DISSERTAÇÃO DE MESTRADO PROFISSIONAL

O papel da Auditoria Interna na Gestão de Riscos Cibernéticos em Instituições Financeiras Brasileiras - Estudo sob a perspectiva das três linhas

Lucas Vinicius Andrade Ferreira

Programa de Pós-Graduação Profissional em Engenharia Elétrica
DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

O papel da Auditoria Interna na Gestão de Riscos Cibernéticos em Instituições Financeiras Brasileiras - Estudo sob a perspectiva das três linhas

Lucas Vinicius Andrade Ferreira

Orientador: Prof. Dr. Rafael Timóteo de Sousa Júnior, ENE/FT/UnB

Coorientador: Prof. Dr. Rafael Rabelo Nunes, ADM/FACE/UnB

PUBLICAÇÃO: PPEE.MP.072

BRASÍLIA-DF

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

O papel da Auditoria Interna na Gestão de Riscos Cibernéticos em Instituições Financeiras Brasileiras - Estudo sob a perspectiva das três linhas

Lucas Vinicius Andrade Ferreira

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Prof. Dr. Rafael Rabelo Nunes, ADM/FACE/UnB _____
Coorientador

Prof. Dr. Carlos André de Melo Alves, ADM/FACE/UnB _____
Examinador Interno

Prof. Dr. Laerte Peotta de Melo _____
Examinador Externo

Prof. Dr. Georges Daniel Amvame Nze, ENE/FT/UnB _____
Suplente

FICHA CATALOGRÁFICA

FERREIRA, LUCAS VINICIUS ANDRADE
O papel da Auditoria Interna na Gestão de Riscos Cibernéticos em Instituições Financeiras Brasileiras - Estudo sob a perspectiva das três linhas [Distrito Federal] 2024.
xvi, 92 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2024).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Auditoria Interna	2. Gestão de Riscos
3. Segurança Cibernética	4. Instituições Financeiras
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

FERREIRA, L.V.A. (2024). *O papel da Auditoria Interna na Gestão de Riscos Cibernéticos em Instituições Financeiras Brasileiras - Estudo sob a perspectiva das três linhas*. Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 92 p.

Lucas Vinicius Andrade Ferreira
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Dedico este trabalho a minha amada esposa Juliana e meus amados filhos Pedro e Luísa, aos meus pais Celso e Edina e à minha querida Vovó Ana Nogueira, que este ano completou 93 anos.

AGRADECIMENTOS

Primeiramente a Deus por conceder-me a sabedoria, paciência, motivação e energia necessárias para concluir esta jornada.

A minha esposa Juliana e meus filhos Pedro e Luísa por entenderem minhas ausências, suportar as responsabilidades acadêmicas e profissionais, mas, acima de tudo por todo amor incondicional expressado diariamente.

Aos meus Pais Celso e Edina, por todo o amor, incentivo e carinho desde sempre.

Aos profissionais que concederam entrevista e cederam o seu tempo para a coleta dos dados e informações que subsidiaram nossas conclusões. As vossas experiências e os conhecimentos compartilhados foram fundamentais para construção desse trabalho.

A instituição financeira que trabalho, ao qual dedico 13 anos da minha carreira. Ela mudou a minha vida e da minha família e me faz aprender algo novo todos os dias.

A coordenação da Pós-Graduação em Engenharia Elétrica (PPEE) e a Universidade de Brasília por proporcionar os recursos necessários.

Aos colegas do grupo de estudo e pesquisa coordenado pelo professor Rafael Rabelo, por tornar essa jornada mais leve e por toda produção científica relevante produzida.

A todos os docentes do curso do PPEE, em especial aos professores Rafael Timóteo e Rafael Rabelo, por toda dedicação, tempo, conhecimento e experiências compartilhadas na orientação desse trabalho.

RESUMO

A crescente digitalização do setor financeiro global, impulsionada pela demanda por serviços rápidos e personalizados, enfrenta desafios significativos com o aumento de ataques cibernéticos, exigindo esforço em conjunto de todos os setores da empresa para gerir riscos cibernéticos. Este trabalho teve como objetivo identificar formas pelas quais a auditoria interna pode gerar valor e contribuir para garantir a efetividade e o aprimoramento dos processos relacionados à gestão dos riscos cibernéticos dentro das instituições financeiras brasileiras. Para alcançar o objetivo proposto, foram realizadas entrevistas semiestruturadas com 16 profissionais das áreas de auditoria interna, gestão de riscos e segurança da informação, representando 10 instituições financeiras. A metodologia de análise de conteúdo de Bardin (2016) foi utilizada para analisar os dados coletados, permitindo a categorização e interpretação das práticas atuais e desafios enfrentados na gestão de riscos cibernéticos. Os resultados demonstraram que a auditoria interna desempenha um papel importante na garantia da eficácia dos controles de segurança cibernética, inclusive, dependendo do contexto, realizando testes de invasão para validar controles implementados. A utilização de dados analíticos para realização de auditoria continua também foi destacada como estratégia eficaz para identificar riscos emergentes. No entanto, ainda há desafios significativos a serem enfrentados, como a necessidade de integrar a gestão de riscos cibernéticos na estratégia corporativa das intuições. Para contornar isso, foi sugerida a realização de avaliações com foco nesses riscos na concepção de novos modelos de negócios e produtos. Em complemento, para se aprimorar a gestão de riscos cibernéticos, os achados sugerem a necessidade de atualização constante dos processos e controles em resposta às novas ameaças, bem como a adoção de novas tecnologias, como inteligência artificial e aprendizado de máquina, que podem melhorar a detecção e mitigação de ameaças cibernéticas. O trabalho identificou 53 unidades de contexto ou fatores-chave de sucesso, além de 50 benefícios e 52 desafios a serem enfrentados na participação ativa da auditoria interna na gestão de riscos cibernéticos dentro de instituições financeiras.

ABSTRACT

The increasing digitalization of the global financial sector, driven by the demand for fast and personalized services, faces significant challenges with the increase in cyberattacks, requiring a joint effort from all sectors of the company to manage cyber risks. This work aimed to identify ways in which internal audit can generate value and contribute to ensuring the effectiveness and improvement of processes related to cyber risk management within Brazilian financial institutions. To achieve the proposed objective, semi-structured interviews were conducted with 16 professionals from the areas of internal audit, risk management and information security, representing 10 financial institutions. Bardin's content analysis methodology (2016) was used to analyze the collected data, allowing the categorization and interpretation of current practices and challenges faced in cyber risk management. The results demonstrated that internal audit plays an important role in ensuring the effectiveness of cybersecurity controls, including, depending on the context, conducting penetration tests to validate implemented controls. The use of analytical data to conduct continuous auditing was also highlighted as an effective strategy to identify emerging risks. However, there are still significant challenges to be faced, such as the need to integrate cyber risk management into the corporate strategy of institutions. To overcome this, it was suggested that assessments focusing on these risks be carried out when designing new business models and products. In addition, to improve cyber risk management, the findings suggest the need for constant updating of processes and controls in response to new threats, as well as the adoption of new technologies, such as artificial intelligence and machine learning, which can improve the detection and mitigation of cyber threats. The work identified 53 context units or key success factors, in addition to 50 benefits and 52 challenges to be faced in the active participation of internal audit in cyber risk management within financial institutions.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

BACEN	Banco Central do Brasil
BCBS	*Basel Committee on Banking Supervision*
BCI	*Business Continuity Institute*
C2M2	*Cybersecurity Capability Maturity Model*
CIS	*Center for Internet Security*
CISA	*Cybersecurity Information Sharing Act*
CMN	Conselho Monetário Nacional
COBIT	*Control Objectives for Information and Related Technologies*
COSO	*Committee of Sponsoring Organizations of the Treadway Commission*
CRM	*Cyber Risk Management*
CSF	*Cybersecurity Framework*
DDoS	*Distributed Denial of Service*
ERM	*Enterprise Risk Management*
FAIR	*Factor Analysis of Information Risk*
FEBRABAN	Federação Nacional dos Bancos
GDPR	*General Data Protection Regulation*
GRC	Gestão de Riscos Cibernéticos
IA	Inteligência Artificial
IDS	*Intrusion Detection System*
IEC	*International Electrotechnical Commission*
IIA	*The Institute of Internal Auditors*
IoT	*Internet of Things*
IPS	*Intrusion Prevention System*
ISACA	*Information Systems Audit and Control Association*
ISO	*International Organization for Standardization*
KPI	*Key Performance Indicator*
KRI	*Key Risk Indicator*
LGPD	Lei Geral de Proteção de Dados

MISP	*Malware Information Sharing Platform*
ML	*Machine Learning*
MTTD	*Mean Time to Detect*
MTTR	*Mean Time to Repair*
NIST	*National Institute of Standards and Technology*
NYCRR	*New York Codes, Rules and Regulations*
NYDFS	*New York State Department of Financial Services*
PCI-DSS	*Payment Card Industry Data Security Standard*
PENTEST	*Penetration Testing*
SFN	Sistema Financeiro Nacional
SGSI	Sistema de Gestão de Segurança da Informação
SIEM	*Security Information and Event Management*
SWIFT	*Society for Worldwide Interbank Financial Telecommunication*
TI	Tecnologia da informação
UEBA	*User and Entity Behavior Analytics*

1 INTRODUÇÃO

Nos últimos anos, tem-se observado um movimento crescente de digitalização dos serviços e transformação digital em diversos setores, com destaque para o setor bancário e financeiro ao redor do mundo. A digitalização tem proporcionado maior eficiência, agilidade e conveniência para os clientes, além de permitir que as instituições financeiras inovem e ofereçam novos produtos e serviços. Tecnologias como inteligência artificial, blockchain e big data estão sendo amplamente adotadas para melhorar a experiência do cliente, aumentar a segurança e otimizar operações internas [1] [2].

A transformação digital no setor financeiro é impulsionada pela demanda dos consumidores por serviços mais rápidos e personalizados, bem como pela necessidade de reduzir custos operacionais e melhorar a competitividade [3]. Os bancos digitais, por exemplo, têm desafiado os bancos tradicionais ao oferecerem serviços bancários completos via aplicativos móveis, sem a necessidade de agências físicas [1].

No entanto, essa crescente digitalização também trouxe consigo um aumento significativo nos ataques cibernéticos contra bancos e instituições financeiras. Globalmente e no Brasil, esses ataques têm se tornado mais sofisticados e frequentes. Um estudo da [4] revelou que o setor financeiro é um dos mais visados por cibercriminosos devido ao alto valor das informações e transações financeiras. Entre os tipos de ataques mais comuns estão o phishing, ransomware e ataques de negação de serviço (DDoS).

No Brasil, a criação do PIX pelo Banco Central do Brasil (BACEN), um sistema de pagamento instantâneo, revolucionou a forma como transações financeiras são realizadas [5]. Embora o PIX tenha trazido inúmeros benefícios, como transações rápidas e gratuitas, ele também se tornou um alvo para atividades fraudulentas. Criminosos têm utilizado o PIX para aplicar golpes e lavar dinheiro de maneira eficiente [6]. Um exemplo notório é o aumento de sequestros relâmpago, onde as vítimas são forçadas a transferir grandes quantias via PIX [7]. Além disso, há registros de golpes de engenharia social, onde os criminosos se passam por representantes de instituições financeiras para obter dados pessoais e realizar transferências não autorizadas [8].

As empresas enfrentam desafios significativos ao gerir os riscos cibernéticos e enfrentar ameaças que podem impactar diretamente seus lucros e resultados. A rápida evolução das tecnologias e a sofisticação dos ataques cibernéticos exigem que as instituições financeiras adotem medidas de segurança cada vez mais robustas e atualizadas [9]. Entre os desafios estão a necessidade de treinamento contínuo dos colaboradores, a implementação de sistemas de detecção e resposta a incidentes cibernéticos e a manutenção da conformidade com regulamentos de segurança de dados.

A Lei Geral de Proteção de Dados (LGPD) no Brasil, por exemplo, impõe requisitos rigorosos sobre a proteção de dados pessoais, exigindo que as empresas implementem controles adequados para evitar vazamentos de informações. A não conformidade com essas regulamentações pode resultar em multas significativas e danos à reputação da organização [10].

O modelo de três linhas é uma abordagem eficaz para auxiliar as organizações na Gestão de Riscos Corporativos. Esse modelo divide as responsabilidades de gerenciamento de risco em três linhas: a

primeira linha é composta pelas unidades operacionais que gerenciam diretamente os riscos no dia a dia; a segunda linha inclui funções de gestão de riscos e conformidade que monitoram e facilitam a implementação de práticas de gestão de risco; e a terceira linha é a auditoria interna, que fornece uma avaliação independente da eficácia dos controles internos e das práticas de gestão de risco [11].

A implementação do modelo de três linhas permite uma abordagem estruturada e coordenada para a gestão de riscos, garantindo que todos os níveis da organização estejam envolvidos na identificação, avaliação e mitigação de riscos cibernéticos [12].

A auditoria interna desempenha um papel de destaque dentro das organizações ao avaliar a eficácia dos controles de segurança cibernética, identificando fragilidades e recomendando melhorias [12]. A auditoria interna também verifica a conformidade com regulamentos e políticas internas, garantindo que as práticas de segurança estejam alinhadas com as melhores práticas do mercado.

Além disso, a auditoria interna pode conduzir avaliações de risco para identificar potenciais ameaças antes que sejam exploradas por atacantes. [13] destaca a atuação da auditoria interna e seus benefícios dentro da estrutura de uma das maiores instituições financeira dos Estados Unidos que sofreu uma violação de dados e o trabalha destaca ações de conformidade que evitariam os danos.

Dessa forma, a auditoria interna não apenas contribui para a segurança da informação, mas também protege a reputação e a sustentabilidade financeira da organização. Ao fornecer uma avaliação independente e objetiva dos controles e processos de segurança, a auditoria interna ajuda a garantir que as organizações estejam bem preparadas para enfrentar as ameaças cibernéticas e manter a confiança de seus clientes e stakeholders [14].

1.1 MOTIVAÇÃO E JUSTIFICATIVA

Nas últimas décadas, a segurança cibernética tornou-se uma preocupação central para organizações de todos os setores. Este foco crescente reflete não apenas a complexidade e a sofisticação das ameaças digitais, mas também o impacto potencial devastador que estas podem ter sobre os negócios. A revisão da literatura recente revela uma série de tendências e desafios que as empresas enfrentam em relação à segurança cibernética e gestão de riscos [15] [16] [17].

A primeira tendência notável é o aumento dos orçamentos e investimentos em segurança cibernética, um reflexo direto das mudanças nas estratégias corporativas. De acordo com um relatório da [2], as empresas estão reconhecendo a necessidade de alocar mais recursos para proteger seus ativos digitais. Esse aumento no investimento é muitas vezes justificado pela necessidade de enfrentar ameaças mais sofisticadas e frequentes, bem como pela pressão para cumprir regulamentos rigorosos de proteção de dados.

Apesar do aumento nos investimentos, muitos desafios persistem. Um deles é o gerenciamento de riscos cibernéticos ineficazes ou inexistentes. [18] destaca que muitas organizações ainda carecem de processos robustos para identificar, avaliar e mitigar riscos cibernéticos. Esse déficit é frequentemente devido à falta de expertise interna e à subestimação das ameaças cibernéticas por parte da alta administração.

Outra tendência preocupante é o crescimento contínuo do número de ataques cibernéticos. Estudos

como [15] e [19] documentam um aumento significativo nos incidentes cibernéticos, incluindo ataques de ransomware, phishing e violações de dados. Esses ataques não só são mais frequentes, mas também mais sofisticados, dificultando a defesa das organizações.

Paralelamente ao aumento dos ataques, observa-se um crescimento na quantidade de vulnerabilidades de sistemas. [16] aponta que a complexidade crescente dos sistemas de TI e a rápida adoção de novas tecnologias frequentemente resultam em vulnerabilidades não corrigidas. Essas falhas são pontos de entrada atraentes para cibercriminosos, exacerbando o risco de ataques bem-sucedidos.

Os custos associados a violações de dados e paralisações de sistemas também estão em ascensão. Segundo o relatório da [4], as empresas estão enfrentando despesas cada vez maiores para recuperar dados, restaurar operações e lidar com as repercussões legais e reputacionais de incidentes de segurança. Estes custos podem ser devastadores, especialmente para pequenas e médias empresas que podem não ter os recursos financeiros para suportar tais perdas.

A reputação de uma organização também pode sofrer danos significativos como resultado de violações de segurança. [20] destaca que a confiança dos consumidores e parceiros pode ser seriamente abalada por incidentes de segurança, levando a uma perda de negócios e oportunidades. A recuperação da confiança é um processo demorado e pode ter um impacto duradouro na viabilidade e sucesso da organização.

Outro desafio crítico é a falta de cooperação e compartilhamento de informações sobre ameaças e vulnerabilidades. [18] sugere que a colaboração entre organizações pode melhorar significativamente a capacidade coletiva de responder a ameaças cibernéticas. No entanto, muitas empresas são relutantes em compartilhar informações devido a preocupações com a privacidade e a competição.

A conformidade com leis e regulamentos de proteção de dados e privacidade é outro aspecto essencial da segurança cibernética. [21]. discute como a não conformidade pode expor as empresas a penalidades severas e sanções regulatórias. Com a proliferação de regulamentações como o Regulamento Geral sobre a Proteção de Dados (GDPR) na Europa e a Lei Geral de Proteção de Dados (LGPD) no Brasil, as empresas devem estar atentas para evitar multas substanciais e danos à reputação.

Além disso, a auditoria interna desempenha um papel fundamental na gestão dos riscos cibernéticos, conforme orientações estabelecidas por várias normas e portarias que reforçam a necessidade de controles robustos e de governança adequada no ambiente financeiro sobre o tema. A exemplo da Portaria CGU nº 2.821/2024 [22], que trata da gestão de competências na atividade de auditoria interna governamental, destacando os conhecimentos em segurança ciberneetica, e da Resolução CMN nº 4.893/2021 [23], que dispõe sobre a necessidade de definição de política de segurança cibernética pelas instituições finaneiras.

Finalmente, a falta de priorização de riscos com base em sua probabilidade e impacto potencial é um problema significativo. [24] argumenta que muitas organizações não possuem um processo estruturado para avaliar a criticidade dos riscos cibernéticos, resultando em alocações ineficazes de recursos e esforços de mitigação.

Sendo assim, a presente pesquisa se justifica pois dentro das instituições financeiras a auditoria interna desempenha papel central na resolução de diversas questões estratégicas e devido ao impacto potencial associado aos risco cibernéticos, se faz premente a identificação de táticas, técnicas e abordagens

para que a atuação da auditoria interna enquanto terceira linha se concretize em ganhos.

1.2 PROBLEMA DE PESQUISA

A segurança cibernética é uma prioridade para organizações de diversos setores, refletindo tanto a complexidade crescente das ameaças digitais quanto o impacto potencial dessas ameaças nos negócios. Estudos recentes apontam algumas tendências importantes, como o aumento dos investimentos em segurança cibernética [2], à medida que empresas alocam mais recursos para proteger seus dados e cumprir regulamentações [21]. No entanto, desafios significativos permanecem, como a gestão ineficiente ou inexistente de riscos cibernéticos, muitas vezes agravada pela falta de especialização interna e subestimação dos riscos pela alta direção [18].

Além disso, o número de ataques cibernéticos continua a crescer, com eventos como ransomware e phishing tornando-se cada vez mais frequentes e sofisticados [15]. A complexidade dos sistemas de TI e a rápida adoção de novas tecnologias também geram vulnerabilidades que são exploradas por cibercriminosos [16]. Esses ataques têm consequências financeiras graves, com custos crescentes para recuperar dados, retomar operações e lidar com as repercussões legais e de reputação. Pequenas e médias empresas, em particular, podem ser gravemente afetadas por esses custos [4].

A reputação das organizações é outro ponto sensível, já que incidentes de segurança podem prejudicar a confiança de clientes e parceiros, resultando em perdas de negócios e de oportunidades [20]. A falta de colaboração entre empresas no compartilhamento de informações sobre ameaças também representa um obstáculo para uma defesa coletiva mais eficaz [18]. Além disso, a conformidade com leis como a LGPD torna-se indispensável para evitar multas [21].

Por fim, muitas empresas falham em priorizar adequadamente os riscos com base em sua gravidade e probabilidade, o que leva a uma alocação inadequada de recursos para mitigação [24].

Diante desse cenário, os seguintes dilema serviram como ponto de partida para o campo de estudo desse trabalho:

Problema de pesquisa 1:

Como a auditoria interna pode contribuir para a mitigação de riscos cibernéticos nas instituições financeiras crescente de ameaças cibernéticas emergentes?

Problema de pesquisa 2:

Como a auditoria interna pode contribuir para a para aprimoramento dos controles de segurança nas instituições financeiras em um cenário de transformação digital com uma crescente digitalização de serviços?

Com o intuito de estabelecer uma relação entre as diversas variáveis, guiar o desenvolvimento metodológico e a análise de dados deste trabalho, foram definidas as seguintes hipóteses a serem aferidas:

Hipótese 1:

A auditoria interna, quando devidamente estruturada e qualificada, contribui significativamente para a identificação precoce e tratamento de riscos cibernéticos.

Hipótese 2:

A auditoria interna, ao identificar e avaliar de forma sistemática os controles de segurança e riscos cibernéticos, pode melhorar significativamente as práticas de gestão de riscos em instituições financeiras.

1.3 OBJETIVOS

1.3.1 OBJETIVO GERAL

Identificar formas pelas quais a auditoria interna pode gerar valor e contribuir para garantir a efetividade e o aprimoramento dos processos relacionados à gestão dos riscos cibernéticos nas instituições financeiras brasileiras.

1.3.2 OBJETIVOS ESPECÍFICOS

- Analisar a função da Auditoria Interna na gestão de riscos cibernéticos.
- Explorar como a auditoria interna pode avaliar e monitorar os controles de segurança cibernética.
- Investigar como a auditoria interna pode interagir junto as demais linhas (gestores operacionais, funções de gestão de riscos e conformidade) para garantir a segurança cibernética
- Analisar as responsabilidades e desafios enfrentados pela auditoria interna ao atuar próximo a gestão de riscos cibernéticos.
- Avaliar as melhores práticas e parâmetros utilizados pela auditoria interna para medir a efetividade dos controles de segurança cibernética.
- Examinar como as novas tecnologias e mudanças emergentes podem influenciar as atividades da auditoria interna.
- Identificar práticas bem-sucedidas e fatores-chave de sucesso para a auditoria interna atuar junto a gestão de riscos cibernéticos.

1.4 METODOLOGIA DE PESQUISA

A pesquisa exploratória descrita neste trabalho utilizou um estudo descritivo com abordagem qualitativa para identificar como a Auditoria Interna pode gerar valor e contribuir para a Gestão dos Riscos Cibernéticos em instituições financeiras. Para isso, foram realizadas entrevistas semiestruturadas com profissionais do setor financeiro e de empresas de auditoria externa.

A pesquisa exploratória visou esclarecer conceitos e estabelecer uma base para estudos futuros, enquanto o estudo descritivo buscou detalhar a distribuição das variáveis estudadas, sem explorar hipóteses causais. A análise qualitativa de dados foi empregada para compreender o fenômeno em seu contexto social, permitindo a formulação de inferências a partir das entrevistas [25].

As entrevistas semiestruturadas, que combinam perguntas abertas e pré-definidas, permitiram flexibilidade ao entrevistador, ajustando o roteiro conforme necessário [26]. A coleta de dados foi complementada por uma revisão de literatura sobre Gestão de Riscos Cibernéticos, o modelo de três linhas e o papel da Auditoria Interna, seguida pela análise de conteúdo de Lawrence Bardin [27].

A amostra de entrevistados foi composta por profissionais com experiência em controles internos, gestão de riscos e auditoria, especificamente em processos relacionados à tecnologia da informação e segurança cibernética, no setor financeiro. A escolha desse setor se deve à sua alta dependência tecnológica e à sua vulnerabilidade a ataques cibernéticos, além de seu papel crítico na economia global [4] [9].

Os entrevistados foram selecionados de forma a refletir a representatividade das instituições financeiras brasileiras, considerando o porte e a atividade internacional, conforme a regulação do BACEN [28]. Durante as entrevistas, os dados foram registrados e analisados qualitativamente, assegurando a confidencialidade dos participantes, que foram identificados por códigos anônimos. O roteiro da entrevista foi baseado em bibliografia apresentada no referencial teórico e estruturado em sete blocos temáticos, totalizando 14 questões.

1.5 ESTRUTURA DA DISSERTAÇÃO

A presente dissertação está organizada em cinco capítulos, iniciando com esta introdução. Os capítulos subsequentes abordarão o referencial teórico sobre riscos cibernéticos, auditoria interna e as suas interseções, a metodologia de pesquisa, a apresentação e análise dos resultados, seguidos pela discussão e as conclusões finais.

1. Introdução: Apresenta o contexto, a motivação, os problemas de pesquisa, os objetivos e a metodologia adotada.

2. Referencial Teórico: Discorre sobre a gestão de riscos cibernéticos, o modelo das três linhas e o papel da auditoria interna.

3. Metodologia: Detalha o método de pesquisa, a amostra de entrevistados, o roteiro das entrevistas e a abordagem de análise de dados.

4. Resultados: Apresenta os achados da pesquisa, categorizados em temas, conforme similaridade identificada na análise do conteúdo das entrevistas, examina esses resultados à luz da literatura existente e discute as suas implicações.

5. Conclusão: Resumo das principais conclusões, limitações do estudo e sugestões para futuras pesquisas.

Essa estrutura foi definida para permitir um fluxo lógico e coeso, facilitando a compreensão sobre a importância da auditoria interna na gestão de riscos cibernéticos e contribuindo para o aprimoramento das práticas de segurança nas organizações financeiras.

2 REFERENCIAL TEÓRICO

2.1 GESTÃO DE RISCOS CIBERNÉTICOS

A Gestão de Riscos Cibernéticos, ou Cyber Risk Management (CRM) refere-se ao processo de identificar, avaliar e responder aos riscos cibernéticos associados aos sistemas de informação de uma organização [15]. Ele se alinha com o gerenciamento de riscos corporativos mais amplo, incorporando medidas de segurança nos processos organizacionais para garantir a continuidade operacional e a proteção contra atividades cibernéticas maliciosas [29].

Os pesquisadores notaram a importância de uma abordagem sistemática ao CRM. Tal abordagem começa com uma compreensão clara dos ativos digitais de uma organização e suas potenciais vulnerabilidades [24]. A organização deve então avaliar as ameaças a esses ativos, que podem variar de internas, como negligência dos funcionários, a externas, como ameaças persistentes avançadas [30]. A próxima etapa envolve a determinação dos impactos potenciais dessas ameaças e a tolerância ao risco da organização [31]. Com base nessas descobertas, as estratégias de mitigação de risco são então formuladas e implementadas.

A eficácia do CRM pode ser aprimorada atualizando continuamente metodologias de avaliação de risco para acompanhar as ameaças em evolução [16]. Embora não exista uma abordagem única para o gerenciamento de riscos cibernéticos, padrões como o ISO 27005 fornecem uma metodologia bem reconhecida e sistemática para gerenciar riscos cibernéticos [32]. Eles oferecem diretrizes para avaliar riscos, determinar respostas e revisar planos de gerenciamento de riscos.

No entanto, a complexidade e a natureza dinâmica das ameaças cibernéticas exigem que as organizações considerem métodos mais sofisticados. A aplicação de inteligência artificial e aprendizado de máquina no gerenciamento de riscos cibernéticos pode ajudar na detecção, mitigação e resposta em tempo real a ameaças cibernéticas [31]. Apesar de seu potencial, a aplicação dessas tecnologias precisa de um exame cuidadoso devido aos riscos associados a falsos positivos e vieses algorítmicos não intencionais.

2.1.1 ENTENDENDO O RISCO CIBERNÉTICO

Compreender as várias dimensões do risco cibernético é essencial para que as organizações protejam dados confidenciais e mantenham a resiliência operacional [33]. Além disso, uma compreensão das fontes e motivações por trás dos ataques cibernéticos permite o desenvolvimento de estratégias de mitigação eficazes [27]. Pesquisadores e profissionais enfatizam a necessidade de estruturas abrangentes para identificar, avaliar e gerenciar o risco cibernético [18] [34].

O cenário de risco cibernético é caracterizado por sua natureza dinâmica e em constante evolução, tornando-o um domínio desafiador para navegar [35] [36]. Os rápidos avanços na tecnologia, juntamente com a crescente sofisticação dos adversários cibernéticos, aumentaram a complexidade e a frequência dos ataques cibernéticos [15]. Além disso, a proliferação de dispositivos conectados à Internet e a expansão do ecossistema digital expandiram a superfície de ataque, ampliando as possíveis consequências de incidentes

cibernéticos [19] [37]. Uma compreensão abrangente do cenário de riscos cibernéticos é fundamental para avaliar possíveis vulnerabilidades e implementar estratégias eficazes de gerenciamento de riscos.

A avaliação precisa do risco cibernético é importante para priorizar recursos e implementar proteções apropriadas. Várias metodologias e estruturas foram desenvolvidas para avaliar o risco cibernético de forma abrangente. O Instituto Nacional de Padrões e Tecnologia (NIST) fornece uma estrutura amplamente adotada, que inclui identificar e priorizar ativos, avaliar vulnerabilidades, determinar a probabilidade e o impacto de ameaças e calcular pontuações de risco [38]. Além disso, abordagens quantitativas, como modelos probabilísticos de avaliação de riscos, permitem que as organizações estimem o impacto financeiro de incidentes cibernéticos [18].

Para gerenciar com eficácia o risco cibernético, as organizações devem considerar as possíveis consequências de uma violação ou incidente cibernético. [39] sugere que os custos associados ao risco cibernético podem ser classificados em custos diretos (por exemplo, honorários advocatícios, notificações de violação) e custos indiretos (por exemplo, danos à reputação, rotatividade de clientes). Além disso, as consequências reputacionais de um incidente cibernético podem ter efeitos duradouros no valor da marca de uma organização e na confiança do cliente [20]. Portanto, entender as implicações financeiras e reputacionais do risco cibernético é vital para tomar decisões informadas sobre estratégias de mitigação de risco.

O risco cibernético emana de uma ampla variedade de fontes, incluindo agentes mal-intencionados, vulnerabilidades tecnológicas e erros humanos. Atores de ameaças, como cibercriminosos, hacktivistas e estados-nação, exploram vulnerabilidades em sistemas de computador para obter acesso não autorizado e causar danos [15]. Vulnerabilidades, como bugs de software e configurações incorretas, criam oportunidades para ataques cibernéticos [19]. Além disso, ameaças internas, como funcionários ou contratados descontentes, representam um risco significativo ao comprometer intencionalmente ou não os sistemas de informação [40]. A compreensão dessas fontes permite que as organizações implementem medidas preventivas e desenvolvam planos eficazes de resposta a incidentes [34].

As consequências do risco cibernético podem ser graves, variando de perdas financeiras a danos físicos. As organizações enfrentam implicações financeiras substanciais devido aos custos associados à resposta a incidentes, recuperação e possíveis consequências legais [41]. Além disso, os ataques cibernéticos podem causar danos à reputação, corroendo a confiança do cliente e afetando a viabilidade dos negócios a longo prazo [30]. Em alguns casos, sistemas de infraestrutura crítica podem ser direcionados, potencialmente colocando em risco a segurança pública [34]. A crescente interconectividade dos sistemas digitais amplia o impacto potencial do risco cibernético, exigindo estratégias robustas de gerenciamento de risco [33].

Para gerenciar com eficácia o risco cibernético, as organizações devem implementar uma série de estratégias de mitigação. Essas estratégias englobam medidas preventivas, como controles robustos de segurança cibernética, treinamento de funcionários e práticas seguras de desenvolvimento de software [42]. A implementação de fortes controles de acesso, segmentação de rede e aplicação regular de patches de software pode ajudar a reduzir vulnerabilidades e impedir ataques em potencial [43]. As organizações também devem estabelecer uma equipe de resposta a incidentes, conduzir programas regulares de treinamento e conscientização e desenvolver procedimentos robustos de backup e recuperação para minimizar o impacto

de incidentes cibernéticos [38] [39].

A resposta a incidentes e os planos de recuperação são importantes para minimizar o impacto dos ataques cibernéticos e o seguro de risco cibernético pode fornecer proteção financeira contra possíveis perdas [33]. Parcerias e colaborações entre organizações, governos e especialistas em segurança cibernética podem facilitar o compartilhamento de informações e a defesa coletiva contra ameaças cibernéticas [18]. Além disso, alavancar tecnologias avançadas, como inteligência artificial e aprendizado de máquina, pode aprimorar os recursos de detecção de ameaças e permitir uma resposta oportuna [44].

O risco cibernético, em seu sentido mais abrangente, refere-se a qualquer risco associado à perda financeira, interrupção ou dano à reputação de uma organização devido a algum tipo de falha em seus sistemas de tecnologia da informação. É um subconjunto do risco de segurança da informação e refere-se ao risco de dano resultante da perda de integridade, disponibilidade, confidencialidade, não repúdio e autenticidade das informações e dados utilizados por uma organização [15].

