Universidade de Brasília

Faculdade de Economia, Administração,Contabilidade e Gestão de Políticas Públicas

Departamento de Administração

GABRIELA ALVES DOS SANTOS

ANÁLISE DA ESTRUTURA DE PROTEÇÃO CONTRA AMEAÇAS CIBERNÉTICAS EM TRIBUNAIS ESTADUAIS DO BRASIL: Uma pesquisa baseada no Modelo das Três Linhas

Brasília-DF

2023

GABRIELA ALVES DOS SANTOS

ANÁLISE DA ESTRUTURA DE PROTEÇÃO CONTRA AMEAÇAS CIBERNÉTICAS EM TRIBUNAIS ESTADUAIS DO BRASIL: Uma pesquisa baseada no Modelo das Três Linhas

Monografia apresentada ao Departamento de Administração como requisito parcial à obtenção do título de Bacharel em Administração.

Professor Orientador: Prof. Dr. Rafael Rabelo Nunes

Brasília-DF
2023

GABRIELA ALVES DOS SANTOS

ANÁLISE DA ESTRUTURA DE PROTEÇÃO CONTRA AMEAÇAS CIBERNÉTICAS EM TRIBUNAIS ESTADUAIS DO BRASIL: uma pesquisa baseada no Modelo das Três Linhas

A Comissão Examinadora, abaixo identificada, aprova o Trabalho de Conclusão do Curso de Administração da Universidade de Brasília da aluna)

Gabriela Alves dos Santos

Prof. Dr. Rafael Rabelo Nunes (Orientador)

Professor-Orientador

Dr., Aldery Silveira Júnior

Professor-Examinador

Ms., Marcus Aurélio Carvalho Georg

Professor-Examinador

Brasília, 21 de dezembro de 2023.

Gratidão a Deus pela oportunidade de ter chegado até aqui. Expresso meu apreço a minha família e em especial ao meu falecido pai por todo apoio dado em vida e por me fazer acreditar nos meus sonhos.

“Não podemos prever o futuro, mas podemos criá-lo.”

Peter Drucker

RESUMO

Nos últimos anos, tem sido observado um incremento na ocorrência de investidas cibernéticas direcionadas ao âmbito governamental, resultando em significativos problemas nos serviços prestados pelo estado. O Poder Judiciário tem sido alvo de ações de *hackers*. Neste contexto, o propósito do estudo foi a avaliação da existência de uma segunda linha se tratando de cibersegurança das entidades judiciais no Brasil, com embasamento no paradigma do Modelo das Três Linhas, conforme divulgado pelo Instituto dos Auditores Internos. Para esta finalidade, foram submetidos à análise documentos oficiais, a exemplo de organogramas, portarias, regulamentos e planos estratégicos, por meio de uma abordagem de análise de conteúdo, objetivando corroborar a consonância da estrutura de cibersegurança com o Modelo das Três Linhas. Este estudo confere uma visão pormenorizada da estrutura organizacional de cibersegurança das Instituições do judiciário na esfera estadual brasileira, fornecendo diretrizes para a sua aderência ao Modelo das Três Linhas e propondo uma futura avaliação potencial quanto à aderência à Estratégia Nacional de Cibersegurança do Poder Judiciário.

Palavras-chave: Estratégias de mitigação de risco cibernético; Medidas de segurança cibernética; Estruturas de governança; Cenários de ameaça digital informação.

ABSTRACT

In recent years, there has been an increase in the occurrence of cyber attacks directed at the governmental sphere, resulting in significant problems in state services. The judiciary has stood out as a common target for hacker actions. In this context, the underlying purpose of this study was to evaluate the existence of a second line in the cybersecurity framework of judicial entities in Brazil, based on the Three Lines Model paradigm, as published by the Institute of Internal Auditors. For this purpose, official documents, such as organizational charts, ordinances, regulations and strategic plans, were subjected to analysis, using a content analysis approach, aiming to corroborate the consistency of the cybersecurity structure with the Three Lines Model. This study provides a detailed view of the organizational cybersecurity architecture of Brazilian judicial institutions, providing guidelines for their adherence to the Three Lines Model and proposing a potential future assessment regarding adherence to the National Cybersecurity Strategy of the Judiciary.

Keywords: Cyberrisk mitigation strategies; Cybersecurity measures; Governance structures; Digital information threat scenarios.

LISTA DE FIGURAS

Figura 1: Princípios 7
Figura 2: Processo 8
Figura 3: O Modelo das Três Linhas do IIA 15

LISTA DE QUADROS

Quadro 1: Resumo dos questionários da Região Norte 33
Quadro 2: Resumo dos questionários da Região Centro-Oeste 38
Quadro 3: Resumo dos questionários da Região Sudeste 41
Quadro 4: Resumo dos questionários da Região Sul 43
Quadro 5: Resumo dos questionários da Região Nordeste 46
Quadro 6: Indicador de respostas dos Tribunais Estaduais e do Distrito Federal 52
Quadro 7: Tabela resumo dos questionários recebidos 57
Quadro 8: Tabela resumo dos questionários não recebidos 57

SUMÁRIO

1 INTRODUÇÃO 19
1.1 Problema de pesquisa 3
1.2 Objetivo Geral 4
1.3 Objetivos Específicos 4
1.4 Justificativa 5
2 REFERENCIAL TEÓRICO 7
2.1 Gestão de Risco 7
2.2 Governança Corporativa 10
2.3 Segurança Cibernética 12
2.4 Modelo das Três Linhas 14
2.5 Caracterizando a 2ª Linha de Defesa 17
2.6 CISO 18
3 METODOLOGIA 20
4 RESULTADOS 23
4.1 Tribunais da Região Norte 24
4.2 Tribunais da Região Centro-Oeste 38
4.3 Tribunais da Região Sudeste 41
4.4 Tribunais da Região Sul 43
4.5 Tribunais da Região Nordeste 46
4.6 Indicador de respostas 52
5 ANÁLISE E DISCUSSÕES 55
CONCLUSÃO 59
REFERÊNCIAS 60
ANEXOS 64
Levantamento dos questionários de cada estado 64

1 INTRODUÇÃO

Conforme destacado por Rezende (2020), a segurança cibernética assume um papel prioritário ao enfatizar que a ameaça é contínua, exigindo um comprometimento constante com o processo de proteção. Este campo está em constante evolução, caracterizado pela emergência constante de novas ameaças e vulnerabilidades. Vale ressaltar que a segurança cibernética não representa um estado estático a ser atingido; ao contrário, configura-se como um processo dinâmico que demanda monitoramento ininterrupto, atualizações de políticas e tecnologias, assim como adaptações às mudanças nas ameaças cibernéticas. A recorrência de ataques cibernéticos tem exercido um impacto adverso sobre as atividades essenciais de diversos tribunais do poder judiciário. Essa realidade evidencia a necessidade urgente de implementação de medidas proativas e estratégias robustas para mitigar os riscos associados à segurança digital. Nesse contexto, a compreensão de que a segurança cibernética é um processo contínuo, permeado pela constante adaptação às transformações no cenário de ameaças, torna-se crucial para garantir a integridade e eficiência das operações judiciais (Rezende, 2020).

Esses incidentes não apenas comprometem a reputação dessas instituições, mas também prejudicam a concretização de seus objetivos estratégicos. Vale ressaltar que o poder judiciário assumiu uma função de destaque na modernização do sistema judiciário brasileiro, incorporando extensivamente a tecnologia aos seus procedimentos judiciais. Essa integração tecnológica, embora tenha contribuído para a eficiência e agilidade do sistema, também os tornou mais vulneráveis a ameaças cibernéticas, destacando a necessidade urgente de medidas de segurança robustas para salvaguardar suas operações e preservar sua integridade institucional.

Segundo a Resolução 396/2021 do Conselho Nacional da Justiça, a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) foi instaurada em 7 de junho de 2021, com o objetivo de aprimorar o nível de maturidade em segurança cibernética nos órgãos do Poder Judiciário, abrangendo os aspectos fundamentais da segurança da informação para o aperfeiçoamento necessário à consecução.

