Proteção Cibernética no Judiciário Brasileiro: Um Estudo Comparativo das Estruturas de Segurança em Tribunais Estaduais

Cybersecurity in Brazilian Judiciary: A Comparative Study of Security Structures in State

Jady Pamella Barbacena da Silva https://orcid.org/0009-0006-4280-3364 Especialização em Cibersegurança. Universidade de Brasília (UnB), Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Brasília – Brasil. jadypamella@gmail.com

Edvan Gomes da Silva https://orcid.org/0009-0005-5271-5328 Mestre em Engenharia Elétrica. Universidade de Brasília (UnB). edvan402@gmail.com

Lucas Vinicius Andrade Ferreira https://orcid.org/0009-0003-9400-5530 Mestre em Engenharia Elétrica. Universidade de Brasília (UnB), Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Brasília – Brasil. lucas.vinicius@live.com

Rafael Rabelo Nunes https://orcid.org/0000-0002-1538-4276 Doutor em Engenharia Elétrica. Professor da Universidade de Brasília, Brasília-DF e do Centro Universitário UniAtenas, Paracatu-MG, –Brasil. rafaelrabelo@unb.br

RESUMO

O recente aumento de ataques cibernéticos direcionados ao setor governamental tem evidenciado vulnerabilidades significativas na proteção dos serviços estatais, destacando a necessidade urgente de fortalecer a cibersegurança, o que inclui os tribunais brasileiros. Este estudo tem como objetivo avaliar as estruturas para se gerenciar riscos cibernéticos em Tribunais, com foco na segunda linha de defesa conforme o Modelo das Três Linhas. A metodologia adotada envolveu a análise documental de informações coletadas através dos portais dos tribunais e informações complementares obtidas por meio da lei de acesso à informação. Os resultados demonstram que, embora haja um esforço de conformidade com as normas de segurança, as práticas efetivas de segurança são inconsistentemente aplicadas e comunicadas, levando a uma proteção ineficiente contra ameaças digitais. As principais contribuições deste estudo incluem a identificação de lacunas críticas entre as políticas de segurança declaradas e as implementações efetivas, além de destacar a necessidade de revisões substanciais para melhorar a coordenação e a eficácia das estratégias de segurança cibernética. As recomendações incluem o desenvolvimento de uma abordagem mais integrada e robusta para a gestão de riscos cibernéticos e das normas estabelecidas, visando reforçar a resiliência de todos os sistemas judiciários estaduais.

Palavras-chave: cibersegurança; tribunais estaduais; ameaças cibernéticas; estratégias de mitigação de risco cibernético; estruturas de governança.

ABSTRACT

The recent increase in cyberattacks targeting the government sector has revealed significant vulnerabilities in the protection of state services, underscoring the urgent need to strengthen cybersecurity measures,

particularly in Brazilian courts. This study aims to assess the structures for managing cyber risks in courts, focusing on the second line of defense according to the Three Lines Model. The methodology adopted involves a documentary analysis of information collected through court portals, supplemented by data obtained via the Access to Information Law. The results indicate that, although there are efforts to comply with security standards, effective security practices are inconsistently applied and poorly communicated, leading to inefficient protection against digital threats The main contributions of this study include identifying critical gaps between declared security policies and their effective implementation, as well as emphasizing the need for substantial revisions to enhance coordination and the effectiveness of cybersecurity strategies. Recommendations include the development of a more integrated and robust approach to cyber risk management and the establishment of standards aimed at strengthening the resilience of judicial systems across the state.

Keywords: cybersecurity; state courts; cyber threats; cyber risk mitigation strategies; governance frameworks.

Recebido em 04/10/2024. Aprovado em 14/11/2024. Avaliado pelo sistema *double blind peer review*. Publicado conforme normas da ABNT.
https://doi.org/10.22279/navus.v14.2032

1 INTRODUÇÃO

Nos últimos anos, a cibersegurança tornou-se um aspecto essencial da governança institucional, especialmente para o setor judiciário, que lida diariamente com informações sensíveis da população. O aumento na frequência e sofisticação dos ataques cibernéticos tem desafiado a segurança das instituições, incluindo tribunais, que são frequentemente alvo de hackers visando vulnerabilidades em seus sistemas de informação (Rezende, 2020). A crescente digitalização dos processos judiciais, acelerada pela pandemia, elevou a importância da proteção de dados, aumentando, por exemplo, o uso de videoconferências, inteligência artificial e outros avanços tecnológicos no sistema de justiça (Martins, 2021; Alves; Georg; Nunes, 2023).

Com isso, a tecnologia tornou-se não apenas um facilitador, mas também uma área de risco significativo para a segurança das operações judiciais. Casos como o ataque de *ransomware* ao Superior Tribunal de Justiça (STJ) em 2020 evidenciam as graves consequências que essas ameaças cibernéticas podem gerar, impactando diretamente o acesso à justiça e a confiança da população no sistema judiciário (Moura, 2022; Alves; Georg; Nunes, 2023). Além da interrupção dos serviços, os ataques podem comprometer a integridade dos dados, permitindo, por exemplo, a alteração de decisões judiciais e a manipulação de processos, como demonstrado em um incidente no Tribunal Regional Federal da 3ª Região (Alves; Georg; Nunes, 2023).

O ambiente cibernético apresenta riscos complexos, que vão além dos danos imediatos. Segundo estudo recente, os principais riscos enfrentados pelos tribunais incluem a interrupção da prestação jurisdicional, vazamentos de informações sigilosas e espionagem por parte de organizações criminosas e governos estrangeiros (Alves; Georg; Nunes, 2023). Tais riscos destacam a importância da implementação de controles de segurança adequados, capazes de mitigar esses desafios e assegurar a continuidade dos serviços judiciais de forma segura e eficiente.

Neste contexto, a necessidade de robustecer as estruturas de segurança cibernética nos tribunais estaduais torna-se premente. O uso de frameworks como o modelo das Três Linhas, que propõe uma segregação clara entre as funções de controle operacional (primeira linha), supervisão de riscos (segunda linha) e auditoria interna (terceira linha), pode contribuir significativamente para essa tarefa (Anderson; Eubanks, 2015;Alves; Queiroz, Nunes, 2023). No entanto, estudos indicam que muitos tribunais ainda não possuem maturidade suficiente em suas estruturas de gestão de riscos cibernéticos, o que resulta em fragilidades na implementação de políticas de segurança e no controle de incidentes (Bevan *et al*., 2018; Alves; Georg; Nunes, 2023).

Este artigo tem como objetivo avaliar as estruturas para se gerenciar riscos cibernéticos em Tribunais. Com isso, avalia o nível de conformidade dessas instituições com as normativas estabelecidas pelo Conselho Nacional de Justiça (CNJ) e investiga a adequação das suas estruturas de segurança às exigências impostas pela crescente sofisticação das ameaças digitais. Mais especificamente, examina-se a existência e a eficácia da segunda linha de defesa, essencial para garantir a segregação das funções de gerenciamento de riscos em relação às operações de TI (Alves; Georg; Nunes, 2023; Alves; Queiroz; Nunes, 2023).

A pesquisa pretende não apenas identificar as lacunas existentes, mas orientar futuras iniciativas de segurança da informação no contexto do judiciário, contribuindo para a proteção da infraestrutura digital e para o fortalecimento da confiança pública nas instituições judiciais brasileiras.

