato. ➢ Processo de gestão de riscos de segurança da informação estabelecido e alinhado ao modelo de gestão de riscos institucional, missão e objetivos estratégicos do órgão ou entidade Riscos registrados com ordem de prioridade. ➢ Riscos registrados com ordem de prioridade. ➢ O processo de gestão de riscos de segurança da informação deverá fornecer à organização os seguintes documentos: I- plano de gestão de riscos de segurança da informação; II - relatório de identificação, análise e avaliação dos riscos de segurança da informação; e III - relatório de tratamento de riscos de segurança da informação. ➢ Documentar **plano de gestão de riscos** com no mínimo: I - a abrangência da aplicação da gestão de riscos, delimitando seu âmbito de atuação e os ativos de informação que serão objeto de tratamento; II - a metodologia a ser utilizada que deverá contemplar, no mínimo, critérios de avaliação e de aceitação de riscos; III - os tipos de riscos; IV - o nível de severidade dos riscos; V - um modelo do relatório de identificação, análise e avaliação dos riscos de segurança da informação com as orientações necessárias para sua elaboração; e VI - um modelo do relatório de tratamento de riscos de segurança da informação com as orientações necessárias para sua elaboração. ➢ Documentar **relatório de tratamento de riscos** de segurança da informação,resultante do relatório de identificação, análise e avaliação dos riscos de segurança da informação, com as possibilidades de tratamento para cada risco identificados.

Fonte: Dados da pesquisa (2022)

Depreende-se do quadro que a análise de riscos para ser feita precisa identificar seus componentes – ativos, riscos , ameaças, vulnerabilidades, grau de severidade (probabilidade de ocorrências e consequências para as propriedades de segurança da informação) e eventos de segurança, dentre outras possibilidades –, analisar os riscos identificados em relação às capacidades atuais e proteção de dados pessoais e, por fim, realizar o mapeamento de riscos institucional.

Até aqui, a organização se concentrou em identificar riscos, vulnerabilidades e ameaças a seus ativos e serviços críticos e realizou o mapeamento dos riscos identificados. De posse desse mapeamento, a próxima etapa do modelo permitirá trabalhar a resposta organizacional a riscos de SI e, para isso, as ações de segurança foram agrupadas nas variáveis: estratégia de resposta e tratamento, gestão de continuidade, gestão de incidentes e ETRI (Equipe de Tratamento e Resposta a Incidentes), conforme pode ser visto no Quadro 17.

Quadro 17 – Ações de SI por variáveis no constructo Resposta a Riscos do MISASI STI

Resposta a Riscos	
Estratégia de Resposta e Tratamento (Plano de Resposta)	➢ Elaborar **relatório de tratamento de riscos de segurança da informação,** resultante do relatório de identificação, análise e avaliação dos riscos de segurança da informação, com as possibilidades de tratamento para cada risco identificado. ➢ Estratégia definida de notificação a Gerente de risco e/ou segurança da informação quando um risco se realiza. ➢ Escolher, para cada risco, uma das 7 (setes) e**stratégias de resposta** : Aceitar, Evitar, Transferir, Mitigar, Compartilhar, Aprimorar e Explorar. Estratégias oferecem melhor retorno do investimento quando aplicadas às interdependências entre riscos, em vez de cada risco individualmente. ➢ Documentar as consequências esperadas se o risco se concretizar. ➢ Estabelecer diretrizes para contato com CTIR GOV informando quando da ocorrência de incidentes. ➢ Fazer uso, preferencial, de canais institucionais para estabelecer comunicação nos aspectos relativos a segurança da informação
Gestão da Continuidade	➢ Requisitos de resiliência documentados visando manter serviços críticos em funcionamento ➢ Plano de continuidade do negócio definido e testado periodicamente, contendo como será realizada a gestão de incidentes, em caso de desastres ou de outras interrupções das operações de negócios, e prazos de recuperação das atividades. ➢ Estratégia de resposta e tratamento do risco da instituição documentada em relatório de tratamento de riscos de segurança da informação ou documento correlato.

Gestão de Incidentes	➢ Manutenção de documento contendo histórico de incidentes. ➢ Lista exemplificativa de possíveis serviços de tratamento de incidentes de segurança em redes de computadores a serem oferecidos:Tratamento de artefatos maliciosos;Tratamento de vulnerabilidades; Emissão de alertas e advertências; Anúncios; Prospecção ou monitoração de novas tecnologias; Avaliação de segurança; Desenvolvimento de ferramentas de segurança; Detecção de intrusão; e Disseminação de informações relacionadas à segurança; ➢ Procedimentos estabelecidos de investigação de danos decorrentes de quebras de segurança. ➢ Ações corretivas e disciplinares estabelecidas para os casos de quebra de segurança da informação
ETRI	➢ Equipe de tratamento e resposta a incidentes em redes computacionais – ETRI implementada ➢ ETRI trabalhando de forma coordenada com a gestão de SI ➢ Definição do modelo de trabalho da ETRI: Centralizado, Descentralizado, Hibrido ou membros da equipe de TI de forma não exclusiva.

Fonte: Dados da pesquisa (2022).

Depreende-se do quadro que a resposta a riscos envolve a estratégia de resposta a ser estabelecida alinhada aos requisitos de resiliência institucionais e, uma vez definida a estratégia de resposta para cada risco identificado na etapa anterior, análise de riscos, deve ser documentada em relatório respectivo para guiar as ações do gestor de riscos ou SI em conjunto com a equipe de tratamento e resposta a incidentes.

Por fim, a última etapa do modelo, monitoramento e melhorias, possui ações, Quadro 18, que buscam uma autoanálise para melhorias e retroalimentação do processo de gerenciamento de riscos, possível por meio de monitoramento das ações de SI e, para isso, o modelo fez uso das variáveis: monitorar e avaliar eficácia do modelo, gestão de mudanças, desenvolvimento seguro e melhorias

Quadro 18 – Ações de SI por variáveis no constructo Monitoramento e Melhorias do MISASI STI

Monitoramento/Melhorias	
Monitorar e avaliar eficácia do modelo	➢ Monitorar plano estabelecido de Gestão de Riscos e critérios de aceite dos riscos. ➢ Fazer uso das tolerâncias de risco da organização para desenvolver métricas que examinem quão bem a organização está respondendo ao risco ao longo do tempo. ➢ Desenvolver métricas para medir a eficácia do programa de gestão de riscos, de modo que ele possa produzir dados significativos que apóiem mudanças e melhorias e documentar as descobertas em um plano de melhoria. ➢ Medir progresso de implementação do plano de resposta e identificar gargalos que estão impedindo seu andamento, como, por exemplo, mudanças nas políticas/procedimentos relacionados. ➢ Líderes da estrutura de governança e gerente de riscos revisam e avaliam programa de gerenciamento de risco, propõe melhorias e repetem o processo. ➢ Entrevistar *stakeholders* para determinar se programa controlou riscos conhecidos efetivamente. ➢ Documentar tudo em planos de melhorias, se possível, abordando elementos como: • investimento • treinamento • comunicação • mudanças de política • planejamento de contingência • mudanças organizacionais (por exemplo, novas equipes) • aquisição de ativos
Gestão de Mudanças	➢ Promover o controle planejado das mudanças. ➢ Classificar mudanças em: **emergencial**, não prevista e de alto impacto, **rotineira**, que equipe técnica tem elevado grau de conhecimento, e **proativa**, que busca trazer maior eficiência. ➢ Realizar monitoramento das mudanças decorrentes de: ▪ [Emergenciais:] de incidentes graves ou modificação nos fatores de risco com alto impacto para os processos da organização; alteração normativa de aplicação imediata;necessidade de modificação significativa imediata nos ativos de informação; ▪ [Rotineiras:] atualização da infraestrutura de tecnologia da informação; e serviços de tecnologia da informação com periodicidade habitual que impliquem mudanças de um ou mais aspectos de segurança; ▪ [Proativa:] ampliação do parque computacional; obsolescência prevista de equipamentos e processos; necessidade de adoção de novas tecnologias; e outros eventos similares ➢ Criar **documento de avaliação e aprovação de mudança** contendo a responsabilidade pela elaboração e aprovação do documento, que deve ser remetido ao gestor de mudanças para análise dos aspectos de SI.
Desenvolvimento Seguro	➢ Processo de desenvolvimento/manutenção de sistemas com requisitos de segurança da informação. ➢ Acesso seguro ao código e banco de dados com registro e monitoramento de segurança.. ➢ Procedimentos formais de controle de mudanças em sistemas nos aspectos relacionados à Segurança da Informação alinhados aos requisitos de segurança ➢ Acompanhamento dos estudos de novas tecnologias quanto a possíveis impactos na segurança da informação e comunicações

Melhorias	➢ Analisar as métricas estabelecidas no programa de gestão de riscos para análise de melhorias. ➢ Elaborar formas de medir o desempenho das respostas a riscos. ➢ Efetividade dos controles avaliadas com as seguintes questões: ▪ Os controles existentes estão atendendo aos objetivos estabelecidos? Como você sabe? ▪ Todos os requisitos de conformidade aplicáveis são tratados suficientemente pelos controles? Se não, pode os controles atuais serem modificados para atender aos requisitos de conformidade? ▪ Os controles atuais satisfazem os objetivos cruciais da organização? Se não, a tolerância a risco da organização justifica ignorar a lacuna? ▪ Existem lacunas nas quais um objetivo de serviço não é atendido de forma adequada por um controle? Se sim, pode os controles atuais serem modificados? ▪ Qual a opção mais econômica para satisfazer os objetivos da organização?

Fonte: Dados da pesquisa (2022).

Essa última etapa do modelo torna o processo cíclico com ações de segurança da informação que buscam retroalimentar o modelo de modo que seja continuamente otimizado e responda à realidade institucional. A variável desenvolvimento seguro aborda a necessidade de monitoramento em SI da manutenção dos sistemas, necessidade essa evidenciada pela pesquisa de realidade das IFES, pois é importante que as mudanças que envolvam sistemas institucionais sejam monitoradas diretamente, como visto na fundamentação teórica, uma vez que envolvem diretamente os processos institucionais, sendo fator crítico de sucesso para a SI na instituição como um todo.

Uma vez visto em detalhes as ações de SI que permeiam o modelo MISASI STI, observou-se a necessidade de trabalhar ações específicas de SI para os setores de tecnologia, pois, embora as ações trazidas até o momento permitam ajustar o processo de SI no setor de tecnologia, para ser completo o modelo buscou ações específicas de SI inerentes a esse setor, abrangendo as dimensões: sistemas, redes, bases de dados dentre outras,uma vez que, para essas áreas, as normas são ricas em controles.

4.3.2 *Checklist*s de Controles

Inspirada na Revisão Sistemática de Literatura, os controles foram categorizados em 3 (três) macrogrupos - Sociais, Tecnológicos e Ambientais ou de Infraestrutura -, para facilitar a leitura das ações de segurança por áreas de interesse, sem deixar de lado a categorização específica por grupos de controles advinda da ABNT NBR ISSO/IEC 27002(2013).

O primeiro checklist de controles, referente aos controles sociais, Quadro 19, abarcam uma série de ações de segurança da informação envolvendo a gestão de pessoas que

trabalham, ou tem acesso, nos setores de tecnologia e foram agrupados, de acordo com a ABNT NBR ISO/IEC 27002 (2013), nos grupos de controles: segurança em recursos humanos (RH), gestão de ativos/classificação da informação, organização interna da segurança da informação, segurança nas comunicações, gestão de incidentes de segurança da informação, aspectos de segurança na gestão da continuidade, trabalhos remotos, controle de acesso e aquisição desenvolvimento e manutenção de sistemas.

Quadro 19 - Controles Sociais

	Controles Sociais
Segurança em RH	✓ Seleção de funcionários/estagiários com menção à segurança da informação. ✓ Assinatura de termo de responsabilidade quanto à segurança da informação no ato da contratação de estagiários ou no momento de posse do servidor. ✓ A Direção solicita que os funcionários pratiquem a segurança da informação conforme estabelecido nos procedimentos e políticas da organização. ✓ Existência de treinamento em conscientização sobre segurança da informação. ✓ Responsabilidades definidas para realizar o encerramento de um contrato ou mudança de local de trabalho. ✓ Processo disciplinar formal para as violações da segurança da informação.
Gestão de ativos/ Classificação da Informação	✓ Inventário dos ativos associados com as informações e um proprietário/responsável definido. ✓ Regras definidas e implementadas quanto ao uso de informações e ativos associados ✓ Procedimento de encerramento do contrato com devolução de ativos. ✓ Classificação da informação em Sigilosa, Pessoal ou Ostensiva, de acordo com legislação. ✓ Procedimento de tratamento da informação de acordo com esquema de classificação adotado pela organização. ✓ As funcionalidades do sistema, base de dados e redes implementadas de acordo com o esquema de classificação da informação. ✓ Gerenciamento de mídias removíveis de modo a proteger a informação de acordo com seu grau de classificação. ✓ Procedimentos formais de descarte de mídias de forma segura e protegida quando não mais necessárias (sanitização). ✓ Procedimento definido para o transporte de mídia de forma segura (protegendo contra acesso não autorizado, uso impróprio ou corrupção).
Organização interna da segurança da informação	✓ Responsabilidades/papéis de segurança da informação claramente definidos. ✓ As áreas de sistema, base de dados e redes com segregação de funções conflitantes. ✓ Procedimentos especificando quais autoridades contactar em caso de incidentes de segurança da informação (bombeiros, energia, telecomunicações, segurança, autoridades fiscalizadoras e organismos regulatórios). ✓ Contatos constantes com grupos de interesse / fóruns especializados em SI. ✓ Projetos inerentes aos setores de tecnologia considerando a segurança da informação desde a etapa inicial de planejamento, havendo comunicação com os responsáveis pela segurança da informação.