O National Institute of Standards and Technology (NIST) define o risco cibernético como "o nível de impacto que um evento potencial de segurança cibernética teria em uma organização"[38]. Este é um aspecto significativo da estrutura de segurança cibernética mais ampla do NIST, que enfatiza a compreensão e o gerenciamento do risco de segurança cibernética em termos de seus impactos potenciais na capacidade de uma organização de cumprir sua missão [45]. Essa estrutura é uma abordagem baseada em risco para gerenciar a segurança cibernética e foi projetada para ser aplicável a organizações de todos os tamanhos e tipos [46].

Tradicionalmente, o risco cibernético tem sido definido no contexto da segurança da informação, com foco no dano potencial resultante de uma falha ou violação dos sistemas de informação [32]. Segundo a International Organization for Standardization (ISO), refere-se ao "potencial de uma determinada ameaça explorar vulnerabilidades de um ativo ou grupo de ativos e, assim, causar danos à organização"[32]. Essa definição enfatiza a interação entre ameaças, vulnerabilidades e ativos organizacionais, colocando os dados e sistemas da organização no centro da análise, conforme Figura 2.1.

A Information Systems Audit and Control Association (ISACA) define o risco em termos do potencial de perda devido a uma ameaça que explora uma vulnerabilidade e recomenda um processo para identificar e gerenciar riscos com base em seu impacto potencial nas operações e objetivos de uma organização, mantendo o risco em linha ao apetite de risco definido pela organização, conforme Figura 2.2 [47]. Na estrutura do COBIT 2019, a ISACA enfatiza que o gerenciamento de riscos requer a compreensão dos objetivos da organização e das ameaças e vulnerabilidades que podem impedir que esses objetivos sejam alcançados [48].

A complexidade do risco cibernético está em sua natureza em constante evolução. À medida que a tecnologia avança, também aumentam as vulnerabilidades e os impactos potenciais associados ao seu uso indevido. Esse aspecto dinâmico do risco cibernético significa que a definição deve ser flexível o suficiente para abranger as inúmeras fontes potenciais de risco, incluindo aquelas que ainda estão por surgir [16].

Além disso, à medida que as organizações operam cada vez mais em ecossistemas digitais, o risco cibernético foi expandido para abranger riscos intraorganizacionais e sistêmicos. Essa visão leva em

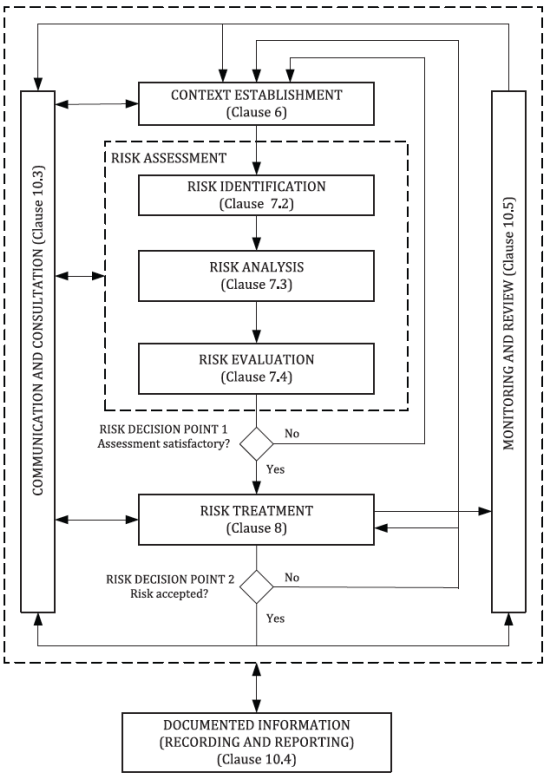

Figura 2.1: Processo de Gestão de Riscos em Segurança na Informação

Fonte: [32]

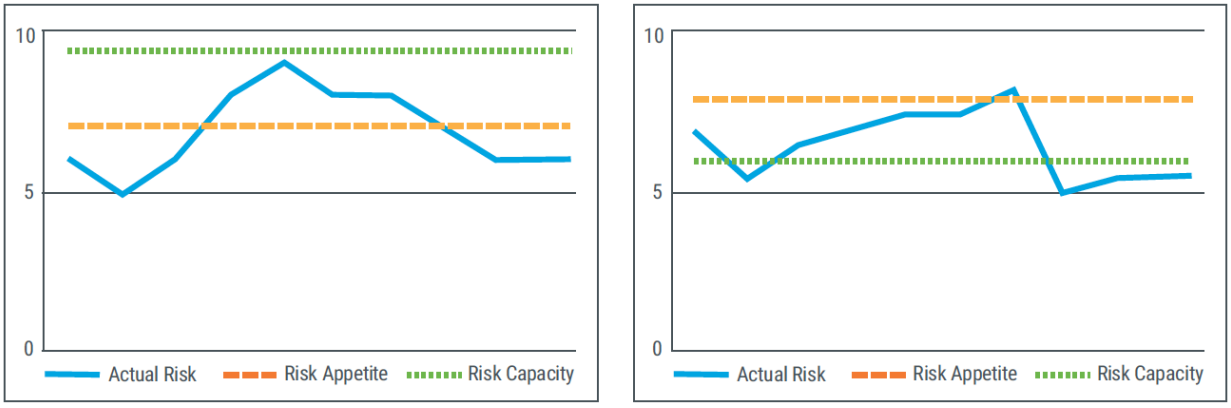

Figura 2.2: Capacidade de Risco, Apetite ao Risco e Risco Medido

Fonte: [47]

consideração a interconectividade e as interdependências inerentes a uma economia em rede, considerando os impactos em cascata que um único evento cibernético pode ter em várias organizações e setores. Essa perspectiva sistêmica reconhece as implicações sociais mais amplas do risco cibernético, destacando assim a necessidade de ação coletiva e governança para gerenciar esses riscos [49].

As violações de dados representam um dos tipos mais comuns de risco cibernético, referindo-se a incidentes em que indivíduos não autorizados obtêm acesso a dados confidenciais [35]. De acordo com o Relatório de investigações de violação de dados de 2020 da Verizon, 94,6% das violações são motivadas

por ganhos financeiros, geralmente levando a danos monetários e de reputação substanciais [50].

Os ataques de ransomware, em que um software malicioso criptografa os dados da vítima até que um resgate seja pago, tornaram-se cada vez mais comuns. O ataque WannaCry de 2017 afetou mais de 200.000 computadores em 150 países, causando danos estimados em bilhões de dólares [51].

As ameaças internas vêm de dentro da organização, como funcionários, ex-funcionários, contratados ou associados, que têm acesso a informações confidenciais [30]. As ameaças internas podem ser acidentais (por exemplo, um funcionário clica acidentalmente em um link de phishing) ou maliciosas (por exemplo, um funcionário insatisfeito vaza informações deliberadamente).

Phishing é um risco cibernético que envolve tentativas fraudulentas de adquirir informações confidenciais, como nomes de usuário, senhas e detalhes de cartão de crédito, disfarçando-se como uma entidade confiável em comunicações eletrônicas [16]. O phishing pode ocorrer por e-mail, sites, mensagens de texto ou telefonemas. Uma variante crescente do phishing, o spear-phishing, é mais direcionado e usa informações detalhadas sobre a vítima para tornar o ataque mais convincente [2].

A engenharia social é um método de manipulação de pessoas para realizar ações ou divulgar informações confidenciais, muitas vezes por meio de fraude. Os cibercriminosos que usam engenharia social geralmente exploram a confiança e a ingenuidade dos indivíduos para obter acesso a sistemas e dados [49]. Os ataques de engenharia social podem variar de simples pretextos (criar um cenário falso para persuadir alguém a liberar informações) até campanhas complexas e multicanais.

A espionagem cibernética representa outro risco significativo, em que atores estatais ou não estatais usam meios digitais para roubar informações confidenciais para ganhos estratégicos, econômicos ou políticos [52]. O caso do Stuxnet, um worm de computador malicioso que se acredita ser um produto da inteligência dos EUA e de Israel, revelou o impacto no mundo real dessas ameaças cibernéticas [53].

Risco cibernético de terceiros – é a exposição potencial a ameaças e vulnerabilidades de segurança cibernética decorrentes da associação de uma organização com entidades terceirizadas. É um componente significativo do risco cibernético geral enfrentado por uma organização, necessitando de estratégias abrangentes de avaliação e mitigação de riscos [52]. Em 2020, hackers infiltraram-se em um software da SolarWinds incorporando código malicioso nas suas atualizações, o que posteriormente permitiu o acesso não autorizado às redes de inúmeras empresas e agências governamentais que utilizavam este software [54].

Por fim, ataques a infraestruturas críticas, como redes elétricas ou redes de transporte, podem ter graves implicações sociais. O ataque cibernético de 2015 à rede elétrica da Ucrânia demonstrou o sério impacto de tais ameaças [55].

2.1.2 RELEVÂNCIA DA GESTÃO DO RISCO CIBERNÉTICO

A crescente frequência e sofisticação dos ataques cibernéticos reforçaram a importância do gerenciamento de riscos cibernéticos. A [2] observou em sua pesquisa "Global Digital Trust Insights" que 65% dos executivos estão aumentado seus orçamentos em segurança cibernética devido a mudanças de estratégia. Essas estatísticas ressaltam a necessidade de uma abordagem abrangente para o gerenciamento de

riscos cibernéticos [2]. Uma estratégia eficaz de gerenciamento de riscos cibernéticos permite que as organizações operem com mais segurança e eficiência, protegendo seus valiosos ativos de informações contra várias ameaças cibernéticas [36].

O gerenciamento eficaz de riscos cibernéticos pode ajudar as organizações a minimizar a probabilidade e o impacto de ataques cibernéticos, reduzindo assim perdas financeiras e danos à reputação [38]. Na era da digitalização, uma violação de dados ou paralisação do sistema pode levar a perdas financeiras significativas, repercussões legais e danos à reputação de uma organização. De acordo com o relatório da [4], "Cost of a Data Breach Report", o custo médio global de uma violação de dados em 2023 foi de cerca de US$ 4,35 milhões, valor que vem crescendo ano a ano conforme Figura 2.3.

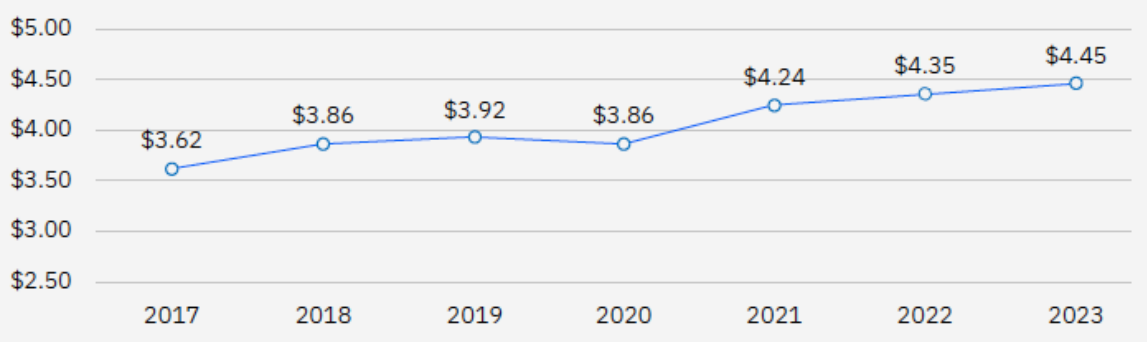

Figura 2.3: Histórico do custo médio global de uma violação de dados

Fonte: [4]

Além disso, uma forte estratégia de gestão de riscos cibernéticos ajuda a garantir a continuidade das operações e serviços, pois as interrupções devido a incidentes cibernéticos podem ter repercussões significativas [56]. O relatório [4] indicou que houveram empresas que experimentaram tempo de inatividade superior a 200 dias após uma violação cibernética, afetando significativamente as operações da organização e a confiança dos clientes.

Segundo [4], o custo médio associado a uma violação de dados no setor financeiro fica atrás apenas do setor de saúde e a frente de diversos outros setores como energia, indústria e transporte, conforme Figura 2.4.

O compartilhamento de informações é outro aspecto importante do gerenciamento de riscos cibernéticos. Ao compartilhar informações sobre ameaças e vulnerabilidades, as organizações podem se preparar melhor e responder a incidentes cibernéticos [57]. Iniciativas do governo e da indústria, como o Cybersecurity Information Sharing Act (CISA) nos Estados Unidos, facilitam esse tipo de troca de informações.

O gerenciamento de riscos cibernéticos também facilita a conformidade com os padrões e regulamentos do setor. Uma estratégia eficaz de gerenciamento de riscos garante a adesão às leis e regulamentos relacionados à proteção de dados e privacidade, evitando assim possíveis penalidades e sanções por não conformidade [21].

Uma abordagem baseada em risco para segurança cibernética permite que as organizações concentrem seus recursos onde podem ser mais eficazes. Isso significa priorizar os riscos com base em sua

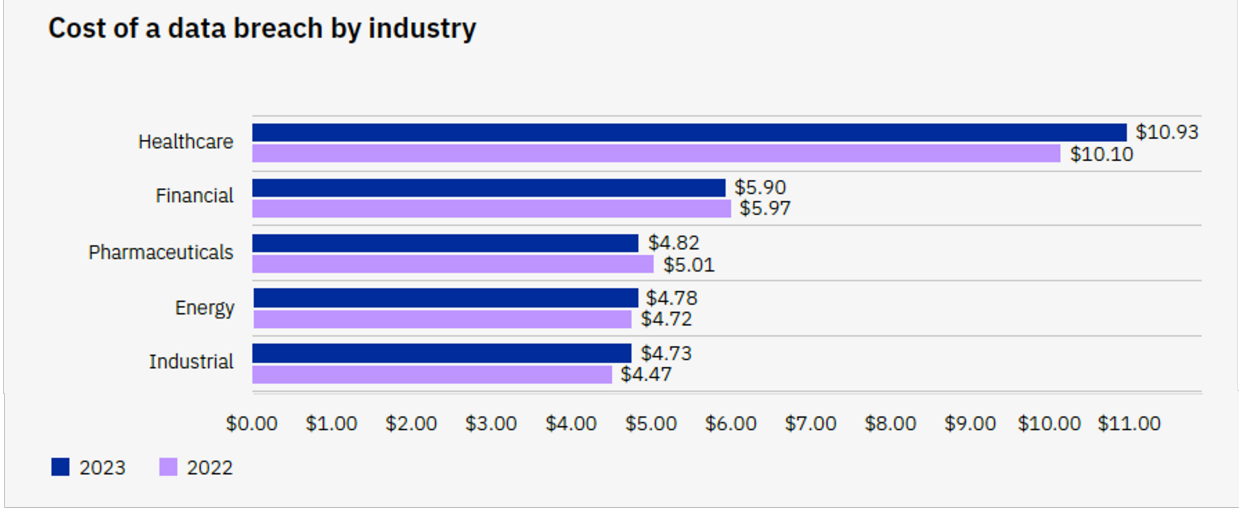

Figura 2.4: Custo médio de uma violação de dados por setor

Fonte: Adaptado de [4]

probabilidade e impacto potencial [24]. Um estudo conduzido por [58] revelou que as empresas que adotam práticas rigorosas de gerenciamento de riscos cibernéticos tiveram menos violações de segurança e eram menos propensas a serem afetadas por elas.

Nos últimos anos, a gestão de riscos cibernéticos evoluiu para um componente essencial da governança corporativa [59]. À medida que as ameaças cibernéticas continuam aumentando em frequência, sofisticação e impacto potencial, os conselhos corporativos e a alta administração estão reconhecendo a importância do gerenciamento de riscos cibernéticos. Portanto, o CRM não é apenas uma questão técnica, mas também uma questão de importância estratégica corporativa [40].

2.1.2.1 PROTEGER INFORMAÇÕES CONFIDENCIAIS

Informações confidenciais, como identificação pessoal, registros de saúde e financeiras, correm continuamente o risco de serem acessadas, mal utilizadas ou roubadas [49]. Proteger essas informações é uma tarefa crítica para empresas, governos e indivíduos para garantir privacidade, integridade de dados e conformidade com leis e regulamentos [60].

A proteção dessas informações tornou-se um aspecto essencial da estratégia de gerenciamento de riscos de todas as organizações [61]. O crescimento exponencial da quantidade e valor dos dados gerados e armazenados em formato digital acentua a importância da segurança cibernética.

A gestão de risco cibernéticos abrange a identificação, avaliação e mitigação das vulnerabilidades que podem comprometer a confidencialidade, a integridade, e a disponibilidade dos sistemas de informação de uma organização [42], com a confidencialidade possibilitando o acesso restrito aos dados, a integridade confirmando a autenticidade dos dados e a disponibilidade garantindo que os dados são acessíveis a partes autorizadas quando necessário [62]. A aplicação desses princípios tem sido um componente central em uma variedade de estruturas de proteção de informações confidenciais [20].

Proteger dados de identificação pessoal e segredos comerciais corporativos, é premente. Invasões que resultem na perda ou comprometimento de tais dados podem levar a perdas financeiras significativas, danos à reputação e consequências legais. As melhores práticas para proteger informações confidenciais envolvem uma combinação de soluções tecnológicas, estruturas de governança robustas e vigilância constante [63].

A criptografia é um método padrão para proteger dados confidenciais, tornando-os ilegíveis para usuários não autorizados. No entanto, a criptografia é tão boa quanto a estratégia de gerenciamento de chaves usada. Portanto, estratégias rigorosas de gerenciamento de chaves e controle de acesso devem ser empregadas juntamente com a criptografia para melhorar a proteção de dados [64].

A adoção de soluções tecnológicas, fortes estruturas de governança e estratégias eficazes de identificação e mitigação de ameaças são componentes essenciais de uma abordagem abrangente para o gerenciamento de riscos cibernéticos [36].

2.1.2.2 MANTER A RESILIÊNCIA OPERACIONAL

A resiliência operacional tornou-se uma das prioridades mais altas para as organizações em diversos setores. A dinâmica das operações de negócios globais e a suscetibilidade a diversas ameaças exigem o desenvolvimento de sistemas robustos que possam resistir, se adaptar e se recuperar rapidamente de interrupções [65].

Refere-se à capacidade de uma organização de manter, proteger e restaurar rapidamente os recursos operacionais para garantir a prestação contínua de serviços durante interrupções. O conceito não é sobre prevenir interrupções, mas sim permitir que a organização lide com eficácia quando ocorrem interrupções [57].

Esse tema é fundamental para a sobrevivência e sucesso das organizações. Isso se refere à capacidade de uma entidade de continuar entregando produtos ou serviços em um nível predefinido aceitável, apesar de eventos operacionais adversos, como violações de dados, falhas de sistema, desastres naturais ou outras interrupções [65]. Uma fusão de gerenciamento de riscos, planejamento de continuidade de negócios e técnicas de recuperação de desastres mantem esses mecanismos de resiliência robustos o para suportar os cenários adversos mais significantes para a organização [56].

2.1.2.3 GARANTIR OS INTERESSES DAS PARTES INTERESSADAS

A gestão das partes interessadas é um aspecto crítico de qualquer negócio, pois ajuda na criação de um ambiente de negócios sustentável e próspero [66]. As partes interessadas abrangem um amplo espectro, incluindo funcionários, clientes, fornecedores, acionistas e comunidades, entre outros. Suas necessidades, expectativas e interesses são diversos e, muitas vezes, concorrentes. Encontrar um equilíbrio entre esses interesses é a essência da proteção dos interesses das partes interessadas, o que resulta em reputação comercial aprimorada, lealdade das partes interessadas e lucratividade de longo prazo [3] .

O gerenciamento bem-sucedido envolve a gestão das preocupações desse publico nos processos de

tomada de decisão estratégica e a garantia de que seus interesses sejam priorizados e protegidos [29].

As partes interessadas, confiam na capacidade da empresa de proteger seus ativos digitais contra possíveis ameaças cibernéticas que podem levar a perdas financeiras substanciais, danos à reputação e interrupção dos negócios, impactando negativamente as partes interessadas [59]. Desta maneira, a aplicação efetiva do Gerenciamento de Riscos Cibernéticos é indispensável para proteger os interesses das partes interessadas [43].

2.2 MODELO DE TRÊS LINHAS

O Modelo das Três Linhas, originalmente conhecido como Modelo das Três Linhas, apresenta uma estrutura abrangente com a finalidade de gerenciar riscos e estabelecer uma governança eficaz nas organizações [11]. Sua revisão mais recente, realizada pelo Institute of Internal Auditors (IIA), em 2020, reformulou o modelo para aperfeiçoar sua adaptabilidade, escalabilidade e facilidade de implementação em uma ampla gama de estruturas organizacionais [67].

As revisões de 2020, mantendo a essência do modelo, tentaram aumentar a sua versatilidade e eliminar algumas das limitações inerentes. Uma mudança importante é a remoção do termo "defesa", sugerindo uma mudança de funções rígidas e isoladas para uma abordagem mais fluida e cooperativa para o gerenciamento de riscos [67]. O modelo atualizado também busca enfatizar a supervisão e os papéis estratégicos do conselho de administração e enfatizar que todas as partes de uma organização contribuem para sua governança e gestão de riscos [11].

O Modelo das Três Linhas fornece uma abordagem estruturada para o gerenciamento de riscos que alinha os objetivos organizacionais com as estratégias de identificação, avaliação e mitigação de riscos [68].

Conforme destacado por IIA [11], o modelo divide as responsabilidades institucionais em três linhas distintas, conforme Figura 2.4.

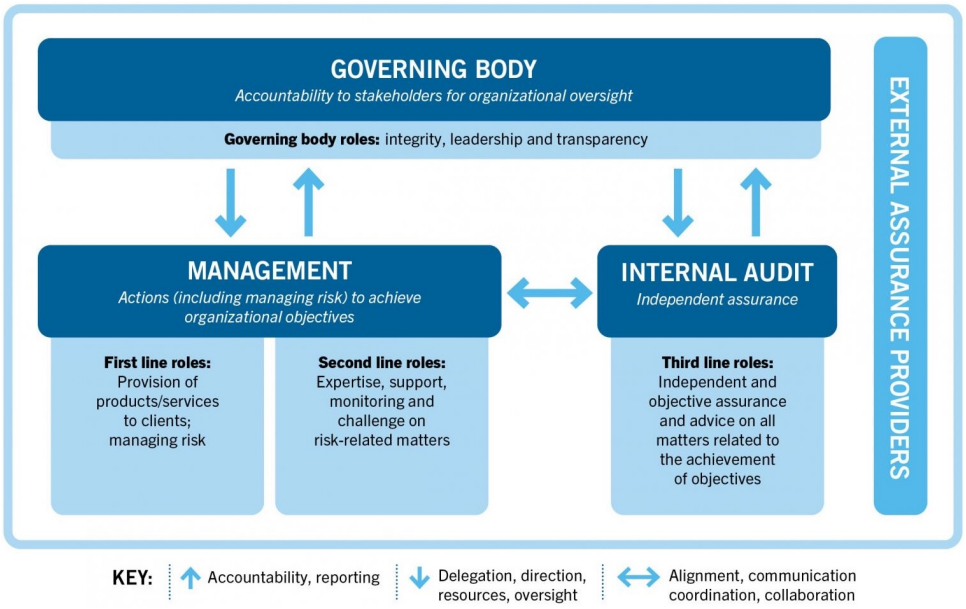

Figura 2.5: Modelo de Três Linhas

Fonte: [11]

A primeira linha inclui a gestão operacional, responsável por identificar, avaliar e gerenciar riscos em suas respectivas áreas. A segunda linha consiste em funções especializadas de gerenciamento de risco e conformidade, que supervisionam o monitoramento de riscos, o desenvolvimento de políticas e a implementação de controles internos. Finalmente, a terceira linha compreende a função de auditoria interna, que fornece garantia e avaliação independente das práticas de gestão de riscos [11].

O modelo enfatiza os papéis distintos, mas complementares, da primeira linha (operações), da segunda linha (funções de risco e conformidade) e da terceira linha (auditoria interna), ao mesmo tempo em que enfatiza que a responsabilidade pela gestão de riscos e controles internos cabe, em última análise, à administração [67].

O modelo ainda redefine os papéis da gestão organizacional, gestão de riscos e auditoria interna, visualizando-os como componentes interconectados, mas distintos de uma estrutura de governança abrangente [11]. Isso representa uma mudança da perspectiva de "defesa"do modelo original para um ponto de vista de "linhas de visão", com foco na responsabilidade organizacional e no gerenciamento de riscos, e não apenas no controle de riscos [69].

Em 2013, o Comitê de Organizações Patrocinadoras da Comissão Treadway (COSO) integrou o Modelo de Três Linhas em seu Controle Interno – Estrutura Integrada atualizada [70]. Essa integração reforça a relevância do modelo em auxiliar as organizações a cumprir suas obrigações regulatórias e melhorar as práticas de gestão de riscos. Além disso, diretrizes regulatórias, como as fornecidas pelo Basel Committee on Banking Supervision [57], enfatizam a importância da implementação do Modelo de Três Linhas como parte de uma estrutura robusta de gerenciamento de riscos no setor financeiro.

A adoção do Modelo de Três Linhas oferece diversos benefícios às organizações. Em primeiro lugar, facilita uma abordagem sistemática e integrada à gestão e governança de riscos, levando a uma melhor identificação e mitigação de riscos [68]. Em segundo lugar, o modelo melhora a comunicação e

coordenação de riscos em diferentes linhas, promovendo uma compreensão unificada dos riscos e objetivos de controle. Em terceiro lugar, o modelo permite que as organizações otimizem a alocação de recursos, alavancando sinergias e evitando a duplicação de esforços [71].

Esse modelo ajudou as organizações a criar uma distinção clara entre responsabilidades, garantir verificações e contrapesos adequados e promover uma cultura de risco positiva [72]. Notavelmente, as atualizações recentes do modelo ampliaram ainda mais sua relevância e utilidade, particularmente no contexto de ambientes de negócios mais complexos e acelerados [71].

2.2.1 PRIMEIRA LINHA

A primeira linha, compreendendo a gestão operacional e as funções de negócios, desempenha um papel relevante na identificação e gestão de riscos dentro de suas respectivas áreas [11]. Por meio de avaliação proativa de riscos, design de controles e monitoramento contínuo, a primeira linha é responsável por incorporar o gerenciamento de riscos às operações diárias. Essa linha garante que a propriedade do risco seja investida nas unidades de negócios e promove uma cultura de consciência de risco em toda a organização [68]. A integração da gestão de riscos na primeira linha permite a identificação oportuna de riscos emergentes, mitigação de ameaças potenciais e aproveitamento de oportunidades estratégicas [66].

[67] afirma que a gestão operacional engloba os donos dos processos que estão diretamente envolvidos nas operações do negócio e são responsáveis pelo desenho, execução, monitoramento e melhoria das atividades e processos. No contexto do Modelo das Três Linhas, esses indivíduos, como parte da Primeira Linha, têm a responsabilidade de garantir que as atividades e processos estejam alinhados com a estratégia e os objetivos da organização [11]. Esses indivíduos são críticos, pois trabalham na linha de frente e muitas vezes são os primeiros a identificar quaisquer discrepâncias ou anomalias que possam indicar riscos.

A primeira linha tem a obrigação de manter o controle sobre os processos da organização, enfatizando que essa função não deve ser delegada ou contornada [11]. Esse envolvimento prático desde a primeira linha garante que as estratégias de gestão de riscos da organização estejam alinhadas com os objetivos organizacionais mais amplos, auxiliando assim na otimização da eficiência operacional [73].

A eficácia da primeira linha geralmente está ligada à sua capacidade de implementar e sustentar um ambiente de controle robusto. Isso inclui, mas não está limitado a definir o tom no topo, promover valores éticos e promover um ambiente que incentive os funcionários a agir com responsabilidade [61] [67]. Um estudo conduzido por [68] [73] demonstrou uma correlação direta entre a força do ambiente de controle e a eficácia geral da gestão de riscos nas organizações. Assim, a primeira linha desempenha um papel fundamental na formação do ambiente de controle e, posteriormente, na eficácia do processo de gestão de riscos da organização.

Além disso, deve-se haver interação constante entre a primeira linha e as outras duas linhas no Modelo de Três Linhas. Uma interação equilibrada entre a primeira linha e a segunda linha (funções de gestão de riscos e compliance), bem como a terceira linha (auditoria interna), pode contribuir significativamente para uma gestão de riscos e governança eficazes na organização [68]. Isso destaca a necessidade de cooperação e comunicação aberta entre essas três linhas para atingir objetivos organizacionais comuns.

2.2.2 SEGUNDA LINHA

A segunda linha abrange funções de gerenciamento de riscos, conformidade e controle que fornecem supervisão independente e suporte à primeira linha. Os profissionais de risco e conformidade colaboram com as equipes operacionais para estabelecer políticas, procedimentos e estruturas de controle robustas [11].

Essa linha garante que os níveis de apetite e tolerância ao risco estejam bem definidos, além de monitorar a aderência aos requisitos regulatórios e políticas internas [67]. Além disso, a segunda linha valida a eficácia dos controles, avalia a qualidade dos dados de risco e suporta relatórios e comunicação de riscos [11]. Por meio dessa colaboração, a segunda linha fortalece a governança de riscos e facilita a tomada de decisões oportuna em toda a organização.

No centro da Segunda Linha estão indivíduos e comitês que têm um papel de monitoramento dentro de uma organização. Esse grupo de pessoas, muitas vezes composto por profissionais de gerenciamento de riscos, conformidade e controle financeiro, fornece suporte para a Primeira Linha monitorando a eficácia dos controles, garantindo a conformidade com políticas e procedimentos e fornecendo garantia de que os riscos estão sendo gerenciados adequadamente [69]. Essa função de supervisão preenche a lacuna entre o gerenciamento operacional e a Avaliação Independente da Terceira Linha, permitindo que a organização seja proativa em vez de reativa em sua abordagem de gerenciamento de riscos [72].

A Segunda Linha desempenha um papel fundamental no aprimoramento das capacidades gerais de gerenciamento de riscos de uma organização. Ao definir padrões e expectativas, fornecer aconselhamento e orientação, monitorar a conformidade e reportar à alta administração, a Segunda Linha fornece uma camada de verificações e balanços que ajuda a mitigar o potencial de anulação da administração e atividades fraudulentas [70]. Também permite uma compreensão mais profunda da cultura, apetite e capacidade de risco, informando assim os processos de tomada de decisão estratégica [11].

Além disso, a segunda linha fornece uma abordagem estruturada para identificar, avaliar e monitorar os riscos que podem impedir o alcance das metas organizacionais [73]. Enquanto a primeira linha é a principal responsável pelo gerenciamento de riscos, a segunda linha fornece as ferramentas e metodologias necessárias, garantindo que o risco seja gerenciado dentro do apetite de risco da organização [11].

Alguns pesquisadores argumentam que o papel da segunda linha deve ser mais proativo do que reativo. Eles acreditam que a segunda linha não deve apenas apoiar a primeira linha, mas também se envolver em atividades que identificam riscos emergentes [68]. Além disso, a segunda linha, devido à sua natureza, requer uma gama diversificada de habilidades, incluindo análise de dados, resolução de problemas e habilidades de comunicação, para monitorar e controlar os riscos com eficácia [73].

Existem diversas aplicações práticas para a Segunda Linha, por exemplo, no setor de serviços financeiros, as equipes de conformidade e as unidades de gerenciamento de risco atuam como a segunda linha, implementando estratégias de mitigação de risco, monitorando a conformidade regulatória e fornecendo orientação às unidades operacionais [74]. No setor de saúde, os departamentos de garantia de qualidade e os comitês de governança clínica desempenham papéis semelhantes, garantindo a adesão aos padrões de saúde e segurança, mantendo a segurança do paciente e melhorando a prestação de serviços [75].

2.2.3 TERCEIRA LINHA

A terceira linha compreende a função de auditoria interna, que avalia de forma independente e fornece garantia sobre a eficácia da gestão de riscos e controles internos [11]. Os auditores internos avaliam a adequação das práticas de gerenciamento de riscos, avaliam a eficácia do controle e identificam áreas de melhoria [76]. Sua função vai além da conformidade e dos relatórios financeiros para abranger riscos estratégicos, tendências emergentes e eficácia da governança. Ao conduzir auditorias independentes e fornecer avaliações objetivas, fortalece a responsabilidade, a transparência e a governança corporativa [2].

Opera independentemente das duas primeiras linhas e fornece garantia objetiva ao conselho e à administração da organização sobre a eficácia da governança, gestão de riscos e controle interno [11]. A independência é fundamental para garantir avaliações imparciais, o que ajuda a manter a integridade nas organizações. A sua importância foi sublinhada em numerosos estudos; por exemplo, [3] observaram uma correlação positiva entre uma função robusta de auditoria interna e uma melhor governança corporativa.