O artigo está estruturado da seguinte forma: após esta introdução, a Seção 2 desenvolve o referencial teórico que suporta o estudo, abordando as principais teorias e modelos de cibersegurança. A Seção 3 detalha a metodologia utilizada para coletar e analisar os dados, enquanto a Seção 4 discute os resultados obtidos, ilustrando as práticas atuais e as lacunas em estratégias de segurança. Finalmente, a Seção 5 oferece conclusões e recomendações baseadas nos achados, propondo caminhos para fortalecer a postura de cibersegurança nos tribunais estaduais.

2 REFERENCIAL TEÓRICO

2.1 Gestão de Riscos Cibernéticos

As organizações enfrentam diversos fatores que podem comprometer o alcance de seus objetivos estratégicos e operacionais (Alves; Georg; Nunes, 2023). Nesse contexto, a gestão de riscos torna-se essencial para que as organizações possam definir estratégias eficazes, atingir suas metas, tomar decisões fundamentadas e, principalmente, criar e proteger valor (Nunes, Perini & Pinto, 2021).

Para que a gestão de riscos seja eficiente, é necessário seguir um processo estruturado que inclua a identificação dos riscos, a medição e estimativa de sua exposição, a análise dos impactos potenciais, a avaliação dos controles existentes em termos de custo-benefício, a implementação de estratégias adequadas de mitigação e a realização de uma avaliação crítica contínua do desempenho do processo de gestão de riscos (Crouhy, Galai; Mark, 2014).

A primeira etapa desse processo, segundo Zottmann *et al*. (2023), é a Identificação de riscos. Esta fase envolve a detecção de ameaças e vulnerabilidades que possam impactar a privacidade dos dados pessoais gerenciados pela organização, bem como a segurança de suas operações.

De acordo com a norma 31000 da Associação Brasileira de Normas Técnicas (ABNT, 2018), a etapa seguinte consiste na análise de riscos, cujo objetivo é compreender a natureza dos riscos e determinar seus níveis, levando em consideração as potenciais consequências e a probabilidade de ocorrência. Essa análise permite decisões informadas sobre quais riscos devem ser tratados prioritariamente e quais medidas de mitigação são mais adequadas.

Após a análise, realiza-se a avaliação de riscos. Conforme estabelece a ABNT 31000 (ABNT, 2018), essa fase visa decidir quais riscos necessitam de tratamento e de que forma. A avaliação permite aos gestores determinar quais riscos são aceitáveis, de acordo com a política de tolerância a riscos da organização, e quais requerem ação imediata, considerando os recursos disponíveis (Nunes; Perini; Pinto, 2021).

No âmbito da segurança cibernética, o gerenciamento de riscos envolve a identificação, avaliação e mitigação de ameaças e vulnerabilidades que possam comprometer a integridade, confidencialidade e disponibilidade dos ativos digitais, sistemas e redes. Essa prática é essencial para proteger informações críticas e assegurar a continuidade das operações (Bermejo *et al*., 2019).

No contexto dos tribunais, a gestão de riscos cibernéticos requer a comparação do nível de risco estimado com os critérios predefinidos. Esse processo inclui a consideração dos impactos potenciais dos eventos de risco sobre os objetivos estratégicos e operacionais dos tribunais, bem como sobre a segurança e privacidade das informações judiciais. A partir dessa avaliação,

decisões podem ser tomadas sobre a necessidade de mitigação ou aceitação do risco, determinando as prioridades para a implementação de controles de segurança (Zottmann *et al*., 2023.

Todas essas etapas devem ser conduzidas com base em um plano de comunicação eficaz. Conforme Bermejo *et al*. (2019), a comunicação e a consulta são fundamentais em cada fase do processo de gestão de riscos, garantindo a participação de diferentes áreas de especialização e a consideração de múltiplas perspectivas na definição dos critérios de risco e na avaliação dos mesmos. Além disso, essas práticas proporcionam informações essenciais para a supervisão contínua dos riscos e a tomada de decisões, promovendo inclusão e responsabilidade entre as partes envolvidas (Crouhy; Galai; Mark, 2014).

A gestão de riscos se mostra útil para assegurar que os recursos de segurança cibernética sejam alocados de maneira eficiente, focando nos riscos que apresentam maior ameaça à operação e à integridade dos sistemas judiciais (Alves; Queiroz; Nunes, 2023). Além disso, essa abordagem permite que os tribunais preparem respostas proativas a possíveis ameaças, fortalecendo sua capacidade de prevenir, detectar e responder a incidentes cibernéticos de maneira eficaz (ABNT, 2018).

2.2 Panorama da Cibersegurança em Tribunais Estaduais

O panorama da cibersegurança nos tribunais estaduais brasileiros é complexo e repleto de riscos. Essas instituições judiciais armazenam uma grande quantidade de dados sensíveis, incluindo informações pessoais e detalhes de casos sob segredo de justiça, o que as torna alvos preferenciais para ataques cibernéticos (Zottmann *et al*., 2023). Ameaças comuns, como ataques de *phishing*, *ransomware* e violações de dados, são frequentemente relatadas, cada uma com potencial para comprometer a integridade e a disponibilidade dos sistemas judiciais. Além disso, a interrupção causada por esses ataques pode ter repercussões devastadoras, não apenas interrompendo as operações diárias, mas também minando a confiança pública no sistema de justiça (Alves; Queiroz; Nunes, 2023).

Com a evolução da tecnologia, as táticas empregadas por cibercriminosos também se sofisticam, tornando as medidas de segurança tradicionais insuficientes para proteger os sistemas de informação dos tribunais (Lobato; Huriel, 2018). A complexidade é ampliada pela diversidade de sistemas de Tecnologia da Informação (TI) utilizados pelos tribunais estaduais, muitos dos quais são sistemas legados com vulnerabilidades conhecidas que são difíceis e onerosas de corrigir. Essa situação é agravada pela escassez de recursos dedicados à cibersegurança, realidade de muitos tribunais que enfrentam orçamentos restritos e falta de pessoal qualificado na área (Alves; Georg; Nunes, 2023).

Em resposta a essas ameaças, alguns tribunais estaduais têm investido na modernização de suas infraestruturas de TI e na implementação de protocolos e controles de segurança mais robustos, em conformidade com a Resolução CNJ nº 396/2021 do Conselho Nacional de Justiça (CNJ, 2021). Essas medidas incluem a adoção de soluções de segurança em múltiplas camadas, o treinamento regular de funcionários em práticas de segurança cibernética e a contratação de especialistas em cibersegurança para fortalecer as equipes internas. Ademais, a colaboração interinstitucional entre diferentes níveis do sistema judiciário tem se mostrado uma estratégia eficaz para compartilhar recursos e conhecimentos em segurança (Zottmann *et al*., 2023).

Segundo Georg *et al.* (2022), persiste um grande desafio na governança da segurança cibernética na esfera pública, já que a maioria dos gestores afirma que as áreas mais estratégicas não se dedicam adequadamente ao tema e que a governança da segurança cibernética ainda é incipiente. Observa-se, portanto, a dificuldade de relacionamento entre as áreas estratégicas e a parte operacional relacionada à segurança cibernética, o que aponta para a necessidade de que a temática seja tratada por estruturas vinculadas ao nível estratégico dos órgãos (Lobato; Huriel, 2018).