A ENSEC-PJ impõe a adesão e o cumprimento de três diretrizes pelos órgãos do Poder Judiciário, à exceção do Supremo Tribunal Federal (STF), de acordo com o Art. 26 da Resolução n. 396/2021, quais sejam: 1. PPINC-PJ (Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário): conjunto de diretrizes para a prevenção a incidentes cibernéticos em seu mais alto nível; 2. PGCC-PJ (Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário): diretrizes para contribuir para a resiliência corporativa por

meio de resposta, tão eficiente quanto possível, a incidentes em que os ativos de informação do Poder Judiciário tenham a sua integridade, confidencialidade ou disponibilidade comprometidos em larga escala ou por longo período; 3. PIINC-PJ (Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário): diretrizes para estabelecer os procedimentos básicos para coleta e preservação de evidências, bem como para comunicar fatos relevantes aos órgãos de investigação e com atribuição para o início da persecução (Conselho Nacional de Justiça, 2021).

Considerando a atual situação de segurança no Poder Judiciário e o potencial impacto de um ataque bem-sucedido nas instituições, este estudo tem como foco analisar as medidas de segurança cibernética adotadas por 26 estados brasileiros e Distrito Federal, a população deste estudo. O objetivo é verificar, por meio de informações confiáveis, se os tribunais estaduais estão em conformidade com as instruções do Conselho Nacional de Justiça (CNJ), especificamente com a Resolução 396/2021.

Segundo Fernandes (2022), à medida que organizações no Brasil abarcam as vantagens da tecnologia para otimizar seus processos, também se tornam alvos potenciais para ameaças cibernéticas. Diante desse contexto, surge a necessidade de analisar e aprimorar as medidas de proteção adotadas dos tribunais do estado para proteger suas operações, dados sensíveis e, por extensão, a confiança pública no sistema de justiça no contexto em que os tribunais estaduais estão em constante ameaça a ataques vindos de *hackers*, que podem trazer vazamentos de informações sensíveis, interrupções de serviços e comprometimento da confiança do público no sistema judiciário (Silva, 2018).

Assim, torna-se relevante avaliar a manutenção da segunda linha de defesa utilizada nos tribunais estaduais brasileiros, visando compreender como essas medidas contribuem para a mitigação das ameaças cibernéticas e o fortalecimento da segurança digital no âmbito judiciário.

Ademais, objetiva-se avaliar a implementação da regulamentação do Conselho Nacional de Justiça (CNJ) nas vinte e seis confederações e o Distrito Federal, com especial atenção à conformidade com a exigência de estabelecimento de um comitê de segurança da informação e gestão de riscos, obrigatória para todos os tribunais, à exceção do Supremo Tribunal Federal (STF). Além disso, busca-se a compreensão da estrutura específica dedicada à segurança da informação em cada tribunal estadual.

A segurança cibernética, enquanto área abrangente e complexa, engloba diversas vertentes que demandam uma abordagem criteriosa e focalizada para uma análise efetiva. Nesse sentido, visando delimitar e concentrar os aspectos mais pertinentes e viáveis no contexto da

pesquisa, optaremos por restringir nossa análise à abordagem das medidas de segurança a partir da segunda linha de defesa. Desta forma, este estudo deve proporcionar informações para aprimorar a postura de cibersegurança dessas instituições em um contexto digital em constante evolução, observando o problema na esfera estadual.

Portanto, em um ambiente onde a confiança pública no sistema de justiça é crucial, a segurança cibernética desempenha um papel vital na proteção dos interesses dos cidadãos e na preservação da integridade do sistema judiciário. Então, a pesquisa proposta é uma etapa importante para fortalecer a segurança digital no âmbito judiciário, garantindo a confiabilidade e a transparência das operações judiciais, o que, por sua vez, contribui para a confiança dos investidores, clientes e partes interessadas na justiça brasileira.

1.1 Problema de pesquisa

Segundo Reina (2022), entre novembro de 2020 e abril de 2022, os tribunais brasileiros sofreram 13 ataques cibernéticos, uma média de um ataque a cada 41 dias, resultando em paralisação dos trabalhos e transtornos significativos para advogados e a população. Esses ataques afetaram cortes federais, criminais, eleitorais, estaduais e do trabalho em várias regiões do país. Essa situação expôs a vulnerabilidade das bases de dados dos tribunais, prejudicando o acesso aos serviços judiciais e causando atrasos em julgamentos e processos judiciais.

A problemática deste estudo está em compreender como os tribunais estaduais do Brasil estão preparados para enfrentar ameaças cibernéticas e proteger suas operações contra invasões análogas de acordo com o que o Conselho Nacional de Justiça regulamenta, a saber:

> Constituir um comitê de governança de segurança da informação (CGSI), ao qual caberá a implementação das ações da ENSEC-PJ; Estabelecer um sistema de Gestão em Segurança da informação baseado em riscos; Elevar o nível de segurança das estruturas críticas; Estabelecer rede de cooperação do judiciário para a segurança cibernética; Estabelecer o modo centralizado de governança cibernética nacional (Conselho Nacional de Justiça, 2021).

Além do mais, conforme a Resolução 396/2021 do CNJ, é necessário estabelecer um engajamento da alta administração de cada tribunal para a consecução das finalidades e das medidas de proteção ao serviço, sobretudo quando implicarem a necessidade de rápida suspensão do acesso público, o ataque cibernético acontecerá. Busca-se evitar os efeitos nocivos desses ataques. Para medir, pode-se desenvolver indicadores que meçam a presença e participação da alta administração em reuniões, workshops e treinamentos relacionados à segurança da informação. Outrossim, realizar avaliações regulares para mensurar o

entendimento e a familiaridade da alta administração com as políticas e práticas de segurança da informação estabelecidas pelo CNJ. Ademais, integrar métricas de engajamento da alta administração nos relatórios de gestão, destacando a importância atribuída à segurança da informação em nível estratégico.

Ao considerar a necessidade da realização de uma avaliação abrangente da estrutura de segurança cibernética existente em cada órgão, a fim de determinar o grau de preparação e resiliência desses tribunais diante de possíveis ameaças cibernéticas, almeja-se, então, compreender a dimensão das medidas de segurança cibernética adotadas pelos tribunais estaduais do Brasil e fornecer informações que possam ajudar a fortalecer a segurança digital no âmbito judiciário. Além disso, a análise da conformidade com as diretrizes do CNJ e a avaliação das estruturas de segurança cibernética em cada tribunal são aspectos fundamentais para mitigar o impacto de futuros ataques cibernéticos e garantir a confiabilidade e a transparência das operações judiciais no país. Nesse contexto, o problema central deste estudo reside na seguinte indagação: Até que ponto os tribunais estaduais brasileiros estão preparados e resilientes diante dos potenciais ameaças cibernéticas, levando em consideração a conformidade com as normativas do CNJ e a eficácia de suas estruturas de segurança?

1.2 Objetivo Geral

Esta investigação visa analisar as estruturas de Tribunais Estaduais para enfrentar riscos de segurança cibernética de acordo com o modelo das três linhas.

1.3 Objetivos Específicos

1. Analisar a conformidade dos tribunais estaduais com as regulamentações do Conselho Nacional de Justiça (CNJ), com especial atenção para a presença ou ausência da segunda linha de defesa nos órgãos judiciários estaduais, no âmbito do setor de Justiça, no contexto da cibersegurança.
2. Realizar uma avaliação aprofundada da extensão da disseminação das atribuições do departamento de segurança cibernética nos órgãos judiciais do setor Judiciário, fundamentada no conceito do Modelo das Três Linhas.

3. Determinar o grau de preparação e resiliência dos tribunais estaduais diante de possíveis ameaças cibernéticas, considerando não apenas a conformidade regulatória, mas também a eficácia das medidas implementadas.
4. Identificar possíveis lacunas na estrutura de segurança cibernética dos tribunais estaduais, propondo recomendações para aprimorar a segurança e mitigar riscos.
5. Contribuir para o avanço do conhecimento sobre a cibersegurança no setor Judiciário, fornecendo engenharias valiosas para futuras iniciativas e políticas no âmbito da segurança da informação.