Segurança nas comunicações	✓ Política especificando a transferência de informação segura (proteção contra interceptação/ cópia/ destruição) por meio dos recursos de comunicação. ✓ Acordos estabelecidos para transferência segura de informações do negócio entre a organização e partes externas. ✓ Orientação na organização para uso de criptografia/assinatura eletrônica quando da transferência de informações sensíveis na forma de anexo. ✓ Uso de acordos de confidencialidade ou acordo de não divulgação que reflitam as necessidades da organização para a proteção da informação.
Gestão de incidentes de segurança da informação	✓ Responsáveis definidos para a gestão de incidentes ✓ Canal de gestão para controle e comunicação dos eventos envolvendo a segurança da informação no sistema ou na rede. ✓ Comportamentos anômalos no sistema vistos como indicadores de possíveis ataques. ✓ Funcionários e usuários da organização instruídos a notificar quaisquer fragilidades de segurança da informação nos sistemas/serviços o mais rápido possível. ✓ Procedimento definido para avaliação de evento de segurança e posterior classificação com o incidente caso necessário. ✓ Procedimentos documentados para reportar incidentes. ✓ Incidentes analisados de modo a documentar o conhecimento e reduzir probabilidade ou impacto de incidentes futuros. ✓ Procedimentos definidos de coleta de evidências para os propósitos de ação legal ou disciplinar.
Aspectos de SI na g. da continuidade	✓ Contatos definidos no Plano de Continuidade do Negócio abrangendo situações adversas envolvendo Sistemas, Redes e Base de Dados. ✓ Procedimentos de recuperação e resposta detalhando como cada setor irá gerenciar um evento de interrupção mantendo certo nível de segurança da informação. ✓ Plano de Continuidade do Negócio revisado a intervalos regulares. ✓ Implementação de redundância dos recursos de processamento da informação de modo a atender aos requisitos de disponibilidade.
Trabalhos remotos	Requisitos de segurança da informação adotados em trabalho remoto devem considerar: ✓ segurança física existente no local do trabalho (prédio e ambiente local) ✓ segurança nas comunicações, considerando necessidade de acesso remoto aos sistemas internos, a sensibilidade da informação acessada e do sistema interno ✓ regras e diretrizes contra acesso indevido por familiares/amigos ✓ revogação de autoridade e direitos de acesso, e devolução de equipamentos quando as atividades de trabalho remoto cessarem
Controle de Acesso	✓ Orientação aos usuários quanto ao uso da informação de autenticação secreta (usuários responsáveis pela proteção de suas informações de autenticação). ✓ Processo formal concedendo/revogando direitos de acesso de usuários no sistema. ✓ Nível de acesso concedido apropriado às políticas de acesso. ✓ Garantia que direitos de acesso não estão ativados antes da respectiva autorização. ✓ Adaptação dos direitos de acesso quando ocorre mudança de função ou bloqueios de direito de acesso quando deixam a organização. ✓ Direitos de acesso analisados criticamente a intervalos regulares. ✓ Responsáveis definidos para registrar/cancelar usuários do setor. ✓ Política de controle de acesso físico e lógico à informação e aos recursos de processamento da informação. ✓ Procedimento estabelecido para atualização no sistema e serviços quando há mudança de função e/ou atualização dos direitos de acesso de um usuário. ✓ Direitos de acesso dos usuários analisados criticamente a intervalos regulares ✓ Retirada de direitos de acesso dos funcionários ao sistema quando do encerramento dos vínculos/contratos ou quando há mudança de função.

Aquisição, desenvolvimento e manutenção de sistemas	✓ Orientação aos servidores que fazem uso dos relatórios do sistema para a importância da verificação de autenticidade eletrônica e aos desenvolvedores para sempre manterem essa funcionalidade quando da geração de relatórios pelos sistemas. ✓ Orientação de proteção quanto às informações que transitam no sistema de modo a proteger sua confidencialidade, integridade ou disponibilidade. ✓ Política de desenvolvimento seguro definida que conscientiza os desenvolvedores a prevenir e corrigir vulnerabilidades. ✓ Procedimentos formais de controle das mudanças no sistema. ✓ Mudanças previstas na plataforma operacional comunicadas em tempo hábil para permitir testes e análise crítica de impacto. ✓ Partindo da premissa que mudanças em pacotes de software devem ser desencorajadas, conscientização no sentido de que as mudanças devem ser limitadas às estritamente necessárias ou às atualizações de segurança.

Fonte: Dados da pesquisa (2022).

De fácil compreensão, percebe-se que os controles sociais se preocupam com a proteção dos ativos e da informação sob custódia das pessoas, evidenciando a necessidade de ações que direcionem a cultura dos setores de tecnologia para a segurança da informação, com medidas de conscientização, responsabilidades definidas e ações corretivas e disciplinares estabelecidas. A gestão de ativos voltada para a segurança da informação está ligada à devida classificação da informação que precisa ser definida pela estrutura de governança da instituição, e, no caso das IFES, há necessidade de uma padronização central advinda do Governo Federal, uma vez que as informações das IFES obedecem aos mesmos critérios de segurança da informação e a pesquisa de realidade das IFES constatou a necessidade das instituições avançarem nesse campo.

Os controles sociais também evidenciam a necessidade de organização interna dos setores de tecnologia para a SI, evidenciando a necessidade de segregação de função conflitante - por exemplo, o administrador de rede, por ter total acesso a essa tecnologia, não deveria ter acesso aos *logs* de segurança do acesso à rede, evidenciando a máxima trazida no referencial teórico "quem vigia o vigilante?"-, bem como contatos constantes com especialistas para troca de experiências em segurança da informação, dentre outras ações envolvendo pessoas elencadas no quadro supracitado.

O termo controles ambientais ou de infraestrutura foi escolhido por representar o ambiente dos setores de tecnologia e sua infraestrutura de *Data Centers*, abrangendo os grupos de controles: Local/Instalações e Segurança física do ambiente e de rede, cujas ações de segurança podem ser vistas no Quadro 20.

Quadro 20 - Controles Ambientais ou de Infraestrutura

Controles Ambientais ou de Infraestrutura	
Local/ Instalações	✓ Remoção/Locomoção de ativos com ▪ Controle na remoção de equipamentos. ▪ Controle na remoção de informações ou software. ▪ Controle da retirada de ativos e posterior devolução. ▪ Responsabilidades definidas para gerenciar a remoção de ativos. ✓ Equipamentos/ativos que operam externos ao setor de tecnologia protegidos contra acesso não autorizado. ✓ Regras claras que garantam proteção de equipamentos não monitorados (Ex: computadores só acessíveis com autenticação e uso de antivírus). ✓ Procedimentos de segurança física nos escritórios, salas e instalações. ✓ Proteção física contra ameaças externas e do meio ambiente (desastres naturais, acidentes, ataques maliciosos). ✓ Procedimentos para trabalho em áreas seguras devem considerar: ▪ Que o pessoal tenha o conhecimento da existência de áreas seguras. ▪ Trabalho supervisionado em áreas seguras. ▪ Áreas seguras vazias são fisicamente trancadas e periodicamente verificadas. ▪ Não seja permitido o uso de máquinas fotográficas, gravadores de vídeo/áudio , salvo se autorizado. ✓ Acesso de pessoas externas para efetuar entrega/carregamento isolado e controlado das instalações de processamento da informação. ✓ Política de mesa limpa/tela limpa para os recursos de processamento da informação.
Segurança física do ambiente de redes	✓ Ativos de rede protegidos contra perdas/roubos. ✓ Meio ambiente com ativos de redes em segurança (condições de temperatura, umidade, radiação eletromagnéticas controladas). ✓ Proteção dos equipamentos contra falta ou sobrecarga de energia elétrica: ▪ As linhas de energia e telecomunicações são subterrâneas sempre que possível ou recebem uma proteção alternativa adequada. ▪ Cabos de energia segregados dos cabos de comunicações para evitar interferências. ▪ Nos sistemas sensíveis/críticos, há instalação de conduítes blindados e salas/caixas trancadas em pontos de inspeção. ▪ Blindagem eletromagnética para a proteção dos dados. ▪ Acesso controlado aos painéis de conexões e às salas do cabo. ✓ Manutenção periódica nos equipamentos.

Fonte: Dados da pesquisa (2022).

Depreende-se do quadro acima que os controles ambientais ou de infraestrutura visam proteger as instalações contra ameaças internas, externas e do meio ambiente, como sobrecarga elétrica, bem como definir perímetro de segurança dentro dos setores de tecnologia para áreas seguras, sujeitas a um controle de acesso mais rigoroso. As ações devem ser feitas visando às instalações e seu acesso, pelo pessoal interno e colaboradores externos que precisem entrar nas instalações físicas.

Não obstante a essencial importância dos controles sociais e ambientais, observa-se que os controles tecnológicos dominam as normas de segurança, foco constante em pesquisas nessa área, conforme evidenciado na RSL, seja pela constante atualização tecnológica seja pelo aumento exponencial da dependência dos processos existentes aos recursos tecnológicos. Nesse contexto, o Quadro 21 traz o *checklist* de controles tecnológicos abrangendo os grupos

de controle: controle de acesso, segurança nas operações, nas comunicações, criptografia, e aquisição, desenvolvimento e manutenção de sistemas.

Quadro 21 - Controles tecnológicos

Controles Tecnológicos	
Controle de Acesso	✓ Manutenção de registro central de acesso concedido ao ID de usuário. ✓ Processo de gerenciamento formal de autenticação secreta (senhas, chaves criptográficas, tokens) definido e controlado regularmente. ✓ Procedimentos estabelecidos no sistema para não uso de senhas default/padrão como "admin/admin". ✓ Requisitos de segurança para autenticação no sistema estabelecidos. ✓ Implementar armazenamento seguro de senhas. ✓ Controle de acesso à rede definido de acordo com o perfil do usuário ✓ Sistemas com: ▪ Procedimento seguro de entrada no sistema (*log-on*). ▪ Registro das tentativas de acesso ao sistema. ▪ Registro de tentativas forçadas no sistema e posterior comunicação do evento. ▪ Responsável por verificar periodicamente anormalidades no acesso ao sistema. ▪ Validação dos dados de entrada somente quando todos os dados são fornecidos. ▪ Ausência de mensagens de ajuda indicando qual parte do dado de entrada fornecido está correta ou incorreta. ▪ Tempo de conexão restrito de modo a reduzir a janela de oportunidade para acesso não autorizado. ▪ Sessões inativas encerradas após um período. ▪ Proteção durante o *log-on*. ▪ Sistema de gerenciamento de senha interativo que assegure senhas de qualidade. ▪ Senhas armazenadas e transmitidas de forma segura. ▪ Usuários obrigados a modificar suas senhas temporárias no primeiro acesso. ▪ Controle dos direitos de acesso dos usuários aos dados que podem acessar (ler, escrever, excluir, executar). ▪ Fornecimento de menus para controlar o acesso às funções dos sistemas de aplicação ✓ Quanto ao código fonte do sistema: ▪ As bibliotecas de programa-fonte encontram-se no mesmo ambiente do sistema em operação. ▪ Acesso ao código fonte de programa restrito e controlado. ▪ Listagens dos programas relacionadas ao sistema mantidas em ambiente seguro. ▪ Registro de auditoria de todos os acessos a código fonte. ✓ Manutenção e cópia das bibliotecas de programa fonte sujeitam-se a procedimentos de controle de mudanças.

Segurança nas operações	✓ Procedimentos documentados e disponibilizados para os usuários sobre: - reinício e recuperação em caso de falha de sistema. - Instalação e configuração de sistemas. - Backups. - Gerenciamento de *logs*. – Monitoramento. - Requisitos de agendamento de tarefas. - Instruções de tratamento de erros. - Contatos para suporte. - Instruções para manuseio de mídias com dados confidenciais. - Procedimentos para. ✓ Mudanças nos processos de negócio/equipamentos/sistemas são documentadas, comunicadas e controladas. ✓ Monitoramento e projeção da capacidade dos recursos de modo a garantir o desempenho requerido. ✓ Registros de eventos (*logs*) das atividades dos usuários produzidos e analisados criticamente com freqüência. *Logs* de exceções/falhas/eventos de segurança produzidos e analisados criticamente com freqüência. Logs protegidos contra acesso não autorizado e adulteração. ✓ Atividades de administradores/operadores do sistema são registradas, protegidas, analisadas criticamente. ✓ Relógios dos sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, precisamente sincronizados. ✓ Vulnerabilidades técnicas do sistema de informação são registradas, analisadas criticamente e com registro de controle das mudanças ligadas a essas vulnerabilidades ✓ Fazer uso de controles contra *malwares:* ▪ Política formal proibindo o uso de software não autorizado. ▪ Controles para prevenir/detectar o uso de software não autorizado (*whitelisting*[21]). ▪ Controles para prevenir/detectar o uso de websites maliciosos/suspeitos (*blacklisting*[22]). ▪ Gerenciamento de vulnerabilidades técnicas que reduzem as vulnerabilidades possíveis de serem exploradas por malwares. ▪ Instalação e atualização regular de software de detecção e remoção de malware. ▪ Boletins com alertas que sejam precisos e informativos. ▪ Procedimentos para coleta regular de informações sobre novos malwares. ▪ Plano de Continuidade do negócio prevendo a recuperação em caso de ataques por malware. ▪ Ambientes passíveis de ataques catastróficos são isolados. ✓ Regras definindo critérios para a instalação de software pelos usuários estabelecidas ✓ As senhas dos usuários criptografadas no banco. ✓ A camada de aplicação do sistema acessa o SGBD com conta administrativa. ✓ Instalação e controle do sistema com: ▪ Procedimentos de controle de configuração/versão do sistema. ▪ Versões anteriores são mantidas como medida de contingência[23]. ▪ Estratégia de restauração às condições anteriores, disponibilizada antes de mudanças feitas no sistema. ✓ Uso de sistema de controle de configuração para manter o controle da implementação do software. ✓ Uso de sistema de controle de configuração para manter o controle da documentação do software. ✓ Separação dos ambientes de desenvolvimento, testes e produção (previne modificação não autorizada no ambiente de produção). ✓ Todo acesso ao sistema monitorado e registrado de modo a produzir uma trilha de auditoria.
	✓ Política de criptografia desenvolvida e implementada visando o uso de controles criptográficos para a proteção da informação. ✓ Política desenvolvida e implementada sobre uso, proteção e tempo de vida das chaves criptográficas considerando as especificações da norma complementar 09 da IN01;GSI/PR/DSIC ✓ Cifração e decifração de informações classificadas, em qualquer grau de sigilo, fazendo uso exclusivo de recurso criptográfico baseado em algoritmo de Estado ,em conformidade com os parâmetros e padrões mínimos estabelecidos no Anexo B da NC09/IN01;GSI/PR/DSIC. ✓ Procedimentos garantindo que toda informação sigilosa - classificada ou não -, independente do algoritmo de criptografia, seja armazenada em centro de processamento de dados fornecido por orgãos e entidades da APF. ✓ Procedimentos especiais de controle para material de acesso ao recurso criptográfico.