2.3 O Modelo das Três Linhas para Cibersegurança em Tribunais Estaduais

O Modelo das Três Linhas é uma abordagem estruturada para a governança e gestão de riscos que tem sido amplamente reconhecida por sua eficácia na organização das responsabilidades relacionadas à cibersegurança. Originado pelo Instituto dos Auditores Internos (IIA), este modelo propõe a divisão clara das funções dentro da organização para melhorar a governança e a gestão de riscos (IIA, 2020).

De acordo com a IIA (2020), adotar uma abordagem baseada em princípios e adaptar o modelo para atender aos objetivos e circunstâncias organizacionais é essencial. Essa estratégia deve focar na contribuição que o gerenciamento de riscos oferece para atingir objetivos e criar valor, além de considerar questões de "defesa" e proteção de valor. É importante compreender claramente os papéis e responsabilidades representados no modelo, bem como os relacionamentos entre eles. Além disso, medidas devem ser implantadas para garantir que as atividades e os objetivos estejam alinhados com os interesses priorizados das partes interessadas (Anderson; Eubanks, 2015).

Segundo Alves *et al.* (2023), as organizações que possuem uma estrutura bem estabelecida das três linhas tendem a gerenciar riscos de forma mais eficaz e inteligente. Elas têm a capacidade de identificar e responder prontamente a riscos emergentes, alocam recursos limitados de maneira mais eficiente para gerir riscos de forma priorizada e mantêm uma transparência interna aprimorada sobre esses riscos. Isso permite que informações críticas sejam compartilhadas entre as diferentes linhas sem a necessidade de duplicação de relatórios ou a realização de múltiplos testes redundantes. Esses fatores são fundamentais para prevenir surpresas e perdas inesperadas, reduzir os custos associados à transferência de risco e assegurar que os objetivos organizacionais sejam atingidos com sucesso (Crouhy; Galai; Mark, 2014).

2.3.1 Primeira Linha de Defesa: Gestão Operacional

A primeira linha consiste nas funções operacionais que gerenciam os riscos cibernéticos. Isso inclui os funcionários que operam e mantêm diariamente os sistemas de tecnologia da informação. Eles são responsáveis pela implementação de políticas de segurança e pela execução de controles técnicos diretos para proteção contra ameaças cibernéticas (Jamison; Morris; Wilkinson, 2018). Esses profissionais também são os primeiros a identificar e tratar riscos, uma função que requer uma vigilância constante e atualização regular de competências para enfrentar novas vulnerabilidades (Silva, 2018).

A primeira linha consiste nas funções operacionais que gerenciam os riscos cibernéticos e é, frequentemente, referida como gerência ou gestão de operações. Tem a responsabilidade de controlar e orientar os processos operacionais nas organizações (Alves; Queiroz; Nunes, 2023). Esses gestores desempenham um papel fundamental na administração, observação e eliminação de riscos, sempre mantendo uma atenção efetiva às suas equipes, garantindo

que todas as operações sejam conduzidas com a máxima segurança e eficiência (IIA, 2020).

No contexto dos tribunais estaduais, a primeira linha é composta por funções operacionais essenciais para o gerenciamento de riscos cibernéticos. Isso inclui gestores de TI e outros funcionários responsáveis pelo funcionamento diário dos sistemas de tecnologia da informação (ALVES; QUEIROZ; NUNES, 2023). Esses profissionais são encarregados de implementar políticas de segurança e executar controles técnicos diretos que são fundamentais para a proteção contra ameaças cibernéticas. A responsabilidade de detectar e responder a incidentes de segurança recai sobre eles, exigindo vigilância constante e uma contínua atualização de competências para combater novas vulnerabilidades e garantir a integridade dos sistemas judiciais.

Dessa forma, a primeira linha de defesa não apenas sustenta a funcionalidade diária das organizações, mas também fortalece a postura de segurança de toda a organização (Anderson; Eubanks, 2015). Os gestores de operações e os profissionais de TI desempenham um papel crítico na manutenção da confiança pública e na proteção das informações judiciais contra os crescentes desafios cibernéticos, garantindo que o sistema judicial possa operar sem interrupções e com total confiabilidade (Alves; Queiroz; Nunes, 2023).

2.3.2 Segunda Linha de Defesa: Supervisão de Riscos

A segunda linha de defesa é onde a supervisão dos riscos é fortalecida. Esta linha é responsável por garantir que as práticas operacionais da primeira linha estejam em conformidade com as políticas e regulamentações internas e externas (IIA, 2020). Funciona como um mecanismo de revisão e reformulação das estratégias de segurança cibernética, adaptando-as para enfrentar ameaças emergentes e apoiando decisões de segurança fundamentadas (Jamison; Morris; Wilkinson, 2018).

A segunda linha é composta por funções de gestão de risco e de conformidade. Essas funções, que também estão submetidas ao controle e à direção da alta administração, são implementadas para garantir que os controles e os processos de gerenciamento de riscos executados pela primeira linha de defesa estejam funcionando de acordo com o planejado, principalmente por meio da atividade de monitoramento contínuo (Anderson; Eubanks, 2015).

Segundo Aguiar (2018), a segunda linha tem a função de supervisionar e coordenar as ações da primeira linha, proporcionando uma certa autonomia gerencial em questões de risco, embora esta autonomia seja restrita, pois ainda está sob a supervisão geral da organização.

No campo da cibersegurança, Jamison, Morris e Wilkinson (2018) destacam que o grupo responsável pela segunda linha gerencia a segurança da informação. Essa equipe é responsável pela implementação e pelo monitoramento de um conjunto extenso de controles que visam identificar comportamentos maliciosos.

Esta função de supervisão e orientação abrange múltiplas responsabilidades, incluindo a vigilância, a avaliação, a execução e o controle dos riscos, com autonomia limitada, mas significativa, em relação às atividades da primeira linha (Jamison; Morris; Wilkinson, 2018).

A segunda linha também inclui funções regulatórias específicas que monitoram o cumprimento de leis e regulamentos aplicáveis, reportando diretamente aos níveis mais altos de gestão e, em alguns casos, aos órgãos de governança (Alves; Queiroz; Nunes, 2023). Essas funções são fundamentais para fortalecer a capacidade organizacional de lidar efetivamente com os

riscos, garantindo não apenas a conformidade, mas também a segurança, qualidade e integridade (Iia, 2020).

Um papel importante na segunda linha de defesa é o CISO (Chief Information Security Officer), ou Diretor de Segurança da Informação em português. De acordo com Shayo e Lin (2019), o CISO tem a tarefa de liderar e gerenciar a estratégia de segurança cibernética de uma organização. Sua principal responsabilidade é implementar e supervisionar políticas, procedimentos e diretrizes de segurança da informação, garantindo a proteção dos dados e sistemas corporativos contra ameaças cibernéticas.

O CISO é fundamental na gestão de incidentes de segurança, na avaliação e mitigação de riscos, no treinamento e conscientização dos funcionários sobre segurança cibernética, e na análise contínua do ambiente de ameaças para assegurar a eficácia das medidas de segurança adotadas (Karanja; Rosso, 2017).

2.3.3 Terceira Linha de Defesa: Auditoria Interna

Finalmente, a terceira linha, que envolve a auditoria interna, fornece uma avaliação independente das duas primeiras linhas. É responsável por verificar a integridade e eficácia dos controles e práticas implementados, garantindo que as vulnerabilidades sejam identificadas e que as ações de mitigação sejam efetivamente executadas (Jamison; Morris; Wilkinson, 2018). Em tribunais estaduais, a função de auditoria interna desempenha um papel fundamental na garantia de que todas as práticas de segurança cibernética estejam em conformidade com as expectativas e exigências do Conselho Nacional de Justiça e outras entidades reguladoras (Nunes, 2012).