1.4 Justificativa

De acordo com relatórios relacionados a pesquisa global de ameaças cibernéticas, constatou-se que o Brasil está entre os principais países que mais sofre ataques cibernéticos (Fortinet, 2022). A multinacional de cibersegurança Trend Micro destacou em seu relatório que de janeiro até junho 2023, o Brasil foi o segundo país a mais sofrer ataques cibernéticos providos de *malwares*, dentre eles os *ransomware.*

Levando em consideração essa informação, levantou-se o interesse em saber o motivo do Brasil estar exposto a essa vulnerabilidade cibernética. Com base no exposto, restringimos nosso foco exclusivamente aos tribunais brasileiros, com o intuito de estudar a vulnerabilidade e as estratégias de defesa dos órgãos estaduais.

Com base nos relatórios relativos à pesquisa global de ameaças cibernéticas, evidencia-se que o Brasil figura entre os países mais impactados por ataques dessa natureza (Fortinet, 2022). Segundo a multinacional de cibersegurança *Trend Micro*, em seu relatório referente ao período de janeiro a junho de 2023, o Brasil ocupou a segunda posição no ranking dos países mais atingidos por ataques cibernéticos, notadamente aqueles relacionados a malwares, incluindo os *ransomware.*

Diante dessa constatação, surge o interesse em compreender as razões que tornam o Brasil suscetível a essa vulnerabilidade cibernética. Nesse contexto, direcionamos nosso enfoque de maneira exclusiva para os tribunais brasileiros, almejando investigar tanto a vulnerabilidade quanto as estratégias de defesa adotadas por esses órgãos estaduais. A pesquisa propõe-se a avaliar se os 26 tribunais estaduais e o Distrito Federal, estão adequadamente preparados para enfrentar possíveis incidentes cibernéticos, buscando assim contribuir para a compreensão e mitigação dessa problemática no âmbito da segurança digital. Então, a

investigação foi especificamente orientada para os tribunais estaduais, devido aos impactos substanciais que podem ter no funcionamento da justiça local e nos serviços públicos.

A interrupção ou corrupção dos sistemas de um tribunal estadual podem resultar em consequências graves para a comunidade e o sistema judicial local. Os tribunais estaduais apresentam dados sensíveis e valiosos, como processos judiciais, dados pessoais e informações sobre casos criminais, informações que são usadas para extorsão, chantagem ou até mesmo vendidas no mercado ilegal de informações. Nesse sentido, este estudo se configura como uma contribuição para ampliar a conscientização acerca da relevância da segurança cibernética.

2 REFERENCIAL TEÓRICO

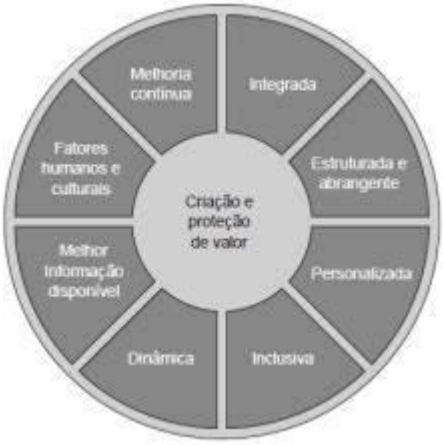
2.1 Gestão de Risco

Risco, conforme definição adotada pela ABNT (2018), consiste no efeito das incertezas sobre os objetivos, sendo este efeito uma variabilidade em relação ao esperado, podendo manifestar-se de maneira positiva, negativa ou ambas. Esses efeitos, por sua vez, podem tanto originar quanto influenciar oportunidades e ameaças, contemplando uma gama diversificada de objetivos que se estendem por diferentes aspectos e categorias, sendo aplicáveis em diversos níveis organizacionais.

A expressão do risco normalmente é articulada em termos de fontes de risco, eventos, potenciais e suas consequências, bem como as probabilidades associadas a esses elementos. O propósito intrínseco ao gerenciamento de riscos é alicerçado na criação e proteção de valor, um impulso que não apenas aprimora o desempenho organizacional, mas também fomenta a inovação, colaborando, assim, para a consecução dos objetivos preconizados.

Os princípios, nesse contexto, constituem a espinha dorsal do gerenciamento de riscos, devendo ser devidamente considerados quando da estruturação e implementação dos processos inerentes a essa gestão no seio da organização. Estes princípios, ao servirem de alicerce, proporcionam à organização as ferramentas necessárias para enfrentar e gerenciar os impactos decorrentes das incertezas sobre seus objetivos (Silva; Neves, 2019).

Figura 1: Princípios de gestão de risco



Fonte: Silva; Neves, 2019.

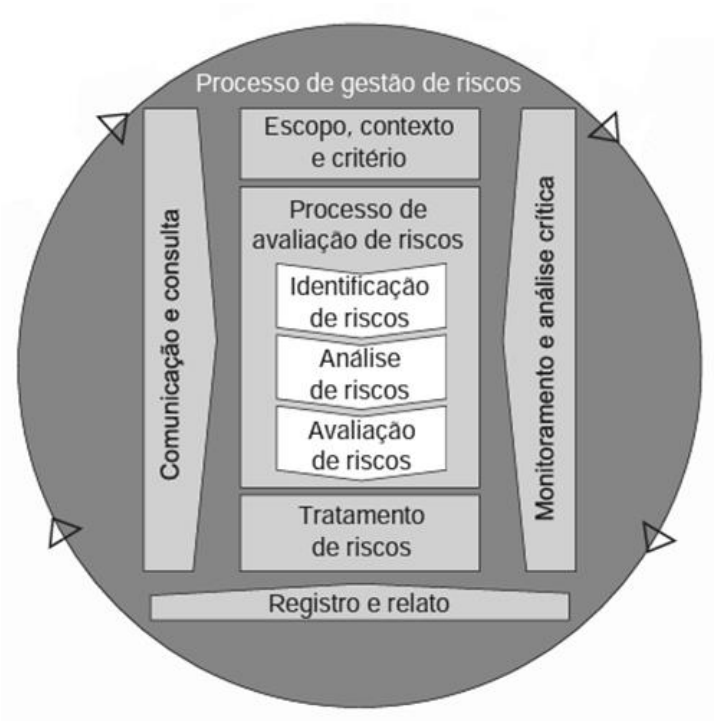
Os princípios da gestão de riscos, definidos pela ISO 31000, preveem: a) Integração; b) Estruturação e Abrangência; c) Personalização; d) Inclusão; e) Dinamicidade; f)

Oferecimento de melhor informação disponível; g) Consideração de fatores humanos e culturais; h) Disposição à melhoria contínua (ABNT, 2018).

Conforme destacado por Pereira (2019), os princípios da gestão de riscos envolvem o reconhecimento da importância de estabelecer estratégias para a mitigação de riscos e a elaboração de um plano de contingência destinado a lidar com imprevistos. Dessa forma, é imperativo realizar periodicamente um novo mapeamento dos riscos, considerando a situação atual da organização, a fim de estar preparado para enfrentar futuras mudanças ou ajustes que possam ocorrer.

Conforme estabelecido pela Norma Brasileira (NBR) ISO 31000 da Associação Brasileira de Normas Técnicas (ABNT) (2018), um planejamento eficiente para o gerenciamento de riscos é subdividido em etapas com foco em escopo, contexto e critério, monitoramento e análise crítica, comunicação e consulta, bem como registro e relato:

Figura 2: Processo de gestão de riscos



Fonte: ABNT, 2018.

A comunicação e consulta fornece apoio às partes interessadas relevantes, ajudando-as a compreender os riscos, a base sobre a qual decisões são tomadas e as razões que justificam a necessidade de ações específicas. A comunicação busca aumentar a

conscientização e o entendimento dos riscos, enquanto a consulta envolve a obtenção de feedbacks e informações para auxiliar na tomada de decisões (Souza, 2018).

É fundamental que haja uma coordenação estreita entre essas atividades para facilitar as trocas de informações, e que estas que sejam baseadas em fatos, oportunas, pertinentes, precisas e de fácil compreensão, levando em consideração a confidencialidade e a integridade e a disponibilidade das informações, bem como o respeito aos direitos de privacidade das pessoas. Deve haver comunicação e consulta com as partes interessadas apropriadas, tanto internas quanto externas, em todas as etapas do processo de gestão de riscos (Bermejo *et al.*, 2019).