[21] Lista de softwares permitidos a acessar o sistema.
[22] Lista de softwares não permitidos.
[23] Convém que versões antigas de software sejam arquivadas juntamente com todas as informações e parâmetros requeridos, procedimentos, detalhes de configurações e software de suporte durante um prazo igual ao prazo de retenção dos dados (ABNT NBR ISO/ IEC 27002, 2013, p. 57).

Segurança nas comunicações	✓ Gerenciamento de rede no intuito de proteger as informações nos sistemas e aplicações. ✓ O acordo de serviços de rede incluem, para serviços internos ou terceirizados, níveis de serviço,mecanismos de segurança e requisitos de gerenciamento desses serviços. ✓ Segregação das redes[24] em: Grupos de serviços de informação, Usuários e Sistemas. ✓ O canal de comunicação seguro (Rede Privada Virtual - VPN) que interligue redes dos órgãos e entidades da APF, direta e indireta, objetivando a troca de informações classificadas, faz uso do recurso criptográfico baseado em algoritmo de Estado.
Aquisição, desenvolvimento e manutenção de sistemas	✓ Desenvolvimento de sistemas seguindo os seguintes princípios norteadores de segurança de sistemas: ▪ Segurança projetada em todas as camadas da arquitetura do sistema. ▪ Técnicas de autenticação de usuários. ▪ Controle de sessões seguras. ▪ Validação de dados sempre feita do lado cliente. ▪ Higienização do código (controle de mudanças a nível de código). ▪ Eliminação de depuração de códigos quando colocado em produção. ✓ Ambiente de desenvolvimento do sistema considerado seguro nos quesitos: ▪ Controle de acesso ao ambiente de desenvolvimento. ▪ Monitoramento de mudanças no código (ocorre revisão por pares...). ▪ Backups armazenados em local seguro externo à organização. ▪ Confiabilidade das pessoas que trabalham no ambiente. ✓ Quanto aos testes de segurança do sistema: ▪ Funcionalidades de segurança do sistema são testadas durante desenvolvimento. ▪ Testes de aceitação do sistema incluem requisitos de segurança da informação. ▪ Dados com informação pessoal ou sensível protegidos durante os testes.

Fonte: Dados da pesquisa (2022).

Como evidenciado, observa-se que a lista de controles tecnológicos é vasta, porém não poderia se esperar menos, uma vez que propostas para setores de tecnologia das IFES, abrangendo ações de segurança nas áreas de redes, sistemas e bases de dados, envolvendo setores de desenvolvimento, manutenção e suporte ao usuário, e gestão de pessoas.

O modelo MISASI STI buscou trazer ações integradas e simplificadas em segurança da informação para os setores de tecnologia das IFES, evitando ações específicas demais, de modo a não perder o foco do modelo nem se tornar cansativo, e evitando ações genéricas demais de modo que não fosse possível compreender as ações necessárias para um limiar mínimo de segurança nesses setores.

Outras ações de segurança foram trazidas no referencial teórico dessa tese como, por exemplo, diretrizes para controle de acesso lógico, físico e biométrico, vistos no Quadro 8, ações específicas aos gestores de segurança, Quadro 11, ações para desenvolvimento seguro de software, e *checklist* de controles específicos para aplicações web, Apêndice A

. O que demonstra um leque vasto de ações em segurança da informação que os setores de tecnologia das IFES devem estar dispostos a realizar, sendo essas ações necessárias para que o modelo integrado e simplificado de ações seja implementado. Porém, conforme evidenciado na pesquisa de realidade dos setores de tecnologia das IFES, sem

[24] Consiste na rede dividida em diferentes domínios de redes de acordo com o nível de confiança, o que pode ser feito tanto em redes físicas quanto em redes lógicas.

comprometimento da alta administração, contratação de pessoal e recursos financeiros pouco se pode avançar na SI.

Como visto, a hipótese da tese foi confirmada, tendo sido possível desenvolver um modelo integrado e simplificado de ações de segurança da informação para os setores de tecnologia das IFES, o MISASI STI, onde definimos os pilares e a dinâmica do modelo, delineamos sua arquitetura e trouxemos seus elementos organizados por constructos, finalizando com um *checklist* de controles. O modelo pode ser aplicado a qualquer setor de tecnologia das IFES que tenham interesse em implementar ações de SI.

Como visto, no referencial teórico, é fortemente recomendado que as IFES pensem em alguma solução de segurança para seus setores de tecnologia, tendo como premissas que publicidade é a regra, o sigilo é a exceção, e o cidadão como principal cliente da gestão de segurança da informação, sendo as ações de SI pautadas para proteger os mesmos de roubo de informações e arbitrariedades, com limite nos interesses da comunidade acadêmica.

A depender da escolha do modelo, desenhar as ações, de acordo com a realidade de cada instituição, torna-se viável. Aqui trouxemos um modelo possível, cujo intuito foi integrar e simplificar a implementação dessas ações. Independentemente do modelo escolhido, fato é que a segurança da informação deve ser planejada e implementada nessas instituições, seja pelo arcabouço acadêmico de que são detentoras, seja pela necessidade organizacional dessas ações na atualidade.

5 CONSIDERAÇÕES FINAIS

O estudo referente às ações de segurança da informação em Instituições Federais de Ensino Superior (IFES), em âmbito nacional, permitiu a efetivação de um conhecimento amplo do panorama da gestão da informação realizada por essas instituições no campo das práticas de segurança. Determinando uma noção sistemática de ações para análise de riscos com ênfase nos fluxos de informação em suportes tecnológicos, perante a grande demanda informacional necessária ao encaminhamento dos processos nessas instituições.

Para tanto, buscou-se o desenvolvimento de uma pesquisa centrada em uma problemática, partindo da hipótese de ser possível simplificar as ações de segurança da informação para análise de riscos, no âmbito dos setores de tecnologia das Instituições Federais de Ensino Superior, por meio de um modelo integrado e simplificado, alinhado aos frameworks reconhecidos internacionalmente e às normas e recomendações do governo federal, foi possível traçar os objetivos específicos, que compreenderam diversos aspectos de ações de segurança na dinâmica do fluxo informacional das IFES. A metodologia traçada foi essencial para a compreensão do contexto científico da área, por intermédio de uma Revisão Sistemática de Literatura, complementada por pesquisas documentais e de investigações, por intermédio de questionário, que permitiram o conhecimento dos aspectos da realidade dessas instituições frente às exigências normativas.

Com base na apropriação desse conhecimento foi possível determinar a viabilidade de aplicação de um modelo integrado e simplificado que permita a promoção de boas práticas de segurança da informação, a serem tratadas nos processos organizacionais dos setores de tecnologia das IFES, com atenção às necessidades dessas instituições em relação à segurança da informação. Uma vez que foi possível criar o modelo denominado MISASI STI, disposto ao longo da tese que respondeu à hipótese definida.

Tendo em vista, os dados obtidos e as análises realizadas, pode-se considerar que foram constatadas deficiências em relação às ações de segurança da informação, nos setores de tecnologia das IFES no Brasil; bem como, também, a observância de que existem instituições que, apesar dessa constatação, estão conseguindo avançar com essas limitações.

Identificou-se, com base nos controles investigados, que as IFES estão enfrentando necessidades financeiras e de pessoal qualificado para essas ações, observando-se, principalmente, a necessidade de apoio da Alta Administração, que deve perpassar, desde o planejamento, com políticas e ações para a promoção de cultura, conscientização e

capacitação, à necessidade de ações envolvendo análise de riscos – que é considerada o pilar das ações de segurança da informação –, resposta a riscos e monitoramento.

No tocante à essencialidade do apoio da Alta Administração, evidencia-se que, sem a intervenção de apoio, as instituições dificilmente prosperarão em segurança da informação. Nesse sentido, com a pesquisa, referente ao constructo Estrutura de Governança, que se encontra presente no modelo MISASI STI, direcionando a instituição para seu programa de gerenciamento de riscos e servindo de guia em relação a papéis e responsabilidades, políticas, recursos e segurança no fluxo de informações, identificou-se a necessidade de ações promotoras de segurança da informação, desde políticas, capacitações, equipes designadas, promoção do adequado tratamento da informação sigilosa, estabelecimento de ações corretivas e disciplinares, dentre outras estratégias em segurança da informação. Com isso, a pesquisa evidenciou deficiências como, por exemplo, a inexistência de ações básicas como orientações em segurança da informação para servidores e estagiários, implicando na necessidade de ações.

Verificou-se, no constructo Análise de Riscos, que possibilita compreender os riscos institucionais ao identificar riscos, ameaças e vulnerabilidades dos ativos, considerado pilar das ações de segurança da informação, sua relevante importância em pesquisas pela comunidade científica, por consistir como um dos pontos críticos para as IFES, porém, foi evidenciada, nos resultados, a escassez de ações voltadas para riscos, seja no campo estratégico, tático ou operacional das IFES. O modelo desenvolvido pela pesquisa, MISASI STI, permite cobrir essa lacuna trazendo diversas ações possíveis de segurança da informação.

Quanto ao constructo Resposta a Riscos, que pré-determina como as instituições pretendem reduzir e responder a riscos, quando se tornam realidade, gerenciando incidentes, os quais consistem na materialização do risco, foi possível evidenciar que é determinante para a resiliência organizacional. Os resultados da pesquisa observaram a necessidade de planejamento nesse sentido, uma vez que as poucas ações que existem são relativas a tratar incidentes que já ocorreram, sendo que nem equipe de respostas a incidentes as IFES possuem.

Destacam-se, também, as ações de monitoramento do programa de gerenciamento de riscos da instituição, concentradas no constructo Monitoramento/Melhorias, que efetivam a análise da eficácia do programa, bem como o monitoramento das mudanças nos aspectos de segurança da informação, com ações de otimização no campo da segurança. Foi constatada, na pesquisa, a necessidade das instituições nesse sentido, uma vez que, se não existem ações básicas de segurança da informação implantadas, é possível inferir os mesmos resultados

negativos para ações de otimização. O modelo desenvolvido, MISASI STI, idealiza o uso de indicadores que, se possível, contribuiriam com ações de monitoramento, fazendo-se necessário o desenvolvimento seguro e análise de métricas com foco nas melhorias.

Considera-se ainda, quanto à proteção de dados pessoais, – observando-se conforme o pressuposto de que privacidade e segurança não são sinônimos; no entanto, não é possível existir privacidade sem segurança –, que as instituições, apesar de aplicarem a Lei Geral de Proteção de Dados Pessoais (LGPD), não fazem a classificação da informação, bem como não estabelecem o devido tratamento da informação classificada. Evidenciando-se que muitas das ações estabelecidas envolvem basicamente notificar os responsáveis da informação com a solicitação de aceite para a sua disposição. Entretanto, essas ações não correspondem à meta de segurança prevista quando à edição da lei respectiva, por ser entendido que segurança não se limita a um *pró-forme*, mas a um conjunto de ações que precisa garantir um nível adequado de proteção da informação. Em vista disso, é premente que as instituições planejem a segurança, como a classificação e tratamento da informação, para garantir as propriedades de segurança, segundo a privacidade determinada na LGPD.

Com a perspectiva geral da pesquisa, considera-se que mesmo com a organização do mapeamento das IFES por regiões, não foi possível estabelecer a identificação de nenhuma região do Brasil que se sobressaísse em relação às ações de segurança da informação, demonstrando que as dificuldades estão distribuídas como um todo em âmbito nacional. Tendo por base as considerações apresentadas, confirmou-se a hipótese geral deduzida pela pesquisa, com a qual foi possível simplificar as ações de segurança da informação para análise de riscos, no domínio dos setores de tecnologia das IFES, com um modelo integrado, alinhado aos *frameworks* reconhecidos internacionalmente e às normas e recomendações do governo federal quanto à segurança da informação – no contexto desta pesquisa, o modelo MISASI STI.

Afirma-se que, com os resultados desta pesquisa, é possível auxiliar na implementação de ações contínuas em segurança da informação nos setores de tecnologia das IFES, de forma a manter um nível contínuo de segurança, por sua importância, quanto ao armazenamento e disponibilização informacional, em meio tecnológico, abrangendo os processos organizacionais dessas instituições que perpassam pelos sistemas de informação. Devendo-se considerar ainda a importância desses resultados no campo científico por corresponder a uma temática de relevância para área da Ciência da Informação.