Os auditores internos são encarregados de fornecer avaliações objetivas e abrangentes para o órgão de governança e a alta administração, mantendo o mais alto nível de independência dentro da organização (Iia, 2020). Eles avaliam a eficácia da governança, do gerenciamento de riscos e dos controles internos, incluindo a eficiência com que a primeira e a segunda linhas de defesa alcançam os objetivos relacionados ao gerenciamento de riscos e controles (Potter; Toburen, 2016)

Anderson e Eubanks (2015) salientam que a independência organizacional e a objetividade são características distintivas da terceira linha. Os auditores internos não estão envolvidos na elaboração ou implementação de controles, nem são responsáveis pelas operações da organização, que são tarefas das outras duas linhas de defesa. Esta elevada independência permite que forneçam uma avaliação confiável e objetiva à alta direção da organização, garantindo uma revisão imparcial e eficaz das práticas e procedimentos adotados (Aguiar, 2018).

3 METODOLOGIA

Trata-se de uma pesquisa aplicada com objetivos descritivos, uma vez que busca descrever as estruturas utilizadas para gerenciar os riscos cibernéticos nos tribunais, além de estabelecer relações entre essas estruturas e o Modelo das Três Linhas.

Quanto à forma, trata-se de uma pesquisa qualitativa, pois os dados coletados são analisados com o intuito de identificar e interpretar as características presentes nas práticas de gestão de riscos dos tribunais. A análise qualitativa permite uma compreensão mais profunda dos fenômenos envolvidos (Gil, 2008).

Os procedimentos técnicos adotados incluem a pesquisa documental, com o uso de documentos públicos disponibilizados pelos tribunais em seus portais,

complementados por solicitações feitas via Lei de Acesso à Informação. As fontes documentais muitas vezes fornecem ao pesquisador dados relevantes e completos, resultando em economia de tempo na pesquisa. Registros escritos fornecidos por instituições governamentais, como projetos de lei e relatórios de órgãos governamentais, podem ser valiosos para a pesquisa social (Gil, 208). Com esses procedimentos, procurou-se responder às questões listadas no Quadro 1. Destaca-se de que, além de se questionar a existência de um cargo específico para Gestor de Se

Quadro 1 – Questões norteadoras do estudo

Pergunta
1. Existe um comitê de segurança da informação formalmente designado? Se sim, com que frequência o comitê se reúne?
2. Quais são as qualificações e experiências dos membros do comitê de segurança da informação?
3. Existe, no Tribunal, um servidor designado como gerente de segurança da informação? Se sim, onde o gerente de segurança da informação está lotado?
4. Existe, no Tribunal, um servidor designado como Encarregado de Proteção de Dados? Onde o Encarregado de Proteção de Dados está lotado?
5. O comitê e/ou o gerente de segurança toma decisões considerando um processo estruturado de gestão de riscos ou de avaliação dos riscos?
6. Como o comitê de segurança da informação mantém os stakeholders (ou alta administração e sociedade) informados sobre os assuntos relacionados à segurança cibernética da organização?
7. Os riscos ou vulnerabilidades de segurança cibernética são formalmente considerados na priorização das demandas de TI pelo comitê gestor de TI?
8. Existe alguma metodologia para a avaliação da maturidade da segurança da informação? Se sim, qual framework utilizam?
9. Como o Tribunal avalia o seu nível de aderência à Resolução CNJ n. 396/2021 (ENSEC-PJ) e aos controles previstos na Portaria CNJ n. 162/2021?
10. O tribunal possui equipe de tratamento de incidentes em redes de computador (ETIR) designada e em funcionamento?

Fonte: Autor (2023).

Para a análise dos dados, empregou-se a técnica de análise de conteúdo de Bardin (2016), que envolveu a codificação dos dados coletados e a identificação de temas recorrentes. Esta técnica possibilitou a interpretação dos dados de maneira sistemática e detalhada, permitindo identificar padrões e tendências nas estratégias de cibersegurança dos tribunais estaduais. Os temas identificados foram então comparados com a literatura existente sobre cibersegurança e governança de TI, a fim de contextualizar os achados dentro de um quadro teórico mais amplo.

Com base em Bardin (2016), a análise de conteúdo passou pelos seguintes procedimentos:

1. Pré-exame: foi realizada a coleta de documentos provenientes de fontes oficiais, que contêm informações sobre a estrutura organizacional dos

tribunais e o funcionamento dos órgãos que compõem essa estrutura, com o propósito de obter dados preparados para a análise.

2. Exploração do material: os dados presentes nos documentos foram analisados e agrupados de forma a caracterizar o que seria estudado, com o intuito de comparar e construir concepções acerca dos elementos constituintes das estruturas no Modelo das Três Linhas dentro do campo da segurança cibernética.

3. Interpretação dos resultados: a partir da análise realizada na segunda etapa, os dados obtidos foram interpretados a fim de chegar a conclusões relacionadas ao objetivo deste estudo.

4 RESULTADOS E DISCUSSÕES

Utilizando o direito assegurado pela Lei de Acesso à Informação, Lei nº 12.527/2011, foram feitos pedidos a todos os 27 tribunais estaduais do Brasil. Esses pedidos, combinados com a pesquisa documental, formaram uma série de questionamentos focados nos comitês de segurança da informação e nas práticas de segurança cibernética.

O Quadro 2 demonstra o indicador de respostas dos tribunais aos pedidos de acesso à informação. A legislação estipula um prazo de 20 a 40 dias para que os órgãos respondam, mas nem todos cumpriram os pedidos.

Quadro 2 – Indicador de Respostas dos Tribunais Estaduais e do Distrito Federal

Órgão	N° de reiterações	Data de Envio	Data de Resposta	Respondeu no Prazo?
Acre	1	15/09/2023	-	Não
Alagoas	1	15/09/2023	11/10/2023	Sim
Amapá	0	15/09/2023	16/10/2023	Sim
Amazonas	1	15/09/2023	03/11/2023	Não
Bahia	6	15/09/2023	Sem Reposta	Não
Ceará	4	15/09/2023	Sem Reposta	Não
Distrito Federal	0	15/09/2023	20/09/2023	Sim
Espírito Santo	3	15/09/2023	23/11/2023	Não
Goiás	0	15/09/2023	14/11/2023	Não
Maranhão	0	15/09/2023	06/11/2023	Não
Mato Grosso	3	15/09/2023	06/10/2023	Sim
Mato Grosso do Sul	1	15/09/2023	16/10/2023	Sim
Minas Gerais	7	15/09/2023	Sem Reposta	Não
Pará	0	15/09/2023	16/10/2023	Sim
Paraíba	0	15/09/2023	19/10/2023	Sim
Pernambuco	7	15/09/2023	Sem Reposta	Não
Piauí	0	15/09/2023	13/11/2023	Não
Rio de Janeiro	0	15/09/2023	16/10/2023	Sim
Rio Grande do Norte	3	15/09/2023	Sem Reposta	Não
Rio Grande do Sul	0	15/09/2023	16/10/2023	Sim
Rondônia	4	15/09/2023	Sem Reposta	Não
Roraima	1	15/09/2023	19/11/2023	Não
Santa Catarina	2	15/09/2023	13/11/2023	Não
São Paulo	4	15/09/2023	Sem Reposta	Não
Sergipe	4	15/09/2023	Sem Reposta	Não
Tocantins	4	15/09/2023	23/11/2023	Não

Fonte: Autor (2023).