A comunicação e a consulta têm como objetivos: reunir diversas áreas de especialização em cada fase do processo de gestão de riscos; garantir que diferentes perspectivas sejam devidamente consideradas na definição de critérios de risco e na avaliação dos riscos; fornecer informações suficientes para facilitar a supervisão dos riscos e a tomada de decisões; promover um sentimento de inclusão e responsabilidade entre as pessoas afetadas pelos riscos (Bermejo *et al.*, 2019).

O objetivo, ao definir o escopo, contexto e critérios, é adaptar o processo de gerenciamento de riscos, possibilitando uma avaliação de riscos eficiente e uma abordagem adequada para o tratamento de riscos. Isso implica em delimitar claramente o âmbito do processo, compreender os fatores contextuais tanto internos quanto externos (ABNT, 2018).

O propósito de definir o escopo, contexto e critérios é personalizar o processo de gestão de riscos, permitindo a realização de uma avaliação de riscos eficaz e a implementação adequada de medidas para lidar com esses riscos. Esses elementos, a saber, o escopo, contexto e critérios, abrangem a determinação do âmbito do processo, compreendendo os ambientes internos e externos da organização.

Ao planejar como abordar a gestão de riscos, consideram-se diversos fatores, conforme indicado por Bermejo et al. (2019). Entre esses elementos estão os objetivos e decisões que precisam ser tomados, os resultados esperados das etapas do processo, questões relacionadas ao tempo, localização e inclusões/exclusões específicas, a escolha das ferramentas e técnicas apropriadas para avaliar os riscos, os recursos necessários, as responsabilidades e a documentação a ser mantida, bem como as relações com outros projetos, processos e atividades. Essa abordagem abrangente visa a promover uma gestão de riscos integral e alinhada aos objetivos organizacionais.

Os contextos externo e interno representam o ambiente no qual a organização busca alcançar seus objetivos. A compreensão aprofundada desse contexto revela-se fundamental,

uma vez que a gestão de riscos se desenvolve intrinsecamente aos objetivos e atividades da organização. Ademais, é crucial reconhecer que fatores internos da organização podem se configurar como fontes de risco, e, nesse cenário, o propósito e o escopo da gestão de riscos mantêm estreita relação com os objetivos globais da organização (ABNT, 2018).

A organização precisa estabelecer os contextos externo e interno do processo de gestão de riscos, levando em consideração os fatores mencionados. A definição de critérios de risco é importante para especificar a quantidade e o tipo de risco que a organização está disposta a assumir em relação aos seus objetivos. Esses critérios também ajudam na avaliação da gravidade dos riscos e na tomada de decisões. Eles devem ser alinhados com a estrutura de gestão de riscos e personalizados de acordo com o propósito e o escopo da atividade em questão (Bermejo *et al.*, 2019, p. 47).

Os critérios de risco devem refletir os valores, objetivos e recursos da organização, bem como estar em conformidade com suas políticas de gestão de riscos e considerar as opiniões das partes interessadas. Esses critérios não são estáticos, e convém que sejam periodicamente revisados e ajustados, conforme necessário, ao longo do processo de avaliação de riscos. Eles devem considerar vários fatores, como a natureza das incertezas que podem afetar os objetivos, a definição das consequências, a probabilidade, o tempo, a consistência e outros elementos relevantes para a gestão de riscos (ABNT, 2018).

Por fim, entende-se que a gestão de riscos cibernéticos, também conhecida como gerenciamento de riscos de segurança cibernética, envolve a identificação, avaliação e mitigação de ameaças e vulnerabilidades relacionadas à segurança da informação. Ela se concentra em proteger sistemas, redes, dados e ativos digitais contra-ataques cibernéticos, garantindo a confidencialidade, integridade e disponibilidade das informações.

2.2 Governança Corporativa

A governança corporativa é o sistema fundamental que orienta a direção, o monitoramento e o estímulo das empresas e outras organizações. Esse sistema engloba os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle, bem como outras partes interessadas (IBGC, 2017, p. 20).

Segundo Ramos e Martinez (2006), a governança corporativa aplica três pilares fundamentais: a transparência que disponibiliza informações para as partes interessadas; a equidade que estabelece a igualdade de tratamento perante todos os envolvidos; e a prestação

de contas que apresenta a responsabilidade dos seus atos apresentada de forma a avaliar o desempenho e a consecução dos objetivos traçados.

Na estrutura da Governança Corporativa, os acionistas compõem a Assembleia Geral dos Acionistas. Interagem com a empresa assim como outros *stakeholders*, como investidores, reguladores do mercado, órgãos governamentais, parceiros de negócios, entre outros. No setor público, a preocupação em promover governança tem foco na prestação de contas para sociedade, dos gastos públicos com efetiva transparência de gestão, cumprimento de metas estabelecidas advindas de demandas sociais, baixo custo da administração pública, qualidade dos serviços públicos e impacto positivo das políticas sobre a sociedade em geral (Borges; Serrão 2005).

A governança pública utiliza ferramentas que promovem transparência e possibilitam a avaliação dos resultados da aplicação de políticas, refletindo o retorno dos impostos arrecadados em bens/serviços de utilidade pública para a sociedade. Embora a definição de governança corporativa seja inicialmente estabelecida para o setor privado, ela é igualmente válida para o setor público e suas organizações. No âmbito do setor público, é essencial reconhecer que os cidadãos desempenham o papel de fornecedores de financiamento para as “empresas” públicas. Sua contribuição, por meio do pagamento de impostos, configura-se como um investimento destinado a assegurar um retorno seguro em termos de serviços públicos de qualidade (Nogueira; Junior, 2013)

A governança corporativa distribui documentos e realiza ações, como políticas e procedimentos da governança corporativa, requisitos de conformidade, metas de desempenho, relatórios e análises financeiras, código de conduta, planos estratégicos, declaração da missão e dos valores, relatório do IBGC de responsabilidade e vigilância, comunicados de boas práticas, organogramas e responsabilidades dos funcionários (IBCG, 2017).

Em síntese, a governança corporativa não é apenas um conjunto de regras e regulamentos, e sim uma abordagem transformadora que impacta a cultura e a estratégia das empresas. Conforme Tarantino (2019), ao adotar práticas de governança sólidas, as organizações não apenas garantem a sustentabilidade de seus negócios, mas também contribuem para a construção de um ambiente empresarial mais ético, transparente e responsável. Dessa forma, a governança corporativa não só estabelece a empresa em si, mas também promove o bem-estar da empresa como um todo.

2.3 Segurança Cibernética

A segurança cibernética pode ser conceitualizada como um desdobramento da disciplina da segurança da informação, orientada para a metodologia da proteção da informação no domínio cibernético. Seu escopo engloba a mitigação do furto e da adulteração de dados (Nunes, 2012).

Para atingir tal objetivo, torna-se importante conceber estratégias inerentes à segurança cibernética, visando à gestão proativa de riscos, identidades e incidentes, propiciando uma pronta e eficaz resposta aos diversos contratempos que podem manifestar-se (Nunes, 2012). Em tempos correntes, à medida em que as tecnologias da informação trilham um curso de crescimento incessante essas informações ganham importância (Laudon; Laudon, 2014).

No ano de 2021, por meio da Resolução n. 396/2021 o Conselho Nacional de Justiça (CNJ) estabeleceu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), com a finalidade de ampliar a capacidade de resistência às ameaças cibernéticas que afetam o âmbito judicial. Neste contexto de pesquisa, é relevante ressaltar as responsabilidades estabelecidas pela ENSEC-PJ para todos os entes que compõem o sistema judiciário, com exceção do Supremo Tribunal Federal. Tais obrigações, delineadas com o intuito de aprimorar a segurança e inclusividade do Judiciário no ambiente digital, bem como fortalecer a resiliência contra ameaças cibernéticas, são enumeradas da seguinte maneira (CNJ, 2021).

Nesse ínterim, as obrigações delineadas pela ENSEC-PJ são tornar o Judiciário mais seguro e inclusivo no ambiente digital e aumentar a resiliência às ameaças cibernéticas. De acordo com o Art. 19 da resolução, compete à alta administração dos órgãos do Poder Judiciário, com exceção do STF, realizar a governança da segurança da informação e especialmente:

> 1) Implementar, no que lhe couber, a Política de Segurança Cibernética do Poder Judiciário; 2) Elaborar a Política de Segurança da Informação e normas internas correlatas ao tema, observadas as normas de segurança da informação editadas pelo CNJ como forma de tornar o Judiciário mais seguro e inclusivo no ambiente digital e aumentar a resiliência às ameaças cibernéticas (CNJ, 2021).