Como elemento de amadurecimento científico, o desenvolvimento desta pesquisa permitiu o reconhecimento de pontos que foram determinantes para uma análise dos aspectos

que foram limitadores de pesquisa que, por sua vez, direcionaram-na por rumos diferentes ou que permitiram abarcar discussões não previstas em seu projeto. Esta pesquisa apresentou como principal limitador, a pandemia de COVID-19, causada pelo SARS-CoV-2, que resultou na instituição de medidas preventivas, a partir do ano de 2020, que foram determinantes para a continuidade da pesquisa, como restrições, isolamento, controles de locais de trabalho e fechamento de instituições de ensino. Perante a condição determinada pela pandemia, que se prolongou por dois anos, inviabilizou a possibilidade da execução do procedimento de coleta de dados, entrevista, que poderia ter proporcionado uma discussão ainda mais enriquecedora sobre as ações de segurança da informação.

Observou-se também, conforme as limitações de pesquisa, que existe um limiar tênue entre o que deve estar público e de fácil acesso, e a privacidade na segurança da informação que, segundo este estudo, precisaria ser mais bem trabalhado no âmbito das IFES, como no contexto desta pesquisa, a coleta de email dos gestores de segurança dessas instituições. Por se tratar de uma função institucional, o email profissional dos gestores deveria ser público e de fácil acesso para os devidos questionamentos referentes à sua respectiva área de atuação. No entanto, conforme a pesquisa constatou, nos *sites* das IFES não existe clareza quanto às informações de designação de um gestor de segurança da informação, condição que direcionou o estudo para a busca de emails de diretores de tecnologia dessas instituições, bem como de gestores de governança ou responsáveis pela proteção de dados – nova função advinda com a LGPD –, funções essas que, em essência, também são responsáveis pelas ações de segurança da informação nos setores de tecnologia das IFES.

Durante o processo de busca pelos emails dos gestores de segurança ou diretores de tecnologia, gestores de governança ou de proteção de dados, foi possível perceber que nos *sites* não constam emails de nenhum gestor, cujo único ponto de acesso da comunidade acadêmica corresponde a um sistema de chamados que, de acordo com a dedução desta pesquisa, refere-se à orientação para “fechar chamados”, enquanto deveria ser uma orientação a responder dúvidas da comunidade acadêmica.

É necessário evidenciar que algumas IFES apresentaram anúncios de substituição da página “Quem Somos”, – obrigatória, em regra, pela Lei de Acesso à Informação –, pela página do *site* do Sistema de Gerenciamento de Recursos Humanos (SIGRH), sistema de recursos humanos institucional. Conforme as análises desta pesquisa, acredita-se se tratar de um mal entendido estabelecido por essas instituições, pois, apesar de o portal público do SIGRH apresentar informações dos funcionários das IFES, incluindo gestores, a comunidade acadêmica precisa de uma página “Quem Somos” para que essa página seja orientada a

funções, permitindo o acesso ao nome do reitor das IFES, bem como aos gestores e coordenadores nomeados, informação primariamente pública, enquanto, no portal público do SIGRH, a busca se dá pelo nome de servidores. Esse processo de busca do SIGRH, acarretou um redirecionamento de pesquisa perante a busca de nomeações de funções por meio do diário oficial para a identificação do nome apresentado na função, para, só depois, retornar ao SIGRH e efetivar a busca pelo email e número de telefone institucionais, quando disponíveis.

Esclarece-se que, apesar de terem sido coletados números de telefones, não foi possível estabelecer contato efetivo, devido às circunstâncias do trabalho remoto estabelecido pela pandemia de COVID-19.

Outro aspecto a ser considerado nas limitações de pesquisa refere-se à dificuldade na obtenção de respostas pelo instrumento de coleta de dados, questionário, que se apresentou como uma condição inesperada, perante a expectativa da pesquisa. Uma vez que, acreditava-se que, por se tratar de um domínio de gestores de segurança, esperava-se por mais pessoas abertas a responder à pesquisa, devido à função que exercem, diferentemente como ocorreria se a pesquisa tivesse sido aplicada aos servidores das IFES em geral. Nesse sentido, muitos gestores, antes de responderem ao questionário, mesmo estando escrito no cabeçalho da pesquisa que os dados seriam mantidos em sigilo, procuraram os responsáveis por esta pesquisa, no intuito de se certificarem que realmente as ações de suas instituições não seriam identificadas. No entanto, como observado nos resultados e discussão da pesquisa, muitas instituições optaram por não responder ao questionário até o final, apesar do envio de muitos emails reiterando a necessidade de finalização para o cumprimento das necessidades da pesquisa.

Ressalta-se que, a partir de uma condição hipotética, essas dificuldades teriam sido consideradas naturais em um processo de pesquisa, cujo objeto se estabeleceria na segurança da informação em instituições financeiras, devido ao alto risco de perda financeira para essas instituições. Entretanto, no contexto das Instituições Federais Ensino Superior, trata-se de uma situação relativamente impensada.

Em aspectos gerais, no contexto desta pesquisa, é importante considerar, que para efetivação de ações de segurança da informação na demanda informacional nos processos organizacionais das IFES, o apoio da Alta Administração é considerado como a principal força, bem como a promoção da cultura em segurança da informação, via conscientização e capacitação; enquanto a falta de apoio financeiro é considerada como a principal fraqueza da segurança da informação nas IFES, assim como a necessidade de pessoal qualificado e grau de comprometimento da comunidade acadêmica. Desse modo, deve-se evidenciar que as

principais oportunidades advindas com o modelo desenvolvido MISASI STI, consistem no rol de implementação de ações de segurança da informação, análise de riscos e monitoramento. No entanto, as principais ameaças à aplicação do modelo, encontram-se na ausência de cultura em segurança da informação e falta de pessoal qualificado.

Referente às reflexões e direcionamentos considerados por esta pesquisa, acredita-se que à medida que ocorram maiores avanços no conhecimento das ações de segurança da informação na esfera das IFES, pressupõe-se uma maior compreensão no campo da gestão da informação, abrangendo as práticas de segurança da informação, condição que implicará na elevação do nível de importância dos assuntos relativos à segurança da informação para as organizações. Como observado, esta pesquisa a partir do desenvolvimento do modelo MISASI STI, não encerra esta discussão. Espera-se, com base em futuras pesquisas, o acompanhamento da implementação desse modelo, sua influência na cultura organizacional em segurança da informação, bem como a avaliação contínua das práticas de segurança frente às ações trazidas pelo modelo ou análise detalhada de cada constructo envolvendo sua contribuição para a área da segurança da informação.

.

REFERÊNCIAS

AICPA, Association of International Certified Professional Accountants. **Illustrative cybersecurity risk management report**. [s.l: s.n.]. Disponível em: <https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/illustrative-cybersercurity-risk-management-report.pdf>.

AL-SAFWANI, Nadher; FAZEA, Yousef; IBRAHIM, Huda. ISCP: In-depth model for selecting critical security controls. **Computers and Security**, v. 77, p. 565–577, 2018.

AL HADIDI, M et al. Methods of risk assessment for information security management. **International Review on Computers and Software**, v. 11, n. 2, p. 81–91, 2016.

ALASSAFI, Madini O. et al. A framework for critical security factors that influence the decision of cloud adoption by Saudi government agencies. **Telematics and Informatics**, v. 34, n. 7, p. 996–1010, 2017.

ALMEIDA, Fernando; CARVALHO, Inês; CRUZ, Fábio. Structure and challenges of a security policy on small and medium enterprises. **KSII Transactions on Internet and Information Systems**, v. 12, n. 2, p. 747–763, 2018.

APPOLINÁRIO, Fabio. **Dicionário de Metodologia Científica**. 2. ed. São Paulo: Atlas, 2011.

ASSANGE, Julian. **Cypherpunks: liberdade e o futuro da internet**. São Paulo: Boitempo, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27005: tecnologia da informação: técnicas de segurança: gestão de riscos de segurança da informação**. Rio de Janeiro: [s.n.].

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27001: Tecnologia da informação: técnicas de segurança: sistemas de gestão da segurança da informação: requisitos**. Rio de Janeiro: [s.n.].

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27002: tecnologia da informação: técnicas de segurança: código de prática para a gestão da segurança da informação**. Rio de Janeiro: [s.n.].

AZAN BASALLO, Y. et al. Artificial intelligence techniques for information security risk assessment. **IEEE Latin America Transactions**, v. 16, n. 3, p. 897–901, 2018.
BARDIN, Laurence. **Análise de conteúdo**. Lisboa: Edição 70, 2010.
BEZERRA, Edson Kowask. **Gestão de riscos de TI: NBR 27005**. Rio de Janeiro: RNP/ESR, 2013.

BHARAT, G.M. Mani; PRASAD, M.S. Seetarama. Fuzzy oriented risk assessment in enterprise information systems. **Journal of Theoretical and Applied Information Technology**, v. 89, n. 1, p. 218–223, 2016.

BHARATHI, S.V. Vijayakumar. Prioritizing and Ranking the Big Data Information Security

Risk Spectrum. **Global Journal of Flexible Systems Management**, v. 18, n. 3, p. 183–201, 2017.

BRASIL. Decreto nº 3.505, de 13 de junho de 2000. Institui a política de segurança da informação nos órgãos e entidades da Administração Pública Federal e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, 2000.

BRASIL. Instrução Normativa GSI Nº 1, de 13 de junho de 2008. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, 2008a.

BRASIL. Norma Complementar nº 02/IN01/DSIC/GSIPR, Metodologia de Gestão de Segurança da Informação e Comunicações. **Diário Oficial [da] República Federativa do Brasil**, 2008b.

BRASIL. Norma Complementar nº 03/IN01/DSIC/GSIPR, Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. **Diário Oficial [da] República Federativa do Brasil**, 2009a.
BRASIL. Norma Complementar nº 05/IN01/DSIC/GSIPR, e seu anexo, Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. **Diário Oficial [da] República Federativa do Brasil**, 2009b.

BRASIL. Norma Complementar nº 08/IN01/DSIC/GSIPR, Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal. **Diário Oficial [da] República Federativa do Brasil**, 2010.
BRASIL. Decreto nº 7.845, de 14 de novembrodeE 2012 Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. **Diário Oficial [da] República Federativa do Brasil**, 2012a.

BRASIL. Norma Complementar nº 10/IN01/DSIC/GSIPR, Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta. **Diário Oficial [da] República Federativa do Brasil**, 2012b.

BRASIL. Norma Complementar nº 16/IN01/DSIC/GSIPR, Estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta. **Diário Oficial [da] República Federativa do Brasil**, 2012c.

BRASIL. Instrução Normativa GSI Nº 2, de 5 de fevereiro de 2013 Dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal. **Diário Oficial [da] República Federativa do Brasil**, 2013a.

BRASIL. Instrução Normativa GSI Nº 3, de 6 de março de 2013. Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal. **Diário Oficial**

[da] República Federativa do Brasil, 2013b.

BRASIL. Norma Complementar nº 18/IN01/DSIC/GSIPR, Estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF). **Diário Oficial [da] República Federativa do Brasil**, 2013c.

BRASIL. Norma Complementar nº 17/IN01/DSIC/GSIPR, Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF). **Diário Oficial [da] República Federativa do Brasil**, 2013d.

BRASIL. Norma Complementar nº 04/IN01/DSIC/GSIPR, e seu anexo, (Revisão 01) Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal. **Diário Oficial [da] República Federativa do Brasil**, 2013e.

BRASIL. Norma Complementar nº 20/IN01/DSIC/GSIPR, (Revisão 01) Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indi. **Diário Oficial [da] República Federativa do Brasil**, 2014a.

BRASIL. Norma Complementar nº 09/IN01/DSIC/GSIPR, (Revisão 02) Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta. **Diário Oficial [da] República Federativa do Brasil**, 2014b.

BRASIL. Norma Complementar nº 21/IN01/DSIC/GSIPR, Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta. **Diário Oficial [da] República Federativa do Brasil**, 2014c.

BRASIL. Norma Complementar nº 07/IN01/DSIC/GSIPR, (Revisão 01) Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. **Diário Oficial [da] República Federativa do Brasil**, 2014d.

BRASIL. Estratégia de governança digital da Administração Pública Federal 2016- 19. p. 36, 2016a.

BRASIL, Ministério do Planejamento / Secretaria de Tecnologia da Informação. **Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações do Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal - MGR-SISP v2.0**, 2016. Disponível em: <https://www.governodigital.gov.br/documentos-e-arquivos/MGR-SISP-V260816.pdf>. Acesso em: 5 dez. 2018.

BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018 Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação. **Diário Oficial [da] República Federativa do Brasil**, 2018a.

BRASIL. Norma Complementar nº 14/IN01/DSIC/GSIPR, estabelece princípios, diretrizes e responsabilidades relacionados à segurança da informação para o tratamento da informação em ambiente de computação em nuvem, nos órgãos e entidades da Administração Pública Fede. **Diário Oficial [da] República Federativa do Brasil**, 2018b.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD), Brasília, DF. **Diário Oficial [da] República Federativa do Brasil**, 2018C.

CAMPOS, Claudinei José Gomes. Método de análise de conteúdo: ferramenta para a análise de dados qualitativos no campo da saúde. **Rev Bras Enferm**, v. 57, n. 5, p. 611–614, 2004.
CARVALHO, Marta Maria Chagas De. **A escola e a república**. São Paulo: Brasiliense, 1989.
CENTRO DE TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO (CTIR GOV). **CTIRGov em números - INCIDENTES**. Disponível em: <https://emnumeros.ctir.gov.br/incidentes/>. Acesso em: 5 nov. 2019.

COOPER, Donald R; SCHINDLER, Pamela S. **Métodos de Pesquisa em Administração**. 12. ed. Porto Alegre: Bookman, 2016.

COMITÊ GESTOR DE INTERNET. **Estatísticas dos Incidentes Reportados ao CERT.br**. Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 6 abr. 2022.

CRESPO, A. A. Estatística Fácil. 19. ed. São Paulo: Saraiva, 2009

DANTAS, Marcus Leal. **Segurança da informação: uma abordagem focada em gestão de riscos**. Olinda: Livro Rápido, 2011.