Dos 27 estados, 12 tribunais responderam dentro do prazo legal, enquanto 15 não cumpriram o prazo ou não responderam. Os pedidos foram enviados com as questões norteadoras apresentadas no Quadro 1.

O Quadro 3 do estudo revela uma análise detalhada das práticas de segurança da informação adotadas pelos tribunais estaduais no Brasil, destacando a presença generalizada de Comitês de Segurança da Informação e a qualificação de seus membros, que são quase universalmente implementados em todos os estados pesquisados. A exceção notável é o Espírito Santo, onde não há um comitê formalmente estabelecido. Além disso, embora a maioria dos tribunais tenha designado um Encarregado de Proteção de Dados, como previsto pela LGPD, a inconsistência ainda é observada em estados como Alagoas e Mato Grosso do Sul, onde essa figura é ausente ou a informação não está disponível.

A análise também expõe uma lacuna significativa no que diz respeito ao tratamento de incidentes de segurança. Apenas pouco mais da metade dos tribunais possui equipes designadas e operacionais para o tratamento de incidentes em redes de computadores (ETIR), indicando uma área crítica que necessita de atenção e reforço nas estruturas de segurança cibernética. Notavelmente, estados como Bahia e São Paulo não forneceram respostas completas a essa questão, o que pode sugerir uma necessidade de maior transparência ou de desenvolvimento de capacidades nesse aspecto crítico de segurança cibernética.

Em dezembro de 2023, investigações adicionais foram realizadas nos sites dos oito tribunais que não cumpriram o prazo inicial. Essas verificações focaram em obter respostas sobre a existência de comitês de segurança cibernética, a frequência de suas reuniões e a competência de seus membros, entre outros aspectos da gestão de riscos e comunicação com partes interessadas, o que permitiu a elaboração do Quadro 4.

Apesar de todos esses tribunais afirmarem possuir Comitês de Segurança da Informação e demonstrarem contar com membros qualificados, a ausência de respostas diretas impede uma avaliação mais profunda da efetividade e da real implementação de políticas e práticas de segurança cibernética.

Notavelmente, a falta de informações sobre a existência de um Gerente de Segurança e a alocação de Encarregados de Proteção de Dados em muitos dos tribunais, especialmente em Ceará e Sergipe, sugere que a governança de segurança da informação pode estar subdesenvolvida ou fragmentada, o que representa um risco significativo em um ambiente cada vez mais digital e ameaçado por ataques cibernéticos. A ausência de uma metodologia clara de avaliação e de uma equipe de tratamento de incidentes, em estados como Minas Gerais e Rio Grande do Norte, aponta para uma vulnerabilidade potencial no manejo de incidentes e na resposta às ameaças emergentes, comprometendo, assim, a capacidade de manter a integridade e a confidencialidade dos dados judiciais.

Quadro 3 – Resumo dos Questionários Recebidos

Informação	AC	AL	AM	AP	DF	ES	GO	MA	MS	MT	PA	PB	PI	PR	RS	RJ	RR	SC	TO
Comitê de Segurança da Informação	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Qualificações e experiências dos membros	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Gerente de segurança e alocação	Sim	Não	Não	Sim	Sim	Sim	Não	Não	Não	Não	Sim	Não	Sim	Sim	Sim	Não	Não	Sim	Não
Encarregado de Proteção de Dados	Sim	-	Sim	Sim	Sim	Não	Sim	Sim	-	Sim	Sim	-	Sim	Sim	-	Sim	Não	Sim	Sim
Tomada de decisão e Gestão de Riscos	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim
Comunicação com stakeholders	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim
Priorização de riscos pelo TI	Sim	Sim	-	Sim	Sim	-	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Metodologia de Avaliação/Framework	Não	Não	Sim	Sim	Sim	Não	-	Sim	Sim	Sim	Não	Sim	-	Sim	Sim	Sim	Não	Sim	-
Conformidade com a CNJ 396/2021 e CNJ 162/2022	Não	-	Sim	Sim	Sim	Não	Sim	Sim	Sim	Sim	Sim	Não	Não	Não	Sim	Sim	Não	Sim	-
Equipe de Tratamento de Incidentes	Não	-	-	-	Sim	Não	Não	Sim	Sim	Sim	Sim	Sim	Não	-	Sim	Sim	Não	Sim	Não

Fonte: Autores (2024).

Quadro 4 – Consolidação das informações obtidas por meio dos portais dos Tribunais

Informação	BA	CE	MG	PE	RN	RO	SE	SP
Comitê de Segurança da Informação	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Qualificações e experiências dos membros	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Gerente de segurança e alocação	-	-	-	-	-	-	-	-
Encarregado de Proteção de Dados	-	-	Não	-	-	-	-	-
Tomada de decisão e Gestão de Riscos	Não	Sim	Não	Sim	Sim	Não	Sim	Sim
Comunicação com stakeholders	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Priorização de riscos pelo TI	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Metodologia de Avaliação/Framework	-	-	-	-	-	-	-	-
Conformidade com a CNJ 396/2021 e CNJ 162/2022	-	-	-	-	-	-	-	-
Equipe de Tratamento de Incidentes	-	-	-	-	-	-	-	-

Fonte: Autores (2024).

4.1 Análise dos resultados por região brasileira

4.1.1 Tribunais da Região Norte

Os tribunais estaduais da região Norte do Brasil têm adotado diversas abordagens para aprimorar a segurança da informação, cada um em diferentes estágios de implementação e conformidade com regulamentações nacionais.

O Tribunal de Justiça do Acre recentemente criou um Comitê de Segurança da Informação e está em fase de elaboração de um plano de ação de segurança da informação. Embora ainda não tenha realizado reuniões, o tribunal está iniciando a implementação de metodologias baseadas em mapeamento de riscos, sinalizando uma fase inicial de aderência às normativas do CNJ.

O Tribunal Estadual do Amapá mantém um Comitê de Segurança da Informação e realiza avaliações de maturidade com base nas regulamentações da CNJ, ressaltando seu compromisso contínuo com a melhoria da postura de segurança e autoavaliando-se com maturidade média na área.

O Tribunal Estadual do Amazonas se destaca com um Comitê de Segurança da Informação formalmente designado, que realiza reuniões regulares, tanto presencialmente quanto por videoconferência. Seus profissionais possuem formação acadêmica específica na área de Segurança da Informação e Proteção de Dados, além de certificações internacionais. A gestão de riscos segue as

normas ABNT 27005 (ABNT, 2023) e ABNT 31000 (ABNT, 2018), indicando aderência às diretrizes da Resolução CNJ 396/2021.

O Tribunal Estadual do Pará implementou um Comitê de Segurança da Informação. Embora a experiência direta em segurança da informação seja limitada a poucos membros, como o Secretário de Informática e Gestor de Segurança da Informação, o tribunal demonstra um compromisso com a proteção de dados e integridade operacional, estando em processo de avaliação de *frameworks* para segurança da informação.

O Tribunal de Justiça do Estado de Rondônia adota uma abordagem multidisciplinar para a segurança da informação, com reuniões bimestrais e uma variedade de canais de comunicação para envolver as partes interessadas. No entanto, a falta de um gerente de segurança e um encarregado de proteção de dados, juntamente com informações incompletas sobre a metodologia de avaliação e *frameworks*, gera algumas dúvidas sobre a eficácia total das suas práticas de segurança.