Uma das suas principais funções é fornecer uma avaliação imparcial e equilibrada dos procedimentos de gerenciamento de risco existentes. Ele fornece garantia de que a primeira e a segunda linhas estão funcionando de forma eficaz e auxilia no refinamento constante dos processos organizacionais [75]. Além disso, auxilia na preservação da integridade da organização ao identificar eventuais lapsos nas medidas de controle e sugerir retificações [11].

Além disso, a auditoria interna serve de ponte entre a gestão da organização e seu conselho ou auditores externos. Ele comunica suas descobertas a essas partes, garantindo uma tomada de decisão informada [77]. A importância da comunicação na função da terceira linha foi destacada por [14]que descobriram que a comunicação eficaz por parte da auditoria interna melhorou as capacidades de supervisão de riscos do conselho.

A auditoria interna também é responsável pela prestação de serviços de assessoria, destinados a agregar valor e melhorar as operações da organização. Esses serviços podem incluir a sugestão de melhorias nos processos de gerenciamento de risco, ajudando a projetar e implementar novos controles e fornecendo treinamento para a equipe sobre conceitos de risco e controle [11]. Um estudo de [71] constatou que esses serviços de consultoria podem levar a melhorias significativas na governança corporativa, principalmente quando são adaptados ao contexto e às necessidades específicas da organização.

Outra responsabilidade é avaliar a conformidade da organização com leis, regulamentos e políticas internas. Isso ajuda a identificar potenciais riscos legais e regulatórios e garante que a organização mantenha uma imagem pública favorável e evite multas dispendiosas [77]. [78] descobriu que auditorias internas eficazes podem reduzir significativamente os riscos regulatórios e melhorar a conformidade de uma organização com leis e regulamentos relevantes.

Por último, a comunicação constitui uma parte relevante das suas responsabilidades. A terceira linha precisa se comunicar de forma eficaz com o conselho e a gestão, garantindo que eles entendam os resultados das auditorias e as implicações para a organização [14]. Também precisa estabelecer contato com auditores externos, reguladores e outras partes interessadas, conforme necessário. A importância da comunicação eficaz foi enfatizada por [78], onde foi destacado seu papel no aumento da eficácia e impacto da auditoria interna na percepção de partes relacionadas.

2.3 A TERCEIRA LINHA E A GESTÃO DE RISCOS CIBERNÉTICOS

A segurança cibernética é um componente crítico das operações de negócios modernas, particularmente no contexto do gerenciamento de riscos. Dentro da estrutura de gerenciamento de riscos, uma abordagem frequentemente usada é o modelo das Três Linhas. A terceira linha em um ambiente corporativo tradicionalmente se refere a auditorias internas que garantem que as duas primeiras linhas – controle de gestão e as funções de gerenciamento de riscos e compliance – estejam funcionando de forma eficaz [79] [80].

No caso da gestão de riscos, fornece uma garantia independente, avaliando a eficácia da governança, gestão de riscos e controle [75], sendo assim, deve ser separada das atividades operacionais da organização e deve ter uma capacidade irrestrita de relatar descobertas ao mais alto nível de governança organizacional, como um conselho de administração ou comitê de auditoria. Esse relatório independente garante que os riscos e controles sejam avaliados de forma objetiva e livre de qualquer viés [77].

No entanto, no contexto da gestão de riscos cibernéticos, esse conceito evoluiu para abranger uma gama mais ampla de atividades, incluindo avaliação de riscos, auditoria de segurança cibernética e revisão de controles de segurança [81].

Numa era digital, onde as ameaças cibernéticas são cada vez mais complexas e frequentes, estratégias robustas de gestão de riscos cibernéticos são uma necessidade. Além disso, o custo dos ataques cibernéticos está aumentando. O custo médio global de uma violação de dados está atingindo valores significativos nos últimos anos. Em 2023, o custo médio global de uma violação de dados foi de US$ 4,35 milhões, um recorde e representando um aumento aproximadamente 2,3 % em relação ao ano anterior [4] [82]. Assim, uma estratégia abrangente e eficaz de gerenciamento de riscos cibernéticos contribui para a proteção de dados confidenciais, mas também para a estabilidade financeira da organização [83].

A auditoria interna auxilia na identificação, avaliação e gerenciamento de riscos cibernéticos que podem impactar os objetivos estratégicos de uma organização. Nessa função, é fundamental para fornecer garantia sobre a eficácia dos programas de segurança cibernética e, como tal, essa função é frequentemente demandada por serviços externos de consultoria em risco cibernético [81].

No contexto da gestão de riscos cibernéticos, a terceira linha adota um papel duplo de garantia e consultoria [12]. As funções de garantia envolvem a avaliação da estrutura de gerenciamento de riscos cibernéticos da organização, enquanto a consultoria abrange funções de aprimoramento dos controles em segurança cibernética. Além disso, promove uma estratégia abrangente de gerenciamento de riscos cibernéticos, garantindo o alinhamento entre práticas operacionais, objetivos estratégicos e estruturas regulatórias [84].

Os auditores externos, mantendo a objetividade, podem trazer conhecimento e experiência específicos do setor para a mesa. Eles podem desafiar e testar a estratégia de gerenciamento de riscos cibernéticos da organização em casos específicos, e quando for o caso, fornecendo recomendações para melhorias. É importante ressaltar que esses profissionais também podem preencher a lacuna de comunicação entre os especialistas técnicos em segurança cibernética e os executivos C-level, traduzindo questões técnicas complexas em linguagem comercial [83].

Para garantir a eficácia das estratégias de gerenciamento de riscos cibernéticos, a terceira linha também envolve monitoramento contínuo. Isso inclui avaliações regulares de risco cibernético, revisões do ambiente de TI da organização e a verificação da conformidade com leis, regulamentos e padrões relevantes [81].

Como parte da auditoria interna, avaliações de segurança cibernética podem ser realizadas para identificar vulnerabilidades, mitigar riscos e fortalecer a postura de segurança de uma organização. Isso envolve examinar sistematicamente a infraestrutura e as práticas cibernéticas de uma organização, identificando possíveis pontos fracos e fazendo recomendações para melhorias [41].

No caso de um incidente cibernético, a terceira linha, pode desempenhar um papel fundamental nas revisões pós-incidente. Isso envolveria analisar a causa do incidente, a resposta e os processos de recuperação e fornecer recomendações para evitar uma ocorrência semelhante [81].

Um elemento importante é avaliar a eficácia do programa de segurança cibernética de uma organização. Essa avaliação abrange a identificação de riscos, avaliação de riscos, resposta a riscos e atividades de controle [85]. Para medir a eficácia, a auditoria interna pode alavancar ferramentas e metodologias, como matrizes de avaliação de risco, comparação com os padrões do setor e autoavaliações de controle [12].

As melhores práticas na gestão de riscos cibernéticos abrangem a adoção de padrões e estruturas de segurança reconhecidas. Isso inclui o Cybersecurity Capability Maturity Model (C2M2) [86], ISO 27001 [87], NIST Cybersecurity Framework (CSF) [88], entre outros. A utilização de tais estruturas pode ajudar as organizações a gerenciar sistematicamente seus riscos cibernéticos.

A comunicação constitui aspecto fundamental para o exercício da função da terceira linha. As interações regulares com as duas primeiras linhas permitem que a equipe de auditoria interna entenda as mudanças nos perfis de risco cibernético, alterações nos regulamentos e mudanças nas estratégias de negócios [47]. Essas interações ajudam a manter um plano de auditoria atualizado e garantem que as atividades estejam alinhadas com os objetivos de gerenciamento de riscos cibernéticos da organização [79].

A eficácia da terceira linha, no entanto, não é isenta de desafios. As organizações lidam com questões como recursos limitados, falta de pessoal qualificado e dificuldades em acompanhar o cenário de ameaças cibernéticas em rápida evolução [58]. Além disso, a independência pode ser comprometida em organizações menores, onde pode haver duplicação de papéis nas três linhas [12].

2.3.1 AVALIAÇÃO INDEPENDENTE PARA GARANTIA DE CONTROLES E PROCESSOS EFICIENTES

A terceira linha em uma organização desempenha um papel significativo no gerenciamento de riscos corporativos, garantindo que os controles e processos sejam eficazes e funcionem conforme o pretendido [11]. Esses mecanismos fornecem garantia sobre o gerenciamento de riscos, abrangendo funções de auditoria interna e supervisão da alta administração [83].

No contexto do risco cibernético, a terceira linha normalmente envolve auditores internos que

revisam os controles e processos implementados pela primeira e segunda linhas para garantir sua adequação e eficácia. Essa camada desempenha um papel crítico no fornecimento de garantia objetiva de que as práticas e controles de gerenciamento de riscos cibernéticos estão funcionando conforme o pretendido. Por exemplo, eles examinam a conformidade da corporação com as obrigações legais e regulatórias e avaliam se a corporação está adequadamente protegida contra ameaças cibernéticas [21].

Controles e processos eficazes para gerenciar riscos cibernéticos incluem elementos como identificação, avaliação, resposta e monitoramento de riscos [87]. É fundamental a garantia que esses elementos funcionam de maneira eficaz, principalmente em termos de monitoramento. Isso envolve a avaliação consistente de controles e processos e a comunicação das descobertas às partes interessadas relevantes, o que pode informar melhorias no gerenciamento de riscos cibernéticos [80].

Nesse contexto, a terceira linha, contribui significativamente para o gerenciamento de riscos cibernéticos, fornecendo garantia independente de que os processos e controles organizacionais são eficazes. Essa função é particularmente relevante no domínio do risco cibernético, onde vulnerabilidades estão surgindo e evoluindo constantemente, validando os controles implementados pela primeira e segunda linhas, reduzindo assim a probabilidade de ocorrência de incidentes cibernéticos significativos [11] [85].

Os processos de gerenciamento de riscos cibernéticos podem ser aprimorados por meio de avaliações regulares dos controles, os auditores podem identificar possíveis pontos fracos nas defesas cibernéticas e realizar recomendações, usando e alavancando a análise de dados, pode identificar tendências e anomalias indicativas de uma ameaça cibernética, permitindo assim uma resposta proativa [21].

As organizações enfrentam vários desafios para garantir o gerenciamento eficaz do risco cibernético. Isso inclui a rápida evolução das ameaças cibernéticas, a complexidade dos sistemas de TI e a crescente dependência de fornecedores terceirizados, cada um apresentando riscos exclusivos [89] e [72]. Portanto, é imperativo que a terceira linha se adapte e melhore continuamente suas habilidades e conhecimentos em gerenciamento de riscos cibernéticos [2].

O gerenciamento eficaz de riscos cibernéticos requer a incorporação de uma variedade de controles técnicos, incluindo firewalls, sistemas de detecção de intrusão e criptografia. Esses controles devem ser constantemente atualizados e testados para garantir que sejam eficazes contra o cenário de ameaças em constante evolução. Auditorias Internas podem garantir que esses controles técnicos estejam em vigor e funcionando de forma eficaz [15].

Várias corporações de grande porte implementam auditorias internas para gerenciar riscos cibernéticos. Por exemplo, a IBM possui uma estratégia onde a terceira linha conduz ativamente avaliações, revisando suas políticas de gerenciamento de riscos cibernéticos e sua eficácia [90]. Eles também fornecem recomendações para melhorias, mantendo assim um ambiente robusto de segurança cibernética.

A violação de dados da Equifax em 2017, destaca-se como um exemplo relevante onde a ausência de atuação da auditoria interna no gerenciamento de riscos cibernéticos foram fundamentais para materialização de um risco [91]. Neste caso, hackers roubaram os dados pessoais de aproximadamente 143 milhões de clientes nos EUA e investigações subsequentes revelaram que a empresa carecia de controles de terceira linha adequados, levando a uma gestão ineficaz de riscos cibernéticos [92].

2.3.2 INTEGRAÇÃO COM GERENCIAMENTO DE RISCOS CORPORATIVOS

A gestão de riscos cibernéticos tornou-se uma preocupação significativa para muitas organizações no século XXI. Abordagens tradicionais de gerenciamento de riscos nem sempre abordam adequadamente a natureza complexa e em constante evolução dos riscos cibernéticos [24]. Os riscos cibernéticos são interconectados de forma única e se propagam rapidamente, muitas vezes ultrapassando fronteiras que outros riscos não cruzam. Por exemplo, uma única violação de dados pode afetar simultaneamente vários sistemas, diferentes tipos de dados e várias partes interessadas. Como tal, a integração dos riscos cibernéticos as estruturas de Gerenciamento de Riscos Corporativos (Enterprise Risk Management ou ERM) torna-se cada vez mais relevante [59].

Integrar riscos cibernéticos ao ERM é uma tarefa complexa devido à natureza única dos riscos cibernéticos. As abordagens tradicionais de gerenciamento de riscos podem não capturar totalmente os aspectos exclusivos do risco cibernético, como sua rápida evolução e potencial de impacto generalizado [60]. Os desafios são técnicos, relacionados à natureza única dos riscos cibernéticos e sua complexidade em rápida evolução, e gerenciais, relacionados à integração do gerenciamento de riscos cibernéticos em uma estrutura mais ampla de ERM. Desta maneira, a integração de risco cibernético e ERM também requer comunicação e colaboração aprimoradas entre os profissionais de gerenciamento de risco e os responsáveis pelo gerenciamento de risco cibernético [41].

A integração do gerenciamento de riscos cibernéticos no ERM deve envolver uma compreensão clara das interdependências entre riscos cibernéticos e outros riscos de negócios. É necessária uma abordagem abrangente para alinhar o gerenciamento de riscos cibernéticos com a estratégia geral de negócios e o apetite ao risco da organização. [29] propõe uma estrutura que mapeia os riscos cibernéticos para os objetivos estratégicos da organização e identifica potenciais interdependências de risco, em um processo contínuo conforme Figura 2.6.

Figura 2.6: Processo de Gerenciamento de Contínuo de Risco

Fonte: [29]

O ERM oferece uma abordagem ampla e em toda a organização para gerenciar riscos e foi proposto como um meio de gerenciar riscos cibernéticos [59]. A estrutura do Committee of Sponsoring Organizations of the Treadway Commission (COSO) para ERM, por exemplo, fornece uma abordagem sistemática

baseada em risco que é adaptável ao gerenciamento de riscos cibernéticos [66].

A integração do risco cibernético com o ERM é ainda apoiada pelo padrão de gerenciamento de risco ISO 31000, que exige o alinhamento dos processos de gerenciamento de risco com os objetivos estratégicos gerais da organização, implicando assim a inclusão do risco cibernético no ERM [93]. A ISO 31000 reforça que todos os tipos de risco, incluindo o risco cibernético, devem ser tratados de forma sistemática e estruturada dentro da organização conforme processo ilustrado na Figura 2.6 [94].

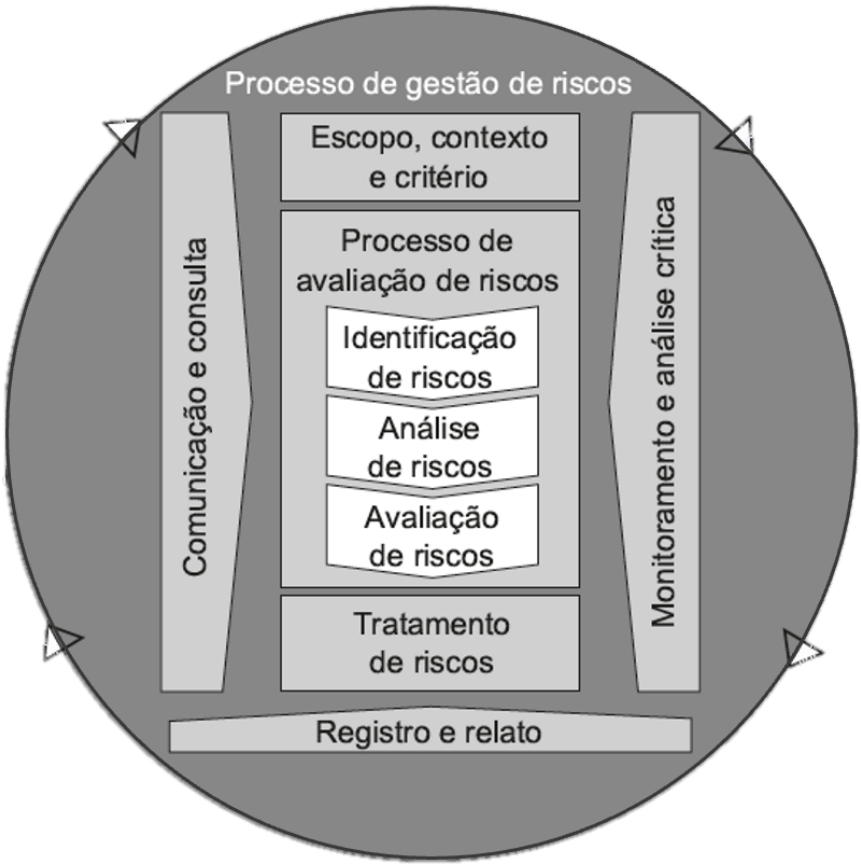

Figura 2.7: Processo de Gestão de Riscos

Fonte: [93]

O envolvimento da alta administração é importante na integração de riscos cibernéticos ao ERM. O compromisso de alto nível pode garantir a alocação adequada de recursos para o gerenciamento de riscos cibernéticos e pode criar uma cultura de segurança cibernética em toda a organização [87]. Além disso, as métricas de segurança cibernética devem ser integradas aos principais indicadores de desempenho que são relatados ao conselho e à alta administração [94].

A eficácia da integração do risco cibernético no ERM pode ser melhorada por meio da adoção de metodologias de quantificação de risco que fornecem avaliações objetivas e baseadas em dados de possíveis ameaças cibernéticas [94]. Tais métodos, incluindo FAIR (Análise de Fatores de Risco de Informação), permitem que as organizações traduzam ameaças cibernéticas abstratas em termos financeiros, permitindo assim uma tomada de decisão e alocação de recursos mais bem fundamentadas [59].

As instituições podem apresentar uma abordagem estratégica para o gerenciamento de riscos, en-

fatizando não apenas os riscos tecnológicos, mas também a interconexão desses riscos com outros riscos corporativos [52]. Assim, ele transcende a abordagem típica de silos, permitindo uma visão abrangente de todo o cenário de risco em toda a empresa. A [2] demonstrou essa abordagem integrada, fornecendo evidências empíricas de empresas com um programa avançado de ERM que experimentam menos eventos cibernéticos prejudiciais.

A terceira linha em ERM pode desempenhar um papel significativo na integração de riscos cibernéticos. Ela é responsável por fornecer garantia independente sobre a eficácia da governança, gestão de riscos e controles internos [11]. A independência da terceira linha em relação às duas primeiras linhas, permite avaliar objetivamente a gestão de riscos cibernéticos e fazer recomendações para melhorias [81]. O desafio é que os auditores podem não ter o conhecimento técnico necessário para avaliar os riscos cibernéticos. Isso levou ao uso crescente de auditores especializados em TI nessa linha. O uso de auditores de TI reúne o conhecimento técnico necessário com uma sólida compreensão do contexto mais amplo de gerenciamento de riscos, permitindo uma integração mais eficaz dos riscos cibernéticos no ERM [83].

2.3.3 VÍNCULOS COM CONFORMIDADE E AUDITORIA INTERNA

A crescente importância do gerenciamento de riscos cibernéticos nas corporações modernas o tornou um aspecto essencial das funções de conformidade e auditoria interna [80]. Um elemento-chave da gestão de risco abrangente, o risco cibernético se concentra em possíveis perdas e danos que podem ocorrer devido ao manuseio incorreto, uso indevido ou acesso não autorizado de sistemas de tecnologia da informação, redes ou dados digitais [21] [34].

Tradicionalmente, as funções de conformidade e auditoria interna lidam com riscos nos domínios físico e financeiro, mas a crescente dependência da tecnologia para operações de negócios tornou o risco cibernético uma preocupação primordial [95].

O gerenciamento de riscos cibernéticos se integra à conformidade por meio de padrões regulatórios estabelecidos por órgãos governamentais que obrigam as empresas a proteger seus sistemas de informação contra ameaças potenciais. Nos Estados Unidos, por exemplo, a Lei Gramm-Leach-Bliley obriga as instituições financeiras a projetar e implementar proteções para proteger as informações dos clientes [24]. Portanto, as funções de conformidade precisam garantir a adesão a esses regulamentos de risco cibernético para evitar penalidades pesadas e danos à reputação dos negócios [21].

O papel da auditoria interna na gestão de riscos cibernéticos evoluiu de uma simples detecção de riscos para uma parte ativa do planejamento estratégico da organização. Com seu profundo conhecimento das operações de negócios, os auditores internos podem identificar possíveis ameaças e vulnerabilidades cibernéticas e avaliar seu impacto potencial. Uma auditoria da estrutura de segurança cibernética de uma organização envolve examinar a eficácia dos controles estabelecidos, incluindo controles físicos, controles técnicos e controles administrativos [17].

A terceira linha também se relaciona com a conformidade, garantindo a adesão da organização a vários regulamentos relacionados à segurança cibernética. As organizações precisam cumprir diferentes leis e padrões de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, o Regula-

mento Geral de Proteção de Dados da União Europeia (GDPR) e o padrão ISO/IEC 27001 da Organização Internacional de Padronização [10] [87]. A terceira linha garante que esses requisitos sejam atendidos, promovendo assim a vinculação da gestão de riscos cibernéticos com conformidade legal [3].

Gerenciamento de risco cibernético, conformidade e auditoria interna, todos trabalham em conjunto para fornecer uma abordagem ampla para gerenciar ameaças de segurança cibernética [81]. Essas funções, coletivamente, mitigam riscos, garantem a conformidade regulatória e protegem a infraestrutura cibernética de uma empresa, contribuindo significativamente para a resiliência e continuidade das operações [63].

2.3.4 RESPONSABILIDADES CHAVES DA TERCEIRA LINHA

No domínio da gestão de riscos cibernéticos, o modelo das três linhas constitui uma estrutura fundamental para alcançar a segurança e a eficiência operacionais ideais [11]. Embora a primeira e a segunda linhas desempenhem papéis significativos no tratamento de riscos cibernéticos, a terceira linha deve fornecer garantia sobre a eficácia do gerenciamento de riscos e dos processos de controle interno. Nesse contexto, a avaliação e monitoramento de riscos, avalições e testes independentes de processos, conformidade e supervisão regulatória e resposta e remediação de incidentes, se destacam como responsabilidades chaves da auditoria interna [57].

A avaliação e monitorização do risco, constituem componentes importantes na gestão do risco cibernético por parte da terceira linha. Essas responsabilidades envolvem reconhecer potenciais ameaças cibernéticas, analisar seu impacto potencial e supervisionar continuamente a eficácia das medidas de defesa existentes [47]. As avaliações de risco devem considerar tanto o impacto potencial quanto a probabilidade de vários riscos, mantendo a organização informada sobre mudanças nos cenários de risco e padrões de ameaças. [36] argumenta que um processo eficaz de avaliação de riscos deve seguir uma abordagem sequencial, incluindo identificação, estimativa, avaliação e tratamento de riscos cibernéticos. O monitoramento, por outro lado, não é uma tarefa única; em vez disso, requer observação e atualização contínuas de ameaças potenciais para manter os perfis de risco atualizados. De acordo com a estrutura de segurança cibernética do [88], o monitoramento envolve revisar os logs do sistema, realizar avaliações de vulnerabilidade e fazer os ajustes necessários em resposta às mudanças no cenário de ameaças cibernéticas.

Ao conduzir análises e testes independentes, a auditoria interna avalia a eficácia e a eficiência da primeira e da segunda linhas. Isso envolve revisar as políticas e procedimentos de gerenciamento de riscos cibernéticos da organização, testar controles e sistemas e validar a conformidade com padrões internos e regulamentos externos. De acordo com [96], a terceira linha realiza auditorias objetivas e revisões de controles de primeira e segunda linha. Essas auditorias abrangem tanto controles internos quanto ameaças externas. É vital para a terceira linha validar de forma independente se os controles e estratégias implementadas pela primeira e segunda linhas são eficazes e consistentes com o apetite de risco da organização. Essa função garante que o programa de gerenciamento de riscos cibernéticos permaneça robusto e relevante, fornecendo uma garantia independente ao conselho e à alta administração [15].

A auditoria interna também tem um papel significativo em Conformidade e Supervisão Regulatória. A tarefa envolve garantir a adesão a vários regulamentos e diretrizes de segurança cibernética esta-

belecidos por órgãos governamentais e não governamentais. Essa função inclui supervisionar a execução de práticas em toda a organização de acordo com esses regulamentos, incluindo medidas de proteção de dados, estruturas de governança de TI e aplicação de políticas de segurança [80]. A terceira linha garante a conformidade da organização com esses regulamentos para evitar penalidades, possíveis danos a reputação e para manter a confiança dos stakeholders. Além disso, fornece garantia de que a organização tem a capacidade de atender aos requisitos regulatórios conforme eles mudam ao longo do tempo [96].

2.4 REGULAÇÃO PRUDENCIAL

A regulação prudencial (Resolução CMN n° 4.553 de 30/1/2017) é uma forma de regulação financeira que impõe normas às instituições financeiras, centrando-se no gerenciamento de riscos e na definição de um patamar mínimo de capital necessário para cobrir os riscos associados às suas operações. Essas medidas de gerenciamento de riscos e capital mínimo ajudam a evitar que uma falência no setor financeiro desencadeie uma reação em cadeia, conhecida como risco sistêmico, que poderia, em última análise, resultar em prejuízos para a sociedade em geral [28].

2.4.1 SEGMENTAÇÃO

As instituições do Sistema Financeiro Nacional (SFN) são divididas em cinco segmentos, com base no tamanho, atividade internacional e perfil de risco. Essa segmentação cria um ambiente regulatório mais apropriado para a aplicação de normas prudenciais, particularmente para as instituições menores, que tendem a ser mais inovadoras e dinâmicas [28].

Com essa divisão, as instituições menores seguem regras mais simples do que as impostas aos bancos de grande porte. Normas prudenciais proporcionais às atividades e ao perfil de risco de cada instituição aumentam a eficiência da intermediação financeira, reduzindo custos e estimulando a competitividade no mercado financeiro [28].

De acordo com a regulação prudencial do Banco Central do Brasil, em setembro de 2023, o Brasil possuía 1291 instituições financeiras distribuídas em cinco segmentos seguindo as regras detalhadas na Tabela 2.1.

Tabela 2.1: Segmentos das Instituições Financeiras Brasileiras

Segmento	**Composição**	**Porte / Atividade Internacional**	**Número de Instituições**
S1	Bancos	Maior ou igual a 10% do PIB (ou atividade internacional relevante)	6
S2	Bancos de tamanho inferior a 10% do PIB e demais instituições com tamanho superior a 1% do PIB	De 1% a 10% do PIB	7
S3	Bancos e instituições não bancários	De 0,1% a 1% do PIB	57
S4	Bancos e instituições não bancárias	Inferior a 0,1%	369
S5	Instituições não bancárias com perfil de risco simplificado	Inferior a 0,1%	844

Fonte: Adaptado de [28]

A alocação de instituições em cada segmento apresentada na Tabela 2.1 foi a mais recente, realizada em abril de 2024. Conforme os dados divulgados, é possível depreender que existe forte concentração de ativos no segmento um, tornando-o mais representativos no cenário econômico nacional.

Segundo o ultimo relatório de estabilidade financeira divulgado pelo Bacen em abril de 2024 [93] [97], embora esteja em redução, 68% das captações de crédito realizadas em 2023 ainda estão concentradas nos bancos do segmento S1, motivo pelo qual optou-se por manter um percentual maior de profissionais que atuam nesse segmento dentre os número de entrevistados.

3 METODOLOGIA

3.1 TIPOLOGIA DA PESQUISA

A pesquisa desenvolvida neste trabalho trat-se de um estudo predominantemente descritivo realizada em caráter exploratório, utilizando-se de abordagem qualitativa, cujo o objetivo central foi identificar formas pelas quais a auditoria interna pode gerar valor e contribuir para garantir a efetividade e o aprimoramento dos processos relacionados à gestão dos riscos cibernéticos nas nstituições financeiras brasileiras. Para atingir esse objetivo, o mecanismo definido foi a realização de entrevistas semiestruturadas com profissionais de instituições financeiras e de empresas de consultoria que possuem operações no Brasil e no exterior.

Pesquisas exploratórias buscam esclarecer conceitos e fornecer uma base para estudos posteriores, possibilitando maior precisão na definição de problemas ou hipóteses oferecendo oferecer uma visão geral e aproximada sobre o fenômeno estudado [26].

Um estudo descritivo é aquele que se destina a descrever a distribuição de uma ou mais variáveis, sem levar em conta qualquer hipótese causal ou outra. Eles fornecem um entendimento detalhado de situações ou populações específicas, frequentemente servindo como ponto inicial de pesquisa para outras metodologias [25].

A Análise de dados qualitativas são uma abordagem de investigação que busca compreender a natureza de um fenômeno, frequentemente em seu contexto social ou natural. Diferentemente das pesquisas quantitativas, que priorizam a mensuração e a análise estatística, as pesquisas qualitativas concentram-se em entender significados, experiências, e interações de maneira mais profunda. Ao considerar as particularidades, expandem-se as possibilidades de incorporar perspectivas divergentes e convergentes sobre o objeto de estudo, contribuindo, dessa forma, para formular inferências que podem confirmar ou refutar as hipóteses da pesquisa [98].

Entrevistas semiestruturadas, também conhecidas como entrevistas em profundidade, são caracterizadas por um conjunto de perguntas abertas e pré-definidas, sem oferecer opções fixas de resposta. Isso dá ao entrevistado liberdade para responder da maneira que preferir, enquanto permite ao entrevistador flexibilidade para ajustar a ordem, a profundidade e o estilo das perguntas conforme as respostas e a situação do entrevistado [26].

Desta maneira, inicialmente foi realizada uma revisão de literatura com o objetivo de elucidar conceitos fundamentais sobre a Gestão de Riscos Cibernéticos, o modelo de três e a atuação da Auditoria Interna, buscando um entendimento preliminar sobre o objeto da pesquisa. Posteriormente, realizou-se a coleta e análise dos dados utilizando entrevistas semiestruturadas e a análise de conteúdo de Lawrence Bardin, respectivamente.

3.2 AMOSTRA DE ENTREVISTADOS

Em função da especificidade determinada para o perfil dos profissionais, a amostra de entrevistados deste trabalho foi realizada de maneira não-probabilística levando em conta as experiências e atuações em atividades de controles internos, gestão de riscos, auditoria interna ou externa e consultoria, em instituições do setor financeiro. Além disso, os entrevistados desempenharam essas atividades e obtiveram as experiências necessariamente em processos relacionados à tecnologia da informação e segurança cibernética.

A opção por instituições do setor financeiro, se deu em função do ambiente complexo e da grande dependência do setor financeiro na tecnologia, tornando-o o segundo setor da indústria com o maior custo médio associado a violação de dados, conforme demonstrado em [4], e suscetível a ataques cibernéticos elaborados.

Além disso, sua interligação com outras áreas da economia pode gerar impactos sistêmicos caso seja atacado, uma vez que compõem a infraestrutura critica de qualquer país. Exemplo disso, é a tendência crescente de ataques visando redes de comunicação financeiras internacionais como a Society for Worldwide Interbank Financial Telecommunication (SWIFT), responsável por transferências internacionais entre bancos, frequentemente realizadas em altas cifras e em moedas fortes como o dólar ou libras esterlinas [9].

Ademais, buscando maior representatividade das instituições financeiras brasileiras, a distribuição dos entrevistados foi realizada buscando refletir o porte e atividade internacional da instituição financeira, segundo a regulação prudencial do Banco Central do Brasil (BACEN). Desta maneira, a quantidade de entrevistados e a distribuição final entre os segmentos pode ser visualizada na Tabela 3.1.

Tabela 3.1: Entrevistados por Seguimento Bancário

Segmento	Quantidade de Entrevistados	(%)
S1	8	50%
S2	2	12,5 %
S3	2	12,5 %
S4	1	6,25 %
S5	1	6,25 %
Auditoria Externa	2	12,5 %
Total	16	100 %

Nota-se que foram entrevistados dois profissionais que atuam em empresas de Auditoria Externa. Essas empresas compõem o que o mercado chama de "Big Four", grupo das maiores empresas internacionais de auditoria. O mercado-alvo dessas empresas são principalmente grandes instituições que operam em vários setores da economia mundial e regiões do mundo. Ao longo dos anos, as "Big Four" têm liderado o mercado global de serviços de auditoria [99].

Os entrevistados foram convidados em função de suas experiências e dos papéis centrais que exerceram na estruturação e avaliação de maturidade em estruturas de Auditorias em Segurança Cibernética e Tecnologia da Informação de bancos do segmento S1, de maneira independente nos últimos anos.

3.3 ENTREVISTAS E ROTEIRO

Durante as entrevistas semiestruturadas o pesquisador pode fazer anotações ou gravar o áudio da conversa, permitindo uma maior concentração na interação. Logo após as entrevistas, os principais temas abordados e os assuntos que forem relevantes para a pesquisa são documentados compondo assim a análise de dados qualitativa.