DAWSON, Maurice. Applying a holistic cybersecurity framework for global IT organizations. **Business Information Review**, v. 35, n. 2, p. 60–67, 2018.

DELL-MASSO, Maria Candida Soares; COTTA, Maria Amélia de Castro; SANTOS, Marisa Aparecida Pereira. **Ética em pesquisa científica: conceitos e finalidades**. São Paulo: UNESP, 2014.

DUARTE, Emeide Nóbrega; SILVA, Alzira Karla Araújo Da; COSTA, Suzana Queiroga Da. GESTÃO DA INFORMAÇÃO E DO CONHECIMENTO: práticas de empresa "excelente em gestão empresarial" extensivas à unidades de informação*. **Informação & Sociedade: Estudos**, v. 17, n. 1, p. 97–107, 2007.

FLEURY, Maria Tereza Leme; WERLANG, Sergio Ribeiro da Costa. **Pesquisa aplicada: conceitos e abordagens**. Rio de Janeiro: Fundação Getúlio Vargas, 2017.

FONTANELLA, Bruno José Barcellos; RICAS, Janete; TURATO, Egberto Ribeiro. Amostragem por saturação em pesquisas qualitativas em saúde: contribuições teóricas. **Cad. Saúde Pública**, v. 24, n. 1, p. 17–27, 2008.

GASPAR, Isaac de Abreu; SHIMOYA, Aldo. **Avaliação da confiabilidade de um pesquisa utilizando o coeficinete alfa de Cronbach**. Goiás: Simpósio de engenharia de produção, 2017.

GUIMARÃES, Leandro Marcos de Oliveira. **RNP – Rede Nacional de Pesquisa cria sua Própria de AC SSL – ICP EDU.** Disponível em: <https://cryptoid.com.br/banco-de-noticias/14301/>. Acesso em: 25 jul. 2019.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2012.
GUIMARÃES, Leandro Marcos de Oliveira. **RNP – Rede Nacional de Pesquisa cria sua Própria de AC SSL – ICP EDU.** Disponível em: <https://cryptoid.com.br/banco-de-noticias/14301/>. Acesso em: 25 jul. 2019.

HAIR, J. F. et al. Análise multivariada de dados. Porto Alegre: Bookman, 2005.

HAN, Z. et al. Risk assessment of digital library information security: A case study. **Electronic Library**, v. 34, n. 3, p. 471–487, 2016.

HARKINS, Malcolm. **Managing Risk and Information Security: Protect to Enable.** Nova York, EUA: Apress, 2013.

HIGGINS, Julian PT; GREEN, Sally. **Cochrane Handbook for Systematic Reviews of Interventions**. Disponível em: <http://handbook-5-1.cochrane.org/>. Acesso em: 29 ago. 2019.

HOSS, Marcelo; TEN CATEN, Carla Schwengber. Processo de validação interna de um questionário em uma survey research sobre ISO 9001:2000. **Produto e Produção**, v. 11, n. 2, p. 104–119, 2010.

IQBAL, M.; MATULEVIČIUS, R. Corda security ontology: Example of post-trade matching and confirmation. **Baltic Journal of Modern Computing**, v. 8, n. 4, p. 638–674, 2021.
JOSHI, Chanchala; SINGH, U.K. Umesh Kumar. Information security risks management framework – A step towards mitigating security risks in university network. **Journal of Information Security and Applications**, v. 35, p. 128–137, 2017.

KIM, Hwankuk; LEE, Kyungho; LIM, Jongin. A study on the impact analysis of security flaws between security controls: An empirical analysis of K-ISMS using case-control study. **KSII Transactions on Internet and Information Systems**, v. 11, n. 9, p. 4588–4608, 2017.
KITCHENHAM, Barbara. **Procedures for Performing Systematic Reviews**. Eversleigh, Australia: [s.n.].

LAVILLE, Christian; DIONE, Jean. **A construção do saber: manual de metodologia da pesquisa em ciências humanas**. Porto Alegre: Artmed, 1999.

LI, S. et al. An improved information security risk assessments method for cyber-physical-social computing and networking. **IEEE Access**, v. 6, p. 10311–10319, 2018.

LOWRY, P.B.; DINEV, T.; WILLISON, R. Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. **European Journal of Information Systems**, v. 26, n. 6, p. 546–563, 2017.

MANSFIELD-DEVINE, S. Data governance: going beyond compliance. **Computer Fraud and Security**, v. 2017, n. 6, p. 12–15, 2017.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

MOHER, David et al. Principais itens para relatar Revisões sistemáticas e Meta-análises : A recomendação PRISMA*. **Epidemiol. Serv. Saúde**, v. 24, n. 2, p. 335–342, 2015.

MOORE, Global Network Limited. **Cyber Risk Report Contents**. UK: [s.n.]. Disponível em: <https://www.moore-global.com/MediaLibsAndFiles/media/MooreStephens/Documents/Cyber-risk-report-for-family-offices.pdf>.

MORESI, Eduardo. **Metodologia da pesquisa**. Brasília, DF: Universidade Católica de Brasília, 2003.

NATIONAL INTITUTE OF STANDARS AND TECHNOLOGY. **Managing information security risk: organization, mission, and information system view**. Gaithersbourgh, MD: National Institute of Standards and Technology, 2011.

NIEMIMAA, Elina; NIEMIMAA, Marko. Information systems security policy implementation in practice: From best practices to situated practices. **European Journal of Information Systems**, v. 26, n. 1, p. 1–20, 2017.

NURSE, J.R.C.; CREESE, S.; DE ROURE, D. Security Risk Assessment in Internet of Things Systems. **IT Professional**, v. 19, n. 5, p. 20–26, 2017.

PAN, L.; TOMLINSON, A. A systematic review of information security risk assessment. **International Journal of Safety and Security Engineering**, v. 6, n. 2, p. 270–281, 2016.
PARDAL, Luís; LOPES, Eugénia Soares. **Métodos e Técnicas de Investigação Social**. Porto: Areal Editores, 2011.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar De. **metodologia do trabalho científico : Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico**. 2. ed. Novo Hanburgo: Feevale, 2013.

RAMPAZZO, Lino. **Metodologia científica**. 8. ed. São Paulo: Edições Loyola, 2005.
RICHARDSON, Roberto Jarry. **Pesquisa social: métodos e técnicas**. 3. ed. São Paulo: Atlas, 2015.

RIOS, Isaac Rozas. **ANÁLISE DE FLUXOS INFORMACIONAIS DO PROCESSO DE AQUISIÇÃO POR PREGÃO ELETRÔNICO DA PRÓ-REITORIA ADMINISTRATIVA DA UNIVERSIDADE FEDERAL DA PARAÍBA**João Pessoa, PBUniversidade Federal da Paraíba, , 2019.

SAMPAIO, Rosana Ferreira; MANCINI, Marisa Cotta. ESTUDOS DE REVISÃO SISTEMÁTICA : UM GUIA PARA SÍNTESE. **Revista Brasileira de Fisioterapia**, v. 11, n. 1, p. 83–89, 2007.

SAMPIERI, Roberto Hernández; COLLADO, Carlos Fernández; LUCIO, María Del Pilar Batista. **Metodologia de pesquisa.** 1. ed. São Paulo: McGraw-Hill, 2006.

SANDI, André Quiroga. **Informação e imagem organizacional: percepções e estratégias digitais.** CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO DA REGIÃO SUL, 8., 2007, Passo Fundo. **Anais**...Passo Fundo: Sociedade Brasileira de Estudos Interdisciplinares da Comunicação, 2007

SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva**. Rio de Janeiro: Campus, 2003.

SEVERINO, Antônio Joaquim. **Metodologia do trabalho científico**. 23. ed. São Paulo: Cortez, 2007.

SHAMELI-SENDI, Alireza; AGHABABAEI-BARZEGAR, Rouzbeh; CHERIET, Mohamed. Taxonomy of information security risk assessment (ISRA). **Computers and Security**, v. 57, p. 14–30, 2016.

SHEDDEN, Piya et al. Asset identification in information security risk assessment: A business practice approach. **Communications of the Association for Information Systems**, v. 39, n. 1, p. 297–320, 2016.

SINGH, U.K. Umesh Kumar; JOSHI, Chanchala. Information security risk management framework for University computing environment. **Journal of Information Security and Applications**, v. 19, n. 5, p. 742–751, 2017.

STERGIOPOULOS, George; GRITZALIS, Dimitris; KOUKTZOGLOU, Vasilis. Using formal distributions for threat likelihood estimation in cloud-enabled IT risk assessment. **Computer Networks**, v. 134, p. 23–45, 2018.

STREINER, David L. Being inconsistent about consistency: when coefficient alpha does and doesn´t matter. Journal of Personallity Assessment. v. 80, p. 217-222. 2003.

TAVAKOL, Mohsen.; DENNICK, Reg. Making sense of Cronbach's alpha. International Journal of
Medical Education, v. 2, p. 53-55, 2011. DOI: https://dx.doi.org/10.5116/ijme.4dfb.8dfd. Disponível em: https://www.ijme.net/archive/2/cronbachs-alpha/. Acesso em: 07 abril 2022.

VALENCIA-DUQUE, Francisco Javier; OROZCO-ALZATE, Mauricio. Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. **RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao**, n. 22, p. 73–88, 2017.

VERGARA, Sylvia Constant. **Métodos De Pesquisa Em Administração**. São Paulo: Atlas, 2010.

WALTERBUSCH, Marc; FIETZ, Adrian; TEUTEBERG, Frank. Missing cloud security awareness: investigating risk exposure in shadow IT. **Journal of Enterprise Information Management**, v. 30, n. 4, p. 644–665, 2017.

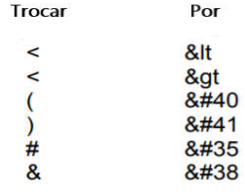
WANGEN, Gaute. Information Security Risk Assessment: A Method Comparison. **Computer**, v. 50, n. 4, p. 52–61, 2017.

XUEPENG, H.; WEI, X. Method of information security risk assessment based on improved fuzzy theory of evidence. **International Journal of Online Engineering**, v. 14, n. 3, p. 188–196, 2018.

ZHAO, Y. et al. Research on architecture of risk assessment system based on block chain. **Computers, Materials and Continua**, v. 61, n. 2, p. 677–686, 2019.

APÊNDICE A - *Checkpoints* de controles para aplicações web

Tipo	*Checkpoints*
Risk Assessment	· Quais aplicações serão afetadas pela mudança requisitada? · Quem são os usuários? Onde estão fisicamente localizados? · A aplicação será anexada a aplicações de missão crítica? Modificará quaisquer dados confidenciais ou críticos? · Onde autenticação adicional de usuário deve ser incorporada? · Onde a aplicação estará fisicamente locaizada na rede? Na DMZ, rede interna? Ele será instalado em um novo equipamento ou compartilhará um servidor existente? Coexistirá bem com as aplicações existentes? · Quaisquer dados considerados sensíveis ou confidenciais serão transmitidos através de links de comunicação externos? · Se o sistema fosse comprometido, resultaria em perda financeira ou perda de reputação? Você pode colocar uma quantia em dólares em qualquer perda? · Qual é o histórico da plataforma do Sistema Operacional em relação à segurança? · O que motivaria alguém a entrar na aplicação? · A aplicação terá alta visibilidade externa, tornando-se um alvo óbvio para os invasores?
Authentication	· Logins com falha devem acionar um bloqueio, após um número determinado de tentativas, que deve ser mantido horas para impedir e desencorajar o atacante de reemitir o ataque. · Toda atividade de autenticação deve ser registrada - logon, logout, logins com falha, solicitações de alteração de senha. Alertas devem ser enviados a um administrador quando a conta estiver bloqueada devido a falhas de login. · Senhas: fortes com no mínimo sete caracteres contendo: números, letras maiúsculas e minúsculas e símbolos. Evitar caracteres repetidos ou seqüenciais. Parecer aleatório e não deve ser encontrada em nenhum dicionário. Expirar periodicamente. Quanto mais crítica a aplicação, menor o intervalo de tempo. · Autenticação de dois fatores para aplicações que requerem alta segurança. · Quando alterar a senha, exija a senha anterior para assegurar que é o proprietário. Após a mudança um email deve ser enviado informando da mudança com sucesso e o usuário deve ser forçado a re-autenticar. · Processo de esqueceu a senha deve forçar a mudança e não a sua "recuperação". O armazenamento de senhas não deve permitir sua recuperação. · O armazenamento de senhas não deve permitir sua recuperação. O uso de questões secretas/respostas é recomendado e a aplicação deve forçar reautenticação após reset. · As senhas e os IDs de usuário devem ser transmitidos e armazenados de maneira segura. Não envie IDs e senhas de usuário em uma mensagem de email em texto não criptografado. Caso isso seja necessário, todas as senhas enviadas em texto não criptografado devem ser criptografadas usando o *Secure Socket Layer* (SSL). · Qualquer lista de senhas deve ser *hashed* (*hash* unidirecional) para garantir que um invasor não consiga ler as informações de autenticação. Para aplicações que exigem segurança intensa, considere combinar um valor *salt* gerado aleatoriamente com o *hash* da senha. · Se for necessário expor as contas de usuário, ou seja, em uma caixa suspensa (*drop down box*), um *alias* deve ser usado para proteger o ID do usuário. · A melhor prática recomenda criptografar toda a transação de logon com SSL. A autenticação baseada em formulários deve usar um POST request para garantir que as credenciais de autenticação não sejam armazenadas em cache no histórico do navegador. O uso do SSL em todas as páginas de login fará isso.· · Use as tags "no cache" para impedir ainda mais que alguém faça backup em uma página de login ou reenvie um logon. · Evitar a funcionalidade “Lembrar-me”, mas se for usada, que seja em partes não críticas