O Tribunal de Justiça do Estado de Roraima recentemente estabeleceu um Comitê de Segurança da Informação e está elaborando seu Plano de Ação de Segurança da Informação. Este tribunal está no início do processo de conformidade com a Resolução CNJ 396/2021, indicando uma jornada de fortalecimento das capacidades de segurança cibernética.

Finalmente, o Tribunal de Justiça do Estado do Tocantins possui uma estrutura formal para segurança da informação e proteção de dados, estabelecida desde 2014. Embora possua um Comitê Gestor de Proteção de Dados Pessoais e divulgue planos de risco e gestão de TI online, faltam informações detalhadas sobre sua metodologia de avaliação e adesão às normativas da CNJ, dificultando uma avaliação completa da sua conformidade.

4.1.2 Tribunais da Região Nordeste

Os tribunais estaduais das regiões Nordeste do Brasil demonstram variados níveis de maturidade em suas políticas de segurança da informação e conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e as resoluções do CNJ. A maioria dos tribunais possui comitês de segurança da informação, como é o caso de Alagoas, Maranhão, Paraíba, Piauí, Bahia, Rio Grande do Norte e Sergipe. No entanto, há diferenças significativas na regularidade das reuniões, na qualificação dos membros e na transparência das informações.

O Tribunal de Justiça de Alagoas recentemente ajustou suas políticas de proteção de dados, mas faltam informações detalhadas sobre a implementação de suas estratégias, enquanto o Tribunal de Justiça do Maranhão adota uma postura proativa, com um comitê que se reúne bimestralmente e utiliza metodologias como os frameworks CIS Controls v8 (CIS, 2024) e NIST (NIST, 2024), além das normas ISO da série 27000.

No Tribunal de Justiça da Paraíba, a governança de dados é coordenada por um Comitê Executivo de Proteção de Dados Pessoais, com um gerente de segurança da informação e um encarregado de proteção de dados, refletindo um compromisso com a Resolução 396/2021 e a Portaria 162/2021, ambas do CNJ. Já no Tribunal de Justiça do Piauí, as reuniões do comitê e a experiência dos membros são mantidas em sigilo por questões de segurança, embora a integração da segurança da informação na gestão de TI seja evidente.

Nos tribunais da Bahia, Rio Grande do Norte e Sergipe, a presença de comitês de segurança da informação é confirmada, mas há uma escassez de informações sobre a periodicidade das reuniões e a metodologia de avaliação utilizada. A comunicação com as partes interessadas é feita principalmente

via e-mails e portais eletrônicos. Esses tribunais, embora comprometidos com a gestão de riscos, carecem de gerentes de segurança e encarregados formais de proteção de dados.

4.1.3 Tribunais da Região Centro-oeste

Os tribunais estaduais da região Centro-Oeste do Brasil adotam diferentes abordagens para a gestão da segurança da informação, com variações nas estruturas e metodologias empregadas.

O Tribunal de Justiça do Estado de Goiás conta com um comitê formal de segurança da informação composto por membros de diversas áreas, incluindo juízes, diretores e profissionais de tecnologia. Apesar de ter um encarregado de proteção de dados, o tribunal ainda carece de uma metodologia formal para avaliar a maturidade da segurança da informação e de uma equipe dedicada ao tratamento de incidentes em redes de computadores.

O Tribunal de Justiça do Mato Grosso demonstra um forte compromisso com a proteção de dados, utilizando metodologias consolidadas como NIST (NIST, 2024), CIS Controls (CIS, 2024) e ABNT 27001(ABNT, 2022). O tribunal avalia sua aderência às normas CNJ 396/2021 e CNJ 162/2021 por meio de uma consultoria externa, garantindo uma abordagem estruturada e ampla.

O Tribunal de Justiça do Mato Grosso do Sul possui um comitê de segurança da informação e um gerente designado para essa área, além de uma equipe de tratamento de incidentes. Utilizam o CIS Controls v8 (CIS, 2024) para a avaliação da maturidade da segurança da informação, e mantêm uma comunicação eficiente com os stakeholders, assegurando uma boa aderência às normativas do CNJ.

Por fim, o Tribunal de Justiça do Distrito Federal e Territórios se destaca pelo alto nível de expertise de seus membros, com mestrados e doutorados em segurança da informação. O tribunal utiliza a metodologia CIS Controls v8 (CIS, 2024) para a avaliação da maturidade da segurança da informação e apresenta alta aderência às resoluções do CNJ, além de um processo estruturado de gestão de riscos e comunicação eficiente com a alta administração.

4.1.4 Tribunais da Região Sudeste

Os tribunais estaduais da região Sudeste adotam diferentes práticas em relação à segurança da informação, com variações na estrutura organizacional e nas metodologias utilizadas.

O Tribunal de Justiça do Rio de Janeiro possui um Comitê de Segurança da Informação formalmente designado, além de um Comitê Gestor de Proteção de Dados Pessoais. O tribunal adota *frameworks* como NIST (NIST, 2024), CIS Controls (CIS, 2024) e ABNT 27001(ABNT, 2022), e mantém um programa de conscientização e de melhoria contínua para garantir a conformidade com as normativas do CNJ, como a Resolução 396/2021 e a Portaria 162/2022.

Em contrapartida, o Tribunal de Justiça do Espírito Santo enfrenta desafios significativos, uma vez que não dispõe de um comitê formal de segurança da informação e seu responsável pela segurança está alocado de forma mais operacional do que estratégica. A ausência de um Encarregado de Proteção de Dados compromete sua conformidade com as regulamentações, resultando em uma baixa aderência às resoluções do CNJ.

O Tribunal de Justiça de São Paulo possui um comitê multidisciplinar de segurança cibernética que se reúne semestralmente, porém não há um gerente de segurança ou encarregado de proteção de dados designados. A comunicação

com os *stakeholders* é feita por e-mails e informações no site, mas o tribunal não especifica a metodologia de avaliação utilizada nem a conformidade com as normativas do CNJ.

Da mesma forma, o Tribunal de Justiça de Minas Gerais também conta com um comitê multidisciplinar de segurança da informação que se reúne bimestralmente. No entanto, faltam um gerente de segurança e um encarregado de proteção de dados. A comunicação com stakeholders é realizada de forma similar, via e-mails e informações online, mas, assim como em São Paulo, o tribunal não especifica o framework de avaliação nem a conformidade com as resoluções do CNJ.

4.1.5 Tribunais da Região Sul

Os tribunais estaduais da região Sul do Brasil têm implementado diversas estratégias para a gestão da segurança da informação, com estruturas e metodologias robustas.

O Tribunal de Justiça do Paraná possui um Comitê de Governança de Segurança da Informação, apoiado por uma Política de Segurança da Informação (PSI) atualizada e regulamentada. A gestão de segurança é liderada por um Gestor de Segurança da Informação, e o tribunal também conta com um Encarregado de Proteção de Dados, refletindo o compromisso com a conformidade legal. Utiliza o CIS Controls v8 (CIS, 2024) para avaliar a maturidade da segurança da informação e possui um plano de ação em execução para garantir a aderência à Resolução CNJ 396/2021 e à Portaria CNJ 162/2022.