A pesquisa qualitativa é fundamental nesse processo, pois possibilita a análise abrangente dos dados, tanto de maneira subjetiva, ampliando o entendimento das experiências e aprofundando a interpretação dos discursos.

Buscando proteger a identidade dos participantes e garantir a confidencialidade de informações sobre processos críticos das instituições envolvidas, os entrevistados foram descaracterizados e cada participante será reconhecido por um identificador único iniciado em ENTR01 até ENTR16. Essa ação não traz prejuízo para o alcance dos objetivos propostos neste estudo e foi importante para passar confiança e deixar o entrevistado a vontade para expressar de maneira mais livre possível as suas ideias e percepções sobre os temas estudados.

O roteiro definido para orientar a entrevista foi elaborado levando em conta as informações contidas nas bibliografias mapeadas na etapa de levantamento do referencial teórico deste trabalho e foi dividido em sete blocos, ou índices conforme definição de Bardin [27], com duas perguntas cada, totalizando 14 questões.

O primeiro bloco de perguntas aplicadas foi reservado para conhecer o entrevistado e traçar o seu perfil profissional conforme Tabela 3.2. Essa perguntas são importantes para compreender como foi

construída a carreira e experiência do profissional e como isso pode influenciar suas respostas. Além disso, foi possível entender a atuação do profissional dentro do contexto organizacional e do modelo de três linhas no momento da entrevista.

Tabela 3.2: Bloco 1 - Perfil e Experiência do Entrevistado

Id.	Pergunta
PE01	Conte um pouco sobre sua formação acadêmica e experiências profissionais
PE02	Como você descreveria seu papel atual em relação à segurança cibernética Auditoria e/ou Interna?

O segundo bloco definido, denominado contexto organizacional, buscou obter do entrevistado como ele entende que a segurança cibernética e os riscos associados devem ser gerenciados e direcionados dentro do contexto organizacional e como esse tema pode ser incluído na estratégia corporativa das instituições financeiras conforme Tabela 3.3.

Tabela 3.3: Bloco 2 - Contexto Organizacional

Id.	Pergunta	Referências
PE03	Como você acredita que a estrutura organizacional deve funcionar, em termos de linhas, em relação à segurança cibernética?	[68] [69] [71] [72]
PE04	Como uma organização pode incluir a gestão de riscos cibernéticos em sua estratégia corporativa?	[24] [41] [59] [60]

O terceiro bloco, nominado de Função da Auditoria Interna, tratou de explorar junto ao entrevistado quais as atribuições da auditoria interna dentro do contexto organizacional no que tange a gestão do risco cibernético e as maneiras que ela pode interagir e trabalhar e colaborar com as demais áreas da empresa para identificar e tratar esses riscos dentro das instituições financeiras conforme Tabela 3.4.

Tabela 3.4: Bloco 3 - Função da Auditoria Interna

Id.	Pergunta	Referências
PE05	Como você enxerga o papel da auditoria interna na gestão de riscos cibernéticos?	[41] [47] [57] [81]
PE06	De que forma a auditoria interna pode trabalhar e colaborar com outras áreas da empresa para identificar e mitigar riscos cibernéticos?	[14] [76] [80]

O quarto bloco, intitulado de Avaliação e Monitoramento de Riscos Cibernéticos, abordou junto ao entrevistado as suas percepções sobre as maneiras que a auditoria pode auxiliar a organização a monitorar e avaliar potenciais ameaças cibernéticas e nesse sentido, quais práticas ou frameworks seriam imprescindíveis para auxiliar a auditoria a avaliar como a organização gerencia e mitiga riscos cibernéticos conforme Tabela 3.5.

Tabela 3.5: Bloco 4 - Avaliação e Monitoramento de Riscos Cibernéticos

Id.	Pergunta	Referências
PE07	Como a auditoria pode auxiliar a organização a monitorar e avaliar potenciais ameaças cibernéticas?	[24] [30] [31]
PE08	Quais práticas ou frameworks você considera imprescindíveis para auxiliar a auditoria a avaliar como a organização gerencia e mitiga riscos cibernéticos?	[48] [87] [88]

O quinto bloco, denominado Avaliação da Efetividade de Controles de Segurança, compreendeu junto ao entrevistado como a auditoria interna deve avaliar a eficácia dos controles de segurança cibernética implementados pela organização e o entendimento que métricas ou indicadores podem ser utilizados pela auditoria interna para medir a efetividade desses controles conforme Tabela 3.6.

Tabela 3.6: Bloco 5 - Avaliação da Efetividade de Controles de Segurança

Id.	Pergunta	Referências
PE09	Como a auditoria interna avalia a efetividade dos controles de segurança cibernética implementados pela organização?	[17] [81] [83]
PE10	Que métricas ou indicadores podem ser utilizados pela auditoria interna para medir a efetividade dos controles de segurança cibernética?	[21] [94]

O sexto bloco, designado Conformidade e Supervisão Regulatória, teve o objetivo de captar do entrevistado as maneiras que a auditoria interna pode contribuir para garantir a conformidade com normas e regulamentos relacionados à segurança cibernética e como as eventuais inconformidades identificadas devem ser tratadas e comunicadas dentro da organização conforme Tabela 3.7.

Tabela 3.7: Bloco 6 - Conformidade e Supervisão Regulatória

Id.	Pergunta	Referências
PE11	Como a auditoria interna pode contribuir para garantir a conformidade com normas e regulamentos relacionados à segurança cibernética?	[3] [21] [34]
PE12	Como as inconformidades identificadas pela auditoria podem ser tratadas e comunicadas dentro da organização?	[39] [41] [47] [81]

O sétimo e último bloco, designado Conclusão, teve o objetivo de compreender em conjunto com o entrevistado e baseado nos conhecimentos e experiências que ele possui, quais são as principais lições aprendidas sobre auditoria interna e risco cibernético que poderiam ser compartilhadas e quais são as tendências e inovações na área de segurança cibernética e auditoria são consideradas por eles como as mais relevantes para serem acompanhadas e mantidas no radar dos auditores internos nos próximos anos conforme Tabela 3.8.

Tabela 3.8: Bloco 7 - Conclusão

Id.	Pergunta	Referências
PE13	Com base em suas experiências, quais são as principais lições aprendidas sobre auditoria interna e/ou risco cibernético?	[59]
PE14	Quais tendências e inovações na área de segurança cibernética e/ou auditoria você considera mais relevantes para os próximos anos?	[59]

Finalmente, buscando certificar-se de o entrevistado tinha realizado todas as contribuições que julgava importantes, era aberto espaço para emissão de outras ideias, opiniões e percepções sobre os tópicos explorados, e se ainda restasse alguma contribuição remanescente ao qual ele julgasse pertinente, novo tópico poderia ser aberto para a expressão de novas questões.

3.4 COLETA DE DADOS

Após a definição do roteiro, que serve como referência e ponto de partida para condução da entrevista semiestruturada, deu-se prosseguimento a fase de coleta dos dados.

Para coletar as percepções e informações dos entrevistados, as entrevistas foram realizadas em videoconferências por meio da ferramenta Microsoft Teams.

Embora tradicionalmente realizadas de forma presencial, as entrevistas realizadas por meio de videoconferências são aceitas pela metodologia científica, principalmente devido ao amplo acesso da população aos meios de comunicação [26].

A ferramenta utilizada possui recurso especifico para gravação e para transcrição automática, com a anuência dos entrevistados, os vídeos e as transcrições geradas, devidamente ajustadas, serviram como ponto de partida para as análises realizadas nas etapas posteriores do trabalho.

As entrevistas foram realizadas de maneira individual com cada entrevistado, entre 14 de março de 2024 e 2 de maio de 2024, com tempo de duração variando entre 46 minutos a 1 hora e 20 minutos.

A primeira entrevista foi utilizada como teste e validação do roteiro pré-definido. O objetivo é identificar possíveis falhas na elaboração do questionário, como: complexidade das questões, imprecisões na redação, irrelevância das perguntas, desconforto para o respondente, exaustão, entre outras.

Para aprimoramento do roteiro, foi indicado realizar contextualização de algumas perguntas para o entrevistado, utilizando de preferência informações já fornecidas por eles durante o curso da entrevista ou conhecidas previamente pelo perfil no Linkedin ou outras fontes.

Além disso, também foi incluída uma declaração no inicio da gravação informando a finalidade da pesquisa, limitando o escopo da entrevista e reforçando o acordo de confidencialidade em relação a identidade dos entrevistados e as instituições ao qual fazem parte.

3.5 ANÁLISE DE CONTEÚDO (ANÁLISE DE DADOS)

Para analisar os dados coletados por meio dos instrumentos definidos na pesquisa em questão, aplicou-se a análise de conteúdo segundo [27]. A técnica consiste em aplicar três etapas bem definidas para realizar a analise de conteúdo de maneira metódica conforme a seguir: (i) pré-análise; (ii) exploração do material; e (iii) tratamento dos resultados, inferência e interpretação, conforme Figura 3.1.

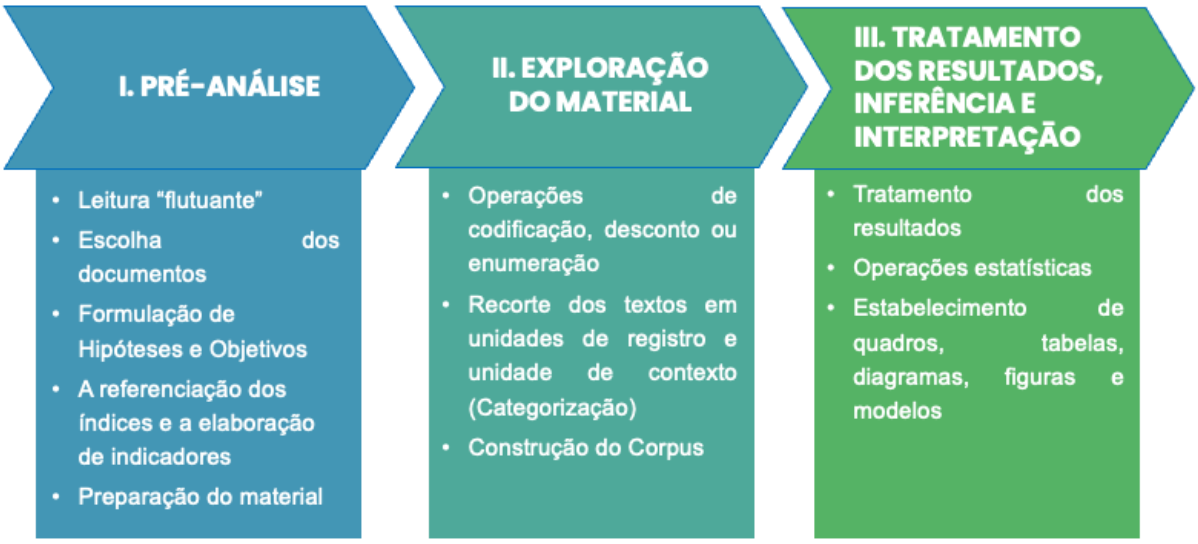

Figura 3.1: Etapas da análise de conteúdo segundo Bardin (2016)

Fonte: Autor

A análise de conteúdo tem como objetivo extrair dos textos narrados, por meio de características metodológicas objetivas e sistematizadas, a inferência do conhecimento e o significado que emerge das mensagens verbalizadas [27].

A análise dos dados permite organizá-los de maneira a fornecer respostas ao problema de pesquisa. Assim, os dados coletados a partir do modelo de informações pessoais possibilitam compreender o universo dos participantes e oferecem dados quantitativos que ajudam a conhecer o perfil sociodemográfico [89]

[26].

Na análise de conteúdo, podem ser utilizadas diversas técnicas, tais como: (i) Análise Categorial, (ii) Análise de Avaliação, (iii) Análise de Enunciação, (iv) Análise Proposicional do Discurso e (v) Análise de Expressão. No presente trabalho, foi escolhida a técnica de Análise Categorial, que opera pelo desmembramento do texto em unidades, categorizadas segundo reagrupamentos analógicos. A técnica de Análise Categorial apresenta bons resultados em pesquisas qualitativas, devido à sua capacidade de realizar interpretações fundamentadas em inferências [27].

3.5.1 (I) PRÉ-ANÁLISE

A pesquisa começou com a escolha e identificação do tema: O Papel da Terceira Linha na Gestão do Risco Cibernético, com foco em instituições financeiras brasileiras. Após uma leitura flutuante utilizando as regras de exaustividade, representatividade, homogeneidade, pertinência e exclusividade, observou-se que havia pouca literatura disponível sobre o assunto, ou seja, a literatura era escassa e não científica. Diante disso, constatou-se a necessidade de pesquisas científicas sobre o tema.

Nesse contexto, foi realizada um estudo dos assuntos envolvidos no tema com o objetivo de analisar a relevância da pesquisa em relação ao objeto escolhido e verificar a abrangência na literatura existente. Esse processo envolveu a análise de diversas fontes acadêmicas e científicas para identificar como e até que ponto o tema é abordado.

Os resultados desses estudos foram apresentados no referencial teórico deste trabalho, que não apenas confirmou a importância e a pertinência do tema escolhido, mas também evidenciou a escassez de produção científica sobre o assunto no país. Essa constatação reforça a necessidade de desenvolver estudos mais aprofundados para preencher essa lacuna no conhecimento e contribuir para a área de gestão do risco cibernético, especialmente no âmbito da Terceira Linha.

Posteriormente, foram elaborados sete indicadores dentro de um corpo teórico, para fundamentar a interpretação final dos dados. Este processo incluiu a criação e desenvolvimento de um roteiro de entrevista semiestruturada, concebido para captar percepções e informações dos entrevistados sobre os temas destacados.

O roteiro foi aplicado junto a profissionais que atuam em segunda e terceira linha, permitindo a coleta de dados qualitativos que enriquecem a análise e interpretação dos resultados. Dessa forma, a combinação de indicadores teóricos e dados empíricos forneceu uma base para uma compreensão do tema estudado, assegurando que as conclusões fossem bem fundamentadas e refletissem com a maior fidelidade a realidade observada.

O contato com os profissionais foi realizado primeiramente levando em consideração conexões profissionais que o autor possui. Em seguida, com indivíduos provenientes de indicações dos primeiros entrevistados, conforme ocorriam as entrevistas.

Buscando maior diversidade e mitigar o viés de confirmação da pesquisa, o autor contatou profissionais que atuem em áreas de segunda e terceira linha em instituições financeiras brasileiras, que possuem perfil verificado e aberto no Linkedin para conferir a disponibilidade deles em participar das entrevistas,

completando assim a amostra da pesquisa.

As ações tomadas e os resultados obtidos com a aplicação dos métodos indicados pela metodologia nessa etapa estão resumidas na Figura 3.2.

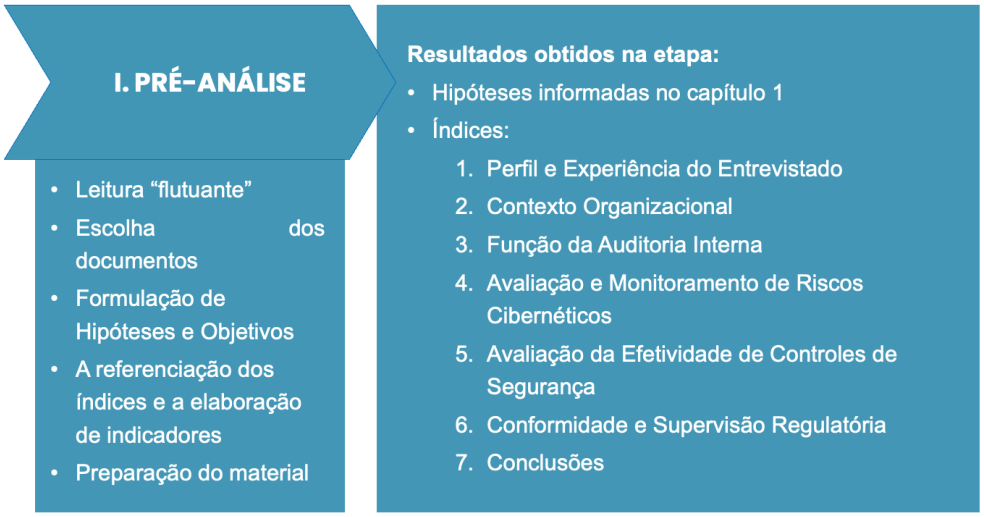

Figura 3.2: Subetapas e Resultados obtidos na Pré-análise

Fonte: Autor

3.5.2 (II) EXPLORAÇÃO DO MATERIAL

Na análise de conteúdo proposta por Lawrence Bardin, a etapa de exploração do material envolve as operações de codificação, desconto e enumeração. A codificação constitui-se na organização sistemática dos dados, onde os textos são minuciosamente lidos e analisados, identificando-se temas, padrões e conceitos recorrentes. Esses elementos são então rotulados com códigos específicos, que podem ser predefinidos com base em teorias existentes ou emergir da própria análise do material. Este processo de categorização permite a construção de uma estrutura analítica que facilita a interpretação subsequente dos dados.

O desconto, também conhecido como redução, é a operação que visa simplificar e sintetizar os dados coletados. Durante esta fase, ocorre a filtragem das informações, removendo-se elementos redundantes ou irrelevantes que não contribuem significativamente para os objetivos da pesquisa. O material é então resumido, com segmentos de texto longos sendo condensados em declarações ou parágrafos mais concisos que capturam a essência do conteúdo analisado. Esta operação é essencial para focar nos aspectos mais pertinentes e garantir a relevância dos dados para a análise.

A enumeração, por sua vez, é a operação que introduz a quantificação no processo de análise qualitativa. Consiste em contar a frequência com que certos temas, palavras ou códigos aparecem no material estudado, permitindo uma análise de frequência que revela a prevalência relativa de diferentes categorias. Esta quantificação dos dados qualitativos facilita a identificação de padrões e tendências, fornecendo uma base quantitativa que complementa a interpretação qualitativa dos dados. A enumeração, portanto, não apenas enriquece a análise com uma dimensão numérica, mas também oferece uma perspectiva adicional para a compreensão dos dados coletados.

O material coletado e selecionado foi recortado em unidades de registro e unidades de contexto, permitindo uma análise estruturada. Essas unidades foram organizadas em caracterizações temáticas, utilizando categorias ou blocos específicos para facilitar a compreensão e a interpretação dos dados. Este processo permitiu uma segmentação do conteúdo, assegurando que cada fragmento de informação fosse analisado dentro de seu devido contexto, contribuindo assim para a construção de uma análise fundamentada.

As ações tomadas e os resultados obtidos com a aplicação dos métodos indicados pela metodologia nessa etapa estão resumidas na Figura 3.3.

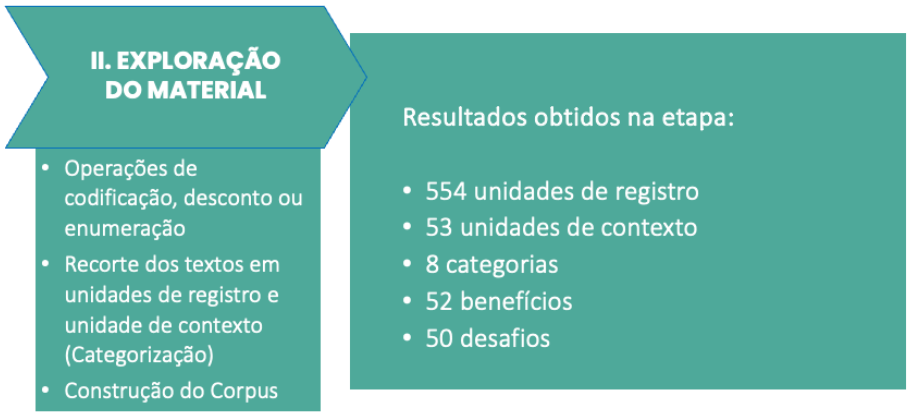

Figura 3.3: Subetapas e Resultados obtidos na Exploração do Material

Fonte: Autor

3.5.3 (III) TRATAMENTO DOS RESULTADOS, INFERÊNCIA E INTERPRETAÇÃO

O tratamento dos resultados envolve a organização sistemática e a síntese dos dados previamente codificados e categorizados. Esta fase busca consolidar e estruturar a informação coletada, garantindo a consistência e coerência dos códigos e categorias estabelecidos. Os dados são revisados, integrados e apresentados de maneira que facilite a análise subsequente. Esse processo permite uma visão coesa e abrangente dos dados, preparando o terreno para as fases de inferência e interpretação, onde significados mais profundos serão extraídos e contextualizados teoricamente, enriquecendo a compreensão do fenômeno estudado.

As operações estatísticas desempenham um papel essencial ao quantificar e analisar os dados qualitativos de maneira sistemática. Estas operações envolvem a contagem de frequências de temas, categorias ou códigos, permitindo a identificação de padrões recorrentes e a comparação quantitativa entre diferentes conjuntos de dados. A aplicação de técnicas estatísticas, como a análise de frequência e a distribuição de dados, oferece uma dimensão quantitativa à análise qualitativa, facilitando a interpretação dos resultados e a formulação de hipóteses. As operações estatísticas, portanto, enriquecem a análise de conteúdo ao proporcionar uma base numérica que complementa a exploração qualitativa, contribuindo para a robustez e a validade dos achados da pesquisa.

Nesta última fase, os resultados foram tratados, confirmando as informações obtidas a partir da

transcrição das entrevistas. Foram elaborados figuras, quadros e tabelas que facilitaram a inferência e a interpretação dos dados. Esses elementos visuais permitiram uma apresentação mais clara dos achados, auxiliando na compreensão das relações e padrões identificados durante a análise. Assim, a combinação de representações gráficas com a transcrição das entrevistas forneceu a base para validar e interpretar os resultados, assegurando uma análise fundamentada.

O estabelecimento de quadros, tabelas, diagramas, figuras e modelos desempenha um papel fundamental na organização e interpretação dos dados. Esses elementos visuais facilitam a compreensão das informações, permitindo a visualização das relações entre os diferentes elementos do estudo. Bardin (2016) enfatiza que a utilização dessas ferramentas não apenas sintetiza os dados de forma mais acessível, mas também destaca padrões, tendências e inferências significativas que poderiam passar despercebidas em uma análise puramente textual. Assim, os quadros e tabelas, por exemplo, estruturam e condensam as informações, enquanto os diagramas e figuras ilustram as conexões e dinâmicas entre os conceitos analisados, contribuindo para uma análise mais robusta e detalhada.

As ações tomadas e os resultados obtidos com a aplicação dos métodos indicados pela metodologia nessa etapa estão resumidas na Figura 3.4.

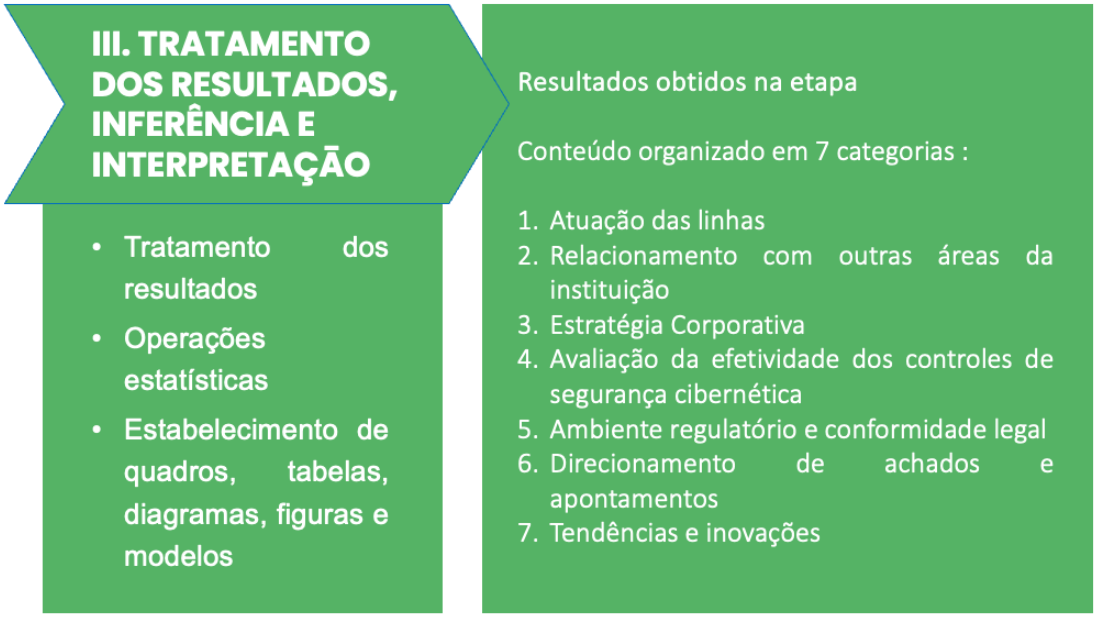

Figura 3.4: Subetapas e Resultados obtidos no tratamento dos resultados

Fonte: Autor

4 RESULTADOS

Com o objetivo de compreender e identificar as maneiras como a Auditoria Interna pode auxiliar as instituições financeiras a gerir devidamente os riscos cibernéticos, as entrevistas focaram em explorar o conhecimento e experiências de profissionais de áreas de controles internos, gestão de riscos, auditorias internas e externas, pois eles são parte relevante do processo, sendo responsáveis por realizar, gerir e avaliar processos corporativos e controles implementados. Além disso, seus conhecimentos especializados nos temas em questão são demonstrados pelas suas experiências e formações acadêmicas. Esses conhecimentos demonstrados pelos entrevistados foram importantes para identificar quais elementos devem sem considerados mais relevantes no direcionamento das estratégias da Auditoria Interna ao abordar a Gestão do Risco Cibernético.

A análise realizada buscou não apenas descrever os dados coletados, mas também interpretar os achados à luz da literatura revisada, permitindo uma compreensão contextualizada dos fenômenos investigados, fornecendo uma visão abrangente dos dados, facilitando a conexão entre os resultados e as teorias discutidas anteriormente.

Neste capítulo, apresenta-se a análise dos dados obtidos, seguindo a metodologia definida e exposta no terceiro capítulo, bem como a fundamentação teórica delineada no segundo capítulo. A abordagem adotada visa garantir a coerência e a robustez da análise, alinhando-se aos princípios metodológicos previamente estabelecidos.

Os resultados descritos a seguir foram examinados e seguem os métodos e técnicas previamente expostos, garantindo que cada etapa do processo analítico seja transparente e replicável.

4.1 PERFIL DOS ENTREVISTADOS E CONTEXTO ORGANIZACIONAL

Essa seção tem por objetivo identificar e caracterizar os entrevistados levando em conta informações relevantes como experiências profissionais, formações acadêmicas e a adoção do Modelo de Três Linhas dentro das instituições financeiras representadas. Os resultados tratados estão disponíveis na Tabela 4.1, onde destaca as características profissionais dos entrevistados, abordando diversos aspectos relacionados à sua atuação. Primeiramente, foram consideradas as posições que cada um ocupa dentro do modelo de três linhas, especificando as responsabilidades e funções que desempenham atualmente. Além disso, a tabela possui informações sobre o tempo de funções exercidas pelos entrevistados, permitindo um panorama de suas experiências adquiridas não apenas na linha atual, mas também em outras linhas ao longo de suas carreiras.

Os cargos atuais de cada entrevistado, também foram analisados oferecendo uma visão clara sobre suas posições hierárquicas e áreas de atuação. Por fim, a tabela apresentou as formações acadêmicas adquiridas por cada um, evidenciando suas qualificações e conhecimentos acadêmicos que complementam suas experiências profissionais.

Tabela 4.1: Perfil e Características dos Entrevistados

Entrevistado	**Posição atual**	**Experiência em Terceira Linha (Anos)**	**Experiência em Segunda Linha (Anos)**	**Experiência em Primeira Linha (Anos)**	**Função Atual**	**Formação**
ENTR01	Terceira Linha	2	4	7	Supervisor de Auditoria Interna em TI e Segurança Cibernética	Graduação em Desenvolvimento de Sistemas e Pós-graduação em Segurança da Informação e Gestão Estratégica
ENTR02	Terceira Linha	13	-	8	Coordenadora de Auditoria em TI	Graduação Ciência da Computação e Pós-graduação em Engenharia de Software
ENTR03	Segunda Linha	10	2	12	Gerente de Controles Internos em TI e Segurança Cibernética	Graduação em Administração de Empresas, Pós-graduação em Inteligência Artificial para Ambientes de Negócio e em Governança de TI
ENTR04	Segunda Linha	-	7	10	Gerente de Riscos em TI, Cibernético, de Terceiros e de Modelo.	Graduação em economia, Pós-graduação em Finanças, Governança de TI e Mestrado em Economia
ENTR05	Auditoria Externa	3	-	14	Gerente Sênior de Segurança Cibernética e Governança	Graduação em Engenharia da Computação e Mestrado em Inteligência Artificial e Segurança de Informação
ENTR06	Terceira Linha	12	-	5	Coordenador de Auditoria em TI, Segurança Cibernética e da Informação	Graduação em Gerenciamento de Sistemas e Pós-graduação em Gestão de Segurança da Informação e Cyber Security
ENTR07	Terceira Linha	12	5	13	Coordenador de Auditoria em TI	Graduação em Análise e Desenvolvimento de Sistemas, Pós-graduação em Gestão de negócios e mestrado em administração de empresas
ENTR08	Terceira Linha	3	3	18	Superintendente de Auditoria de TI e Segurança Cibernética	Graduação em Engenharia Elétrica e Pós-graduação em Segurança Cibernética

Tabela 4.1 – Perfil e Características dos Entrevistados

Entrevistado	**Posição atual**	**Experiência em Terceira Linha (Anos)**	**Experiência em Segunda Linha (Anos)**	**Experiência em Primeira Linha (Anos)**	**Função Atual**	**Formação**
ENTR09	Segunda Linha	10	1	3	Coordenador de Riscos Cibernéticos	Graduação em Engenharia de Redes e Pós-graduação em Segurança Cibernética e Gestão de Projetos
ENTR10	Segunda Linha	-	3	15	Gerente de Compliance em TI e Segurança Cibernética	Graduação em Sistemas de Informação e Pós-graduação Gestão Empresarial
ENTR11	Segunda Linha	5	2	10	Coordenador de Riscos e Controles Internos em TI e Segurança Cibernética	Graduação em Ciência da Computação e Pós-graduação m Segurança da Informação e Ciência de Dados
ENTR12	Terceira Linha	15	-	6	Gerente de auditoria em TI e Segurança Cibernética	Graduação em Sistemas da Informação e Pós-graduação em Segurança da Informação
ENTR13	Auditoria Externa	16	-	1	Gerente Sênior de Risco de Tecnologia	Graduação em Engenharia Eletrônica e Pós-graduação em Gestão de TI
ENTR14	Terceira Linha	2	-	14	Gerente de Auditoria em Segurança Cibernética	Graduação em Ciência da Computação e Pós-graduação em Segurança da Informação
ENTR15	Segunda Linha	-	2	10	Especialista em Riscos Cibernéticos	Graduação em Ciência da Computação e Pós-graduação em Gestão de TI
ENTR16	Segunda Linha	5	8	15	Gerente em Controles Internos de Segurança	Graduação em Ciência da Computação e Pós-graduação em Auditoria, Riscos e Inteligência Artificial
	Média	8,31	3,70	10,25		

Atuação Profissional - Dos 16 profissionais entrevistados, sete atualmente desempenham funções na terceira linha (44%), sete atualmente desempenham funções na segunda linha (44%) e dois entrevistados (12%) atualmente desempenham funções em auditoria externa, conforme Figura 4.1.

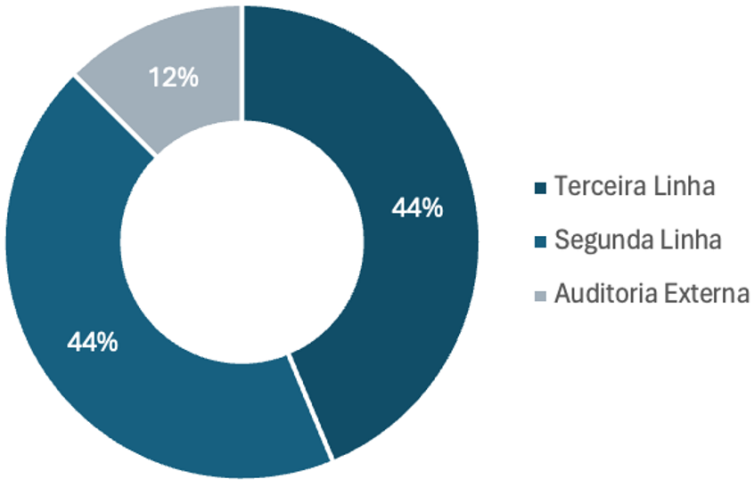

Figura 4.1: Entrevistados por Linha

15 entrevistados (93,7%) tem perfil gerencial ou de coordenação, ou seja, tomam decisões, direcionam avaliações e gerenciam times ou equipes de auditoria em processos relacionadas aos temas de Segurança Cibernética, Segurança e Tecnologia da Informação. Apenas um entrevistado (6,25%) trabalha como especialista em riscos. Entretanto, dentro do contexto da instituição, esse cargo é equivalente ao de Coordenador de Riscos e sua atribuição principal é prestar consultoria especializada sobre Gestão de Riscos Cibernéticos, de Segurança e de TI aos gestores. Essas informações denotam alto grau de responsabilidade dos profissionais com os temas abordados nesse trabalho.