Authorization and Access Control	· Na fase de projeto, as funções de usuário devem ser definidas com base no modelo de "menor privilégio". Se uma função de usuário não modificar dados, ela não deverá ter a oportunidade de editar, excluir ou adicionar dados ao banco de dados crítico. Documente as funções de usuário e determine quem terá a responsabilidade de atribuir usuários a papéis específicos · Na fase de projeto, a equipe deve ter a documentação completa do banco de dados de missão crítica, incluído descrição dos campos e tabelas, comprimento dos dados e valores esperados para um campo, com as permissões atribuídas. · Não armazenar a atividade dos usuários em cache ao manipular informações confidenciais. Clicar na seta para voltar não deve levar às últimas páginas visitadas. · Use direitos de acesso ao sistema de arquivos apenas como uma última defesa. · Testar a aplicação web antes de levar ao ambiente de produção, incluindo revisão da documentação da função do usuário e uma revisão do código que implementa os controles de acesso. O teste de invasão será necessário para garantir que todo controle de acesso foi testado e impede acesso não autorizado.
Session Management	· Como os *cookies* são transmitidos em texto não criptografado, o conteúdo do *cookie* não deve conter ou ser usado para obter informações confidenciais. Os mecanismos de estado não foram projetados para gerenciar informações confidenciais, logo não devem ser usados para autenticar usuários. O usuário deve estar ciente e concordar com o uso de *cookies* pelas aplicações web e deve poder excluir imediatamente o *cookie* e o estado associado a ele. Qualquer informação armazenada no *cookie* não deve ser divulgada a terceiros sem o consentimento dos usuários. · Os IDs de sessão devem ser exclusivos dos usuários e emitidos após a autenticação bem-sucedida, sendo gerados aleatoriamente usando uma fonte de randomização respeitada. O ID da sessão nunca deve conter informações pessoais, sendo sempre atribuídos, nunca escolhido pelo usuário final. O espaço de chaves do *token* deve ser o maior possível para combater adivinhações e outros ataques. Um espaço de chave de 12 dígitos possui 1 trilhão (1012) de possíveis palavras de código diferentes. À medida que a largura de banda aumenta, o tamanho do *keyspace* deve aumentar para manter os hackers afastados. · Os IDs de sessão devem ser protegidos durante todo o ciclo de vida para impedir o seqüestro. eles devem ter um tempo limite definido para sessões inativas. As sessões ativas também devem ter um tempo definido para expirar e regenerar um novo *token* de sessão. Isso reduz a janela de tempo que um hacker teria que invadir uma sessão. · Os IDs de sessão devem ser protegidos com SSL, mudar rotineiramente e sempre durante as principais transições. Para transações altamente seguras, a re-autenticação e um novo ID de sessão devem ser emitidos antes do processamento da transação solicitada. · No *logout*, o ID da sessão deve ser sobrescrito
Data and InPut	· A defesa mais forte contra ataques *Cross-Site Scripting* e *Command Injection* é a validação dos dados de entrada. Se o servidor web validar todos os dados que entram com base em bons critérios conhecidos, diminui as chances de um ataque bem-sucedido. O ônus da validação da segurança deve recair sobre servidor, em vez do cliente. A validação do lado do cliente é frequentemente usada como uma validação primária para "reduzir as viagens de ida e volta ao servidor", mas não deve ser usada como defesa de segurança. · Faça uso estrito da canonização. Saiba o que o servidor está esperando em todos os campos e toda entrada de dados deve ser reduzida para esse formato puro. A validação de entrada permite estabelecer conjuntos de caracteres no servidor para estabelecer a forma canônica que a entrada deve assumir.
Cross Site	Quando uma aplicação Web cria um *output* do *input* do usuário sem validar os dados, a saída pode incluir código malicioso. Todo o código deve ser revisado para variáveis de *input* que resultem em *output* e não tenham validação incluída. Todos os *headers*, *cookies*, *query strings*, campos de formulário e campos ocultos que aceitam entrada são validados com relação a listas de dados aceitáveis. Todo campo deve ter uma lista de valores aceitáveis. Substituir os caracteres conforme figura. 

Command Injection Flaws	· A revisão para SQL *Injection* consome tempo. Todos os parâmetros devem ser examinados para chamadas para fontes externas. Revise o código para qualquer instância em que o *input* de um HTTP *Request* possa ser gravado em qualquer uma dessas chamadas externas. Crie filtros que verifiquem se apenas os dados esperados estão incluídos. Se símbolos forem necessários, assegure-se de que eles sejam convertidos em HTML · O servidor SQL vem com uma variedade de chamadas a procedimentos armazenados *(stored procedures*). Muitos não são usados em aplicações específicas. Conceda aos usuários acesso apenas aos procedimentos armazenados necessários, os demais devem ser armazenados longe da aplicação web. · Sempre que possível, evite comandos de *shell* e chamadas do sistema. Em muitos casos, existem bibliotecas de idiomas que executam as mesmas funções sem usar um interpretador de *shell* do sistema. Onde os comandos do *shell* não puderem ser evitados, o código deve validar a entrada em uma lista de entradas válida para garantir que não inclua código malicioso. · Considere todas as entradas fornecidas como dados, reduzindo, embora não eliminando chamadas externas. · No caso de dados não aceitáveis, deve haver um mecanismo para bloquear e atingir o tempo limite da sessão.
Buffer	· Todo o código que aceita entrada de usuários deve ser revisado para garantir que ele possa identificar uma entrada grande. Depois que dados inadequados são identificados, a atividade deve ser registrada e os dados descartados. · Todos os campos de entrada de dados devem ter comprimentos de campo razoáveis e tipos de dados específicos. Limite a quantidade de texto permitida nos campos de formato livre. · Verifique regularmente o código durante o desenvolvimento para garantir que o projeto seja protegido conforme construído.
Insecure Use of	· Determine quais dados são críticos ou vulneráveis e desenvolva esquemas de criptografia para proteger esses dados. A criptografia adiciona latência; portanto, pode ser prudente aplicar a criptografia a partes específicas do site, por exemplo, às páginas de autenticação. · Revise o código para saber como os dados críticos são protegidos. A revisão também deve identificar como as chaves, senhas e outros segredos são armazenados, carregados, processados e limpos da memória. · Garanta que a escolha de aleatoriedade e algoritmo do desenvolvedor seja de alta qualidade. O programador não deve criar o algoritmo ou a aleatoriedade. Existem inúmeras fontes profissionais disponíveis para ambos
Error Handling	· Durante o desenvolvimento, escreva uma política para lidar com erros. No entanto, um invasor pode aprender uma quantidade enorme de informações sobre um site a partir de mensagens de erro padrão. As mensagens "arquivo não encontrado" ou "acesso negado" fornecem aos hackers informações sobre a estrutura do sistema de arquivos e suas permissões. Determine quais erros devem ser registrados. · Teste minuciosamente para determinar os possíveis erros. Decida a resposta aos erros conhecidos. Escreva páginas de erro que refletem informações suficientes para o usuário final sem fornecer ao usuário informações sobre o código, o sistema de arquivos ou permissões. · Quando ocorre um erro que faz com que o programa ou parte dele falhe, é vital que o sistema "falhe ao fechar", impedindo que um usuário não autorizado chegue ao sistema operacional ou ao site. A ação que causou o erro deve ser registrada e bloqueada. · Registre erros não manipulados em um *log* de eventos. Inclua hora e data, ID do usuário, código de erro, se possível a linha de código. Esse *log* deve ser criptografado, pois é uma informação crítica

Logging	Os logs fornecem responsabilidade individual. Eles são vitais para a reconstrução de eventos que levam à falha do programa · Comece sincronizando seus servidores e o servidor syslog a um servidor de horário. Os carimbos de data e hora devem ser precisos. · Preserve uma linha de base da sua rede para ser usada como um ponto de comparação em caso de falha do sistema. · Os seguintes itens tornarão significativa qualquer entrada de log: Data e hora, Processo de iniciação, Proprietário do processo, e Descrição. · Registre todos os eventos de autenticação e autorização - *logon, logout, logins* com falha. Eles devem incluir data / hora, sucesso / falha, recursos sendo autorizados e o usuário solicitando a autorização, se apropriado, um endereço IP ou local da Tentativa de Autenticação. · Registre todas as atividades do administrador. · Registre a exclusão de qualquer dado. · Registre qualquer modificação nas características dos dados: permissões, localização, tipo de campo. · Arquivos de *log* são dados críticos e devem ser criptografados. Se o seu ambiente for altamente seguro, considere a tecnologia WORM para proteger os arquivos de *log* contra exclusão ou modificação.
Remote	No cenário mais seguro, a administração remota não é permitida. Como isso geralmente não é possível, é necessário projetar um sistema seguro para conexões remotas ao servidor. · Determine como o site deve ser administrado e a ferramenta eficaz para gerenciamento remoto, como uma solução VPN, autenticação forte com tokens ou certificados. Documente quem tem o direito de fazer alterações e quando podem ser feitas. · Assegure-se de que as funções de usuário e de administração estejam claramente definidas e que o programa mantenha as funções para o uso pretendido. Você também pode vincular funções de administrador a endereços IP específicos usando a Filtragem de IP.
Web Application and Server Configuration	Para evitar as vulnerabilidades de servidores: · Configure os discos do servidor para permitir a separação do sistema operacional e do servidor da web. Isso permitirá a restrição da passagem do diretório para locais inadequados. · Verifique se as permissões de arquivo e diretório atribuídas foram aplicadas corretamente usando o modo "menos privilégio". · Desative quaisquer serviços que não sejam usados pelo servidor ou aplicativos da web. · Exclua contas padrão e suas senhas padrão. Renomeie a conta de administrador padrão ou torne-a inacessível. Exclua todas as contas de convidados. · Desabilite funções de depuração. · Edite mensagens de erro para fornecer o mínimo de informações possível a um hacker. · Não use certificados SSL auto-assinados ou certificados padrão. Verifique se os certificados SSL e as configurações de criptografia estão configuradas corretamente. · Escaneie a partir da rede externa para garantir que todas as portas desnecessárias estejam fechadas. Execute varreduras de portas mensalmente para garantir que nada foi alterado. · Atribua manutenção de segurança a um indivíduo ou equipe responsável por: monitorar as vulnerabilidades de segurança mais recentes; testando e aplicando os *patches* mais recentes; atualizar diretrizes de configuração de segurança; verificação regular de vulnerabilidades; relatórios regulares de status à alta gerência; e documentar a prática ou postura geral de segurança.

Fonte: Adaptado para Quadro de SANS (2019, p. 1-12).

APÊNDICE B – Formulário de questionário

Pesquisa para Modelo de Ações de Segurança da Informação

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Este é um convite para você participar da pesquisa "**ANÁLISE DE RISCOS EM SEGURANÇA DA INFORMAÇÃO: modelo simplificado de ações para as Instituições Federais de Ensino Superior (IFES)**", desenvolvida pela doutoranda Rafaela Romaniuc Batista, do Programa de Pós-Graduação em Ciência da Informação da Universidade Federal da Paraíba, sob orientação do Prof. Dr. Wagner Junqueira de Araújo, da UFPB. O objetivo principal do estudo é: Estabelecer elementos conceituais que permitam desenvolver um modelo simplificado de ações para análise de riscos de segurança da informação específico para os setores de tecnologia das instituições federais de ensino superior.

A sua participação é muito importante! O tempo de preenchimento será de aproximadamente 18 minutos.
Sua privacidade será respeitada de modo que suas informações serão sigilosas e nenhuma delas poderá identificá-lo.
Caso não saiba da resposta basta responder coluna do meio e escrever NS ou Não sei em Outros e resposta não será considerada.

** 1. Para você responder este questionário clique em **CONCORDO EM PARTICIPAR DA PESQUISA** abaixo. Ao clicar nesta alternativa, o(a) senhor(a) declara que está ciente do Termo de Consentimento Livre e Esclarecido.*

☐ CONCORDO EM PARTICIPAR DA PESQUISA

Informações Gerais

** 2. Qual a Instituição Federal de Ensino Superior que você atua?*

** 3. Está lotado em qual setor?*

○ Interno no setor de tecnologia
○ Externo ao setor de tecnologia, na Alta Administração (Reitoria...)
○ Externo ao setor de tecnologia, nos Centros/ Departamentos
○ Outro (especifique)

** 4. Qual função exerce?*

○ Gestor de Riscos
○ Gestor da área de Segurança da Informação
○ Outro (especifique)

Estrutura de Governança

A estrutura de governança da instituição direciona para seu programa de gerenciamento de riscos e serve de guia em relação a papéis e responsabilidades, políticas, recursos e segurança no fluxo de informações.