O Tribunal de Justiça de Santa Catarina mantém uma estrutura sólida de segurança da informação, com um Comitê formal, além de um Gerente de Segurança e um Encarregado de Proteção de Dados. O tribunal utiliza o framework ABNT 27001 (ABNT, 2022) para a avaliação da maturidade da segurança e realiza verificações regulares de conformidade com as regulamentações do CNJ.

Por sua vez, o Tribunal de Justiça do Rio Grande do Sul também conta com um Comitê de Segurança da Informação, mas a gestão de segurança é centralizada na Seção de Segurança da Informação, subordinada à Direção de TI. O tribunal utiliza o iGovTIC-JUD e o ITKeyMetrics do Gartner para avaliação de maturidade, além de seguir indicadores estratégicos do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC). A conformidade com as resoluções do CNJ é monitorada pela auditoria interna e processos de acompanhamento.

4.2 Discussões

Apesar de a maioria dos tribunais estaduais brasileiros ter formalmente adotado medidas para estruturar suas operações de cibersegurança, os resultados obtidos na prática revelam uma considerável heterogeneidade e inconsistência. A análise documental conduzida neste estudo evidencia que existe uma lacuna significativa na implementação efetiva dessas diretrizes no âmbito operacional. Essa desconexão entre a teoria e a prática compromete a eficácia geral e expõe os tribunais a riscos cibernéticos substanciais (Georg *et al.*, 2022).

A primeira linha de defesa, responsável pelas operações diárias e pela gestão direta dos riscos, enfrenta uma série de desafios que limitam sua capacidade de atuar de forma eficaz. Relatos indicam uma insuficiência crônica de recursos, tanto em infraestrutura tecnológica quanto em pessoal qualificado, dificultando a resposta apropriada às ameaças cibernéticas cada vez mais sofisticadas. Silva (2018) observa que as equipes de segurança da

informação frequentemente se encontram sobrecarregadas e incapazes de acompanhar o ritmo acelerado das inovações tecnológicas e das ameaças emergentes, resultando em lacunas significativas na postura de segurança dos tribunais.

No que concerne à segunda linha de defesa, encarregada da supervisão e do monitoramento dos riscos, identifica-se uma falta de alinhamento crítico entre as funções de gerenciamento de risco e as operações diárias. Essa desconexão resulta em uma aplicação inconsistente das políticas e procedimentos de cibersegurança, minando a eficácia das medidas implementadas e comprometendo a capacidade dos gestores de risco de exercerem suas funções de forma plena. A falta de autoridade decisória e de recursos adequados para implementar as mudanças necessárias agrava ainda mais esse cenário, criando um ambiente propício para a persistência de vulnerabilidades (Alvez; Queiroz; Nunes, 2023).

Um aspecto adicional e igualmente crítico é a ausência de uma cultura organizacional voltada para a cibersegurança entre os funcionários dos tribunais. A pesquisa indica uma deficiência significativa em programas de treinamento contínuo e iniciativas de conscientização, o que aumenta o risco de incidentes de segurança decorrentes de erro humano ou negligência. Sem um esforço consistente para educar e engajar os funcionários em todos os níveis hierárquicos, as políticas de segurança tendem a ser ineficazes, permanecendo apenas no âmbito formal sem impacto real nas práticas cotidianas (Nunes, 2012).

A colaboração interinstitucional entre os tribunais, que poderia servir como um mecanismo para fortalecer coletivamente as defesas cibernéticas, tem sido limitada e não sistematizada. Embora existam algumas iniciativas pontuais de compartilhamento de melhores práticas, estas não são amplamente adotadas nem ocorrem de maneira regular. Esse fato evidencia um potencial significativo inexplorado para a melhoria na cooperação intertribunal. A criação de mecanismos formais de colaboração e troca de informações poderia ampliar a capacidade dos tribunais de enfrentar os desafios comuns de cibersegurança, promovendo a adoção de estratégias mais eficazes e coesas (Lobato; Huriel, 2018).

Diante desse panorama, torna-se evidente que a implementação efetiva do Modelo das Três Linhas nos tribunais estaduais brasileiros requer ajustes substanciais e uma abordagem mais integrada. É imperativo que haja um fortalecimento da liderança institucional no compromisso com a segurança da informação, incluindo a alocação adequada de recursos e o empoderamento dos gestores de risco. Conforme sugerido por Rezende (2020), a integração eficaz de tecnologia, processos e pessoal é essencial para elevar o nível de maturidade em cibersegurança.

5 CONCLUSÃO

A pesquisa sobre proteção contra ameaças cibernéticas nos tribunais estaduais do Brasil revelou uma complexidade desafiadora. O Modelo das Três Linhas, apesar de endossado teoricamente, é inconsistente na prática, com lacunas que afetam a eficácia das estratégias de cibersegurança. Este estudo ressaltou as dificuldades enfrentadas por cada linha de defesa, destacando a necessidade urgente de uma abordagem mais integrada e robusta na gestão de riscos cibernéticos.

A primeira linha de defesa, responsável pelas operações diárias e pela gestão direta dos riscos, sofre com a falta de recursos e tecnologias avançadas. A segunda linha, encarregada de supervisionar a eficácia das

políticas de cibersegurança, frequentemente se desalinha das práticas operacionais, o que enfraquece a supervisão dos riscos. Já a terceira linha, a auditoria interna, embora essencial para a avaliação independente, é muitas vezes subutilizada e não foca nas áreas de risco de cibersegurança mais críticas.

Além disso, a falta de conscientização e treinamento em cibersegurança é um problema grave, que pode comprometer até as defesas mais sólidas. A implementação de programas de treinamento contínuos e eficazes é fundamental para fortalecer a segurança nos tribunais estaduais. Além disso, a colaboração entre tribunais é uma medida essencial, pois a partilha de recursos e melhores práticas pode fortalecer significativamente a segurança cibernética em um ambiente jurídico cada vez mais digital.

Em geral, foi observado um comprometimento amplo dos tribunais com a segurança da informação, evidenciado pelo uso de processos estruturados de gestão de riscos, com alguns tribunais adotando metodologias específicas como as ABNT 27001 (ABNT, 2022), ABNT 27005 (ABNT, 2023) e ABNT 31000 (ABNT, 2018), bem como frameworks amplamente adotados no âmbito da segurança da informação, como o CIS Controls (CIS, 2024) e o NIST (NIST, 2024).

No que diz respeito à conformidade com as normativas estabelecidas, há uma variação entre os tribunais, com alguns demonstrando um forte empenho em atingir altos níveis de aderência, enquanto outros apresentam uma aderência mais baixa.

É importante que a liderança dos tribunais assuma um papel ativo na promoção de uma cultura de segurança que integre práticas de cibersegurança em todas as operações judiciais. O investimento em tecnologia, treinamento e colaboração ultrapassa a necessidade operacional, configurando-se como uma estratégia essencial para a proteção da integridade e confiabilidade do sistema judicial.

Este artigo oferece uma base para investigações futuras e desenvolvimentos na área de segurança cibernética em tribunais, evidenciando a necessidade de ação coordenada e imediata para enfrentar os desafios emergentes, bem como, uma maior organização de acesso à informação. Uma limitação deste estudo diz respeito às dificuldades encontradas na obtenção de informações claras e precisas dentro do tempo desejado, devido a desafios enfrentados por alguns tribunais na atualização de seus organogramas e sites. Em especial, observou-se que os tribunais do Amapá e do Mato Grosso do Sul não forneceram respostas completas a certas indagações.