Experiências Profissionais - Ao analisar as informações contidas na Tabela 4.1, destaca-se a informação de que os profissionais que desempenharam funções durante menos tempo em primeira, segunda e terceira linha foram respectivamente três, um e dois anos e que os profissionais que desempenharam funções durante mais tempo em primeira, segunda e terceira linha foram respectivamente 18, 11 e 16 anos. A despeito dessas informações, observa-se que os tempos médios em anos que os entrevistados possuem desempenhando funções em primeira, segunda e terceira linha são respectivamente 10,25, 3,7 e 8,31 anos, conforme Figura 4.2.

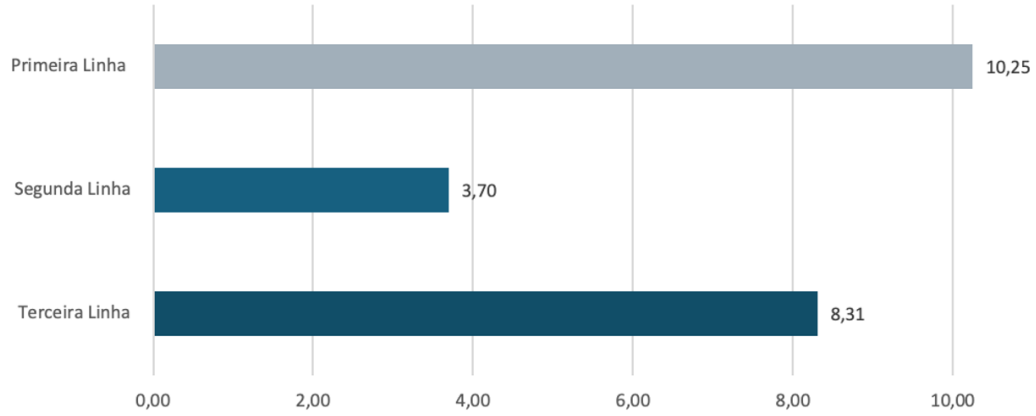

Figura 4.2: Média de Experiência dos Entrevistados por Linha (Anos)

Isso evidencia o alto nível de experiência atuando em primeira linha que, de maneira geral, os profissionais devem possuir para ascender à segunda e terceira linha e atuar com atividade de controles internos, gestão de riscos ou auditoria interna.

Formações Acadêmicas - Ao explorar os dados e informações contidas na Tabela 4.1, destaca-se a informação de que 13 profissionais entrevistados (81,25%) possuem graduações em cursos ligados a Engenharia/TI ou similares e três entrevistados (18,75%) são graduados em cursos ligados a área de gestão/negócios ou similares, conforme Figura 4.3.

Por outro lado, quando se analisa as informações referentes a pós graduações realizadas pelos componentes da amostra, destaca-se que 14 entrevistados (87,50%) possuem pós-graduações em Engenharia/TI ou similares e 11 entrevistados (68,75%) possuem pós-graduações relacionadas as áreas de Gestão/Negócios ou similares, conforme Figura 4.3. Importante ressaltar que alguns entrevistados possuem mais de uma pós-graduação.

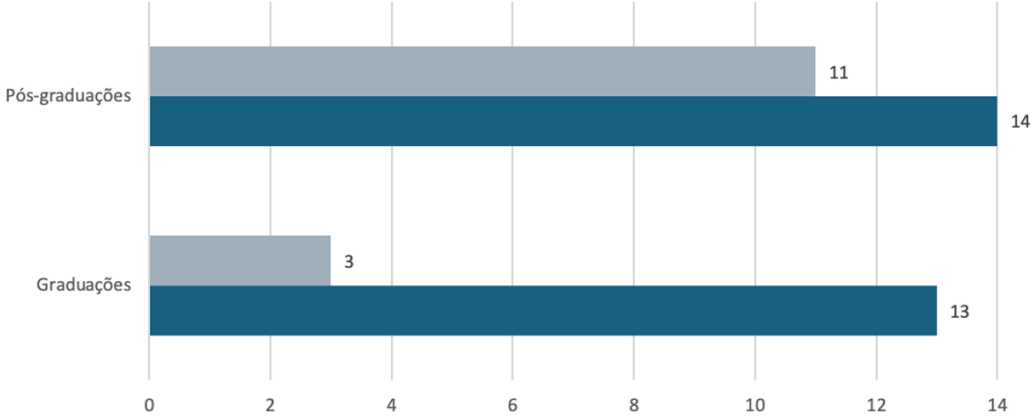

Figura 4.3: Formações Acadêmicas dos Entrevistados

As informações apresentadas deixam claro que entre os 13 graduados em Engenharia/TI ou similares oito procuraram se especializar em área de gestão/negócios ou similares e que os três profissionais graduados em área de gestão/negócios ou similares buscaram se especializar em Engenharia/TI ou similares, demonstrando que profissionais que atuam em áreas de controles internos, gestão de riscos ou auditoria interna, devem possuir conhecimentos abrangentes em áreas diversas.

Tabela 4.2: Unidades de Contexto da Amostra

Perfil dos entrevistados e contexto organizacional
Perfil dos entrevistados e das organizações representadas na pesquisa segundo o modelo de três linhas
I. A atuação em segunda e terceira linha por parte dos profissionais denotam alto grau de responsabilidade com os temas de auditoria interna e gestão de riscos cibernéticos. II. Experiências adquiridas atuando em primeira linha são relevantes e contribuem para avaliações mais efetivas por parte da segunda e terceira linha. III. Formações e conhecimentos em áreas de negócios e de TI/Segurança cibernética são complementares e diferenciais para atuação em áreas de segunda e terceira linha.

4.2 CATEGORIA 1 - ATUAÇÃO DAS LINHAS

A Categoria 1, intitulada "Atuação das linhas", tem como objetivo expandir a compreensão acerca de como os entrevistados percebem e interpretam o papel e a atuação de cada linha no contexto da segurança cibernética dentro das organizações, considerando o modelo de três linhas. Esta categoria busca detalhar e esclarecer as percepções dos participantes sobre as funções, responsabilidades e interações de cada linha, fornecendo uma visão sobre a forma como essas linhas contribuem para a gestão da segurança cibernética nas empresas.

Adoção do Modelo de Três Linhas - Na tabela 4.3 pode-se visualizar as intuições e seus respectivos segmentos segundo regulação prudencial do BACEN [28], conforme detalhado anteriormente na seção 2.4.1 do segundo capítulo.

Destaca-se que, apesar de terem sido realizadas 16 entrevistas, observa-se apenas 12 organizações representadas. Isso deve-se ao fato de que dois bancos do segmentos S1 tiveram mais de um entrevistado, abrangendo segunda e terceira linha, buscando maior pluralidade de opiniões. Outras duas organizações, apesar de representadas no quadro, não são classificadas pelo BACEN pois tratam-se de empresas de auditorias externas (Big Four), conforme detalhado na seção 2.4.1 do segundo capítulo.

Vale salientar que o entrevistado que trabalha na instituição INST06, conforme Tabela 4.2, declarou que a mesma não adota o modelo de três linhas oficialmente. Entretanto, ela possui áreas de auditoria interna, gestão de riscos e conformidade, atuando em um modelo próximo ao de três linhas trabalhando próximo aos gestores e áreas de negocio avaliando processos organizacionais semelhante ao modelo do IIA.

Apesar das empresas de auditorias externas possuem áreas de controles internos, suas atuações

Tabela 4.3: Instituição Financeira por Segmento e a Adoção do Modelo de Três Linhas

Instituição	Segmento BACEN (Quando for o caso)	Adoção do Modelo de Três Linhas
BANK1	S1	Sim
BANK2	S1	Sim
BANK3	S1	Sim
BANK4	S1	Sim
INST1	S4	Sim
INST2	S2	Sim
INST3	S3	Sim
INST4	S3	Sim
INST5	S2	Sim
INST6	S5	Não
AUD1		
AUD2		

estão delimitadas dentro de um outra área de atuação e o qual não estão sujeitas aos mesmo riscos que as instituições financeiras, entretanto, conforme será explorado a seguir, os entrevistados acreditam que o modelo de três linhas é o modelo mais ajustado para comportar a dinâmica de gestão de riscos, conformidade e controles internos dentro de instituições financeiras.

Desta maneira, retirando as empesas de auditoria externa da amostra específica desta categoria, observa-se que 9/10 instituições financeiras (90%) adotam o modelo de três linhas, o que evidencia uma adoção expressiva deste modelo dentro do ecossistema financeiro brasileiro.

Adequação do Modelo de Três Linhas - Os entrevistados foram praticamente unânimes em mencionar que o modelo de três linhas é o modelo mais robusto e adequado para abranger os temas de gestão de riscos, controles internos e auditoria interna. A seguir, destaca-se a unidade de registro do entrevistado ENTR01 sobre o tema:

> *"O modelo de três linhas hoje é o modelo que melhor abrange e acomoda as atividades de auditoria interna e controles internos dentro da organização, por essa razão ele é amplamente adotado pelas organizações, mesmo havendo criticas pontuais em relação a atuação muito intrusiva por alguns profissionais e das eventuais sobreposições de funções que possam ocorrer".*

O mesmo entrevistado mencionou:

> *"Eu acredito, no modelo das três linhas, porque elas são importantes para que a gente possa evitar o que chamamos de queijo suíço, que possui uma série de buracos, certo? Nesse caso, o ideal é evitar que esses buracos se alinhem e seja possível atravessar de um lado para o outro do queijo".*

Em última análise, os buracos mencionados pelo entrevistado dizem respeito a fragilidades em processos corporativos que quando sobre posicionadas podem materializar o risco e gerar prejuízos das mais diversas ordem as organizações.

Evolução do Modelo - O entrevistado ENTR04 citou que: *"Embora reconheça a importância do modelo e ache que ele seja o que tem de melhor disponível atualmente, entende que o modelo precisa evoluir para responder de maneira mais eficaz as demandas do negócio"*, e o entrevistado ENTR03 mencionou que *"O modelo referencial de três linhas é um bom ponto de partida para organizações ate o atingimento de tal grau de maturidade que lhe permita a evolução esse modelo, porém, essa evolução fica condicionada a maturidade da empresa e dos profissionais que irão conduzir os processos"*.

Todavia, nenhum entrevistado apresentou outras alternativas ao modelo de três linhas ou fez alguma referência sobre como isso impactaria de qualquer maneira a gestão dos riscos cibernéticos dentro das instituições.

Definição de Papéis e Responsabilidades - Diversos entrevistados reforçaram a importância da devida definição de papéis e responsabilidades de cada linha dentro do modelo em suas respostas. Entretanto, destaco aqui a unidade de registro do entrevistado ENTR07, onde reforçou: *"Embora o modelo seja eficiente e amplamente utilizado, para funcionar de maneira efetiva, o modelo deve ser implementado corretamente e as linhas devem ter seus papéis e responsabilidades institucionais bem definidos para atingir corretamente os objetivos propostos"*.

Primeira Linha - Segundo os entrevistados, a primeira linha deve ser formada pelos gestores operacionais, que são responsáveis pelo gerenciamento direto dos riscos cibernéticos no dia a dia. Eles devem implementar e manter controles, realizar avaliações regulares de riscos e assegurar que as políticas de segurança sejam seguidas por todos. Além disso, essa linha é responsável por educar os funcionários sobre práticas seguras de TI e conscientização sobre segurança.

O ENTR10 destacou a seguinte fala em uma de suas unidades de registro:

> *"Em outras palavras, a primeira linha implementa e operacionaliza os controles de segurança cibernética no dia a dia. No contexto da segurança cibernética envolve a implementação e a manutenção de controles básicos de segurança como políticas de senha forte, criptografia de informações, controle de acesso e segurança física, por exemplo"*.

Segunda Linha - Inclui as funções de gestão de riscos e conformidade, que monitoram e facilitam a implementação de práticas de governança de TI e segurança cibernética. Esta linha assegura que a primeira linha esteja operando conforme os padrões estabelecidos e que os riscos sejam identificados, avaliados e mitigados de forma adequada. Também são responsáveis por desenvolver políticas, fornecer ferramentas, recursos, orientações estratégicas e suporte para a primeira linha, e garantir a conformidade com as leis e regulamentos aplicáveis.

Sobre esse tópico, o entrevistado ENTR13, realizou a seguinte contribuição em sua unidade de registro sobre o tema: *"A segunda linha pode realizar avaliações de risco, desenvolver frameworks de*

controle e aplicar testes para verificar a conformidade com as regulamentações e normas, como a ISO/IEC 27001".

Terceira Linha - Os entrevistados entendem que a Terceira Linha compreende a posição da auditoria interna dentro do modelo, e que sua função primordial é fornecer avaliações independente e objetivas sobre a eficácia dos controles e processos estabelecidos pelas duas primeiras linhas.

Além disso, verifica se o quadro de gestão de riscos está sendo efetivamente aplicado e se é suficiente para proteger a organização contra ameaças cibernéticas, realização de Auditorias regulares e independentes dos sistemas e processos de segurança cibernética, revisão da conformidade com políticas, procedimentos e regulamentações de segurança, identificação de lacunas, recomendação de melhorias nos controles de segurança e relatórios ao conselho ou ao comitê de auditoria sobre o estado da segurança cibernética.

A unidade de registro do entrevistado ENTR07 destacou o seguinte sobre o tópico: *"A Auditoria Interna deve trabalhar complementando as análises de primeira e segunda linha, avaliando como a gestão está sendo realizada, verificando se os riscos mapeados são de fato os mais relevantes e se os controles implementados de fato podem mitigar esses riscos".*

Identificação de Riscos e Fragilidades - Os entrevistados destacam que a auditoria interna não apenas avalia e monitora os controles existentes, mas também identifica fragilidades, propõe melhorias e recomenda medidas corretivas. Dessa forma, a atuação da auditoria interna é vista como um componente essencial para garantir a segurança cibernética, fornecendo uma análise independente e especializada que contribui para a mitigação eficaz dos riscos digitais enfrentados pelas organizações.

Nesse sentido, destaca-se o comentário do entrevistado ENTR07 em sua unidade de registro sobre o assunto: *"A atuação da auditoria interna é parte essencial para garantir a segurança cibernética, proporcionando uma análise independente e especializada que contribui para a mitigação eficaz dos riscos digitais e ameaças cibernéticas enfrentadas pelas instituições".* Isso esta aderente ao afirmado por [2], [72], [75] e [85] que frisam que a avaliação independente da terceira linha deve ser proativa em sua abordagem de gerenciamento de riscos.

Sinergia e Parceria - Para que a auditoria interna seja eficaz, é essencial manter uma sinergia e parceria com as diversas áreas e gestores da empresa, sem comprometer a independência e imparcialidade nas avaliações. É importante que os auditados entendam que a auditoria é uma aliada no negócio. Afinal, todos trabalham na mesma empresa e estão mobilizados para atingir os mesmos objetivos.

A seguir, destaca-se a unidade de registro do entrevistado ENTR15 sobre o tema:

> *"A parceria com as diversas áreas e gestores da empresa é elemento essencial para garantir o sucesso das avaliações da auditoria e para gestão eficaz do risco cibernético dentro das instituições. Nesse ponto, é necessário atenção a resistência de gestores em relação à auditoria. Onde há fumaça, há fogo. Se há resistência em receber a auditoria, a atenção deve ser redobrada, pois pode indicar a existência de questões que*

necessitam de atenção especial".

[71] frisou que essa parceria aprimora a comunicação e a coordenação de riscos nas diferentes linhas. Ela promove uma compreensão unificada dos riscos e dos objetivos de controle, permitindo que as organizações otimizem a alocação de recursos, alavanquem sinergias e evitem a duplicação de esforços.

Tabela 4.4: Unidades de Contexto da Categoria 1

Categoria 1 - Atuação das linhas
O modelo de três linhas e como as linhas podem atuar no contexto da segurança cibernética dentro das organizações
I. O modelo de três linhas é amplamente adotado pelas instituições que compõem o ecossistema financeiro brasileiro. II. O modelo de três linhas é robusto e adequado para auxiliar as instituições a gerir riscos corporativos. III. O modelo de três linhas precisa ser reavaliado constantemente para evoluir continuamente e responder de maneira mais eficaz as demandas do negócio. IV. O modelo de três linhas para ser efetivo precisa deve ser implementado corretamente e as linhas de vem ter seus papéis e responsabilidades institucionais bem definidos para evitar a sobreposição de funções. V. A primeira linha deve ser formada pelos gestores operacionais e deve ser responsável pelo gerenciamento direto dos riscos cibernéticos no dia a dia. VI. A Segunda Linha engloba a gestão de riscos e conformidade, que monitoram e facilitam a implementação de práticas de governança de TI e segurança cibernética. VII. Terceira Linha deve fornecer avaliações independente e objetivas sobre a eficácia dos controles e processos estabelecidos pelas duas primeiras linhas. VIII. A terceira linha deve identificar riscos e fragilidades, propor melhorias e recomendar medidas corretivas. IV. É essencial manter sinergia e parceria entre a terceira linha com as diversas áreas e gestores da empresa, sem comprometer a independência e imparcialidade nas avaliações.

Segundo os entrevistados, alguns benefícios da adoção do Modelo de Três Linhas incluem:

- Clareza nas Responsabilidades: Define claramente as funções e responsabilidades de cada linha.
- Cobertura Abrangente: Garante que todas as áreas de segurança cibernética sejam abordadas de maneira integrada e coordenada.
- Resiliência Organizacional: Aumenta a capacidade da organização de prevenir, detectar e responder a incidentes de segurança cibernética.
- Confiança e Conformidade: Melhora a confiança de stakeholders e assegura conformidade com regulamentações de segurança cibernética.

Da mesma forma, foi possível consolidar os seguintes desafios na adoção do Modelo:

- Integração e Colaboração: Assegurar uma comunicação eficaz e colaboração entre as três linhas.

- Recursos e Capacitação: Fornecer recursos adequados e capacitação contínua para todas as linhas.
- Adaptação e Flexibilidade: Ajustar a estrutura conforme as ameaças evoluem e as necessidades organizacionais mudam.

4.3 CATEGORIA 2 - RELACIONAMENTO COM AS DEMAIS ÁREAS DA INSTITUIÇÃO

A Categoria 2, chamada “Relacionamento com as demais áreas da instituição”, tem como finalidade principal identificar as formas pelas quais a auditoria interna pode colaborar e interagir com outras áreas da empresa para identificar e mitigar riscos cibernéticos. Este objetivo envolve a análise de como a auditoria interna se comunica, coordena e trabalha em conjunto com departamentos como Tecnologia da Informação (TI), Segurança da Informação e outras áreas operacionais e administrativas.

Parceira e Colaboração com os departamentos de TI e de Segurança Cibernética - A terceira linha pode revisar e validar as políticas e práticas implementadas por esses departamentos, oferecendo uma perspectiva externa e imparcial, além de identificar lacunas nos controles de segurança existentes e trabalhar junto com esses departamentos para o desenvolvimento de soluções robustas. Em contrapartida, a TI e a segurança da informação também podem fornecer informações técnicas e atualizações sobre as ameaças emergentes que a auditoria interna deve considerar em suas avaliações.

[68] e [69], realçaram que a parceira e colaboração com os departamentos de TI e de Segurança Cibernética são importantes, pois, todas as áreas de negócio e processos empresariais são afetados pelas tecnologias e pelas ameaças cibernéticas. De maneira complementar, pode-se destacar a unidade de registro do ENTR07, que realizou a seguinte observação: *"A auditoria interna pode atuar como uma parceira das áreas de TI e segurança cibernética ao realizar avaliações de riscos nas cadeias de suprimento de software da organização, fornecendo reporte e indicando melhorias quando necessário".*

Interação com as Áreas de Negócio - A auditoria interna deve manter uma comunicação regular com as áreas de negócio para entender como os processos empresariais são afetados pelas tecnologias e pelas ameaças cibernéticas. Ao interagir com essas áreas, a terceira linha pode identificar e fortalecer pontos críticos onde os riscos cibernéticos poderiam ter um impacto mais significativo.

Sobre essa unidade de contexto, o entrevistado ENTR03 fez a seguinte contribuição: *"A auditoria interna pode ajudar a mapear onde os dados sensíveis são armazenados e processados e avaliar os riscos específicos de cada área. Essa análise permite que medidas de segurança personalizadas sejam implementadas nas operações cotidianas".*

Projetos de Auditoria Colaborativa - Realizar projetos de auditoria em colaboração com outras funções auditáveis para uma compreensão mais profunda das operações e dos desafios específicos enfrentados por diferentes áreas.

O entrevistado ENTR04 destacou o seguinte em sua unidade de contexto sobre o tópico: *"A terceira linha deve realizar auditorias conjuntas com departamentos como Finanças e Operações para entender e*

examinar como os riscos cibernéticos podem afetar essas áreas".

Integração com a Gestão de Riscos - Trabalhar de forma integrada com o departamento de gestão de riscos permite que a auditoria interna compreenda melhor o panorama de riscos da organização. Juntos, eles podem desenvolver uma visão abrangente dos riscos cibernéticos, priorizando-os de acordo com o impacto potencial sobre a empresa. A gestão de riscos também pode ajudar a auditoria interna a alinhar suas iniciativas de auditoria com as estratégias mais amplas de gerenciamento de riscos da empresa.

Adicionalmente, o ENTR06 realizou o seguinte comentário sobre o tópico: *"Quando a terceira linha trabalha de maneira integrada com a Gestão de Riscos contribui para o estabelecimento de uma linguagem de uso comum dentro da organização, desenvolvendo uma visão abrangente sobre os riscos e ameaças emergentes".*

[47] afirma que as interações regulares com as duas primeiras linhas permitem que a equipe de auditoria interna compreenda as mudanças nos perfis de risco cibernético, as alterações nos regulamentos e as modificações nas estratégias de negócios.

Comunicação e Reportes Regulares para a Alta Direção - A auditoria interna deve relatar periodicamente à alta direção suas preocupações, os apontamentos realizados e sobre o estado da segurança cibernética na organização, incluindo riscos identificados, progresso das iniciativas de mitigação, recomendações para melhorias e atualizações sobre as ações corretivas tomadas. Isso garante que os administradores estejam cientes dos riscos cibernéticos enfrentados pela organização e bem informados para a tomada de decisões estratégicas. Em contrapartida, a alta direção, por sua vez, pode apoiar a implementação de iniciativas e recomendações de auditoria por meio de políticas, alocação de recursos e promovendo o trabalho dos auditoria.

O entrevistado ENTR15 fez a seguinte contribuição em sua unidade de registro sobre o assunto: *"Ao realizar um planejamento periódico e demandar a aprovação da alta administração da empresa para a sua execução, a terceira linha tem a oportunidade de direcionar os esforços nos temas e riscos mais estratégicos para a organização".*

[3], [14], [29] e [78], sublinharam a pertinência de reporte periódico a alta administração sobre preocupações, apontamentos e conclusões de avaliações. Os entrevistados de mesmo modo, enfatizaram que o relacionamento com os intervenientes é fundamental para garantir o sucesso das avaliações.

Participação em Comitês - A auditoria interna deve ter uma presença ativa em comitês relevantes. Isso permite que a auditoria interna compartilhe suas descobertas e trabalhe de maneira proativa com outras partes da organização para endereçar e mitigar riscos a nível estratégico, fornecendo avaliações abrangentes baseadas em suas auditorias e ajudar na formulação de políticas.

O entrevistado ENTR07 adicionou a seguinte informação em sua unidade de registro sobre o assunto: *"Além da participação em comitês estratégicos como de Risco, Segurança e Tecnologia, é fundamental a existencia de um comitê de auditoria para discutir e direcionar as ações e as avaliações da auditoria interna dentro do contexto organizacional".*

A participação ativa da auditoria interna em Comitês de Risco, Segurança e Tecnologia foi destacado por [69] e [75] e endossada pelos entrevistados, que acrescentaram que a realização de treinamentos

conjuntos e simulações de crise em conjunto com áreas intervenientes podem ser uteis para preparar os atores para casos reais.

Treinamentos Conjuntos e Simulações de Crise - Realizar treinamentos e simulações de crise em conjunto com diferentes áreas pode ajudar a preparar a organização para responder com mais efetividade a incidentes críticos. Essas atividades ajudam a testar a eficácia dos planos de resposta e a melhorar a coordenação entre os departamentos durante uma crise real.

Em relação a essa unidade de contexto, o entrevistado ENTR05 fez o seguinte comentário: *"Em uma simulação de um ataque cibernético, a auditoria interna pode analisar a comunicação entre as equipes de TI e de gestão de crise. Essa participação permite identificar áreas de melhoria e garantir que a organização esteja melhor preparada para lidar com incidentes reais".*

Tabela 4.5: Unidades de Contexto da Categoria 2

Categoria 2 - Relacionamento com as demais áreas da instituição
Como a auditoria interna pode colaborar e interagir com outras áreas da empresa para identificar e mitigar riscos cibernéticos
I. Atuar em estreita parceira e colaboração com os departamentos de TI e de segurança cibernética, para identificar eventuais lacunas nos controles de segurança existentes. II. Manter uma comunicação regular com as áreas de negócio para entender como os processos empresariais são afetados pelas tecnologias e pelas ameaças cibernéticas. III. Realizar projetos de auditoria em colaboração com outras funções auditáveis para uma compreensão mais profunda das operações e dos desafios específicos enfrentados por diferentes áreas. IV. Trabalhar de forma integrada com o departamento de gestão de riscos para alinhar suas iniciativas de auditoria com as estratégias mais amplas de gerenciamento de riscos da empresa. V. Comunicar e reportar regularmente à alta direção as preocupações, os apontamentos realizados e sobre o estado da segurança cibernética na organização. VI. Participação em comitês relevantes, compartilhando descobertas e trabalhando de maneira proativa com outras partes da organização para endereçar e mitigar riscos a nível estratégico. VII. Participando de treinamentos e simulações de crise em conjunto com diferentes áreas para preparar a organização a responder com mais efetividade a incidentes críticos.

Segundo os entrevistados, alguns benefícios do relacionamento próximo da Auditoria Interna com as demais Áreas da Instituição incluem:

- Perspectiva Externa e Imparcial: A auditoria interna oferece uma visão independente das políticas e práticas, ajudando a identificar lacunas nos controles de segurança e a desenvolver soluções robustas.
- Informações Técnicas e Atualizações: TI e Segurança da Informação fornecem informações sobre ameaças emergentes, enriquecendo a avaliação da auditoria interna.
- Compreensão dos Processos Empresariais: Ao interagir com as áreas de negócio, a auditoria interna entende como as tecnologias e ameaças cibernéticas impactam os processos empresariais, permitindo uma abordagem mais direcionada na mitigação de riscos.
- Mapeamento de Dados Sensíveis: Identificação e avaliação dos riscos específicos de cada área, promovendo medidas de segurança personalizadas.

- Visão Aprofundada das Operações: Realizar auditorias conjuntas com outras funções permite uma compreensão mais detalhada dos desafios enfrentados, especialmente em áreas como Finanças e Operações, e como os riscos cibernéticos podem afetá-las.
- Visão Abrangente dos Riscos: Trabalhar junto com a gestão de riscos ajuda a desenvolver uma visão completa dos riscos cibernéticos, priorizando-os de acordo com seu impacto potencial.
- Alinhamento Estratégico: As iniciativas de auditoria interna são alinhadas com as estratégias de gerenciamento de riscos da empresa.
- Tomada de Decisões Informadas: Relatórios periódicos garantem que a alta direção esteja ciente dos riscos cibernéticos, possibilitando decisões estratégicas bem-informadas.
- Apoio na Implementação de Iniciativas: A alta direção pode alocar recursos e promover as recomendações da auditoria interna.
- Compartilhamento de Descobertas: A presença em comitês permite que a auditoria interna compartilhe suas descobertas e trabalhe de maneira proativa na formulação de políticas e mitigação de riscos.
- Preparação para Incidentes Críticos: Treinamentos e simulações melhoram a resposta a crises, testando a eficácia dos planos de resposta e a coordenação entre departamentos.

Da mesma forma, foi possível consolidar os seguintes desafios na relação da Auditoria Interna com as demais Áreas da Instituição:

- Barreiras de Comunicação: Diferenças de terminologia e foco entre departamentos podem dificultar a comunicação eficaz.
- Coordenação Complexa: Sincronizar agendas e prioridades entre diferentes áreas pode ser desafiador, especialmente em grandes organizações.
- Cultura Organizacional: Pode haver resistência à auditoria interna por parte de outras áreas que veem as auditorias como intrusivas ou críticas.
- Implementação de Recomendações: A adoção das recomendações da auditoria pode ser lenta ou encontrar resistência, especialmente se envolver mudanças significativas nos processos.
- Alocação de Recursos: Garantir que a auditoria interna tenha os recursos necessários para colaborar efetivamente com outras áreas pode ser um desafio, especialmente em tempos de restrições orçamentárias.
- Conflitos de Prioridade: As diferentes áreas podem ter prioridades conflitantes, dificultando a colaboração em iniciativas de auditoria.
- Compatibilidade de Sistemas: Integrar diferentes sistemas tecnológicos utilizados por TI, Segurança da Informação e outras áreas pode ser tecnicamente complexo.
- Atualização Contínua: Manter-se atualizado com as rápidas mudanças tecnológicas e novas ameaças cibernéticas exige um esforço contínuo de todas as áreas envolvidas.
- Proteção de Informações Sensíveis: Colaborar com outras áreas requer a troca de informações sensíveis, aumentando o risco de vazamentos ou uso indevido.

- Compliance e Regulamentações: Assegurar que todas as colaborações estejam em conformidade com regulamentações de proteção de dados, como a LGPD, pode adicionar complexidade às interações.

4.4 CATEGORIA 3 - ESTRATÉGIA CORPORATIVA

A Categoria 3, denominada "Estratégia Corporativa", tem como objetivo aprofundar a compreensão sobre a maneira como os entrevistados percebem que as instituições financeiras devem integrar a gestão de riscos cibernéticos em sua estratégia corporativa. Ao analisar as percepções dos participantes, a categoria pretende fornecer uma visão sobre a integração dos riscos cibernéticos na estratégia corporativa e o papel da auditoria interna em assegurar essa integração de maneira eficiente e alinhada com os objetivos organizacionais.

Envolvimento da Alta Gestão - O aspecto mais importante destacado envolve o comprometimento dos níveis mais altos de gestão, incluindo o conselho de diretores e a alta administração. Eles devem entender a importância da segurança cibernética e apoiar a integração da gestão de riscos cibernéticos nas decisões estratégicas. Isso pode ser alcançado através de apresentações regulares sobre o estado da segurança cibernética e os riscos emergentes que podem impactar a organização.

A respeito dessa unidade de contexto, o entrevistado ENTR02 realizou a seguinte contribuição:

> *"Para envolver a alta administração no tema é importante que os gestores, com apoio das áreas de controles internos e de auditoria, busquem os administradores com uma avaliação prévia da maturidade da organização em segurança cibernética, para assim, mostrar ao conselho qual a real situação atual da instituição. Se a maturidade for boa, é importante não pode deixar o nível cair, porém, infelizmente, o que geralmente acontece é que a empresa tem nível de maturidade baixo e precisa aportar capital significativo, de maneira rápida, para fazer frente as ameaças existentes".*

[86] enfatiza a importância de monitorar continuamente a maturidade das capacidades de cibersegurança como uma prática essencial para a gestão eficaz de riscos cibernéticos e a resiliência organizacional, mencionando que a participação da alta administração é considerada crítica para o sucesso das iniciativas de cibersegurança dentro de uma organização.

Gestão de Riscos Cibernéticos e Planejamento Estratégico - A segurança cibernética deve estar alinhada com a estratégia de negócios da organização. Isso inclui a compreensão dos objetivos de negócios e de como as práticas de segurança cibernética podem apoiar esses objetivos. A integração assegura que as medidas de segurança não apenas protejam os ativos tecnológicos, mas também promovam os interesses

comerciais da empresa.

Outro ponto levantando foi a inclusão da gestão de riscos cibernéticos nos processos de planejamento estratégico e de negócios. Isso garante que as considerações de segurança sejam parte integrante do desenvolvimento e evolução de produtos, da entrada em novos mercados e das alterações nos processos operacionais. Nesse sentido, a atividade de consultoria realizada pela auditoria interna pode contribuir de sobremaneira para construção de processos e produtos mais resilientes e robustos.