A literatura acadêmica afirma que existe uma trindade sagrada da segurança da informação. Cumpre dizer, antes, que a literatura acadêmica refere-se ao corpo de conhecimento produzido e publicado por acadêmicos, pesquisadores e especialistas em diversas áreas do saber. Ela abrange uma ampla gama de textos, incluindo livros, artigos de revistas científicas, teses, dissertações, conferências e outros materiais escritos que passaram por

revisão por pares e são reconhecidos como fontes confiáveis e relevantes dentro de um campo específico. São três princípios, também chamados de propriedades ou atributos: “Confidencialidade, Integridade e Disponibilidade”, conhecidos pela sigla CID (Costa, 2011). Se um ou mais desses princípios sejam violados em qualquer instância, isso indica a ocorrência de um incidente de segurança da informação. Basicamente, a confidencialidade é o princípio de que a informação não esteja disponível ou seja revelada a indivíduos, entidades ou processos não autorizados; a integridade é o princípio da exatidão e completeza de informação; e a disponibilidade é o princípio da capacidade de estar acessível e utilizável quando demandada por uma entidade autorizada (Awang *et al.,* 2020).

Conforme Boekl e Fagan (2019), a segurança cibernética é realizada por meio da seleção de possíveis controles que devem se basear na avaliação de riscos. Os controles podem variar em natureza de proteger a confidencialidade, integridade ou disponibilidade de informações. Em geral, eles são divididos em vários tipos e alguns deles são:

> CONTROLES FÍSICOS: São barreiras que impedem ou limitam o acesso físico direto às informações ou à infraestrutura que contém as informações. Ex: portas, trancas, paredes, blindagem, vigilantes, geradores, sistemas de câmeras, alarmes, catracas, cadeados, salas-cofre, alarmes de incêndio, crachás de identificação, entre outros.
> CONTROLES LÓGICOS: Também chamados de controles técnicos, são barreiras que impedem ou limitam o acesso à informação por meio do monitoramento e controle de acesso a informações e a sistemas de computação. Ex: senhas, firewalls, listas de controle de acesso, criptografia, biometria, IDS, IPS, entre outros (Boekl; Fagan (2019, p. 32).

Conforme descreve Canongia (2009), a problemática da Segurança Cibernética é uma das principais preocupações das empresas, pois vivemos em um mundo cada vez mais digital e isso acaba por aumentar os riscos para as empresas e seus dados confidenciais. Um dos principais riscos são os *Malwares*, que são programas maliciosos desenvolvidos para interromper, interferir ou acessar os dados de um dispositivo de forma indesejada.

Segundo Canongia (2009), um dos tipos de *Malware* mais comum é o *Ransomwar*e, que bloqueia o acesso a dados de um computador ou sistema atacado, exigindo o pagamento de uma quantia em dinheiro para liberar os dados. Assim, as empresas acabam, muitas vezes, sendo obrigadas a pagar ou correr o risco de que os seus dados sejam inutilizáveis. Para prevenir os danos causados pelos *Ransomwares*, é necessário que as empresas criem políticas de Segurança Cibernética adequadas, como a realização de *backups* frequentes de seus dados em ambientes protegidos, a adoção de soluções de segurança avançadas e a educação de usuários sobre os perigos desses *Malwares*.

Em síntese, a segurança cibernética é uma preocupação crítica em um mundo cada vez mais dependente da tecnologia e interconectado digitalmente (Hosang, 2010). Empresas, organizações governamentais e indivíduos precisam estar constantemente atentos às ameaças cibernéticas e investir em medidas de segurança robustas para proteger suas informações e operações (Lobato; Huriel, 2018). Conforme explicitado acima, a segurança cibernética busca garantir a confidencialidade, integridade e disponibilidade das organizações, bem como a privacidade dos usuários e a funcionalidade contínua dos sistemas, de modo a impedir que organizações parem suas atividades por conta de invasões feitas por criminosos cibernéticos.

2.4 Modelo das Três Linhas

O Modelo de Três Linhas, definido pelo Instituto dos Auditores Internos (IIA), oferece às organizações formas de reconhecer como suas estruturas e processos contribuem para o cumprimento de seus objetivos e possibilitam governança sólida e controle de riscos (IIA, 2020). Esta ferramenta pode ser útil para toda organização e é escalável por meio de:

> Adotar uma abordagem baseada em princípios e adaptar o modelo para atender aos objetivos e circunstâncias organizacionais.
> Focar na contribuição que o gerenciamento de riscos oferece para atingir objetivos e criar valor, bem como questões de "defesa" e proteção de valor.
> Compreender claramente os papéis e responsabilidades representados no modelo e os relacionamentos entre eles.
> Implantar medidas para garantir que as atividades e os objetivos estejam alinhados com os interesses priorizados dos *stakeholders* (IIA, 2020).

Segundo o IIA (2013), no modelo de Três Linhas, a primeira linha de defesa no gerenciamento de riscos é o controle da gerência, sendo a segunda linha de defesa as diversas funções de controle de riscos e supervisão de conformidades estabelecidas pela gerência e como terceira, a avaliação independente. Assim, individualmente, cada uma das três linhas exerce papel importante na estrutura de governança da organização. Ademais, para o IIA (2013), os órgãos de governança e a alta administração têm o dever de prestar contas sobre a determinação dos objetivos da entidade, bem como a definição de métodos estratégicos ao alcance de tais objetivos e o estabelecimento de processos de governança a fim de melhor gerenciamento dos riscos no decurso da efetivação desses objetivos. No modelo de Três Linhas, há diferença nos três grupos compreendidos no gerenciamento eficaz de riscos:

> Funções que gerenciam e têm propriedade sobre riscos;
> Funções que supervisionam riscos;
> Funções que fornecem avaliações independentes (IIA, 2013).

A primeira linha de trabalhadores tem a incumbência de controlar e guiar os processos operacionais (Glynn et al, 2016). O cargo é frequentemente referido como gerência ou gestão de operações, que tem como meta gerenciar, observar, administrar e eliminar riscos nas organizações, prestando atenção efetiva às suas equipes (IIA, 2013).

É essencial enfatizar que, de acordo com Anderson e Eubanks (2015), as tarefas de gerenciamento de risco e controle da linha de frente são responsabilidade do gerente direto, responsável pelas operações cotidianas, assim como das gestões de nível intermédio. Já a segunda linha fornece uma perspectiva de controle, supervisionando a aplicação adequada das estratégias de gerenciamento de riscos definidas para a primeira linha. Isso significa que essa segunda linha agirá como auxiliar para a primeira linha, auxiliando-a na implementação de práticas adequadas de gerenciamento, assegurando que a gestão operacional seja conduzida conforme as diretrizes, mantendo um certo grau de autonomia das três linhas de defesa (IIA, 2013). De acordo com Anderson e Eubanks (2015), funções gerenciais da segunda linha comumente estão associadas à supervisão de controles e perspectivas de risco, frequentemente colaborando com a operação administrativa para criar planos práticos, fornecer conhecimento especial sobre riscos, implementar regras e protocolos, e obter fatos relevantes para ter uma vasta noção da organização no que tange aos riscos e controles.

A Terceira Linha compreende a Auditoria Interna, que é independente e supervisiona as duas anteriores, e informa aos altos administradores da organização (IIA, 2013). A terceira linha trabalha para garantir a eficácia das duas primeiras linhas (BRASIL, 2017).

Figura 3: O Modelo das Três Linhas do IIA

Fonte: IIA, 2020.

Organizações que têm as linhas de defesa tendem a tomar decisões mais esclarecidas com respeito a ameaças. Elas são capazes de perceber e responder com rapidez a riscos, colocar em prática de modo mais eficiente recursos limitados para administrar a insegurança de maneira hierárquica e obter maior transparência de incertezas internos de modo que possam aproveitar informação entre as áreas, não necessitando refazer documentos ou testes complexos. Tais práticas ajudam a excluir surpresas inesperadas e prejuízos, diminuir as despesas de transferência de incertezas e relacionar com maior propensão de que os objetivos da entidade sejam alcançados (Potter; Toburen, 2016)

Incidentes de fraude são manifestantes quando a gestão de riscos não é executada de maneira adequada, particularmente quando existe uma lacuna entre o primeiro e o segundo nível de defesa. Principalmente se a segunda linha é incapaz de detectar riscos e reportar às autoridades administrativas da empresa (Brasiliano, 2015). A credibilidade da organização é ameaçada quando há fraudes e frequentemente há uma realocação repentina de prioridades, particularmente das partes relacionadas aos auditores internos (Araj, 2015).