Uma oportunidade para trabalho futuro seria a realização de um estudo comparativo entre tribunais estaduais e federais no Brasil, com foco nas práticas de cibersegurança e nas estruturas de gerenciamento de riscos cibernéticos adotadas por essas instituições. Tal investigação poderia identificar divergências nas estratégias de proteção digital e destacar fatores regionais, orçamentários e operacionais que influenciam a implementação dessas práticas.

REFERÊNCIAS

AGUIAR, Anderson Silva de. **As três linhas de defesa no Exército Brasileiro:** um estudo da sistemática de gerenciamento de controles internos e riscos. (Trabalho de Conclusão de Curso) - Escola de Formação Complementar do Exército / Escola de Aperfeiçoamento de Oficiais, 2018.

ALVES, Renato Solimar; GEORG, Marcus Aurélio Carvalho; NUNES, Rafael Rabelo. Judiciário sob ataque hacker: riscos de negócio para segurança cibernética em tribunais brasileiros. **Revista Ibérica de Sistemas e Tecnologias de Informação**, n. E56, p. 344-357, fev. 2023.

ALVES, Renato Solimar; QUEIROZ, Carlos Eduardo Mancini; NUNES, Rafael Rabelo. Os tribunais têm estrutura para gerenciar riscos de segurança da informação? Um estudo à luz das Três Linhas. **Revista CEJ**, Brasília, v. 27, n. 86, p. 145-160, jul./dez. 2023.

ANDERSON, Douglas J.; EUBANKS, Gina. **Leveraging COSO Across the Three Lines of Defense**. [S.l.], 2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2022:** Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação – Requisitos. Rio de Janeiro: ABNT, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27005:2023:** Segurança da informação, segurança cibernética e proteção à privacidade — Orientações para gestão de riscos de segurança da informação. Rio de Janeiro: ABNT, 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 31000:2018:** Gestão de riscos – Diretrizes. Rio de Janeiro: ABNT, 2018.

BARDIN, Laurence. **Análise de Conteúdo**. São Paulo: Almedina Brasil, 2016.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011. Lei de Acesso à Informação.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União: seção 1, Edição Extra, Brasília, DF, p. 1, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 21 abr. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, p. 59, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 abr. 2024.

BERMEJO, Paulo Henrique de Souza; SANT'ANA, Tomás Dias; SALGADO, Eduardo Gomes *et al*. **ForRisco:** gerenciamento de riscos em instituições públicas na prática. São Paulo: FDSMPRESS, 2019.

CENTER FOR INTERNET SECURITY. **CIS Controls v8**. Enhanced to address evolving technology and threats, including cloud and mobile technologies. Disponível em: https://learn.cisecurity.org/cis-controls-download. Acesso em: 21 abr. 2024.

CONSELHO NACIONAL DE JUSTIÇA. **Portaria n° 162, de 10 de junho de 2021.** Aprova Protocolos e Manuais criados pela Resolução CNJ n° 396/2021. Diário da Justiça do Conselho Nacional de Justiça, Brasília, DF, 22 fev. 2022. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3284. Acesso em: 21 abr. 2024.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução n° 363, de 12 de janeiro de 2021.** Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais. Diário de Justiça Eletrônico (DJe) do CNJ, Brasília, DF, n. 11, p. 2-4, 18 jan. 2021. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3668. Acesso em: 21 abr. 2024.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução n° 396, de 7 de junho de 2021.** Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Diário de Justiça Eletrônico (DJe), Brasília, DF, n. 248, p. 3-10, 24 set. 2021. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3975. Acesso em: 21 abr. 2024.

CROUHY, Michel; GALAI, Dan; MARK, Robert. **The Essentials of Risk Management.** 2. ed. New York: McGraw-Hill Education, 2014.

FERNANDES, Marquésia Pereira. **Crimes Digitais na Era do Metaverso no Brasil.** (Trabalho de Conclusão de Curso) - Pontifícia Universidade Católica de Goiás, Escola de Direito, Negócios e Comunicação, Coordenação Adjunta de Trabalho de Curso, Goiânia, 2022. Disponível em: https://www.conjur.com.br/2022-abr-15/onda-invasoes-hackers-estruturas-tecnologicas-tribunais. Acesso em: 21 abr. 2024.

GEORG, Marcus Aurélio Carvalho *et al*. Os desafios da Segurança Cibernética no setor público federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação. RISTI - **Revista Ibérica de Sistemas e Tecnologias de Informação**, n. E54, p. 602-616, nov. 2022.

GIL, Antonio Carlos. **Métodos e Técnicas de Pesquisa Social.** 6. ed. São Paulo: Atlas S.A., 2008.

INSTITUTO DOS AUDITORES INTERNOS (IIA). **Modelo das três linhas do IIA 2020.** Florida-EUA, 2020. Disponível em: https://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/20200758glob-th-editorHTML-00000013-20072020131817.pdf. Acesso em: 21 abr. 2024.

JAMISON, John; MORRIS, Lucas; WILKINSON, Christopher. **The Future of Cybersecurity in Internal Audit**. Internal Audit Foundation, 2018.

KARANJA, Erastus; ROSSO, Mark. **The Chief Information Security Officer: An Exploratory Study**. North Carolina Central University, 2017.

LOBATO, Luisa Cruz; HURIEL, Louise Marie. **Uma Estratégia para a Governança da Segurança Cibernética no Brasil**. Instituto Iguarapé, 2018.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST Cybersecurity Framework**. Versão mais recente com orientações sobre a segurança cibernética. Disponível em: https://www.nist.gov/cyberframework. Acesso em: 21 abr. 2024.

NUNES, Paulo Fernando Viegas. **A definição de uma estratégia nacional de cibersegurança:** cibersegurança. Lisboa, 2012.

POTTER, Patrick; TOBUREN, Marshall. **The 3 Lines of Defense for Good Risk Management. Risk Management**. 2016, p. 16. Disponível em: https://www.rmmagazine.com/articles/article/2016/06/01/-The-3-Lines-of-Defense-for
GoodRisk-Management-. Acesso em: 05 nov. 2023.

REZENDE, Mauricio Vianna de. **Avaliação de segurança cibernética no desenvolvimento de software embarcado automotivo:** uma abordagem ontológica. (Tese de doutorado) - Universidade FUMEC, Faculdade de Ciências Empresariais - FACE, Belo Horizonte, 2020.

SHAYO, Conrad.; LIN, Frank. An Exploration of the Evolving Reporting Organizational Structure for the Chief Information Security Officer (CISO) Function. **Journal of Computer Science and Information Technology**, v. 7, n. 1, p. 1-20, 2019. DOI: 10.15640/jcsit.v6n2a1.

SILVA, Marcos Ricardo Cruz da. **Compliance:** Um estudo de caso sobre a estruturação do sistema de conformidade da Odebrecht S.A. (Dissertação de mestrado) - Faculdade de Economia da Universidade Estadual de Campinas, Campinas, 2018.

ZOTTMANN, Carlos Eduardo Miranda; GEORG, Marcus Aurélio Carvalho; ALVES, Renato Solimar; da SILVA, Marcelo Antônio; NUNES, Rafael Rabelo. Proposta de Metodologia para Avaliação de Riscos de Privacidade para Órgãos do Poder Judiciário no Brasil. **Encontro de Administração da Justiça** (ENAJUS), Brasília, 2023.