Neste Sentido, o entrevistado ENTR11 acrescentou o seguinte comentário:

> *"Para a integração do gerenciamento de riscos cibernéticos com o gerenciamento de riscos corporativos ser aplicado na prática, se faz necessário o envolvimento de alta administração em uma abordagem top-down, com incentivos e definições vindo de cima e descendo ate o nível operacional. Para isso tem de haver comunicação e colaboração afiada entre os profissionais".*

[29], [40], [59] e [60] destacaram a necessidade de integração do gerenciamento de riscos cibernéticos com o gerenciamento de riscos corporativos de maneira mais ampla, incorporando medidas de segurança nos processos organizacionais para garantir a continuidade operacional e a proteção contra atividades cibernéticas maliciosas.

Políticas de Segurança - O estabelecimento de políticas claras de segurança cibernética que estejam alinhadas com os objetivos estratégicos da empresa, foi outro fator importante mencionado. Isso inclui definir responsabilidades, processos de resposta a incidentes, e critérios para avaliação e aceitação de riscos. Neste sentido cabe ressaltar que a segurança não pode ser um “cotovelo” na instituição, atrapalhando a estratégia corporativa e o "Time do Market"da organização.

Referente a essa unidade de contexto, o entrevistado ENTR16 registrou a seguinte observação: *"A simples criação e atualização de uma politica de segurança, com a obrigatoriedade de leitura, de concordância formal e realização de workshops de conscientização para os funcionários pode ser uma mensagem clara do direcionamento estratégico da organização".*

[87] fornece requisitos para um sistema de gestão de segurança da informação (SGSI), incluindo a necessidade de políticas de segurança da informação.

Declaração de Apetite a Risco - Para que a gestão de riscos cibernéticos seja verdadeiramente eficaz, é fundamental que a declaração de apetite a risco seja elaborada de maneira clara, bem ajustada e realista. Essa declaração deve orientar a alocação apropriada de recursos financeiros destinados à implementação de controles, que devem ser suficientemente robustos para mitigar os riscos identificados, e ao mesmo tempo, não devem resultar em um investimento que exceda potenciais prejuízos observados nas análises de riscos quantitativos.

A declaração de apetite a risco precisa ser cuidadosamente desenvolvida para assegurar que os recursos sejam utilizados de forma otimizada, garantindo uma abordagem equilibrada que maximize a

proteção contra ameaças cibernéticas sem comprometer a eficiência financeira da organização. Sobre o tema, o ENTR04 afirmou o seguinte em sua unidade de registro:

> *"O exemplo mais óbvio relacionado a riscos quantitativos é a perda financeira máxima aceitável devido a um incidente de segurança. Isso pode incluir custos diretos, como multas e penalidades, ou custos indiretos, como perda de reputação e interrupção de negócios. Mas posso citar outro exemplo, o nível de exposição a vulnerabilidades, uma organização que realiza avaliações de vulnerabilidade de maneira regular, pode definir o número máximo de vulnerabilidades críticas que irá tolerar em seus sistemas antes de tomar ações corretivas".*

A alta direção e o conselho de administração desempenham um papel de destaque nesse ponto, endossando a cultura de segurança, alocando recursos e estabelecendo a direção estratégica para a gestão de riscos cibernéticos, conforme frisou [29], [67], [69] e [96].

Colaboração e Compartilhamento de Informações - A segurança cibernética é uma responsabilidade compartilhada que transcende os limites departamentais e por isso deve envolver uma cooperação estreita entre departamentos, incluindo negócio, TI, segurança, compliance e auditoria interna. Compartilhar informações e trabalhar em conjunto pode ajudar a identificar e mitigar riscos de forma mais eficiente. Além disso, compartilhar informações sobre ameaças e melhores práticas com outras organizações e agências reguladoras pode ajudar a melhorar a postura de segurança de todos os envolvidos.

O entrevistado ENTR04 realizou a seguinte observação em sua unidade de registro sobre o tema:

> *"A colaboração e compartilhamento de informações entre os setores da empresa são indispensáveis para manter a segurança do negócio. A segurança cibernética é uma responsabilidade compartilhada que transcende os limites departamentais e por isso deve envolver uma cooperação estreita entre departamentos, incluindo negócio, TI, segurança, compliance e auditoria interna".*

[57], foi além, e afirmou que quando as empresas compartilham informações sobre ameaças e vulnerabilidades, elas se prepararam melhor e respondem de maneira mais efetiva a incidentes cibernéticos. Por esse motivo, iniciativas como a Cybersecurity Information Sharing Act (CISA) nos Estados Unidos e o MISP (Malware Information Sharing Platform), de maneira global, são fundamentais para construção de um ecossistema mais robusto de proteção.

Cultura de Risco e Segurança – O tema deve permear todos os níveis da instituição, pois somente a tecnologia por si só não é suficiente para garantir a segurança do negócio. Envolver não apenas

a implementação de políticas e procedimentos, mas também a promoção ativa de conscientização sobre riscos e segurança cibernética entre todos os funcionários. Treinamentos regulares e comunicações claras sobre as políticas de segurança e gestão de riscos são fundamentais para manter todos alinhados e conscientes de suas responsabilidades. A prevenção de incidentes muitas vezes depende do comportamento dos funcionários, que devem estar preparados para identificar ameaças potenciais e os riscos associados.

O entrevistado ENTR06 adicionou a seguinte informação em sua unidade de registro sobre o assunto:

> *"Uma maneira da alta administração promover a cultura de riscos na organização é cobrar avaliações de risco na proposição de modelos de novos negócios e não aprovar iniciativas ou produtos expostos em ambientes digitais que não possuem avaliação de risco cibernético, cobrando essa visão dos gestores e induzindo a cultura na organização".*

Treinamentos contínuos e Simulações - Promover uma cultura de segurança cibernética na organização através de programas de conscientização e treinamento, assegurando que todos os colaboradores estejam informados sobre os riscos e as melhores práticas para mitigá-los. Promover programas de formação e conscientização para todos os funcionários, destacando a importância da segurança cibernética e o papel de cada um na proteção dos ativos da empresa. Isso ajuda a criar uma cultura de segurança e a reduzir os riscos de incidentes causados por erro humano.

O entrevistado registrou a seguinte contribuição em sua unidade de registro sobre o assunto:

> *"Capacitação e conscientização nesse contexto é essencial nesse pois os controles, ferramentas e soluções aplicadas para mitigar riscos cibernéticos estão se tornando mais complexas e dispendiosas financeiramente, e na ausência de mão de obra qualificada para operar essas ferramentas, avaliar e monitorar continuamente os processo os quais elas estão inseridas, pode se tornar um ponto de vulnerabilidade no processo, colocando todo o investimento realizado em risco. Desta maneira, um profissional bem treinando e capacitado em temas de segurança cibernética pode se tornar um "firewall humano", filtrando e exterminando ameaças cibernéticas mais frequentes e convencionais como o phising".*

[38] e [39], destacaram a importância de fomentar a cultura organizacional de riscos cibernéticos por meio de capacitação e de programas de conscientização e treinamento como simulações de phishing, semelhantes a [2] e [16]. Os entrevistados corroboraram essa informações acrescentando que avaliações de risco na proposição e alteração de modelos negócios podem ser uteis para promoção dessa cultura.

Tabela 4.6: Unidades de Contexto da Categoria 3

Categoria 3 - Estratégia Corporativa
Como as instituições financeiras podem integrar a gestão de riscos cibernéticos em sua estratégia corporativa
I. A Alta Gestão deve entender a importância da segurança cibernética e apoiar a integração da gestão de riscos cibernéticos nas decisões estratégicas. II. A Gestão de Riscos Cibernéticos deve estar alinhada com a estratégia da organização, compreendendo como as práticas de segurança cibernética podem apoiar os objetivos do negócio. III. Estabelecendo políticas claras de segurança cibernética que estejam alinhadas com os objetivos estratégicos da empresa. IV. Elaboração de declaração de apetite a risco clara, orientando a alocação apropriada de recursos financeiros destinados à implementação de controles. V. Colaboração e compartilhamento de informações entre departamentos, como objetivo de tornar mais efetivo a identificação e o tratamento dos riscos. VI. Promoção ativa de uma cultura de riscos e de segurança cibernética, com programas e campanhas de conscientização entre todos os funcionários VII. Capacitar os funcionários com treinamentos contínuos e simulações de ameaças com vistas a prepará-los para proteger os ativos da empresa em cenários reais de risco.

Segundo os entrevistados, alguns benefícios da inclusão da Gestão de Riscos Cibernéticos na Estratégia Corporativa incluem:

- Compromisso aparente da alta administração com a segurança cibernética.
- Liderança ativa na promoção da cultura de segurança
- Reputação e Confiança - Melhora a confiança dos clientes, parceiros e partes interessadas na capacidade da organização de proteger suas informações e reduz o risco de danos à reputação decorrentes de violações de dados.
- Vantagem Competitiva - Diferencia a organização no mercado como um líder em segurança cibernética. Pode ser usada como um fator de venda, destacando o compromisso com a proteção de dados.
- Redução de Custos - Minimiza os custos associados a incidentes cibernéticos, como recuperação de dados, tempo de inatividade e danos à reputação. Reduz os gastos com resposta a incidentes e investigações forenses.
- Promoção de uma Cultura de Segurança Cibernética com programas periódicos de educação e conscientização para todos os funcionários.

Da mesma forma, foi possível consolidar os seguintes desafios na inclusão da Gestão de Riscos Cibernéticos na Estratégia Corporativa:

- Complexidade Técnica - A segurança cibernética envolve tecnologias complexas e constantemente evolutivas, o que requer uma equipe qualificada, com conhecimento atualizado e estratégias bem definidas.
- Custo Inicial Elevado - Implementar medidas eficazes de segurança cibernética pode exigir um

investimento significativo em tecnologia e treinamento. Pode ser difícil justificar esses custos inicialmente sem uma compreensão clara dos riscos.

- Mudança Cultural - Alterar a cultura organizacional para priorizar a segurança cibernética pode ser desafiador pois requer um compromisso de todos os níveis da organização, desde a alta administração até os colaboradores.
- Integração com Processos de Negócio - Integrar a gestão de riscos cibernéticos com os processos de negócio existentes pode ser complexo pois requer coordenação entre diferentes departamentos, funções e áreas de conhecimento equidistantes.
- Necessidade de mão de obra qualificada para operar, avaliar e monitorar continuamente esses processos.
- Realização de simulações de ameaças como phishing e outros ataques para preparar os funcionários.

4.5 CATEGORIA 4 - AVALIAÇÃO DA EFETIVIDADE DOS CONTROLES DE SEGURANÇA CIBERNÉTICA

A Categoria 4, intitulada "Avaliação da efetividade dos controles de segurança cibernética", tem como objetivo principal mapear e compreender como a auditoria interna pode avaliar a efetividade dos controles de segurança cibernética implementados nas instituições. Esta categoria busca explorar os métodos e práticas utilizados para assegurar que esses controles estejam funcionando conforme o esperado, identificando possíveis falhas e sugerindo melhorias. Além disso, ela visa proporcionar uma visão sobre a capacidade desses controles de proteger as instituições contra ameaças cibernéticas, garantindo a integridade, confidencialidade e disponibilidade das informações. Dessa forma, a auditoria interna pode desempenhar um papel fundamental na manutenção da segurança cibernética, contribuindo para o fortalecimento da resiliência organizacional frente aos riscos digitais.

Profundidade das avaliações realizadas pela Auditoria Interna - Foi um tema que suscitou diferentes opiniões e reflexões. De um lado, sete entrevistados defendem que a auditoria interna deve focar nos aspectos mais gerais da gestão e governança dos processos, evitando uma abordagem granular na execução de atividades. Esta visão propõe que, ao se concentrar em avaliações de alto nível e estratégicas, a auditoria interna pode proporcionar uma visão mais abrangente e duradoura, capaz de promover ajustes sistêmicos que beneficiem toda a organização.

Nesse caso, a auditoria interna deve concentrar seus esforços nos aspectos mais amplos da gestão e governança dos processos. Esses defensores acreditam que a auditoria interna deve priorizar a avaliação das políticas, estruturas de controle e práticas de governança que regem a organização como um todo. A ideia é que, ao focar nessas áreas mais gerais, a auditoria pode garantir que os princípios fundamentais da boa gestão e governança estejam sendo seguidos, o que por sua vez, proporciona uma base sólida para a operação da organização.

O entrevistado ENTR02 forneceu o seguinte comentário em sua unidade de registro referente ao tópico:

> *"Pressupondo que a primeira e segunda linha são atuantes e realizam alguma gestão de risco, a auditoria pode atuar de maneira complementar, aproveitando as análises de primeira e segunda linha. Desta maneira, deve-se avaliar como essa gestão está sendo realizada, verificar se os riscos mapeados são de fato os mais relevantes e se os controles implementados podem de fato mitigar os riscos".*

Por outro lado, seis entrevistados reforçaram que a independência da terceira linha permite que ela também debruce suas avaliações sobre aspectos operacionais, inclusive pra efetuar novamente testes e procedimentos já realizados pela segunda linha, se for o caso.

Nesse caso, a auditoria interna também deve se dedicar a avaliações detalhadas de aspectos operacionais. Esse ponto de vista sugere que a auditoria interna deve não apenas revisar a gestão de alto nível, mas também realizar testes e procedimentos operacionais já efetuados pela segunda linha, se necessário. Isso incluiria a reavaliação de controles operacionais, a verificação de procedimentos cotidianos e a identificação de falhas ou áreas de melhoria que possam não ter sido detectadas anteriormente. Dessa forma, a auditoria interna poderia assegurar que todos os níveis da organização, desde a governança até as operações diárias, estejam funcionando de maneira eficiente e eficaz.

Em relação a essa unidade de contexto, o entrevistado ENTR09 fez o seguinte comentário: *"A auditoria interna deve se aprofundar nas atividades operacionais da primeira linha em situações onde há sinais de que os controles não estão sendo implementados de forma eficaz ou onde há riscos significativos que precisam de uma avaliação mais detalhada".*

Adicionalmente, o entrevistado ENTR03 fez o seguinte apontamento acerca do tema:

> *"A reprodução de testes pela auditoria interna também serve como um mecanismo de verificação e validação. Ela oferece uma camada adicional de garantia de que os processos estão funcionando conforme o esperado e que os riscos estão sendo gerenciados de maneira adequada. Isso é particularmente importante em áreas como segurança cibernética, que são de alta criticidade, onde os riscos podem ter consequências Incalculáveis para qualquer organização".*

A profundidade das avaliações realizadas pela auditoria interna é abordada por [11] e [84] mas não limita sua atuação. [57] e [79] destacaram a contribuição da auditoria interna na gestão do risco cibernético, fornecendo garantia independente que os processos e os controles aplicados organizacionalmente são eficazes. Para tanto, a terceira linha pode aplicar testes na primeira e segunda linha para avaliar e relatar a eficácia desses controles.

Testes de Invasão (Internos ou Externos) – Entre os apoiadores da tese de aprofundamento dos testes de auditoria em atividades mais operacionais, os testes de Invasão ou de Penetração (PenTest) foi

uma proposta de teste sugerida. Eles poderiam ser realizados pelos próprios auditores ou por empresas especializadas contratadas, com a finalidade de testar a eficácia de processos como: análise de vulnerabilidade, gestão de patches de segurança, resposta a incidentes cibernéticos, etc. Nesse caso, seria importante que as capacidades técnicas fossem bem desenvolvidas, com a finalidade de validar processos de primeira linha e identificar oportunidades de aprimoramento de maneira mais efetiva.

A respeito dessa unidade de contexto, o entrevistado ENTR03 realizou a seguinte contribuição:

> *"A contratação de empresas especializadas pode ser realizada com previsão de curva e repasse de conhecimento, onde inicialmente ela executaria os testes e, com o passar do tempo, iria transferindo o conhecimento, a responsabilidade para a auditoria, até o ponto em que esta assuma a total responsabilidade pelos testes de maneira contínua, realizando os apontamentos para a primeira linha de forma mais tempestiva. Nesse ponto, alguns podem argumentar que a independência da terceira linha poderia ser afetada, porém, ao deixar claro e documentado todos os métodos, ferramentas e critérios utilizados nos testes, essa estratégia pode contribuir muito para avaliações cada vez mais relevantes e aprofundadas da auditoria no tema".*

Gestão de Processos - Em contraponto, os apoiadores da tese de que a auditoria deve focar na gestão do processo em si, nas ferramentas utilizadas, nas etapas estabelecidas, documentação gerada e regras definidas e aplicadas, defendem que atuando dessa maneira as mudanças seriam mais estruturantes e duradouras, além de destacar desafios relacionadas a recursos humanos e financeiros.

O entrevistado ENTR04 adicionou a seguinte informação em sua unidade de registro sobre o assunto:

> *"Apesar de interessante na teoria, a absorção ou adoção de práticas de Red Team pela terceira linha, por exemplo, na execução de testes de penetração, com finalidade de desafiar o modelo e buscar fragilidades nos controles, acaba sendo inviável na prática devido à quantidade de mão de obra geralmente alocada para atividades de auditoria e dada a quantidade de atribuições e responsabilidades que esses profissionais possuem. Em dado momento, a ideia acaba sendo dissuadida em função da indisponibilidade de recursos técnicos, humanos e financeiros. Nesse ponto, a auditoria focando na gestão do processo em si, nas ferramentas utilizadas, nas etapas estabelecidas, do-*

> *cumentação gerada e regras definidas e aplicadas, realizaria mudanças mais estruturantes e duradouras. Por fim, as instituições e equipes técnicas, de maneira geral, já possuem ferramentas extremamente dispendiosas e profissionais altamente especializadas no tema, pode não ser operacionalmente eficiente desembolsar mais dinheiro contratando outras empresas e ferramentas que vão impactar tecnicamente o desempenho das redes de comunicação e de outros recursos de TI para desafiar e estressar os sistemas".*

Avaliações e Testes Conjuntos – Por outro lado, a auditoria interna pode trabalhar de perto com as equipes de TI e Segurança Cibernética para entender as políticas de segurança vigentes, os processos estabelecidos, as tecnologias implementadas e controles aplicados. A realização de avaliações e testes de segurança em conjunto, pode ajudar a identificar vulnerabilidades e ameaças mais complexas, antes que sejam exploradas por atacantes. A auditoria interna pode trazer uma perspectiva externa, independente e imparcial nessas avaliações, ajudando a identificar riscos e garantindo que todos os aspectos da segurança sejam meticulosamente testados.

Referente a essa unidade de contexto, o entrevistado ENTR05 registrou a seguinte observação:

> *"A terceira linha pode trabalhar em conjunto com as áreas de segurança cibernética e TI entendendo os processos estabelecidos, controles implementados, políticas de segurança vigentes, ferramentas e tecnologias empregadas, para realizar avaliações mais técnicas e aprofundadas e quando for o caso, emitir recomendações de melhorias mais assertivas".*

Auditoria contínua baseada em Análises Avançadas de Dados - Para auxiliar a execução das atividades de auditoria, os entrevistados reforçaram a utilização da estratégia de auditoria contínua baseada em dados, o qual, representa uma abordagem inovadora e proativa para a proteção de ativos digitais e informações sensíveis. Diferente das auditorias tradicionais, que são realizadas periodicamente, a auditoria contínua utiliza análise de dados, podendo ser inclusive em tempo real, para monitorar e avaliar continuamente os controles e processos de segurança.

Em relação a essa unidade de contexto, o entrevistado ENTR12 fez o seguinte comentário:

> *"Decisões baseadas em dados concretos tornam mais confiável a gestão de riscos cibernéticos. Utilizar ferramentas analíticas para auditoria e monitoramento de riscos cibernéticos pode significativamente aumentar a capacidade de detectar e responder a riscos emergentes. Usar dados e métricas para fundamentar recomendações e ações melhoram a credibilidade e a*

eficácia das iniciativas de segurança".

Nesse ponto, foi observada outro ponto de discordância entre os entrevistados, um lado destacou o elevado grau de precisão, a visão completa e detalhada das análises estatísticas realizadas no universo da população. Nesse contexto, destaca-se a unidade de registro do ENTR03 sobre o assunto:

"Na existência de mil ativos críticos, se novecentos ativos forem testados, eu não posso afirmar com grau de certeza, embora estatisticamente seja correto, que a organização está segura, pois é necessário apenas um ativo vulnerável ser explorado para desencadear um cadeia de eventos catastróficos".

Como contraponto, o outro lado destacou a rapidez e eficiência que pode ser alcançada em análises estatísticas realizadas em amostras, desde que devidamente escolhidas de maneira a representar o universo total com qualidade e representatividade. A respeito dessa unidade de contexto, o entrevistado ENTR06 fez a seguinte contribuição:

"Em um contexto de escassez de recursos, pode ser interessante separar uma amostra representativa para representar o todo ou ate mesmo priorizar o que pode estar mais exposto ou é mais critico para a organização".

A estratégia de auditoria contínua baseada em dados também foi destacada nos trabalhos de [15] [18] [21] e [94]. De maneira complementar, [21] e [73] apontaram que o alavancar a análise de dados, a terceira linha pode identificar tendências e anomalias indicativas de uma ameaça cibernética, permitindo assim uma resposta proativa e uma tomada de decisão torna mais confiável para a gestão de riscos cibernéticos.

Estratégia de Monitoramento Contínuo de Segurança e Integração de Tecnologias Avançadas - A auditoria interna pode avaliar como as áreas de segurança cibernética e TI implementam ferramentas de monitoramento contínuo que detectem atividades anormais ou suspeitas em tempo real. Isso inclui o uso de sistemas de detecção e prevenção de intrusões (IDS/IPS), monitoramento de tráfego de rede, análise de comportamento de usuários e entidades (UEBA) e SIEM (Security Information and Event Management), que agrega e analisa dados de segurança em tempo real para identificar potenciais ameaças. Caso a estratégia da instituição não integre de maneira efetiva esses dipositivos ou não apresente resultados consistentes, a auditoria pode recomendar o estudo de viabilidade e criação de plano de ação para realizar os ajustes nos processos.

O entrevistado ENTR14 realizou o seguinte comentário em sua unidade de contexto referente ao tópico:

"Investir em tecnologia de ponta para monitoramento, detecção e resposta a ameaças pode significar a diferença entre uma violação menor e uma catástrofe. Ferramentas avançadas, como IA para detecção de anomalias e automação para resposta a incidentes permitem uma abordagem mais dinâmica e adaptativa para enfrentar os riscos cibernéticos e aumentam significativamente a capacidade de uma organização de

responder a ameaças".

Inteligência de Ameaças e Análise de Tendências - Os auditores podem compilar e analisar dados sobre violações e incidentes de segurança anteriores, além de tendências atuais em segurança cibernética para prever áreas de risco emergentes. Isso pode incluir parcerias com outras organizações, agências governamentais ou grupos da indústria para compartilhar informações sobre ameaças.

Em relação a essa unidade de contexto, o entrevistado ENTR10 fez o seguinte comentário:

> *"As informações obtidas com a inteligência podem aconselhar a gestão sobre áreas que precisam de atenção imediata ou reforço de segurança. Compilar e apresentar relatórios sobre tendências de ameaças cibernéticas e incidentes de segurança podem fornecer informações importantes para direcionar o trabalho da terceira linha, além de auxiliar a alta administração na tomada de decisões estratégicas e nos investimentos em segurança cibernética".*

Relatórios de Segurança e Painéis de Controle - Desenvolver relatórios de segurança e painéis de controle que apresentem uma visão do status da segurança cibernética da organização. Estes relatórios podem destacar vulnerabilidades, incidentes de segurança, e o progresso das iniciativas de mitigação. Para viabilizar a montagem e o acompanhamento desses painéis, a auditoria pode atuar de maneira continua com auxilio de ferramentas analíticas para visualização dos dados. Isso pode ser muito útil em um cenário em que a primeira e segunda linha geralmente já possuem bases de dados e datalakes com diversas informações disponíveis sobre os processos.

O entrevistado ENTR01 fez o seguinte apontamento em sua unidade de registro acerca do tema:

> *"Com a volatilidade apresentada hoje no mundo corporativo, de TI e de segurança cibernética, auditorias com ciclos de avaliações periódicas podem não ser suficientes para identificar de maneira tempestiva os principais riscos emergentes aos quais a instituição está sujeita. Isso pode resultar em prejuízos financeiros, de marca e prejudicar a geração de valor à organização por parte da área de auditoria. Qualquer alteração no ambiente tecnológico pode mudar o cenário de exposição a riscos da instituição, e um trabalho de produção continua de informações em forma de um painel sobre o estado da segurança pode ser mais assertivo na proposição de melhorias estruturantes".*

[21], [81] e [94] destacaram que dados obtidos devem subsidiar a construção de relatórios de segurança com informações sobre a quantificação de riscos e painéis de controle que apresentem uma visão do status da segurança cibernética da organização. De maneira equivalente, os entrevistados enfatizaram

que os auditores podem criar análise de tendências e acompanhar relatórios de inteligência de ameaças para definir estratégias de analise e quantificação de risco dentro das instituições, construído indicadores de desempenho e de risco próprios ou em conjunto com as áreas e, esforço conjunto.

Métricas e uso de indicadores - Métricas e indicadores podem fornecer uma visão clara e objetiva do estado atual da segurança cibernética na organização. Através da utilização dessas métricas, a auditoria interna pode identificar áreas que necessitam de melhorias, fornecer recomendações precisas e mensuráveis, e assegurar que os controles de segurança estão alinhados com os objetivos estratégicos da empresa.

A auditoria, em conjunto com as áreas de segurança cibernética e de TI, pode estabelecer indicadores-chave de risco (KRI) e indicadores-chave de desempenho (KPI) para monitorar continuamente o ambiente de segurança cibernética da instituição. Esses indicadores são projetados para fornecer uma visão abrangente e em tempo real das ameaças e vulnerabilidades potenciais.

Os entrevistados reconhecem que métricas e indicadores para auditar e monitorar continuamente os processo de segurança cibernética contribui sobremaneira para indicar fragilidades e oportunidades de melhoria. A respeito dessa unidade de contexto, o entrevistado ENTR05 disse o seguinte:

> *"Alterações nos KRIs, como um aumento repentino no número de tentativas de intrusão ou na frequência de vulnerabilidades detectadas, podem indicar a necessidade de uma revisão mais detalhada das defesas atuais ou ações imediatas para mitigar riscos emergentes. Da mesma forma, KPIs podem ser utilizados para avaliar a eficácia das políticas de segurança implementadas, como o tempo de resposta a incidentes, a taxa de sucesso na mitigação de ameaças e a conformidade com os padrões de segurança estabelecidos".*

[21], [56] e [94], ressaltaram a importância de as organizações definirem e acompanharem indicadores de performance e desempenho em seus trabalhos.

Entre os indicadores apontados pelos entrevistado, destaca-se como imprescindíveis para qualquer instituição financeira:

- Taxa de Incidentes de Segurança em período específicos.
- Tempo Médio para Detectar (MTTD) e Tempo Médio para Responder ou Recuperar (MTTR) de incidentes de segurança.
- Percentual de correções de vulnerabilidades dentro e fora dos prazos.
- Taxa de Falsos Positivos e Negativos gerados por soluções.
- Nível de Conscientização e taxa de participação em treinamentos de segurança.
- Efetividade dos Planos de Continuidade de Negócios e de Resposta a Simulações de Ataque.

Frameworks e boas práticas - Os entrevistados destacam a importância de adotar frameworks que oferecem estruturas padronizadas para a gestão de processos, avaliação de riscos e controles de segurança.

A utilização de boas práticas e frameworks é essencial para garantir que a auditoria interna possa avaliar de maneira completa, precisa e eficiente a gestão de riscos cibernéticos, promovendo uma maior segurança e resiliência organizacional.

O entrevistado ENTR07 realizou a seguinte observação em sua unidade de registro sobre o tema:

> *"Frameworks e boas práticas geralmente são produtos testados, aprovados e melhorados constantemente pela comunidade e oferecem uma oportunidade para "conversar" com o "resto do mundo"em eventos, fóruns e organizações".*

Os entrevistados indicaram o NIST CSF [88], ISO/IEC 27001 [87], COBIT 2019 [48] e o CIS Controls como estruturas essências para ajudar tanto a organização quanto a auditoria interna a gerir e avaliar riscos cibernéticos. A pesquisa bibliográfica ainda indicou que o Cybersecurity Capability Maturity Model (C2M2) (C2M2, 2021) pode ser útil na verificação e na monitoração da maturidade cibernética da empresa.

Tabela 4.7: Unidades de Contexto da Categoria 4

Categoria 4 - Avaliação da efetividade dos controles de segurança cibernética
Como a auditoria interna pode avaliar a efetividade dos controles de segurança cibernética implementados nas instituições
I. Verificar aspectos de gestão e governança dos processos, realizando avaliações de alto nível e estratégicas.
II. Realizar ou contratar empresas especializadas para efetuar testes de Invasão ou de Penetração (PenTest).
III. Avaliar o processo de gestão de vulnerabilidade, nas ferramentas utilizadas, nas etapas estabelecidas, documentação gerada e regras definidas e aplicadas.
IV. Realizar avaliações e testes de segurança em conjunto equipes de TI e Segurança Cibernética.
V. Utilizar auditoria contínua baseada em dados e informações para monitorar e avaliar continuamente os controles e processos de segurança.
VI. Avaliar como as áreas de segurança cibernética e TI implementam ferramentas de monitoramento contínuo que detectem atividades anormais ou suspeitas em tempo real.
VII. Compilar e analisar dados sobre violações e incidentes de segurança anteriores, além de tendências atuais em segurança cibernética para identificar áreas de risco emergente.
VIII. Desenvolver relatórios de segurança e painéis de controle que apresentem uma visão do status da segurança cibernética da organização.
IX. Estabelecer Métricas e indicadores que forneçam uma visão clara e objetiva do estado atual da segurança cibernética na organização.
X. Adotar frameworks que oferecem estruturas padronizadas para a gestão de processos, avaliação de riscos e controles de segurança.

Segundo os entrevistados, alguns benefícios da avaliações da efetividade de controles de segurança cibernética realizadas pela Auditoria Interna incluem:

- Visibilidade: Relatórios de segurança e painéis de controle fornecem uma visão clara do estado

da segurança cibernética, facilitando a tomada de decisões informadas.

- Identificação de Vulnerabilidades: Ajuda na identificação de vulnerabilidades e na priorização das ações de mitigação.
- Previsão de Riscos: A análise de tendências permite prever áreas de risco emergentes e se preparar para ameaças futuras.
- Tomada de Decisão: Relatórios de inteligência fornecem informações relevantes para a alta administração, auxiliando na alocação de recursos e investimentos em segurança.
- Monitoramento Contínuo: KRIs e KPIs permitem o monitoramento contínuo e em tempo real da segurança cibernética, facilitando a detecção precoce de problemas.
- Avaliação da Eficácia: Ajudam a medir a eficácia das políticas e práticas de segurança implementadas.
- Ação Proativa: Permitem uma resposta rápida e proativa a alterações nos indicadores, mitigando riscos emergentes.
- Fortalecimento da Resiliência Organizacional: Uma auditoria eficaz reforça a capacidade da organização de resistir e se recuperar de incidentes cibernéticos.
- Validação de Processos: Testes de penetração ajudam a validar processos como análise de vulnerabilidade, gestão de patches de segurança e resposta a incidentes cibernéticos.
- Desenvolvimento de Capacidades Técnicas: A prática pode desenvolver as capacidades técnicas da equipe interna, especialmente se houver um processo de transferência de conhecimento de empresas especializadas para a equipe de auditoria.
- Independência da Auditoria: A auditoria pode atuar de forma independente ao realizar testes e apontar melhorias, contribuindo para uma visão imparcial dos riscos.
- Eficiência Operacional: Focar na gestão dos processos de segurança pode resultar em mudanças estruturantes e duradouras, aumentando a eficiência operacional.
- Auditoria Planejada: Torna a preparação e execução das auditorias mais estruturada e eficiente.
- Uniformidade nas Avaliações: Proporciona uma abordagem padronizada que garante consistência na avaliação de riscos cibernéticos.
- Identificação Completa de Riscos: Frameworks abrangentes ajudam a identificar todos os possíveis riscos e vulnerabilidades.
- Detalhamento de Controles: Fornecem uma lista detalhada de controles de segurança a serem implementados.
- Otimização de Recursos: Permite que os recursos sejam direcionados para áreas de maior risco e evita o desperdício de recursos financeiros e técnicos em ferramentas e serviços adicionais desnecessários, aproveitando ao máximo as capacidades existentes.
- Medida da Efetividade dos Controles de Segurança - Permite avaliar a performance e a eficiência das medidas de segurança implementadas pela organização, garantindo que estão alinhadas com os objetivos estratégicos.

- Identificação de Áreas de Melhoria - Através das métricas, a auditoria interna pode identificar áreas que necessitam de melhorias, fornecendo recomendações precisas e mensuráveis.
- Transparência e Comunicação - Melhora a comunicação e a transparência com stakeholders internos e externos sobre o estado da segurança cibernética da organização.