Para evitar falhas e assegurar a integridade dos processos, as empresas estão adotando uma postura vigilante e proativa diante dos riscos existentes. A utilização das três linhas de defesa emerge como uma estratégia para identificar e gerenciar os riscos relacionados a prejuízos decorrentes de erros e processos ineficazes. Essas linhas desempenham um papel crucial ao mapear e supervisionar as situações de risco ligadas a falhas operativas (Soares, 2020).

Com o propósito de aprimorar a eficácia das estruturas organizacionais e dos processos, foi estabelecido um conjunto de três barreiras de proteção, alinhadas com os princípios da governança corporativa, voltadas para o gerenciamento de riscos e controles internos. Estas linhas de defesa visam fortalecer a abordagem das entidades em relação às falhas, contribuindo para a mitigação eficaz desses eventos. O método foi desenvolvido para possibilitar a supervisão e a vigilância dos principais diretores sobre todos os membros da organização, promovendo, assim, o aperfeiçoamento contínuo de todas as políticas existentes (Coutinho, 2022).

O modelo das três linhas de defesa ajuda a criar uma estrutura clara de responsabilidades e prestação de contas, reduzindo os riscos operacionais, melhorando a governança e a tomada de decisão, o objetivo é enfatizar a colaboração entre as três linhas a fim de garantir uma abordagem eficaz e equilibrada na gestão de riscos e controle em toda a organização (IIA, 2013).

2.5 Caracterizando a 2ª Linha de Defesa

Segundo o Instituto de Auditores Internos (2013), a segunda linha de defesa é uma parte essencial do Modelo das Três Linhas de Defesa, utilizado para descrever a estrutura de gerenciamento de riscos e controle em uma organização. A função da segunda linha consiste em oferecer supervisão, orientação e suporte à primeira linha, assegurando que os riscos sejam gerenciados de maneira eficaz e que os controles internos sejam implementados corretamente.

Embora não seja totalmente autônomo, é primordial a existência de equipes preparadas na segunda linha, já que é esperado um alto nível de objetividade ao disponibilizar informações importantes à administração de nível superior e ao conselho de administração em relação à gestão de risco pelo primeiro time de defesa (Anderson; Eubanks, 2015). Como necessita ter-se uma interação contínua entre direção e auditoria interna, a fim de que a função da terceira linha seja significativa e conforme às necessidades, é então essencial fortalecer a cooperação entre as equipes da primeira, segunda e terceira linha de defesa (IIA, 2020).

Seguindo a orientação do Instituto dos Auditores Internos (2013), a segunda linha de defesa desempenha papéis predominantes em quase todas as entidades, cada um deles possuindo autonomia em relação às atividades da primeira linha, mas sendo de natureza administrativa. Essas funções principais envolvem vigilância, avaliação, execução e controle de riscos por auditores internos.

Esta estrutura de gestão de riscos busca facilitar e verificar a implementação de práticas eficazes de gerenciamento de riscos pelos proprietários de riscos, auxiliando na definição de metas e relatórios adequados de riscos para o negócio (IIA, 2013).

Além disso, a segunda linha de defesa inclui uma função regulatória que monitora riscos específicos, como a conformidade com leis e regulamentos relevantes. Esta função geralmente reporta informações diretamente ao alto escalão e, em alguns segmentos do negócio, diretamente para órgãos de governança. Múltiplas funções regulatórias podem coexistir em uma organização, cada uma com a responsabilidade de controle específico de compliance, abrangendo áreas como segurança, fornecimento, ambiental e qualidade (IIA, 2013). Essas diversas funções trabalham em conjunto para fortalecer a capacidade da organização em lidar efetivamente com os riscos.

Desde a perspectiva da segurança cibernética, a função de gestão de risco está no cerne da segunda linha, contribuindo e monitorizando as operações de segurança, assumindo a responsabilidade da primeira linha (Bevan et al., 2018). Mabwe, Ring e Webb (2017) conduziram uma investigação sobre o Modelo das Três Linhas, chegando à conclusão de que

há indefinição entre o propósito das duas primeiras linhas e que o papel de supervisão da segunda linha sobre a primeira compromete a sua independência, introduzindo discrepâncias entre a teoria e a realidade prática.

No âmbito dos órgãos e entidades da Administração Pública Federal, a estrutura de controles internos necessita seguir o Modelo das Três Linhas, a fim de operar de forma eficaz e organizada (Brasil, 2017). Nesse contexto, a primeira linha de proteção, dependente da segunda linha, conta com funções específicas:

> 1. A responsabilidade da primeira linha é controlar, identificar, mensurar e suprimir os riscos, auxiliando na aplicação e desempenho de procedimentos e diretrizes internos destinados a verificar a finalidade dos objetivos estabelecidos pela organização. 2. Nesta linha de defesa, incluem-se os controles principais, que necessitam ser construídos e conseguidos por gestores responsáveis por realizar tarefas e atividades dentro dos seus pináculos primordiais e apoio. 3. A fim de certificar que os controles internos possuam a adequação e eficácia tendo suas medidas proporcionalizadas aos riscos existentes, estes devem estar ancorados ao plano de gerência, considerando a estrutura, missão, vastidão e especificidades da organização (Brasil, 2017, p. 3).

Seguindo a função orientadora abaixo da primeira linha, são dadas à segunda linha de defesa as seguintes tarefas:

> 1. As tarefas da segunda linha de defesa são estabelecidas a nível da gestão para garantir que as ações realizadas pela primeira linha sejam executadas de forma adequada. 2. A segunda linha de defesa aprova o desenvolvimento dos controles internos da gestão, realizando tarefas de supervisão, monitoramento e avaliação das atividades desempenhadas pela primeira linha, tais como: gerenciamento de riscos, conformidade, verificação de qualidade, fiscalização financeira, orientação e instrução. 3. As Assessorados e Assessorias Especiais de Controle Interno (AECI), nos Ministérios, desempenham essas funções da segunda linha de defesa. Ações coordenadas são adicionadas por outras estruturas previstas pelas organizações (Brasil, 2017, p. 3).

De acordo com Aguiar (2018), a segunda linha de defesa assume a responsabilidade de supervisionar e coordenar as operações da primeira linha, garantindo uma autonomia gerencial nos domínios de risco, embora limitada, uma vez que permanece sob o controle direcional da entidade organizacional. Conforme argumentado por Jamison, Morris e Wilkinson (2018), no contexto da cibersegurança, a equipe responsável pela segunda linha de defesa é encarregada da segurança da informação, incumbindo-lhe a implementação e monitoramento de uma variedade abrangente de controles destinados a detectar atividades maliciosas.

2.6 CISO

Conforme Shayo e Lin (2019), o CISO, acrônimo para Chief Information Security Officer ou, em português, Diretor de Segurança da Informação, assume a responsabilidade de

liderar e gerenciar a estratégia de segurança cibernética em uma organização. Sua atribuição principal é implementar e supervisionar políticas, procedimentos e diretrizes de segurança da informação, assegurando a proteção dos dados e sistemas corporativos contra ameaças cibernéticas. O CISO desempenha um papel crucial na gestão de incidentes de segurança, na avaliação e mitigação de riscos, na conscientização e treinamento dos funcionários em segurança cibernética, além de realizar uma análise constante do panorama de ameaças para garantir a eficácia das medidas de segurança implementadas.

Segundo Karanja e Rosso (2017), o CISO, ou Chief Information Security Officer, tem como principal responsabilidade desenvolver e implementar estratégias que assegurem a integridade, confidencialidade e disponibilidade das informações das organizações. Isso engloba a proteção contra-ataques cibernéticos, a identificação de vulnerabilidades e a adoção de medidas preventivas para minimizar os riscos. A constante atualização sobre as tendências e evoluções no campo de segurança cibernética é essencial, exigindo do profissional um comprometimento contínuo com estudos e informações sobre novas ameaças, técnicas de ataque e soluções de segurança, visando antecipar possíveis ameaças e garantir a proteção da organização.