** 5. Há alinhamento entre a gestão de riscos e/ou gestão de segurança da informação e a missão e objetivos estratégicos da instituição presentes no PDI.*

Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
○ Nunca	○ Raramente	○ Ocasionalmente	○ Quase sempre	○ Sempre

Outro (especifique)

** 6. As políticas de segurança da informação são revisadas.*

Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
○ Nunca	○ Raramente	○ Ocasionalmente	○ Quase sempre	○ Sempre

Outro (especifique)

** 7. A sua instituição difunde e exige o cumprimento da política de segurança da informação, das normas de segurança e da legislação vigente acerca do tema.*

Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
○ Nunca	○ Raramente	○ Ocasionalmente	○ Quase sempre	○ Sempre

Outro (especifique)

** 8. Quando há demanda de atualização tecnológica, os setores de tecnologia fazem acompanhamento para estudos de novas tecnologias quanto a possíveis impactos na segurança da informação.*

Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
○ Nunca	○ Raramente	○ Ocasionalmente	○ Quase sempre	○ Sempre

Outro (especifique)

** 9. A correta manipulação de informações, classificadas como Sigilosa, Pessoal ou Ostensiva, é difundida e exigida na sua instituição.*

Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
○ Nunca	○ Raramente	○ Ocasionalmente	○ Quase sempre	○ Sempre

Outro (especifique)

** 10. O setor de tecnologia verifica se a informação por ele produzida, recebida ou custodiada se enquadra em quaisquer hipóteses de sigilo, a fim de adotar as medidas de segurança cabíveis quanto ao tratamento de informação. (Ex: Observância da não divulgação de dados de informação sigilosa a terceiros)*

Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
○ Nunca	○ Raramente	○ Ocasionalmente	○ Quase sempre	○ Sempre

Outro (especifique)

** 11. Os sistemas de informação estruturantes da Universidade possuem seu desenvolvimento e manutenção regidos pela política de segurança ou por normativo específico que disciplinam seu uso, controles e perfis de acesso.*

Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
○ Nunca	○ Raramente	○ Ocasionalmente	○ Quase sempre	○ Sempre

Outro (especifique)

** 12. O setor que coordena as ações de segurança da informação e comunicações encontra-se onde na instituição ? (Pode marcar mais de uma opção)*

- ☐ Interno ao Setor de Tecnologia
- ☐ Externo ao Setor de Tecnologia, na Alta Administração
- ☐ Externo ao Setor de Tecnologia, nos Centros/ Departamentos

- [ ] Não há setor nesse sentido
- [ ] Outro (especifique)

** 13. Em que momento servidores /estagiários da instituição recebem orientações em segurança da informação?*

- ○ Somente durante ambientação
- ○ Somente durante formação inicial
- ○ Durante formação inicial e/ou continuada
- ○ Não há orientações nesse sentido
- ○ Outro (especifique)

** 14. Que medidas de conscientização em segurança da informação há na instituição? (Pode marcar mais de uma opção)*

- [ ] Assinatura de Termo de Responsabilidade em segurança da informação que é difundido e assinado individualmente pelos técnicos administrativos/docentes
- [ ] Campanhas de conscientização direta via email, sistemas e etc
- [ ] Responsabilidades estabelecidas por meio de políticas
- [ ] Campanhas de conscientização amplas em redes sociais
- [ ] Cursos de capacitação
- [ ] Outro (especifique)

15. Quais das políticas de segurança da informação abaixo existem em sua instituição?

- [ ] Política de segurança a informação e comunicação - POSIC
- [ ] Política de gerenciamento de riscos
- [ ] Norma de backup
- [ ] Norma para uso seguro da rede
- [ ] Norma para desenvolvimento seguro
- [ ] Norma para uso de correio eletrônico
- [ ] Norma para uso de dispositivos móveis
- [ ] Outro (especifique)

** 16. Como a cultura de segurança da informação e comunicações (SIC) é promovida na sua instituição? (Pode marcar mais de uma opção)*

- [ ] Estabelece treinamentos, ciclo de palestras, seminários, reuniões e outros eventos que contribuam para o constante processo de compartilhamento e absorção do conhecimento nos domínios da SIC.
- [ ] Promove a troca de conhecimento e experiências no contexto e domínios de SIC por meio de grupos de trabalho formalmente instituídos com a presença de profissionais da área de SIC
- [ ] Designa profissionais da área de SIC para participarem da elaboração do planejamento estratégico e da programação orçamentária do órgão ou entidade na qual mantenham vínculo.
- [ ] Estabelece no planejamento estratégico e tático ações que contemplem os aspectos de formação educacional, retenção e compartilhamento do conhecimento em SIC.
- [ ] Outro (especifique)

** 17. Quem ou que comissão/comitê toma decisão sobre riscos de SIC? (Pode marcar mais de uma opção)*

- [ ] Comitê de Segurança da Informação ou estrutura equivalente
- [ ] Gestor na área de Segurança da Informação
- [ ] Gestor de Riscos
- [ ] Reitoria (Alta Administração)
- [ ] Outro (especifique)

** 18. Quais os canais de comunicação para averiguar sugestões de melhorias ou denuncias de quebra de segurança pela comunidade acadêmica? (Pode marcar mais de uma opção)*

- [ ] E-mail
- [ ] Site institucional
- [ ] Redes sociais
- [ ] Telefone
- [ ] Não existe ponto de contato para se reportar incidentes, fornecer denuncias de quebra de segurança ou sugestões de melhoria
- [ ] Outro (especifique)

Estrutura de Governança - artefatos de gerenciamento de riscos

A estrutura de governança revisa periodicamente alguns artefatos de gerenciamento de riscos como Catalogo de Ativos, Registro de Riscos, Declaração de Tolerância a Riscos dentre outros.

** 19. A instituição registra os principais ativos da instituição em um catálogo de ativos informacionais.*

Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
○ Nunca	○ Raramente	○ Ocasionalmente	○ Quase sempre	○ Sempre

Outro (especifique)

** 20. É possível identificar no catálogo os ativos informacionais críticos que auxiliam nos serviços considerados críticos.*

Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
○ Nunca	○ Raramente	○ Ocasionalmente	○ Quase sempre	○ Sempre

Outro (especifique)

** 21. Os ativos informacionais, quando classificados como sigilosos, possuem procedimentos especiais de controle de acesso físico/lógico.*

Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
○ Nunca	○ Raramente	○ Ocasionalmente	○ Quase sempre	○ Sempre

Outro (especifique)

** 22. Quanto à devida classificação da informação, a instituição estabelece rótulos relativos ao proprietário/ custodiante da informação, estabelecendo suas responsabilidades quando há necessidade de sigilo.*

Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
○ Nunca	○ Raramente	○ Ocasionalmente	○ Quase sempre	○ Sempre

Outro (especifique)

** 23. Há algum documento onde esteja definida a tolerância a risco da instituição? (Pode marcar mais de uma opção)*

- ☐ Declaração de Tolerância a Risco
- ☐ Política de Gestão de Riscos
- ☐ Registro de Riscos
- ☐ Não há documento estabelecido
- ☐ Outro (especifique)

** 24. O setor de tecnologia adequou quais processos à Lei Geral de Proteção de Dados:*

- ☐ Orientação aos funcionários e os contratados da organização a respeito das práticas a serem tomadas para tratamento de dados pessoais.
- ☐ O tratamento de dados pessoais sensíveis ocorre, em regra, com o consentimento do titular.
- ☐ O consentimento para tratamento dos dados pessoais é feito, em regra, por escrito.
- ☐ Criação de relatório de impacto à proteção de dados
- ☐ Confirmação da existência ou fornecimento de acesso a dados pessoais mediante requisição do titular
- ☐ Descrição dos tipos de dados coletados e da metodologia utilizada para a sua coleta de dados.
- ☐ Avaliação de forma permanente das salvaguardas e mecanismos de mitigação de riscos adotados.
- ☐ Canal de comunicação para aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências
- ☐ Receber comunicações da autoridade nacional e adotar providências.
- ☐ Mantém registro das operações realizadas para tratamento de dados pessoais.
- ☐ Nenhuma das anteriores

Análise de Riscos

Possibilidade de compreender os riscos institucionais ao identificar: Riscos, Ameaças e Vulnerabilidades de Ativos.

** 25. Sua instituição faz algum tipo de gestão de riscos de segurança da informação.*

	Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
	○	○	○	○	○

Outro (especifique)

** 26. Os critérios de aceite dos riscos estão definidos e registrados em documento.*

	Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
	○	○	○	○	○

Outro (especifique)

** 27. Sua instituição identifica que tipos de riscos?*

- ☐ Riscos estratégicos (ligados aos objetivos/missões)
- ☐ Riscos táticos (ligados a processo)
- ☐ Riscos operacionais (ligado as operações/sistemas)
- ☐ Não identifica riscos
- ☐ Outro (especifique)

28. Onde são registrados os riscos identificados?

- ☐ Catálogo de ativos

- [ ] Registro de riscos
- [ ] Relatório de identificação, análise e avaliação dos risco
- [ ] Em um documento privado
- [ ] Não são registrados
- [ ] Outro (especifique)

29. Para quais categorias de ativos a instituição identifica riscos ? (Pode marcar mais de uma opção)

- [ ] Pessoas
- [ ] Informação
- [ ] Instalações
- [ ] Tecnologias
- [ ] Outro (especifique)

30. Quais das categorias abaixo fazem parte da análise de riscos feita por sua instituição? (Pode marcar mais de uma opção ou sugerir categorias em Outros)

- [ ] Cálculo dos Riscos (para cada ativo)
- [ ] Ameaças (possíveis para cada ativo)
- [ ] Vulnerabilidades (existentes em cada ativo)
- [ ] Impacto (no negócio caso o risco se torne realidade)
- [ ] Probabilidade (de cada ameaça se tornar realidade)
- [ ] Consequências (do impacto nas propriedades de segurança: Confidencialidade, Integridade, Disponibilidade)
- [ ] Outro (especifique)

Resposta a Riscos - Incidentes

Plano de resposta pré-determina como as instituições pretendem reduzir riscos e responder quando se tornam realidade. Incidentes consistem na materialização do risco e resiliência se preocupa com a continuidade do negócio pós-incidente.

** 31. Gerente de risco e/ou segurança da informação são notificados quando um risco se realiza (incidente ocorre).*

Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
○	○	○	○	○

Outro (especifique)

** 32. A instituição documenta requisitos de continuidade do negócio pelo menos quanto aos ativos críticos.*

Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
○	○	○	○	○

Outro (especifique)

** 33. O plano de continuidade do negócio é testado com que frequência?*

- ○ A cada quatro anos
- ○ A cada dois anos
- ○ Anual
- ○ Semestral
- ○ Não é testado
- ○ Bimestral
- ○ Mensal
- ○ Não é testado
- ○ Desconheço a existência do Plano de Continuidade

** 34. Os danos decorrentes de quebras de segurança são investigados e avaliados.*

Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre

Nunca Raramente Ocasionalmente Quase sempre Sempre

Nunca Raramente Ocasionalmente Quase sempre Sempre

Outro (especifique)

** 35. Quando ocorre casos de quebra de segurança da informação, a instituição aplica ações corretivas e disciplinares.*

Nunca Raramente Ocasionalmente Quase sempre Sempre

Nunca Raramente Ocasionalmente Quase sempre Sempre

Outros (especifique)

** 36. O usuário é responsabilizado pela quebra de segurança ocorrida com a utilização de sua respectiva conta de acesso.*

Nunca Raramente Ocasionalmente Quase sempre Sempre

Nunca Raramente Ocasionalmente Quase sempre Sempre

Outro (especifique)

** 37. A instituição possui uma equipe para tratamento e resposta a incidentes em redes computacionais (ETRI) que atua quando para reparar os danos e tomar as providências necessárias.*

Nunca Raramente Ocasionalmente Quase sempre Sempre

Nunca Raramente Ocasionalmente Quase sempre Sempre

Outro (especifique)

38. A ETRI trabalha de forma coordenada com a gestão de segurança da informação.

Nunca Raramente Ocasionalmente Quase sempre Sempre

Nunca Raramente Ocasionalmente Quase sempre Sempre

39. A ETRI utiliza que modelo?

- Centralizado
- Descentralizado
- Híbrido
- Membros da equipe de TI de forma não exclusiva
- Outro (especifique)

** 40. Onde a instituição documenta a estratégia de resposta e tratamento do risco?*

- Relatório de tratamento de riscos de segurança da informação
- Plano de gerenciamento de riscos
- Não documenta
- Outro (especifique)

** 41. Quais incidentes de segurança relacionados aos aspectos humanos ocorrem com mais frequência na sua instituição? (Ex: Ransomware, Phishing, Engenharia Social, Acesso indevido por compartilhamento de senhas)? Por qual motivo?*

MONITORAMENTO

Monitorar o programa de gerenciamento de riscos da instituição, fazendo análise de sua eficácia, e monitorar as mudanças nos aspectos de segurança da informação.

** 42. Há métricas definidas para monitoramento de risco.*

Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
○	○	◉	○	○

Quais? (especifique)

** 43. Quando há mudanças solicitadas em sistemas, é feito um controle de mudanças nos aspectos relacionados à Segurança da Informação.*

Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
○	○	◉	○	○

Outro (especifique)

** 44. Há monitoramento, nos aspectos de segurança da informação, das mudanças decorrentes de: (Pode marcar mais de uma opção)*

- ☐ Incidentes graves ou modificação nos fatores de risco com alto impacto para os processos da organização
- ☐ Alteração normativa de aplicação imediata
- ☐ Necessidade de modificação significativa imediata nos ativos de informação
- ☐ Atualização da infraestrutura de tecnologia da informação
- ☐ Serviços de tecnologia da informação com periodicidade habitual que impliquem mudanças de um ou mais aspectos de segurança
- ☐ Ampliação do parque computacional
- ☐ Obsolescência prevista de equipamentos e processos
- ☐ Necessidade de adoção de novas tecnologias
- ☐ Outro (especifique)

Monitoramento - Comunicações

A melhoria do processo de gerenciamento de riscos contempla a correta comunicação.

** 45. Há contato direto com o Departamento de Segurança da Informação e Comunicações (DSIC) para o trato de assuntos relativos à segurança da informação.*

Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
○	○	○	○	○

Outro (especifique)

** 46. Os incidentes são informados ao Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR GOV).*

Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
○	○	○	○	○

Outro (especifique)

** 47. A informação a ser disponibilizada pelo setor de tecnologia à comunidade acadêmica é objeto de prévia análise a fim de que se identifiquem parcelas da informação com restrição de acesso.*

Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
○	○	○	○	○

Outro (especifique)

** 48. A publicação de informação institucional é realizada prioritariamente por meio dos canais oficiais do órgão e entidade da APF.*

Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
○	○	○	○	○

Outro (especifique)

Controles de Segurança

** 49. Abaixo tem uma breve lista de controles de segurança. Marque as opções existentes na sua instituição:*

☐ Controles Ambientais: visam proteger recursos computacionais contra danos provocados por desastres naturais e falhas estruturais (ex: sistema de energia, refrigeração, detectores/supressores de água e fogo, redundância, backup etc).