Da mesma forma, foi possível consolidar os seguintes desafios:

- Ausência ou insuficiência de atuação da segunda linha pode sobrecarregar a terceira linha e comprometer as avaliações realizadas, além de expor a auditoria junto a primeira linha.
- Atuação em consultoria pela auditoria interna avançar ao ponto de tornar a auditoria parte do processo comprometendo a sua independência e objetividade.
- Custo de Implementação: As ferramentas de monitoramento contínuo podem ser caras e exigem investimento significativo em infraestrutura e treinamento.
- Complexidade Operacional: Gerenciar e analisar os dados gerados por essas ferramentas pode ser complexo e exigir recursos especializados.
- Integração de Dados: Agregar dados de diferentes fontes pode ser complicado e demorado.
- Manutenção e Atualização: Manter os painéis e relatórios atualizados exige esforços contínuos.
- Coleta e Análise de Dados - Dificuldade na coleta e análise de dados precisos e consistentes, especialmente em organizações com sistemas e processos complexos.
- Confiança nas Fontes: A confiabilidade e a precisão dos dados de inteligência são imprescindíveis e podem variar entre diferentes fontes.
- Interpretação dos Resultados - Interpretação das métricas pode ser complexa e exigir conhecimentos especializados para evitar conclusões erradas.
- Definição de Indicadores e Métricas Relevantes - Desafio em definir quais indicadores e métricas são mais relevantes e alinhadas com os objetivos e riscos específicos da organização.
- Desenvolvimento de Habilidades: Necessidade de constante atualização e desenvolvimento das capacidades técnicas da equipe de auditoria para acompanhar as evoluções das ameaças cibernéticas.
- Dependência de Especialistas: Dependência de empresas especializadas inicialmente para realizar testes de penetração e transferência de conhecimento.
- Conflitos de Interesse: A realização de testes de penetração pela própria equipe de auditoria pode afetar a independência, necessitando de uma clara documentação dos métodos e critérios utilizados.
- Disponibilidade de Mão de Obra: Limitação de recursos humanos e técnicos, dificultando a absorção de práticas de Red Team pela equipe de auditoria.
- Orçamento Restrito: Restrição financeira para a contratação de ferramentas e serviços adicionais, o que pode impactar a capacidade de realizar testes de segurança mais abrangentes.
- Alinhamento entre Departamentos: Desafio de alinhar os objetivos e processos entre a auditoria interna e as equipes de TI e Segurança Cibernética.

- Customização: Frameworks muitas vezes precisam ser adaptados às necessidades e contextos específicos da organização, o que pode ser desafiador.
- Complexidade: Implementação pode ser complexa e exigir um alto nível de conhecimento e experiência.
- Investimento Inicial: Pode haver um custo inicial significativo para implementar frameworks e práticas recomendadas.
- Capacitação: Necessidade de pessoal qualificado para implementar e manter os frameworks.

4.6 CATEGORIA 5 - AMBIENTE REGULATÓRIO E CONFORMIDADE

A Categoria 5, intitulada "Ambiente regulatório e conformidade", tem como objetivo aprofundar a compreensão sobre como a auditoria interna pode desempenhar um papel significativo na garantia da conformidade com normas e regulamentos relacionados à segurança cibernética dentro das instituições. Esta categoria busca identificar e detalhar as formas pelas quais a auditoria interna pode atuar para assegurar que as instituições estejam aderindo às normas, boas práticas, exigências legais e regulamentares vigentes no campo da segurança cibernética.

Monitoramento Contínuo – Estabelecer processos de monitoramento contínuo é vital para que a organização permaneça em conformidade ao longo do tempo, mesmo que novas regulamentações sejam introduzidas ou as existentes sejam atualizadas. Isso pode incluir a implementação de sistemas de gestão de conformidade que utilizam tecnologia para rastrear mudanças regulatórias e avaliar o impacto na organização, além de envolver o uso de indicadores-chave de desempenho (KPIs), indicadores-chave de risco (KRIs) e outras métricas para medir a eficácia contínua dos controles e a aderência às práticas de conformidade.

A respeito dessa unidade de contexto, o ENTR01 realizou a seguinte contribuição:

> *"O ambiente regulatório atualmente é complexo para qualquer organização, quando se trata do setor financeiro, a situação fica ainda mais agravada pois elas são extremamente visadas e atacadas. Com a aceleração digital dos últimos anos e o aumento massivo do uso de dispositivos móveis, a possibilidades de ataques cibernéticos se multiplicaram exponencialmente. Nesse sentido, instituições, principalmente com operações globais, estão sujeitas a diversos tipos de normas e regulações, e para realizar o monitoramento desse ambiente regulatório, estabelecer uma estratégia ou um framework pode auxiliar a organização a gerir de maneira eficaz o risco de não conformidade".*

O entrevistado ENTR09 indicou o seguinte exemplo de exigência regulatória em sua unidade de

registro sobre o tema:

> *“A título de exemplo, a NYDFS 23 NYCRR 500, do Departamento de Serviços Financeiros do Estado de Nova York (DFS), exige que as instituições financeiras que fazem negócio em território americano realizem varreduras de vulnerabilidade e testes de invasão periodicamente em suas estruturas, exigindo inclusive a apresentação dos relatórios e cobrando a correção das vulnerabilidades classificadas como alta ou críticas".*

De maneira complementar, o entrevistado ENTR16 indicou o seguinte exemplo referente a conformidade:

> *"Para estar em conformidade com o PCI DSS, as intuições devem realizar obrigatoriamente um teste de penetração a cada doze meses ou a cada grande mudança na infraestrutura, especialmente no ambiente de dados do titular do cartão. (Requisito 11.4 e 11.4.2 - PCI-DSS v4.0 - Diretrizes de segurança)".*

[21], [80] e [96] enfatizaram a relevância da auditoria interna na garantia da conformidade legal, o apoio na monitoração do ambiente regulatório e os impactos e danos que podem ser causados na imagem e reputação das organizações como consequência de ataques cibernéticos. De maneira complementar, [81] enfatizou o desafio de monitorar continuamente o ambiente regulatório para certificar que alterações e criações de normas sejam devidamente refletidas nas politicas e nos processos da instituição.

Colaboração com a Segunda Linha – Trabalhar em estreita colaboração com a Segunda Linha e setores de conformidade é fundamental para garantir uma visão unificada e suficientemente abrangente da conformidade em toda instituição. Isso pode envolver a realização de auditorias conjuntas e o desenvolvimento de uma estratégia integrada para lidar com os requisitos legais e regulatórios.

> *"Ao Identificar e avaliar riscos associados à não conformidade com regulamentos específicos, a auditoria interna deve entender não apenas os requisitos técnicos, mas também o impacto potencial de não os atender, ajudando a priorizar as áreas que requerem atenção imediata".*

[47] e [68] destacaram a importância da comunicação entre as diversas linhas para permitir que a auditoria interna entenda as mudanças nos perfis de risco cibernético, eventuais alterações normas e mudanças nas estratégias de negócios.

Auditorias Regulares - Ainda que atue de maneira próxima a segunda linha, a Auditoria Interna não pode abster-se de realizar avaliações periódicas em conformidade pois essas auditorias ajudam a iden-

tificar áreas onde a organização pode estar em risco de não conformidade, permitindo correções antes que possam resultar em sanções, multas ou danos reputacionais.

> *"Acima de tudo, a Terceira Linha tem a prerrogativa da independência e a responsabilidade de relatar para o conselho de administração o status da conformidade da organização com as normas e regulamentos de segurança cibernética. Esses relatórios ajudam os líderes empresariais a compreenderem os riscos de conformidade e a tomarem decisões informadas sobre como endereçá-los".*

[77] e [78] descobriram que auditorias internas atuantes podem reduzir significativamente os riscos regulatórios e aumentar a conformidade de uma instituição a normas, leis e regulamentos relevantes.

Interface com Reguladores, Auditores e Consultores Externos – A Terceira Linha deve atuar como ponto de contato, coordenando a preparação da instituição para auditorias regulatórias externas, assegurando que toda a documentação necessária esteja pronta, certificando-se de que as questões de conformidade sejam adequadamente abordadas, facilitando as inspeções e compartilhando informações sobre práticas de segurança e conformidade. Isso inclui preparar documentação e evidências de conformidade para revisão regulatória.

Em relação a essa unidade de contexto, o entrevistado ENTR13 fez o seguinte comentário:

> *"A auditoria interna pode colaborar com consultores externos ou especialistas em segurança cibernética para realizar auditorias especializadas ou para obter orientações sobre regulamentações complexas. Isso assegura que a organização esteja utilizando as melhores práticas da indústria e cumprindo com as normas mais recentes".*

Esses registros também foram realizados nas pesquisas de [14] e [77], que além disso, destacaram qua a terceira linha deve ser a ponte entre a gestão da organização e seu conselho.

Conformidade não necessariamente é igual a segurança - Manter-se atualizado com os regulamentos de segurança cibernética e as obrigações legais é fundamental para evitar penalidades e garantir a confiança das partes interessadas, entretanto, isso não garante segurança total.

O entrevistado ENTR08 adicionou a seguinte informação em sua unidade de registro sobre o assunto: *"É importante ir além dos requisitos de conformidade para construir uma arquitetura de segurança que realmente proteja adequadamente os ativos mais críticos da organização".*

[21] afirmou que o trabalho da auditoria interna é relevante pois eles examinam a conformidade da corporação com as obrigações legais e regulatórias e avaliam se a corporação está adequadamente protegida contra ameaças cibernéticas.

Tabela 4.8: Unidades de Contexto da Categoria 5

Categoria 5 - Ambiente regulatório e conformidade
Como a terceira linha pode contribuir para garantia da conformidade com normas e regulamentos relacionados à segurança cibernética dentro das instituições
I. Monitoramento contínuo para identificar quando novas regulamentações foram introduzidas ou atualizações serem realizadas em normas existentes. II. Trabalhar em colaboração com a Segunda Linha para obter uma visão unificada e suficientemente abrangente da conformidade em toda instituição. III. Realizar Auditorias Regulares em conformidade para identificar áreas com risco de não conformidade IV. Realizando a interface com Reguladores, Auditores e Consultores Externos para auditorias regulatórias externas. V. Ir além da mera conformidade nas avaliações para verificar se os ativos mais críticos da organização estão adequadamente protegidos.

Segundo os entrevistados, alguns benefícios da atuação da Auditoria Interna no monitoramento do ambiente regulatório e de conformidade legal incluem:

- Eficiência: Estabelecer processos contínuos de monitoramento ajuda a garantir que a organização esteja sempre em conformidade com as regulamentações, mesmo quando novas leis são introduzidas ou existentes são alteradas.
- Visão Unificada: Trabalhar em conjunto com a segunda linha e setores de conformidade proporciona uma visão abrangente e integrada da conformidade em toda a organização.
- Estratégia Integrada: Desenvolvimento de estratégias conjuntas para lidar com os requisitos legais e regulatórios, identificando e priorizando áreas de risco.
- Identificação de Riscos: Auditorias periódicas ajudam a identificar áreas onde a organização pode estar em risco de não conformidade, permitindo ações corretivas antes que problemas se agravem.

Da mesma forma, foi possível consolidar os seguintes desafios na atuação da Auditoria Interna no monitoramento do ambiente regulatório e de conformidade legal:

- Ambiente Regulatório Dinâmico: A constante mudança e complexidade das regulamentações, especialmente em setores altamente visados como o financeiro, representam um desafio significativo para a conformidade contínua.
- Multiplicação de Ameaças: Com a transformação digital e o aumento do uso de dispositivos móveis, a superfície de ataque se expande, exigindo uma vigilância e adaptação constantes para manter a conformidade e a segurança.
- Integração entre Equipes: Garantir uma colaboração eficaz entre a auditoria interna, a segunda linha e outros setores pode ser desafiador devido à necessidade de alinhar objetivos e práticas.
- Coordenação Interna: A preparação e coordenação para auditorias externas requerem um alto nível de organização e comunicação interna, além de uma gestão eficaz da documentação e evidências de conformidade.

4.7 CATEGORIA 6 - DIRECIONAMENTO DE ACHADOS E APONTAMENTOS

A Categoria 6, denominada “Direcionamento de achados e apontamentos”, tem como finalidade principal identificar e analisar de como a terceira linha pode direcionar e acompanhar o andamento de achados e apontamentos oriundos das avaliações de auditoria. Este objetivo envolve a exploração de métodos e práticas através dos quais a auditoria interna pode identificar e documentar achados e apontamentos relacionados a possíveis desvios ou não conformidades com os padrões estabelecidos. A categoria examina como a auditoria interna pode elaborar relatórios detalhados, contendo recomendações específicas e acionáveis, que orientem a organização na correção de falhas ou fragilidades.

Documentação Detalhada das Inconformidades - O primeiro passo geralmente envolve a revisão de toda a documentação relacionada à segurança cibernética, incluindo políticas, procedimentos e padrões de segurança. A auditoria verifica se as políticas estão atualizadas e se refletem adequadamente as ameaças atuais. Também avalia se os procedimentos estão sendo seguidos pelos funcionários e se os padrões de segurança atendem às normas industriais e regulamentações relevantes.

O entrevistado ENTR03 realizou a seguinte observação em sua unidade de registro sobre o tópico:

> *"Cada inconformidade deve ser claramente descrita, especificando como ela diverge das políticas da empresa, padrões de conformidade, ou leis aplicáveis. As inconformidades identificadas devem ser detalhadamente documentadas durante a auditoria, incluindo evidências específicas, como registros de logs, configurações de sistemas, ou declarações de gestores e executantes dos processos, que apoiem a descoberta".*

Avaliação de impacto e Classificação de Riscos - As inconformidades devem ser classificadas de acordo com seu potencial impacto e probabilidade de ocorrência. Isso ajuda a priorizar as ações de remediação, concentrando recursos nos problemas mais críticos que possam ter impactos mais graves na organização. Isso inclui considerar como a inconformidade pode afetar as operações da organização, a segurança dos dados e a conformidade regulatória, além de avaliar os riscos legais, financeiros e de reputação associados.

Referente a essa unidade de contexto, o entrevistado ENTR11 realizou a seguinte contribuição:

> *"Sei que não é simples, mas fazer a avaliação do Impacto e classificar devidamente o risco do achado é "importantíssimo"para convencer as partes envolvidas da gravidade do achado, para direcionar os esforços e priorizar as correções necessárias no processo. Isso vai permitir identificar e entender os riscos mais significativos, focando em áreas que necessitam de maior atenção e alocando recursos de forma eficiente, facilitando assim a implementação não somente corretivas,*

mas também preventivas".

Desenvolvimento de Planos de Ação - Para cada inconformidade identificada, um plano de ação corretivo detalhado deve ser desenvolvido. Este plano deve incluir medidas específicas para corrigir a falha, os responsáveis pela implementação dessas medidas, e um cronograma para a resolução. Dependendo da avaliação de impacto e classificação de risco da inconformidade, podem ser necessárias ações imediatas ou um projeto de melhoria a longo prazo. Convém que o tempo de implementação das ações seja determinado com base na classificação e no esforço envolvido no trabalho. É importante que as ações sejam realistas e adequadas ao nível de risco apresentado.

O entrevistado ENTR15 fez o seguinte comentário em sua unidade de registro sobre o assunto.

> *"De maneira geral, eu creio que inconformidades com normas e politicas, ou pior, com leis e regulações, e casos de riscos em processos já existentes, devem ser corrigidas rapidamente por meio de recomendações. Nos casos de identificação de riscos em processos que eventualmente não estão existem, envolvam mais de um interveniente ou necessite de plano de investimentos, o plano de ação pode ser uma ferramenta útil para direcionamento do achado".*

Verificação da Eficácia das Ações Corretivas - As equipes responsáveis devem implementar as ações corretivas de acordo com o plano estabelecido e após a implementação dessas ações, a auditoria interna deve verificar sua eficácia. Isso envolve revisitar as áreas originalmente em não conformidade para garantir que as correções foram implementadas adequadamente e que os problemas originais foram resolvidos. Isso pode envolver a realização de check-ins regulares com os responsáveis por cada ação e a atualização contínua do progresso para a alta gestão.

Sobre o tema em questão, o entrevistado ENTR11, realizou a seguinte observação em sua unidade de registro:

> *"Planos de ação longos exigem cuidado redobrado por parte da terceira linha, pois tantos as políticas, normas, regulamentos e processos podem sofrer alterações no meio tempo da implementações das ações, quanto os gestores, auditores e partes interessadas podem ser alterados. Desse modo, os termos e acordos tem de ser bem claros e documentados para não serem esquecidos ou se tornarem inexequíveis no futuro".*

Monitoramento e Follow-up - Após a realização das correções, a auditoria interna deve proceder com um monitoramento contínuo dos efeitos das medidas implementadas para assegurar que a inconformidade foi devidamente resolvida e que as ações tomadas são eficazes na prevenção de futuras ocorrências. Esse processo envolve a realização de revisões periódicas e auditorias de acompanhamento ou follow-up, com o objetivo de verificar se as medidas corretivas foram efetivas.

O entrevistado ENTR05 realizou o seguinte comentário em sua unidade de registro sobre o assunto:

> *"É importante verificar se novas inconformidades surgiram como consequência das mudanças aplicadas. Dessa forma, a terceira linha pode garantir que o sistema permanece em conformidade e que está continuamente se aprimorando para evitar problemas semelhantes no futuro".*

Comunicação com as Partes Interessadas - Os resultados da auditoria, incluindo inconformidades, devem ser comunicados às partes interessadas relevantes. Isso geralmente inclui a Direção, os Gestores dos departamentos afetados e quando for o caso, a alta administração. A comunicação deve ser clara, objetiva e deve incluir sugestões práticas para a resolução dos problemas, geralmente realizada por meio de relatórios formais de auditoria, reuniões de revisão e, em casos críticos, alertas imediatos.

Referente a essa unidade de contexto, o entrevistado ENTR08 ofereceu a seguinte contribuição:

> *"É importante disseminar as lições aprendidas com as inconformidades em toda a organização, para aumentar a conscientização e evitar a repetição de situações de inconformidades similares em diferentes departamentos ou unidades de negócio".*

[81] ressaltou em sua pesquisa que os auditores internos devem atuar avaliando a adequação das práticas de gerenciamento de riscos, a eficácia do controle e identificando áreas de melhoria. Para tanto, [94] destaca a adoção de metodologias de quantificação de risco para fornecer avaliações objetivas e baseadas em dados. Segundo [76] e [83] a auditoria interna deve emitir recomendações para direcionar as melhorias a serem implementadas nos processos corporativos.

A comunicação e o gerenciamento bem-sucedido das partes interessadas, foram destacados nos estudo de [3] e [29], onde a gestão das preocupações desse público nos processos de tomada de decisão estratégica e a garantia de que seus interesses sejam priorizados e protegidos foram reforçados.

Tabela 4.9: Unidades de Contexto da Categoria 6

Categoria 6 - Direcionamento de achados e apontamentos
Como direcionar e acompanhar o andamento dos apontamentos provenientes das avaliações de auditoria
I. Documentar detalhadamente as inconformidades identificadas.
II. Avaliar o impacto e classificar os riscos associados ao apontamento.
III. Desenvolver de planos de ação junto aos gestores para tratamento.
IV. Verificar a eficácia das ações corretivas após as suas implementações.
V. Monitorar os efeitos das medidas implementadas para assegurar que a inconformidade foi devidamente resolvida.
VI. Comunicar periodicamente as partes envolvidas sobre o andamento das ações e os resultados obtidos.

Segundo os entrevistados, alguns benefícios do direcionamento de achados e apontamentos pela

Auditoria Interna incluem:

- Correção de Erros: Tratamento eficaz das inconformidades leva à correção de erros e falhas nos processos, melhorando a eficiência operacional.
- Aprimoramento dos Controles Internos: Implementação de ações corretivas fortalece os controles internos, reduzindo riscos futuros.
- Conformidade Regulatória: Garantir que a organização esteja em conformidade com regulamentações e padrões, evita penalidades e multas.
- Mitigação de Riscos: Endereçar inconformidades diminui a exposição a riscos, tanto financeiros quanto de reputação.
- Confiança dos Stakeholders: Comunicação clara e eficaz sobre as ações corretivas aumenta a confiança de stakeholders internos e externos.
- Cultura de Transparência: Promove uma cultura de transparência e responsabilidade dentro da organização.
- Engajamento dos Colaboradores: Envolver a equipe no processo de melhoria contínua pode aumentar o engajamento e a motivação.

Da mesma forma, foi possível consolidar os seguintes desafios no direcionamento de achados e apontamentos pela Auditoria Interna:

- Cultura Organizacional: Resistência por parte dos colaboradores e gestores a mudanças nos processos estabelecidos.
- Inércia Institucional: Tendência da organização a manter o status quo.
- Recursos Humanos e Financeiros: Escassez de recursos para implementar ações corretivas e melhorias.
- Prioridades Conflitantes: Dificuldade em priorizar ações corretivas em relação a outras iniciativas estratégicas.
- Clareza e Consistência: Dificuldade em garantir que a comunicação sobre as inconformidades e as ações corretivas seja clara e consistente em todos os níveis da organização.
- Engajamento dos Stakeholders: Garantir que todos os stakeholders relevantes sejam devidamente informados e envolvidos no processo.
- Sustentabilidade das Melhorias: Garantir que as melhorias sejam sustentáveis a longo prazo e não apenas soluções temporárias.

4.8 CATEGORIA 7 - TENDÊNCIAS E INOVAÇÕES

A Categoria 7, designada “Tendências e inovações”, tem como objetivo principal identificar e analisar, com base nas experiências e percepções dos entrevistados, quais são as principais tendências e inovações no contexto da auditoria interna e da gestão de riscos cibernéticos que devem ser acompanhadas nos próximos anos. Esta categoria busca explorar as previsões e percepções dos profissionais sobre as

mudanças emergentes e as novas tecnologias que estão moldando o campo da segurança cibernética e a prática da auditoria interna.

Inteligência Artificial (IA) e Aprendizado de Máquina (ML) - Um perspectiva envolve os temas como objeto de auditoria, nesse sentido, a análise envolve como a organização está utilizando a inteligência artificial para viabilizar o atingimento de seus objetivos estratégicos de maneira segura e ética. Outra perspectiva, envolve as avaliações realizadas pela auditoria podem ser potencializadas com essas tecnologias. Isso pode ocorrer tanto na estratégia de auditoria contínua quanto no apoio à produção de documentos, evidências ou na priorização de riscos que necessitam ser avaliados. A inteligência artificial também pode ser um recurso valioso para analisar grandes volumes de dados, permitindo a detecção de padrões de riscos e inconformidades de maneira mais eficiente.

O entrevistado ENTR07 incluiu a seguinte observação em sua unidade de registro sobre o tópico:

> *"Essas tecnologias têm a capacidade de examinar vastas quantidades de dados para identificar comportamentos anormais, riscos potenciais e ameaças, o que, por sua vez, aprimora significativamente as capacidades de prevenção e resposta das organizações. Esse uso permite que as organizações melhorem não apenas a sua conformidade e segurança, mas também a eficácia geral das suas operações".*

[31] e [44] frisaram que a inteligência artificial (IA) e aprendizado de máquina podem ser muito úteis para alavancar as capacidades das organizações em identificar e responder às ameaças cibernéticas.

Computação Quântica e Criptografia Pós-Quântica - Embora ainda esteja em estágios iniciais, a computação quântica promete trazer desafios significativos para a segurança cibernética, especialmente no campo da criptografia. À medida que essa tecnologia avança, as instituições precisam estar atentas e começar a se preparar para o impacto potencial que ela poderá ter nas práticas atuais de criptografia e segurança de dados. Preparar as defesas cibernéticas para um futuro onde as técnicas quânticas possam ser usadas para comprometer sistemas atuais é uma necessidade urgente. Assim, as organizações devem começar a explorar e implementar essas novas técnicas de criptografia para garantir a segurança e integridade dos dados em um mundo pós-quântico e a terceira linha precisa estar atenta aos avanços apresentados no tema.

Com relação a essa unidade de contexto, o entrevistado ENTR03 fez a seguinte observação:

> *"A capacidade dos computadores quânticos de processar informações em velocidades exponencialmente maiores do que os computadores clássicos pode tornar as técnicas de criptografia atuais vulneráveis a ataques. Para enfrentar essa ameaça emergente, será fundamental investir em pesquisa e desenvolvimento em criptografia pós-quântica. Este novo ramo da criptografia visa criar algoritmos que possam resistir às*

capacidades de processamento dos futuros computadores quânticos".

[64] em seu trabalho abordou a importância do uso de criptografia para proteger dados e informações confidenciais.

Blockchain – O uso de blockchain está sendo amplamente explorado para diversas aplicações de segurança, incluindo a proteção de dados descentralizados, o gerenciamento de identidades e o controle de acessos. Devido à sua natureza descentralizada e imutável, o blockchain oferece uma maneira eficaz de criar registros transparentes e permanentes para transações e atividades, o que, por sua vez, aumenta a segurança e a audibilidade de processos críticos. Além disso, ele proporciona um método robusto para proteger dados e garantir a integridade das transações. Essa característica é especialmente relevante para o setor financeiro, que lida com transações altamente críticas e dados extremamente sensíveis. A incorporação de tecnologias de blockchain nas estratégias de segurança cibernética e auditoria interna das instituições financeiras não é apenas recomendada, mas essencial para manter a integridade e a segurança em um ambiente financeiro cada vez mais digital e interconectado.

O entrevistado ENTR13 realizou a seguinte observação em sua unidade de registro sobre o tópico:

"O blockchain está expandindo suas aplicações e deve continuar a crescer com a adoção de moedas digitais oficiais, como o Real Digital. Essa expansão torna o tema uma prioridade nas auditorias de segurança das instituições financeiras. As novas capacidades proporcionadas pelo blockchain podem transformar a maneira como os dados são protegidos e as transações são verificadas, oferecendo uma camada adicional de segurança que é tanto transparente quanto resistente a manipulações".

Privacidade e Proteção de Dados – À medida que aumentam a ocorrência de violações e a preocupação com a privacidade dos dados pessoais, surgem diversas inovações em técnicas de anonimização, gestão de consentimento, segurança de dados, e regulamentações como a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral sobre a Proteção de Dados (GDPR). Essas regulamentações impulsionam inovações tanto em tecnologias de proteção de dados quanto em práticas de auditoria que assegurem a conformidade contínua. Nesse contexto, ferramentas que ajudam as organizações a proteger a privacidade dos usuários sem comprometer a usabilidade estão se tornando cada vez mais indispensáveis.

O entrevistado ENTR12 registrou a seguinte contribuição em sua unidade de registro sobre o tema:

"Há um foco significativo no aprimoramento de políticas de privacidade, procedimentos de consentimento de dados e mecanismos de resposta a violações de dados. Essas inovações não apenas fortalecem a segurança dos dados, mas também podem promover a confiança dos usuários nas empresas, e isso vem se

tornando cada vez mais tema estratégico dentro das instituições".

Expansão do Perímetro de Segurança e o Edge Computing - Com o aumento significativo do número de dispositivos IoT (Internet of Things) em uso e a expansão do Edge Computing (Computação de Borda), tanto em contextos pessoais quanto empresariais, a segurança desses dispositivos se tornou uma preocupação de extrema importância. A auditoria interna precisará desenvolver e implementar estratégias abrangentes para avaliar as proteções contra as vulnerabilidades específicas associadas aos dispositivos IoT. Essas estratégias deverão incluir a segurança das redes que interconectam esses dispositivos e a proteção dos dados transmitidos por eles.

Sobre o tema dessa unidade de contexto, o entrevistado ENTR09 fez a seguinte observação:

"Os dados pessoais processados nesses dispositivos de borda apresentam desafios adicionais em termos de privacidade e proteção de dados para as auditorias. Eles ressaltaram que a natureza descentralizada do Edge Computing, combinada com a vasta quantidade de dados sensíveis sendo processados, aumenta a complexidade das questões de segurança. A auditoria interna terá que se adaptar a essas novas realidades, considerando não apenas as vulnerabilidades técnicas, mas também as implicações regulatórias e de conformidade associadas ao tratamento de dados pessoais".

[19] e [37] destacaram a que o aumento de dispositivos conectados à Internet processando informações e dados, fenômeno conhecido como edge computing, aumentaram a superfície de ataque e complexidade das redes, ampliando o perímetro de segurança e os eventuais impactos decorrentes de incidentes cibernéticos.

Segurança Baseada na Identidade (Zero Trust) – Este paradigma de segurança para redes corporativas exige uma verificação rigorosa de todas as entidades, independentemente de estarem dentro ou fora da rede da organização. O modelo Zero Trust opera sob a premissa de que ameaças podem surgir tanto internamente quanto externamente, e que nenhum usuário ou dispositivo deve ser automaticamente confiável. Esse modelo requer autenticação e autorização para qualquer indivíduo ou dispositivo que tente acessar os recursos da rede, com o objetivo de reduzir a superfície de ataque.

O Zero Trust é impulsionado pela necessidade crescente de segurança rigorosa em ambientes cada vez mais complexos e interconectados. À medida que as redes corporativas se expandem e se tornam mais integradas com diversas tecnologias e dispositivos, a adoção de um modelo de segurança que não confia automaticamente em nenhum elemento se torna essencial.

O entrevistado ENTR15 incluiu a seguinte observação em sua unidade de registro sobre o tópico:

"A estratégia de segurança baseada no conceito de Zero Trust é um tema de importância crescente para

os auditores que atuam na área de segurança cibernética. Devido à complexidade e à diversidade dos ambientes de TI modernos, a implementação do Zero Trust é uma alternativa viável para garantir uma proteção robusta. Manter-se atualizado com as práticas e tecnologias associadas ao Zero Trust será fundamental para os profissionais de auditoria que desejam efetivamente avaliar e melhorar a postura de segurança de suas organizações.".

Tabela 4.10: Unidades de Contexto da Categoria 7

Categoria 7 - Desafios, tendências e inovações
Principais tendências e inovações no contexto da auditoria interna e na gestão de riscos cibernéticos
I. Inteligência Artificial (IA) e Aprendizado de Máquina (ML) como objeto a ser avaliado e para alavancar as análises da auditoria.
II. Computação Quântica e Criptografia Pós-Quântica devidos aos seus impactos nas práticas atuais de criptografia e segurança de dados.
III. Blockchain devido a criação das moedas digitais e expansão do seu uso no ecosistema financeiro digital e interconectado.
IV. Privacidade e proteção de dados em função do aumento na quantidade de ocorrência de violações e a preocupação com a privacidade dos dados pessoais.
V. Expansão do Perímetro de Segurança e Edge Computing, devido a necessidade de desenvolver e implementar estratégias para avaliar as proteções contra as vulnerabilidades específicas dessa tecnologia.
VI. Segurança Baseada na Identidade (Zero Trust) e a crescente necessidade de segurança rigorosa em ambientes mais complexos e interconectados.

5 CONCLUSÕES

O trabalho apresentou uma análise sobre a atuação da auditoria interna no contexto da gestão de riscos cibernéticos em instituições financeiras brasileiras, seguindo o modelo das três linhas. O estudo teve como objetivo identificar formas pelas quais a auditoria interna pode gerar valor e contribuir para garantir a efetividade e o aprimoramento dos processos relacionados a esses riscos.

Para atingir o objetivo proposto, foram realizadas entrevistas semiestruturadas com gestores atuantes em segunda e terceira linha, dentro do modelo de três linhas, de dez instituições financeiras brasileiras e duas empresas internacionais de auditoria externa.

Grande parte das instituições financeiras representadas adotam o modelo de três linhas e os entrevistados acreditam que o modelo é o mais efetivo para acomodar as atividades de auditoria interna, controles internos e gestão de riscos corporativos dentro das intuições, embora tenha sido levantados aspectos importantes sobre o papel dos intervenientes.

A integração com a gestão de riscos corporativos mais amplos, foi indicada como aspecto fundamental para garantir que as medidas de segurança sejam incorporadas nos processos organizacionais e assegurar a continuidade operacional. A pesquisa qualitativa indica que os auditores internos, através de avaliações independentes, podem priorizar os riscos com base em sua probabilidade e impacto potencial, o que é vital para a alocação eficiente de recursos.

A colaboração entre as três linhas foi destacada como fator crítico para garantir uma gestão de risco cibernético robusta. As interações regulares e a comunicação clara entre essas linhas facilitam a identificação e mitigação de riscos de maneira mais eficiente. Do mesmo modo, foi destacada a sinergia e parceria com as demais áreas da empresa, onde foi enfatizado que a auditoria interna é parte importante da empresa, sendo aliada do negócio e se mobilizando para atingimento dos objetivos estratégicos propostos.

Nesse sentido, foi enfatizado que as interações com as áreas de negócio devem ser constantes e a colaboração com os departamentos de TI e de Segurança Cibernética devem ocorrer com a realização de treinamentos em conjunto e com simulações de crise corporativas.