A presença de um CISO na estrutura organizacional fortalece a cultura de segurança cibernética, desempenhando um papel de liderança ao orientar e educar os colaboradores sobre a importância da segurança da informação. Essa conscientização torna-se fundamental, uma vez que muitos incidentes ocorrem devido a descuidos ou ações mal-intencionadas por parte dos funcionários.

De acordo com Munkvold (2021), o CISO desempenha um papel crucial na elaboração e execução de políticas de segurança cibernética, incluindo a definição de diretrizes para o uso seguro de sistemas, a implementação de controle de acessos, a criptografia de dados sensíveis e a garantia de conformidade com regulamentos, como a Lei Geral de Proteção de Dados (LGPD).

Em suma, o diretor de sistema de informação é essencial na atuação da segunda linha de defesa, pois diante da atualidade a qual há ataques cibernéticos com cada vez mais constância, o CISO é essencial para garantir a proteção das entidades e manter a organização em funcionamento (Sveen, 2021). O CISO é um profissional estratégico que desempenha um papel vital na proteção de dados, na segurança cibernética e na resiliência organizacional, um guardião cibernético que objetiva preservar a confiança dos clientes, manutenção e reputação das empresas e garantir o sucesso contínuo e o funcionamento da organização.

3 METODOLOGIA

Essa pesquisa enquadra-se como aplicada, na perspectiva qualitativa. O processo de coleta de informações fez uso da pesquisa em documentos, e por meio de pedidos de acesso à informação, e os dados analisados através da análise de conteúdo.

Classifica-se como exploratória pois têm como objetivo desenvolver, esclarecer e modificar conceitos e ideias, buscando a formulação de problemas de pesquisa mais específicos para estudos futuros (Gil, 2008).

Para a elaboração deste estudo, foi adotada uma abordagem de natureza qualitativa, com o intuito de compreender profundamente os fenômenos do mundo social, estabelecendo uma conexão estreita entre os indicadores estudados e aquilo que eles indicam, entre as teorias propostas e os dados coletados, e entre o contexto em que ocorrem e as ações observadas (Maneem, 1979). Conforme Magalhães, Pinheiro e Minayo (2009, p. 21), a pesquisa qualitativa baseia-se no "universo dos significados, dos motivos, das aspirações, das crenças, dos valores e das atitudes".

No que diz respeito ao método de coleta de dados, foram realizadas pesquisas documentais no período compreendido entre agosto e outubro de 2023. Os principais documentos utilizados foram organogramas, portarias, resoluções, atas de reuniões e documentos oficiais disponibilizados publicamente nos websites dos respectivos tribunais investigados. Além disso, também foram obtidos dados por meio de solicitações de acesso à informação, utilizando os canais disponibilizados pelas ouvidorias e pelos órgãos oficiais, em conformidade com a Lei n. 12.527, de 18 de novembro de 2011, que estabelece o direito de acesso à informação.

Seguindo a definição de Cellard (2008), a pesquisa documental baseia-se na utilização de documentos, os quais são considerados instrumentos escritos que atestam fatos. Por sua vez, de acordo com Flick (2004), a pesquisa documental é caracterizada quando se configura como a única abordagem qualitativa adotada, sendo utilizada como um método autônomo.

Com o objetivo de se obter a documentação a ser analisada buscou-se os dados nos sítios eletrônicos dos tribunais, utilizando fontes como atas, organogramas e ofícios disponíveis online, porém, após análise dos sites, constatou-se que as informações disponíveis não eram suficientes para atender às demandas da pesquisa.

De forma a se complementar as informações coletadas nos documentos, enviou-se requerimentos de acesso à informação foram submetidos de maneira integralmente eletrônica, por meio de formulários virtuais ou correio eletrônico. Dois conjuntos de informações foram requisitados nas solicitações, ambos relacionados aos comitês encarregados da segurança da informação nos tribunais, identificados por meio de uma análise documental.

Com o pedido de acesso à informação buscou-se confirmar a existência dos comitês, assim como a existência de outros comitês relacionados à segurança da informação no órgão em questão. Além de ter o objetivo de confirmar a situação desses comitês e se eles continuam se reunindo regularmente. As perguntas em questão foram:

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?

5. Onde o Encarregado de Proteção de Dados está lotado?

6. O comitê e/ou o gerente de segurança toma decisões considerando um processo estruturado de gestão de riscos ou de avaliação dos riscos?

7.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?

8.Os riscos ou vulnerabilidades de segurança cibernética são formalmente considerados na priorização das demandas de TI pelo comitê gestor de TI?

9. Existe alguma metodologia para a avaliação da maturidade da segurança da informação? Se sim, qual *framework* utilizam?

10. 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?

11. O tribunal possui equipe de tratamento de incidentes em redes de computador (ETIR) designada e em funcionamento?

Na análise dos dados, foi utilizada a técnica de análise de conteúdo dos documentos governamentais obtidos, relacionando as informações apresentadas nesses documentos com as definições do Modelo das Três Linhas em conjunto com o contexto de segurança cibernética, a

fim de alcançar os objetivos deste estudo. A análise documental como método de tratamento de dados busca facilitar o acesso às informações relevantes para o observador, garantindo a máxima quantidade e pertinência de informação possível (Bardin, 2016, p. 51).

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.

Segundo Gil (2008), as fontes documentais muitas vezes fornecem ao pesquisador dados relevantes e completos, resultando em economia de tempo na pesquisa. Em diversos casos, a investigação social só é possível por meio de documentos. Gil destaca também que registros escritos fornecidos por instituições governamentais, como projetos de lei e relatórios de órgãos governamentais, podem ser valiosos para a pesquisa social. Com base nessas afirmações, definiu-se a metodologia deste estudo.

4 RESULTADOS

Como resultado, o ajuste na estratégia de coleta de dados está alinhado com o objetivo principal da pesquisa, que é analisar se os tribunais estaduais estão em conformidade com as regulamentações do Conselho Nacional de Justiça (CNJ). Para atingir este objetivo, foi preciso obter informações detalhadas sobre o Comitê de Segurança Cibernética e a estrutura de Segurança da Informação em cada tribunal.

Dessa forma, ao adaptar a abordagem de coleta de dados para incluir pedidos de acesso à informação, a pesquisa buscou assegurar a abrangência e a precisão necessárias para avaliar a segunda linha de defesa em relação à estrutura de segurança cibernética de cada tribunal. Esse ajuste reforça o comprometimento em determinar o grau de preparação e resiliência desses tribunais diante de possíveis ameaças cibernéticas, um dos objetivos centrais da pesquisa.

A pesquisa avançou então para a etapa de encaminhamento dessas perguntas aos sites dos tribunais estaduais por meio dos pedidos de acesso à informação. Este método busca obter dados precisos e atualizados diretamente das fontes oficiais, garantindo a confiabilidade e a integridade das informações coletadas.

Ao adotar essa abordagem ajustada, a pesquisa superou as limitações inicialmente identificadas, buscando informações de maneira mais direta e detalhada através da colaboração dos órgãos responsáveis pela segurança cibernética nos tribunais estaduais.

No exercício do direito garantido pela Lei de Acesso à Informação, n. 12.527/2011, foram solicitadas informações específicas aos vinte e sete tribunais estaduais brasileiros. O pedido de acesso à informação atrelado a uma pesquisa documental consiste em uma série de questionamentos relacionados ao seu comitê de segurança da informação e as práticas de segurança cibernética. A segurança da informação e a proteção de dados tornaram-se preocupações fundamentais para as organizações em todo o mundo. Entretanto, em decorrência da ausência de informações sólidas para análise disponibilizadas nos sites dos Tribunais, a análise será feita a partir das informações recebidas. Ao adotar essa abordagem ajustada, a pesquisa busca superar as limitações inicialmente identificadas, buscando informações de maneira mais direta e detalhada através da colaboração dos órgãos responsáveis pela segurança cibernética nos tribunais estaduais.