☐ Soluções básicas de segurança (Proteção de tela automática, antivirus, cartão de identificação)

☐ Controle de senhas (Regras de composição (exigência de senhas de qualidade), Tamanhos máximo e mínimo, Tempo de validade, Histórico para não reutilização, Armazenada de forma de hash (via de mão única) ou criptografada, Senhas de demissionários inativadas).

☐ Controles de sistemas (Restrições a sessões concorrentes (mesmo usuário), Limitação do horário de trabalho, Tentativas de acesso controladas, logs)

☐ Controles das Instalações (perímetro de segurança para áreas críticas uso de credenciais físicas, barreiras físicas)

☐ Controles informacionais (classificação da informação, regras de tratamento da informação sigilosa, ativos de informação sigilosos com procedimentos especiais para controle de acesso físico)

☐ Controles de redes (Firewall, VPN, IDS/IPS, logs)

☐ Controles de processo em sistemas (controle de acesso baseado em papéis de usuário, uso do menor privilégio, segregação de funções, normas internas para aquisição ou desenvolvimento de software seguro)

☐ Controles Sociais (Regras para uso de Internet, correio Eletrônico e Mensagens instantâneas)

☐ Controles de Aspectos Humanos (exigir cumprimento das políticas, conscientização e capacitação em segurança, termo de responsabilidade assinado, responsabilização do usuário)

☐ Controles de Bases de Dados (Backups, registro de acessos - logs, controle de integridade)

Outro (especifique)

** 50. Quais desses instrumentos de controle existem na sua instituição? (Marque quantas opções forem necessárias).*

☐ Controle de acesso físico ao ambiente de trabalho

☐ Política de Classificação da Informação

☐ Política de Mesa Limpa/Tela Limpa

☐ Política de Senhas

☐ Termo de responsabilidade e confidencialidade dando ciência do conhecimento das normas e suas principais responsabilidades em relação à segurança da informação

☐ Treinamento em conscientização da segurança da informação

☐ Campanhas de conscientização em segurança da informação.

☐ Outro (especifique)

51. Se possível comente sobre uma necessidade importante de segurança da informação para sua instituição, mas que há fortes limitações para aquisição ou manutenção.

Agradecemos sua contribuição na pesquisa!

ANEXO A – Parecer Consubstanciado do CEP

CENTRO DE CIÊNCIAS DA SAÚDE DA UNIVERSIDADE FEDERAL DA PARAÍBA - CCS/UFPB

PARECER CONSUBSTANCIADO DO CEP

DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: ANÁLISE DE RISCOS EM SEGURANÇA DA INFORMAÇÃO: modelo simplificado de ações de segurança da informação para instituições federais de ensino superior (ifes)

Pesquisador: RAFAELA ROMANIUC BATISTA
Área Temática:
Versão: 2
CAAE: 53211021.4.0000.5188
Instituição Proponente: Universidade Federal da Paraíba
Patrocinador Principal: Financiamento Próprio

DADOS DO PARECER

Número do Parecer: 5.246.672

Apresentação do Projeto:

Trata-se de um protocolo de pesquisa egresso do PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO, do CENTRO DE CIÊNCIAS SOCIAIS APLICADAS, da UNIVERSIDADE FEDERAL DA PARAÍBA, da aluna RAFAELA ROMANIUC BATISTA, sob orientação do Prof. Dr. Wagner Junqueira de Araújo.

Ao longo das últimas três décadas, os mercados de bens e serviços passaram por determinantes transformações perante as exigências do atual contexto da sociedade, fundamentado nos aspectos informacionais e tecnológicos. As organizações, com seus novos padrões administrativos, alicerçados nos planejamentos interativo e liberal, estão compreendendo a informação e o conhecimento como principais componentes do planejamento estratégico, em termos da manutenção do grau da competitividade referente aos seus bens e serviços.

Com base nas novas formas de modelo administrativo, as organizações passaram a entender a importância dos documentos e informações, mediante a preocupação do processo de gerenciamento, de modo a buscar um processo eficaz de organização, armazenamento, disseminação e compartilhamento – processo caracterizado como fluxo formal de informação (DUARTE; SILVA; COSTA, 2007, p. 97-104). Em organizações, o fluxo informacional tornou-se

Endereço: Prédio da Reitoria da UFPB ¿ 1º Andar
Bairro: Cidade Universitária **CEP:** 58.051-900
UF: PB **Município:** JOAO PESSOA
Telefone: (83)3216-7791 **Fax:** (83)3216-7791 **E-mail:** comitedeetica@ccs.ufpb.br

3.4 TÉCNICAS DE COLETA DE DADOS

Para o procedimento de coleta de dados, a pesquisa proposta adotará um conjunto de instrumentos específicos que serão necessários, em virtude da interação entre as pesquisas exploratória e descritiva, para poder alcançar os objetivos propostos pela pesquisa abordada neste projeto. Nesse sentido, para a fase da pesquisa exploratória, serão adotados o procedimento de pesquisa documental e a técnica de pré-teste, e, para a fase da pesquisa descritiva, será adotada a técnica de questionário.

3.4.1 Pesquisa Documental

Presente na fase da pesquisa exploratória, o procedimento da pesquisa documental será estabelecido para se obter os documentos específicos relacionados à segurança da informação, conforme determinado nos objetivos específicos da proposta de pesquisa. No que concerne a esse procedimento, Carvalho (1989, p. 154) observa que a pesquisa documental se vale de documentos cientificamente autênticos, não fraudados, de amplo uso nas ciências sociais e humanas, devido à possibilidade de efetuar análises qualitativas do fenômeno pesquisado. De acordo com Gil (2012, p. 51), apesar da semelhança com a pesquisa bibliográfica, a diferença entre ambas encontra-se na natureza das fontes, pois, enquanto a pesquisa bibliográfica baseia-se nas contribuições de diversos autores sobre um assunto específico, a pesquisa documental faz uso de materiais que não receberam tratamento analítico por completo, podendo ser reelaborados de acordo com os objetivos da pesquisa.

Objetivo da Pesquisa:

Na avaliação dos objetivos apresentados os mesmos estão coerentes com o propósito do estudo:

Objetivo Primário:

Estabelecer elementos conceituais que permitam desenvolver um modelo simplificado de ações para análise de riscos de segurança da informação específico para os fluxos de informação em suportes tecnológicos das instituições federais de ensino superior.

Objetivos Secundários:

a) Realizar Revisão Sistemática de Literatura para conhecimento dos métodos de análise de riscos pesquisados pela comunidade científica;

b) Realizar pesquisa documental dos principais frameworks de gerenciamento de riscos, normas do governo federal, e normas específicas, relacionadas à segurança da informação;

c) Pesquisar a realidade do setor de tecnologia da UFPB quanto às ações, de processo e operacionais, de segurança da informação à luz do framework reconhecido internacionalmente OCTAVE Fort e das normas do governo federal para segurança da informação em setores de tecnologia;

d) Propor checklist de controles de segurança da informação para subsidiar o modelo de ações para análise de riscos para o fluxo de informação em suportes tecnológicos.

Avaliação dos Riscos e Benefícios:

Na avaliação dos riscos e benefícios apresentados estão coerentes com a Resolução 466/2012 CNS, item V "Toda pesquisa com seres humanos envolve riscos em tipos e gradações variadas. Quanto maiores e mais evidentes os riscos, maiores devem ser os cuidados para minimizá-los e a proteção oferecida pelo Sistema CEP/CONEP aos participantes.

No item II.4 - benefícios da pesquisa - proveito direto ou indireto, imediato ou posterior, auferido pelo participante e/ou sua comunidade em decorrência de sua participação na pesquisa.

Riscos:

Não existem riscos que sejam previsíveis com relação à pesquisa, no entanto é preciso considerar a ocorrência de situações de constrangimento do participante quanto à realização das tarefas ao responder o questionário. Em caso de algum momento de ocorrência de constrangimento, o participante poderá, naturalmente, se recusar a executar as tarefas, bem como não responder ao questionário. Ocorrendo a sua desistência em participar da pesquisa, a decisão do participante será respeitada.

Benefícios:

Os benefícios da pesquisa proposta estão na possibilidade do conhecimento das ações de segurança da informação aplicadas ao cotidiano do setor de tecnologia da UFPB, à luz das normas de segurança da informação e do framework OCTAVE Fort, o que beneficiará ações para manutenção e políticas de segurança, bem como a motivação para a simplificação do modelo de ações de segurança para análise de riscos de segurança da informação.

Comentários e Considerações sobre a Pesquisa:

O presente projeto apresenta coerência científica, mostrando relevância para a academia, haja vista a ampliação do conhecimento, onde se busca, principalmente, estabelecer elementos conceituais que permitam desenvolver um modelo simplificado de ações para análise de riscos de segurança da informação específico para os fluxos de informação em suportes tecnológicos das instituições federais de ensino superior.

Considerações sobre os Termos de apresentação obrigatória:

Os Termos de Apresentação Obrigatória, foram anexados tempestivamente.

Recomendações:

RECOMENDAMOS QUE, CASO OCORRA QUALQUER ALTERAÇÃO NO PROJETO (MUDANÇA NO TÍTULO, NA AMOSTRA OU QUALQUER OUTRA), A PESQUISADORA RESPONSÁVEL DEVERÁ SUBMETER EMENDA SOLICITANDO TAL(IS) ALTERAÇÃO(ÕES), ANEXANDO OS DOCUMENTOS NECESSÁRIOS.

RECOMENDAMOS TAMBÉM QUE AO TÉRMINO DA PESQUISA A PESQUISADORA RESPONSÁVEL ENCAMINHE AO COMITÊ DE ÉTICA PESQUISA DO CENTRO DE CIÊNCIAS DA SAÚDE DA UNIVERSIDADE FEDERAL DA PARAÍBA, RELATÓRIO FINAL E DOCUMENTO DEVOLUTIVO COMPROVANDO QUE OS DADOS FORAM DIVULGADOS JUNTO À(S) INSTITUIÇÃO(ÕES) ONDE OS MESMOS FORAM COLETADOS, AMBOS EM PDF, VIA PLATAFORMA BRASIL, ATRAVÉS DE NOTIFICAÇÃO, PARA OBTENÇÃO DA CERTIDÃO DEFINITIVA.

Conclusões ou Pendências e Lista de Inadequações:

TENDO EM VISTA O CUMPRIMENTO DAS PENDÊNCIAS ELENCADAS NO PARECER ANTERIOR E A NÃO OBSERVÂNCIA DE NENHUM IMPEDIMENTO ÉTICO, SOMOS DE PARECER FAVORÁVEL A EXECUÇÃO DO PRESENTE PROJETO, DA FORMA COMO SE APRESENTA, SALVO MELHOR JUÍZO.

Considerações Finais a critério do CEP:

Certifico que o Comitê de Ética em Pesquisa do Centro de Ciências da Saúde da Universidade Federal da Paraíba – CEP/CCS aprovou a execução do referido projeto de pesquisa. Outrossim,

CENTRO DE CIÊNCIAS DA SAÚDE DA UNIVERSIDADE FEDERAL DA PARAÍBA - CCS/UFPB

informo que a autorização para posterior publicação fica condicionada à submissão do Relatório Final na Plataforma Brasil, via Notificação, para fins de apreciação e aprovação por este egrégio Comitê.

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

Tipo Documento	Arquivo	Postagem	Autor	Situação
Informações Básicas do Projeto	PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_1853651.pdf	04/01/2022 22:35:06		Aceito
Outros	CARTA_RESPOSTA.pdf	04/01/2022 22:34:16	RAFAELA ROMANIUC BATISTA	Aceito
Projeto Detalhado / Brochura Investigador	PROJETO_DETALHADO.pdf	04/01/2022 22:31:24	RAFAELA ROMANIUC BATISTA	Aceito
Outros	Ata.pdf	04/01/2022 21:46:39	RAFAELA ROMANIUC BATISTA	Aceito
Outros	CERTIDAO_92_2021_PPGCI63432525 63062868760.pdf	04/01/2022 20:21:35	RAFAELA ROMANIUC BATISTA	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	03_termo_consentimento_livre_esclareci doRafaela.doc	04/01/2022 14:48:07	RAFAELA ROMANIUC BATISTA	Aceito
Cronograma	cronograma.docx	04/01/2022 14:04:10	RAFAELA ROMANIUC BATISTA	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	Termo_anuencia_instituicao.pdf	09/11/2021 20:13:54	RAFAELA ROMANIUC BATISTA	Aceito
Folha de Rosto	folha_rosto_FINAL.pdf	09/11/2021 19:34:15	RAFAELA ROMANIUC BATISTA	Aceito

Situação do Parecer:
Aprovado

Endereço: Prédio da Reitoria da UFPB ¿ 1° Andar
Bairro: Cidade Universitária **CEP:** 58.051-900
UF: PB **Município:** JOAO PESSOA
Telefone: (83)3216-7791 **Fax:** (83)3216-7791 **E-mail:** comitedeetica@ccs.ufpb.br

CENTRO DE CIÊNCIAS DA SAÚDE DA UNIVERSIDADE FEDERAL DA PARAÍBA - CCS/UFPB

Necessita Apreciação da CONEP:
Não

JOAO PESSOA, 16 de Fevereiro de 2022

Assinado por:
Eliane Marques Duarte de Sousa
(Coordenador(a))

Endereço: Prédio da Reitoria da UFPB ¿ 1° Andar
Bairro: Cidade Universitária **CEP:** 58.051-900
UF: PB **Município:** JOAO PESSOA
Telefone: (83)3216-7791 **Fax:** (83)3216-7791 **E-mail:** comitedeetica@ccs.ufpb.br