A integração da gestão de riscos cibernéticos na estratégia corporativa das intuições foi um tópico amplamente explorado pelos entrevistados. As Políticas de Segurança foram indicadas como ponto de partida importante para sinalização do direcionamento da organização. Além disso, o envolvimento da alta gestão foi frisado como essencial para promoção de cultura de riscos e de segurança, e algumas táticas para integração da segurança cibernética nas estratégias corporativas foram compartilhadas, entre elas destaca-se a atividade de consultoria da terceira linha para avaliação de processos corporativos e a obrigatoriedade da realização de uma análise de risco cibernético para aprovação de novos modelos de negócios. Por fim, capacitação e conscientização foram apontadas como fator decisivo para tornar mais robustas as estratégias de gestão de riscos cibernéticos.

A terceira linha foi identificada como essencial na avaliação da eficácia dos controles de segurança cibernética e na identificação de oportunidades de melhorias. Em relação a avaliação da eficácia dos

controles de segurança cibernética, foi reforçada a independência da área, entretanto houve discordâncias sobre a real efetividade da auditoria realizar atividades típicas de primeira e segunda linha.

Acerca da profundidade das avaliações realizadas pela Auditoria Interna, foram apresentadas duas perspectivas antagônicas, a primeira sugere que a auditoria interna deve focar em aspectos de alto nível da gestão e governança, a segunda defende que a auditoria interna também deve realizar avaliações detalhadas de atividades operacionais.

Sobre esse ponto, foi proposta a realização de testes de invasão (PenTest) para a avaliação da eficácia dos processos de segurança cibernética pelo time da terceira linha, ou por empresas contratadas com o objetivo de validar e aprimorar processos operacionais. Entretanto, a ideia pode ser inviável na prática devido à limitação técnica, e orçamentária, além de ineficiente operacionalmente quando já existir ferramental e profissionais especializados na primeira linha realizando estas atividades. Como solução alternativa, foi sugerida a atuação em conjunto entre as linhas onde cada uma poderia contribuir dentro das suas atribuições especificas.

A auditoria contínua baseada em dados foi apontada como uma ferramenta muito útil para monitorar e avaliar continuamente os controles e processos de segurança, melhorando a gestão de riscos cibernéticos. As ferramentas analíticas aumentam a capacidade de detecção e resposta a riscos emergentes, tornando as recomendações e ações mais efetivas. No entanto, houve dissenso sobre a precisão das análises estatísticas em grandes populações versus a eficiência e representatividade das amostras em contextos de recursos limitados.

Devido à volatilidade do ambiente corporativo e tecnológico, auditorias contínuas são mais eficazes que ciclos periódicos para identificar riscos emergentes e propor melhorias. Relatórios e painéis de controle devem destacar riscos e o progresso das medidas de mitigação. A análise da utilização das informações geradas por ferramentas de monitoramento contínuo para identificar atividades suspeitas em tempo real foi indicada como ponto relevante de verificação para avaliação em auditorias e o uso de tecnologias avançadas, como IA e automação, é importante para uma resposta adaptativa a ameaças cibernéticas emergentes.

Nesse sentido, a construção de métricas, indicadores-chave de risco (KRI) e de desempenho (KPI) para monitoração continua de processos foram enfatizadas como recursos imprescindíveis para gestão de riscos cibernéticos. Essas métricas ajudam a identificar fragilidades e oportunidades de melhoria, com KRIs destacando possíveis ameaças e KPIs avaliando a eficácia das políticas de segurança, como resposta a incidentes e conformidade com padrões estabelecidos.

A aplicação de boas práticas e frameworks é relevante para que a terceira linha avalie de forma abrangente e eficiente a gestão de riscos cibernéticos, promovendo maior segurança e resiliência organizacional. Esses frameworks, continuamente testados e aprimorados pela comunidade, também facilitam a troca de experiências em eventos e fóruns.

O desafio de monitorar o ambiente regulatório para assegurar que as alterações e as criações de normas sejam adequadamente refletidas nas políticas e nos processos da organização, foi outro ponto de destaque observado. Nesse sentido, processos de monitoramento para rastrear mudanças regulatórias e indicadores de desempenho para avaliar controles, a colaboração com a Segunda Linha para construção de

uma visão integrada da conformidade e a realização de avaliações regulares para identificar e mitigar riscos foram indicadas como táticas eficientes para manutenção da conformidade.

Além disso, a terceira linha deve relatar ao conselho sobre o status do nível de conformidade da organização e preparar a instituição para auditorias externas. A colaboração com consultores externos pode assegurar a adesão às melhores práticas e regulamentos atuais, porém, a segurança completa exige uma arquitetura de segurança robusta além da simples conformidade.

Para mais, foram identificados aspectos importantes para realizar o devido direcionamento de achados e apontamentos identificados pela auditoria, o qual devem ser detalhadamente relatadas e classificadas por impacto e probabilidade, priorizando ações corretivas nos problemas mais críticos. Um plano de ação específico deve ser criado para cada fragilidade, com medidas corretivas, responsáveis e cronogramas definidos. Após a implementação, a eficácia das ações deve ser verificada por auditorias de acompanhamento, a comunicação dos resultados deve ser clara e objetiva, abrangendo todas as partes interessadas e as lições aprendidas compartilhadas para prevenir recorrências.

Por fim, foram destacadas e relacionadas as tendências e inovações emergentes mais relevantes para serem monitoradas pois a forma como a auditoria interna trabalhará nos próximos anos pode ser fortemente afetada por elas. Dessa forma, destacam-se: Inteligência Artificial (IA) e Aprendizado de Máquina (ML), Computação quântica e a criptografia pós-quântica, blockchain, privacidade e proteção de dados, expansão do perímetro de segurança com o Edge Computing e a Segurança Baseada na Identidade (Zero Trust).

As implicações práticas deste estudo são diversas. As instituições financeiras podem se beneficiar diretamente das conclusões obtidas, especialmente no que diz respeito à integração da auditoria interna com as outras duas linhas e ao uso de tecnologias emergentes para melhorar a eficácia dos controles de segurança cibernética. A pesquisa também destaca a importância de uma cultura organizacional forte em relação à segurança cibernética, onde todos os níveis da instituição estão cientes e preparados para enfrentar os riscos emergentes. Teoricamente, este estudo contribui para a literatura existente ao fornecer uma análise detalhada do papel da terceira linha na gestão dos riscos cibernéticos, utilizando o modelo de três linhas. As descobertas reforçam a importância de uma abordagem integrada e colaborativa para a gestão de riscos cibernéticos, oferecendo uma base sólida para pesquisas futuras neste campo.

Apesar dos resultados obtidos, este estudo está exposto a algumas limitações. Primeiramente, a amostra foi composta por um número limitado de entrevistados, o que pode não representar todas as perspectivas e experiências possíveis dentro do universo das instituições financeiras brasileiras. A diversidade da amostra foi restrita, com predominância de profissionais de instituições financeiras de grande porte, o que pode não refletir completamente a realidade de instituições menores ou de outros setores econômicos.

Outra limitação é a natureza qualitativa da pesquisa, que, embora permita uma compreensão profunda e detalhada dos fenômenos estudados, pode não proporcionar a generalização dos resultados para outras organizações ou contextos. A subjetividade inerente à análise de conteúdo pode influenciar a interpretação dos dados, apesar dos esforços para garantir a objetividade e a sistematização do processo analítico.

A partir das conclusões alcançadas com este estudo, oportunidades para pesquisas futuras surgem.

Uma delas é a realização de estudos quantitativos que possam complementar os achados qualitativos aqui apresentados, proporcionando uma base estatística que permita a generalização dos resultados para um contexto mais amplo. Estudos que envolvam um maior número de instituições financeiras, incluindo uma variedade de portes, perfis, também podem fornecer informações adicionais e mais abrangentes sobre a eficácia da atuação da Auditoria Interna e sua contribuição para gestão de riscos cibernéticos.

Além disso, futuras pesquisas poderiam explorar a aplicação de tecnologias emergentes, como inteligência artificial e machine learning, na prática da auditoria interna. Tais estudos poderiam investigar como essas tecnologias podem aprimorar a identificação, monitoramento e mitigação de riscos cibernéticos, oferecendo novos métodos e ferramentas para auditores internos, considerando a complexidade das atividades de cada instituição financeira, dentor de seu segmento.

Outras oportunidades de pesquisas, seria explorar o tema de auditoria continua: comparar a efetividade da auditoria contínua com a auditoria tradicional em termos de detecção precoce de ameaças, resposta a incidentes e prevenção de violações de segurança; desenvolver modelos de risco específicos que integrem a auditoria contínua como uma variável crítica na avaliação da exposição ao risco cibernético; pesquisas qualitativas buscando entender a percepção dos profissionais de segurança da informação sobre a efetividade e os desafios da auditoria contínua na gestão de riscos cibernéticos.

Sobre a integração da modelagem de ameaças nos processos de auditoria interna, um estudo pode ser conduzido para investigar métodos para integrar a modelagem de ameaças nos processos de auditoria interna, desde a fase de planejamento até a execução e relatório, ou criar e validar ferramentas específicas que possam ser utilizadas pela auditoria interna para realizar modelagem de ameaças de forma eficiente e eficaz.

Por fim, estudos podem investigar como a auditoria interna pode integrar testes de invasão de forma sistemática em suas avaliações de segurança ou explorar a efetividade da realização de testes de penetração pela terceira linha.

REFERÊNCIAS BIBLIOGRÁFICAS

1 FEBRABAN. Federação nacional dos bancos. *Pesquisa de Tecnologia Bancária*, 2024. Disponível em: <https://portal.febraban.org.br/pagina/3106/48/pt-br/pesquisa>.

2 PWC. Pricewaterhousecoopers. *Global Digital Trust Insights 2023, A C-suite united on cyber-ready futures*, 2024. Disponível em: <https://www.pwc.com/mu/en/services/consulting/global-digital-trust-insights.html>.

3 ZAIDIRINA; LINDRIANASARI; BANGSAWAN, S. Implementation of corporate governance and mandatory disclosure in the indonesian banking sector: good news or bad news. *International Journal of Monetary Economics and Finance*, v. 10, p. 281–294, 2017. Disponível em: <https://doi.org/10.1504/IJMEF.2017.087474>.

4 IBM. International business machines. *Cost of a Data Breach Report 2023*, 2023. Disponível em: <https://www.ibm.com/reports/data-breach>.

5 BRASIL. Banco central do brasil. *PIX - Pagamentos instantâneos*, 2020. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/pix>.

6 SARAIVA, M. H. A.; CUSTÓDIO, P. H. de S.; PINTO, F. N. P. A responsabilidade das instituições financeiras em fraudes bancárias: Uma análise sobre o pix. *Facit Business and Technology Journal*, v. 2, n. 47, 2023. Disponível em: <https://revistas.faculdadefacit.edu.br/index.php/JNT/article/view/2678>.

7 WORLDWIDE, A.; GLOBALDATA. Scamscope fraud report. *APP scam trends in the U.S., U.K., India, Brazil, Australia and Saudi Arabia*, 2023. Disponível em: <https://www.aciworldwide.com/wp-content/uploads/2023/11/ACI-SCAMSCOPE-Fraud-Report.pdf>.

8 OLANIYI, O. O.; ASONZE, C. U.; AJAYI, S. A.; OLABANJI, S. O.; ADIGWE, C. S. A regressional study on the impact of organizational security culture and transformational leadership on social engineering awareness among bank employees: The interplay of security education and behavioral change. *Asian Journal of Economics, Business and Accounting*, v. 23, p. 128–143, 2023. Disponível em: <https://doi.org/10.9734/ajeba%2F2023%2Fv23i231176>.

9 SHALABI, K.; AL-FAYOUMI, M. A.; AL-HAIJA, Q. A. Enhancing financial system resilience against cyber threats via swift customer security framework. *2023 International Conference on Information Technology (ICIT)*, p. 260–265, 2023. Disponível em: <https://doi.org/10.1109/ICIT58056.2023.10226165>.

10 MACHADO, D. D. Lei geral de proteção de dados pessoais - lgpd. *Revista Científica Multidisciplinar Núcleo do Conhecimento*, 2021. Disponível em: <https://doi.org/10.32749/nucleodoconhecimento.com.br/lei/geral-de-protecao>.

11 IIA. Institute of internal auditors. *The IIA's Three Lines Model: An update of the Three Lines of Defense*, 2020. Disponível em: <https://www.theiia.org/en/content/position-papers/2020/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense>.

12 PROTIVITI. Protiviti. *Protiviti's 2020 internal audit capabilities and needs survey - Exploring the Next Generation of Internal Auditing*, 2020. Disponível em: <https://www.protiviti.com/us-en/survey/protivitis-2020-internal-audit-capabilities-and-needs-survey>.

13 NETO, N. N.; MADNICK, S. E.; PAULA, A. M. G. de; BORGES, N. M. A case study of the capital one data breach. *ERN: Regulation & Supervision (Topic)*, 2020. Disponível em: <http://dx.doi.org/10.2139/ssrn.3570138>.

14 SETYANINGRUM, D.; KUNTADI, C. The effects of competence, independence, audit work, and communication on the effectiveness of internal audit. *Journal of Economics, Business, and Accountancy | Ventura*, v. 22, p. 39–47, 2019. Disponível em: <https://doi.org/10.14414/jebav.v22i1.879>.

15 CREMER, F.; SHEEHAN, B.; FORTMANN, M.; KIA, A.; MULLINS, M.; MURPHY, F.; MATERNE, S. Cyber risk and cybersecurity: A systematic review of data availability. *Geneva Papers on Risk and Insurance - Issues and Practice*, v. 47, p. 698–736, 2022. Disponível em: <https://doi.org/10.1057/s41288-022-00266-6>.

16 MCSHANE, M. K.; ELING, M.; NGUYEN, T. Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, 2021. Disponível em: <https://doi.org/10.1111/RMIR.12169>.

17 ROSATI, P.; GOGOLIN, F.; LYNN, T. Cyber-security incidents and audit quality. *European Accounting Review*, v. 31, p. 701 – 728, 2017. Disponível em: <https://doi.org/10.1080/09638180.2020.1856162>.

18 BENZ, M.; CHATTERJEE, D. Calculated risk? a cybersecurity evaluation tool for smes. *Business Horizons*, v. 63, p. 531–540, 2020. Disponível em: <https://doi.org/10.1016/j.bushor.2020.03.010>.

19 VERIZON. Verizon business. *2021 Data Breach Investigations Report*, 2021. Disponível em: <https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf>.

20 TRIPATHI, M.; MUKHOPADHYAY, A. Does privacy breach affect firm performance? an analysis incorporating event-induced changes and event clustering. *Inf. Manag.*, v. 59, p. 24, 2022. Disponível em: <https://doi.org/10.1016/j.im.2022.103707>.

21 AFRIFAH, W.; EPIPHANIOU, G.; ERSOTELOS, N.; MAPLE, C. Barriers and opportunities in cyber risk and compliance management for data-driven supply chains. In: *Hawaii International Conference on System Sciences*. [s.n.], 2022. Disponível em: <https://doi.org/10.24251/hicss.2022.225>.

22 BRASIL. Controladoria geral da união. *Portaria Nº 2.821, de 29 de agosto de 2024*, 2024. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-2.821-de-29-de-agosto-de-2024-581189836>.

23 BRASIL. Conselho monetário nacional. *Resolução CMN Nº 4.893, de 26 de fevereiro de 2021*, 2021. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=RESOLU%C3%87%C3%83O%20CMN&numero=4893>.

24 CHONG, W. F.; FENG, R.; HU, H.; ZHANG, L. Cyber risk assessment for capital management. *ArXiv*, abs/2205.08435, 2022. Disponível em: <https://doi.org/10.48550/arxiv.2205.08435>.

25 AGGARWAL, R.; RANGANATHAN, P. Study designs: Part 2 – descriptive studies. *Perspectives in Clinical Research*, v. 10, p. 34 – 36, 2019. Disponível em: <https://doi.org/10.4103/picr.PICR_154_18>.

26 GIL, A. C. *Métodos e Técnicas de Pesquisa Social*. [S.l.]: Atlas; 7ª edição, 2019. 248 p. ISBN 8597020571.

27 BARDIN, L. *Análise de Conteúdo*. [S.l.]: São Paulo: Edições 70 - Almedina Brasil, 2016. 232 p. ISBN 9788562938047.

28 BRASIL. Banco central do brasil. *Regulação Prudencial - Resolução CMN n° 4.553 de 30/1/2017.*, 2017. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/regprudencialsegmentacao>.

29 WALKER, P. L.; SHENKIR, W. G. Enterprise risk management: Frameworks, elements, and integration. *Risk Management Journal*, v. 33(4), p. 36–42, 2018. Disponível em: <https://www.imanet.org/research-publications/statements-on-management-accounting/enterprise-risk-management-frameworks-elements-and-integration>.

30 ALAHMARI, A.; DUNCAN, B. Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, p. 1–5, 2020. Disponível em: <https://doi.org/10.1109/CyberSA49311.2020.9139638>.

31 DEEBAK, B. D.; AL-TURJMAN, F. M. Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements. *J. Inf. Secur. Appl.*, v. 58, p. 102749, 2021. Disponível em: <https://doi.org/10.1016/j.jisa.2021.102749>.

32 ISO/IEC. International organization for standardization/international electrotechnical commission. *ISO/IEC 27005 - Information technology — Security techniques — Information security, cybersecurity and privacy protection — Guidance on managing information security risks*, 2022.

33 BOYER, M. M.; ELING, M. New advances on cyber risk and cyber insurance. *The Geneva Papers on Risk and Insurance - Issues and Practice*, v. 48, p. 267–274, 2023. Disponível em: <https://doi.org/10.1057/s41288-023-00294-w>.

34 DACOROGNA, M. M.; DEBBABI, N.; KRATZ, M. Building up cyber resilience by better grasping cyber risk via a new algorithm for modelling heavy-tailed data. *Eur. J. Oper. Res.*, v. 311, p. 708–729, 2022. Disponível em: <https://doi.org/10.48550/arXiv.2209.02845>.

35 IBM. International business machines. *2021 Cost of a Data Breach Study: Global Analysis*, 2021. Disponível em: <https://www.ibm.com/reports/data-breach>.

36 SHEEHAN, B.; MURPHY, F.; KIA, A.; KIELY, R. A quantitative bow-tie cyber risk classification and assessment framework. *Journal of Risk Research*, v. 24, p. 1619 – 1638, 2021. Disponível em: <https://doi.org/10.1080/13669877.2021.1900337>.

37 LIM, M. S. S. Business continuity management and cybersecurity in the cyber risk handbook. *John Wiley & Sons, Ltd*, v. 13, p. 185–192, 2017. Disponível em: <https://doi.org/10.1002/9781119309741.ch13>.

38 NIST. National institute of standards and technology. *NIST SP 800-30 Rev. 1 - Guide for Conducting Risk Assessments*, 2012. Disponível em: <https://doi.org/10.6028/nist.sp.800-30r1>.

39 IBM. International business machines. *Cost of a Data Breach Report 2020*, 2020. Disponível em: <https://www.ibm.com/reports/data-breach>.

40 SCHAIK, P. van; JESKE, D.; ONIBOKUN, J. A.; COVENTRY, L. M.; JANSEN, J.; KUSEV, P. Risk perceptions of cyber-security and precautionary behaviour. *Comput. Hum. Behav.*, v. 75, p. 547–559, 2017. Disponível em: <https://doi.org/10.1016/J.CHB.2017.05.038>.

41 ELING, M.; ELVEDI, M.; FALCO, G. The economic impact of extreme cyber risk scenarios. *North American Actuarial Journal*, v. 27, p. 429 – 443, 2022. Disponível em: <https://doi.org/10.1080/10920277.2022.2034507>.

42 FIELDER, A.; KÖNIG, S.; PANAOUSIS, E. A.; SCHAUER, S.; RASS, S. Risk assessment uncertainties in cybersecurity investments. *Games*, v. 9, p. 34, 2018. Disponível em: <https://doi.org/10.3390/g9020034>.

43 KURE, H. I.; ISLAM, S.; RAZZAQUE, M. A. An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, 2018. Disponível em: <https://doi.org/10.3390/APP8060898>.

44 OSENI, A.; MOUSTAFA, N.; JANICKE, H.; LIU, P.; TARI, Z.; VASILAKOS, A. V. Security and privacy for artificial intelligence: Opportunities and challenges. *ArXiv*, abs/2102.04661, 2021. Disponível em: <https://doi.org/10.48550/arXiv.2102.04661>.

45 NIST. National institute of standards and technology. *NIST SP 800-39 - Managing Information Security Risk: Organization, Mission, and Information System View*, 2011. Disponível em: <https://doi.org/10.6028/NIST.SP.800-39>.

46 NIST. National institute of standards and technology. *NIST SP 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations*, 2020. Disponível em: <https://doi.org/10.6028/NIST.SP.800-53r5>.

47 ISACA. Information systems audit and control association. *N*, 2020.

48 ISACA. Information systems audit and control association. *COBIT® 2019 Framework: Governance and Management of Enterprise IT*, 2019.

49 KOPP, E.; KAFFENBERGER, L.; WILSON, C. J. Cyber risk, market failures, and financial stability. *Risk Management & Analysis in Financial Institutions eJournal*, 2017. Disponível em: <https://doi.org/10.5089/9781484313787.001.A001>.

50 VERIZON. Verizon business. *2023 Data Breach Investigations Report*, 2023. Disponível em: <https://enterprise.verizon.com/resources/reports/dbir/>.

51 MOHURLE, S.; PATIL, M. M. A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, v. 8, p. 1938–1940, 2017. Disponível em: <https://doi.org/10.26483/IJARCS.V8I5.4021>.

52 FERNANDO, Y.; TSENG, M.; WAHYUNI-TD, I. S.; JABBOUR, A. B. L. de S.; JABBOUR, C. J. C.; FOROPON, C. R. H. Cyber supply chain risk management and performance in industry 4.0 era: information system security practices in malaysia. *Journal of Industrial and Production Engineering*, v. 40, p. 102 – 116, 2022. Disponível em: <https://doi.org/10.1080/21681015.2022.2116495>.

53 ZETTER, K. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. [S.l.]: New York: Crown Publishing Group, 2014. 448 p. ISBN 978-0-7704-3617-9.

54 LAMAR, D.; KURALT, M.; ZIDOR-GUERRIER, C. Enterprise risk management post solar winds hack. *International Journal of Business and Applied Social Science*, p. 13–19, 09 2021. Disponível em: <http://dx.doi.org/10.33642/ijbass.v7n9p2>.

55 ANSARIA, A. Analysis of ukraine power grid cyber-attack 2015. *World Journal of Advanced Engineering Technology and Sciences*, 2024. Disponível em: <https://doi.org/10.30574/wjaets.2024.11.1.0024>.

56 BCI. Business continuity institute. *Good Practice Guidelines*, 2018. Disponível em: <https://www.thebci.org/static/cf455e45-b2c2-4a44-b77da7c99fd6df77/BCI-GPG-2018-Edition.pdf>.

57 BCBS. Basel committee on banking supervision - bank for international settlements (bis). *Cyber-resilience: range of practices*, 2018. Disponível em: <https://www.bis.org/bcbs/publ/d454.pdf>.

58 EY. Ernst and young global limited. *2021 Global Information Security Survey*, 2021. Disponível em: <https://assets.ey.com/content/dam/ey-sites/ey-com/es_cl/webcast/2021/09/ey-chile-global-information-security-survey-2021.pdf>.

59 KIKUCHI, M.; OKUBO, T. Cyber governance complex in firms. *Proceedings of the 2nd International Conference on Control and Computer Vision*, 2019. Disponível em: <https://doi.org/10.1145/3341016.3341037>.

60 BRUNNER, M.; SAUERWEIN, C.; FELDERER, M.; BREU, R. Risk management practices in information security: Exploring the status quo in the dach region. *Comput. Secur.*, v. 92, p. 101776, 2020. Disponível em: <https://doi.org/10.1016/j.cose.2020.101776>.

61 TSIODRA, M.; PANDA, S.; CHRONOPOULOS, M.; PANAOUSIS, E. A. Cyber risk assessment and optimization: A small business case study. *IEEE Access*, v. 11, p. 44467–44481, 2023. Disponível em: <https://doi.org/10.1109/ACCESS.2023.3272670>.

62 VACCA, J. R. *Computer and Information Security Handbook*. Elsevier Inc., 2017. ISBN 978-0-12-374354-1. Disponível em: <https://doi.org/10.1016/b978-0-12-374354-1.x0001-5>.

63 NO, W. G.; VASARHELYI, M. A. Cybersecurity and continuous assurance. *Journal of Emerging Technologies in Accounting*, v. 14, p. 1–12, 2017. Disponível em: <https://doi.org/10.2308/JETA-10539>.

64 MENEZES, A.; OORSCHOT, P. C. van; VANSTONE, S. A. *Handbook of Applied Cryptography*. CRC Press, 2018. 810 p. ISBN 9780429466335. Disponível em: <https://doi.org/10.1201/9781439821916>.

65 PARISE, G.; PARISE, L.; ALLEGRI, M.; MARCO, A. D.; ANTHONY, M. A. Operational resilience of hospital power systems in the digital age. *IEEE Transactions on Industry Applications*, v. 57, p. 94–100, 2021. Disponível em: <https://doi.org/10.1109/TIA.2020.3032941>.

66 COSO. Committee of sponsoring organizations of the treadway commission. *Enterprise Risk Management - Integrating with Strategy and Performance*, 2017.

67 BANTLEON, U.; D'ARCY, A.; EULERICH, M.; HUCKE, A.; PEDELL, B.; RATZINGER-SAKEL, N. V. S. Coordination challenges in implementing the three lines of defense model. *Corporate Governance: Internal Governance*, 2020. Disponível em: <https://doi.org/10.2139/ssrn.3663955>.

68 DELOITTE. Deloitte touche tohmatsu limited. *Modernizing the three lines of defense model*, 2020. Disponível em: <https://www2.deloitte.com/us/en/pages/advisory/articles/modernizing-the-three-lines-of-defense-model.html>.

69 EULERICH, M. The new three lines model for structuring corporate governance – a critical discussion of similarities and differences. *Entrepreneurship & the Social Sciences eJournal*, 2021. Disponível em: <https://doi.org/10.2139/ssrn.3777392>.

70 COSO. Committee of sponsoring organizations of the treadway commission. *Internal Control - Integrated Framework*, 2013.

71 EULERICH, A. K.; EULERICH, M. What is the value of internal auditing? – a literature review on qualitative and quantitative perspectives. *Corporate Governance: Actors & Players eJournal*, 2020. Disponível em: <https://doi.org/10.5117/mab.94.50375>.

72 STAVEREN, M. T. van. What can controllers and internal auditors do to support risk ownership. *Maandblad voor Accountancy en Bedrijfseconomie 95*, 2021. Disponível em: <https://doi.org/10.5117/MAB.95.68744>.

73 MUHSYAF, S. A.; CAHYANINGTYAS, S. R.; SASANTI, E. E. Three line of defense: An effective risk management. *Proceedings of the 18th International Symposium on Management (INSYMA 2021)*, 2021. Disponível em: <https://doi.org/10.2991/aebmr.k.210628.015>.

74 BIG. Basel institute on governance. *Basel AML Index 2021 - Ranking money laundering and terrorist financing risks around the world*, 2021. Disponível em: <https://baselgovernance.org/publications/basel-aml-index-2021>.

75 JOHNSTONE, K. M.; GRAMLING, A. A.; RITTENBERG, L. E. *Auditing: A Risk-Based Approach to Conducting a Quality Audit*. [S.l.]: Cengage Learning, 2016. 960 p. ISBN 9780357687871.

76 JOHARI, R. J.; RAZALI, F. M.; HASHIM, A. Enterprise risk management: Internal auditor's role perspective. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, 2022. Disponível em: <https://doi.org/10.6007/ijarafms%2Fv12-i1%2F11413>.

77 TAWFIK, O. I.; DURRAH, O.; ALJAWHAR, K. A. The role of the internal auditor in strengthening the governance of economic organizations using the three lines of defense model. *Journal of Risk and Financial Management*, 2023. Disponível em: <https://doi.org/10.3390/jrfm16070341>.

78 CARCELLO, J. V.; EULERICH, M.; MASLI, A.; WOOD, D. A. Are internal audits associated with reductions in perceived risk? *CGN: Risk Management Practice (Topic)*, 2020. Disponível em: <https://doi.org/10.2139/ssrn.2970045>.

79 IIA. Institute of internal auditors. *Global Perspectives & Insights: Cybersecurity*, 2023. Disponível em: <https://www.theiia.org/en/content/articles/global-perspectives-and-insights/2023/global-perspectives--insights-cybersecurity>.

80 CHEN, Y.; GALLETTA, D. F.; LOWRY, P. B.; LUO, X. R.; MOODY, G.; WILLISON, R. Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model. *Inf. Syst. Res.*, v. 32, p. 1043–1065, 2021. Disponível em: <https://doi.org/10.1287/ISRE.2021.1014>.

81 KAHYAOGLU, S. B.; ÇALıYURT, K. T. Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, v. 33, p. 360–376, 2018. Disponível em: <https://doi.org/10.1108/MAJ-02-2018-1804>.

82 IBM. International business machines. *Cost of a Data Breach Report 2022*, 2022. Disponível em: <https://www.ibm.com/reports/data-breach>.

83 LOIS, P.; DROGALAS, G.; KARAGIORGOS, A.; THRASSOU, A.; VRONTIS, D. Internal auditing and cyber security: audit role and procedural contribution. *International Journal of Managerial and Financial Accounting*, 2021. Disponível em: <https://doi.org/10.1504/ijmfa.2021.10039257>.

84 DELOITTE. Deloitte touche tohmatsu limited. *Risk Management in the Digital Age - Bitcoin futures and hedge accounting*, 2019. Disponível em: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-management-in-the-digital-age.pdf>.

85 BCBS. Basel committee on banking supervision - bank for international settlements. *Principles for enhancing corporate governance*, 2018. Disponível em: <https://www.bis.org/publ/bcbs176.htm>.

86 USA. Office of cybersecurity, energy security, and emergency response. *Cybersecurity Capability Maturity Model (C2M2) - Version 2.1*, 2022. Disponível em: <https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2>.

87 ISO/IEC. International organization for standardization/international electrotechnical commission. *ISO/IEC 27001:2022 - Information technology – Security techniques – Information Security Management Systems – Requirements*, 2022.

88 NIST. National institute of standards and technology. *The NIST Cybersecurity Framework (CSF) 2.0*, 2024. Disponível em: <https://doi.org/10.6028/nist.cswp.29>.

89 NIST. National institute of standards and technology. *NIST IR 8286 - Integrating Cybersecurity and Enterprise Risk Management (ERM)*, 2020. Disponível em: <https://doi.org/10.6028/NIST.IR.8286>.

90 IBM. International business machines. *2020 IBM's Investor Annual Report*, 2020. Disponível em: <https://www.ibm.com/annualreport/assets/downloads/IBM_Annual_Report_2020.pdf>.

91 KABANOV, I.; MADNICK, S. Applying the lessons from the equifax cybersecurity incident to build a better defense. *MIS Quarterly Executive*, v. 20, p. 4, 06 2021. Disponível em: <https://doi.org/10.17705/2msqe.00044>.

92 USA. U.s. house of representatives. *The Equifax Data Breach. Committee Releases Report Revealing New Information on Equifax Data Breach*, 2018. Disponível em: <https://oversight.house.gov/report/committee-releases-report-revealing-new-information-on-equifax-data-breach>.

93 ISO/IEC. International organization for standardization/international electrotechnical commission. *ISO/IEC 31000:2018 - Risk management – Guidelines*, 2018.

94 HUBBARD, D.; SEIERSEN, R. *How to Measure Anything in Cybersecurity Risk*. John Wiley & Sons, Inc, 2016. 304 p. ISBN 9781119162315. Disponível em: <https://onlinelibrary.wiley.com/doi/book/10.1002/9781119162315>.

95 ISACA. Information systems audit and control association. *Roles of Three Lines of Defense for Information Security and Governance*, 2018. Disponível em: <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-4/roles-of-three-lines-of-defense-for-information-security-and-governance>.

96 XIAO, T.; GENG, C.; YUAN, C. How audit effort affects audit quality: An audit process and audit output perspective. *China journal of accounting research*, v. 13, p. 109–127, 2020. Disponível em: <https://doi.org/10.1016/j.cjar.2020.02.002>.

97 BRASIL. Banco central do brasil. *Relatório de Estabilidade Financeira n° 26*, 2024. Disponível em: <https://www.bcb.gov.br/publicacoes/ref>.

98 VALLE, P. R.; FERREIRA, J. Content analysis in the perspective of bardin: Contributions and limitations for qualitative research in education. *SciELO Preprints*, v. 13, 2024. Disponível em: <https://doi.org/10.1590/SciELOPreprints.7697>.

99 GORDIEIEVA, T.; TSATURIAN, A. Analysis of trends and determinants of the 'big 4' companies in the global audit market. *Technology audit and production reserves*, v. 4, p. 6–11, 2023. Disponível em: <https://doi.org/10.15587/2706-5448.2023.286076>.