Assim, nos quadros de 1 a 9 serão expostas as informações e conceitos relacionados às respostas disponibilizadas pelos respectivos Tribunais de Justiça dos Estados e do Distrito Federal, concedidos através dos pedidos de acesso à informação solicitados aos órgãos. Por meio destes, almeja-se contribuir para o debate sobre a importância do acesso à informação no

contexto do poder judiciário, bem como fornecer subsídios para aprimorar as práticas de transparência e a estrutura organizacional do TJDFT, visando ao cumprimento das normativas do CNJ, bem como analisar as práticas de segurança e proteção de dados.

4.1 Tribunais da Região Norte

O Quadro 1 resume os resultados obtidos em relação aos tribunais estaduais da Região Norte do País.

Quadro 1: Resumo dos questionários da Região Norte

		AC	AM	AP	PA	RO	RR	TO
1	Comitê de Segurança da Informação	Sim, criado recentemente, em processo de elaboração do plano de ação.	Sim, reúne-se regularmente.	Sim, reúne-se bimestralmente.	Sim, reúne-se ordinariamente a cada 60 dias.	Sim. Reúne-se bimestralmente	Sim, reúne-se bimestralmente.	Sim, reúne-se trimestralmente.
2	Qualificações e experiências dos membros	Multidisciplinar	Profissionais formados na área de Segurança da Informação e Proteção de Dados, com certificações internacionais na área e experiência no mercado.	Representantes da Administração do Tribunal, Corregedoria, Secretarias de Sistemas e Infraestrutura, e Coordenadoria de Segurança da Informação.	A maioria dos membros possui experiência gerencial, com exceção do Secretário de Informática e do CISO, que têm experiência direta em Segurança da Informação.	Comitê multidisciplinar.	Dentre outros com experiência gerencial, há o Secretário de Tecnologia da Informação e o Analista de Sistemas Especialista em Segurança da Informação.	Dentre outros com experiência gerencial, há a Diretora de Tecnologia da Informação.
3	Gerente de segurança e alocação	Designado e alocado na Gerência de Segurança. da Informação.	Não, existe uma Assessoria de Segurança da Informação e Proteção de Dados lotada na SETIC.	Sim, alocado na Secretaria de Estrutura de Tecnologia da Informação.	Sim, alocado na Secretaria de Informática.	Não existe.	Não existe	Não existe este cargo específico, mas há a Divisão de Administração e Segurança de Redes.
4/5	Encarregado de Proteção de Dados e alocação	Sim, o comitê conta com especialista e representante da e Encarregado de Proteção de Dados.	Sim, mas não foi especificado.	Sim, lotado na Secretaria de Gestão de Sistemas.	Sim, gerenciado por um comitê composto por Desembargador, Juiz Auxiliar, representante da Secretaria de Administração e da Secretaria de Informática.	Não existe.	Não existe	Sim, conta com um Comitê Multidisciplinar.

6	Tomada de decisão e Gestão de Riscos	Os procedimentos estão sendo reavaliados para atender à gestão e avaliação dos riscos.	O Encarregado está lotado na Presidência, e usam como referência a ISO 27005 e ISO 31000.	O comitê de segurança da informação toma decisões considerando um processo estruturado de gestão de riscos ou avaliação dos riscos.	Processo estruturado de gestão de riscos.	O comitê toma decisões considerando o processo de gestão de riscos	O comitê toma decisões considerando o processo de gestão de riscos.	Há um processo de tomada de decisões considerando o processo de Gestão de Riscos, o Plano de Gestão de Riscos e Plano de Continuidade de Negócio e Serviços de TIC, disponíveis online.
7	Comunicação com *stakeholders*	Utilização de comunicações internas para manter a alta administração informada.	A alta administração recebe atualizações sobre segurança a partir do acompanhamento dos Projetos de Segurança.	Relatórios e reuniões.	Atas das reuniões do Comitê de Segurança da Informação são publicadas no Portal Institucional.	Atas, reuniões, e-mails, cartilhas, campanhas de conscientização.	Realização de campanhas de conscientização e elaboração de cartilhas de orientação para Magistrados, Servidores e Estagiários.	Atas das reuniões do comitê são encaminhadas internamente e são realizadas campanhas de conscientização e divulgação de instruções.
8	Priorização de riscos pelo TI	Formalização e tratamento imediato de vulnerabilidades; mapeamento no Plano de Gestão de Risco e Plano de Contratações de TIC.	São demandas prioritárias	São demandas prioritárias.	São demandas prioritárias.	São demandas prioritárias.	Demandas priorizadas com base em riscos e vulnerabilidades identificados.	Sim, conforme Plano de Gestão de Riscos de TIC e Plano de Gestão da Continuidade do Negócio e Serviços de TIC, disponíveis online.
9	Metodologia de Avaliação/*Framework*	Em andamento.	Adota *frameworks*, orientações e *checklists* definidos na Resolução CNJ 396/2021.	Utilizam a Resolução CNJ 396/2021 e Portaria 162/2021 como metodologia.	Em andamento.	Não informado	Em andamento.	Não informado

10	Conformidade com a CNJ 396/2021 e CNJ 162/2022	Em adesão.	Não informado	O tribunal avalia seu nível de aderência como "maturidade média".	Por meio de questionários fornecidos pelo CNJ.	Não informado	Em adesão.	Não informado
11	Equipe de Tratamento de Incidentes	Em implementação.	Não informado	NÃO INFORMADO.	Comitê de Crise Cibernética.	Não informado	Em implementação.	Não informado

Fonte: Elaborado pelo autor, 2023.

De acordo com as informações fornecidas, o Tribunal Estadual do Amazonas possui um Comitê de Segurança da Informação formalmente designado que se reúne regularmente, presencialmente ou por videoconferência. Seus profissionais com formação acadêmica na área de Segurança da Informação e Proteção de Dados, certificações internacionais e vasta experiência no mercado. Informaram que as decisões quanto à segurança são baseadas na Gestão de Riscos, seguindo as normas ISO 27.005 e ISO 31000. Utilizam *frameworks*, orientações e *checklists* definidos na CNJ 396/2021, porém não foram especificados. Apesar da ausência de informações específicas, pode-se perceber que o tribunal apresenta um nível alto de aderência à Resolução CNJ 396/2021 e aos controles previstos na Portaria CNJ 162/2022.

O Tribunal Estadual do Pará, de acordo com sua Resolução 016/2022, tem implementado um Comitê de Governança de Segurança da Informação responsável por supervisionar as práticas de segurança cibernética. Parte significativa dos seus membros possui experiência em atividades gerenciais, e apenas o Secretário de Informática e o CISO possuem experiência direta na área de Segurança da Informação. Além disso, possui um Encarregado de Proteção de Dados (DPO) e um Comitê de Proteção de Dados. Apesar disso, não detalham a metodologia específica usada para avaliar a maturidade da segurança da informação do tribunal, mas informam que estão avaliando *frameworks* para utilização. Assim, percebe-se que o tribunal tem implementado medidas e conta com pessoal capacitado, e preocupa-se com a proteção dos dados e integridade das operações no ambiente digital, apresentando um nível alto de aderência à Resolução CNJ 396/2021 e aos controles previstos na Portaria CNJ 162/2022.

O Tribunal de Justiça do Estado do Acre criou recentemente um comitê de segurança da informação, estabelecido portaria 2997/2023 de 25 de agosto de 2023. Até o momento, o comitê não realizou reuniões, pois seu plano de ação de segurança da informação está em elaboração. Ainda assim possui pessoal capacitado na área, contando com Gerente de Segurança da Informação e Encarregado de Proteção de Dados. O tribunal está em processo de implementação de uma metodologia/*framework* e estão realizando estudos para adotar uma abordagem apropriada com base no mapeamento de riscos e vulnerabilidades do Plano de Gestão de Risco. Assim, considera-se que o tribunal está iniciando sua adesão à Resolução CNJ 396/2021 e à Portaria CNJ 162/2022.

O Tribunal Estadual de Roraima estabeleceu, recentemente, um comitê de segurança da informação, e está no processo de elaboração de um Plano de Ação de Segurança da Informação por parte do Comitê de Segurança da Informação, que conta, em sua equipe, com um Secretário de TI e um Analista de Sistemas especialista em TI. Assim, embora não esteja em adesão à Resolução CNJ 396/2021 e aos controles previstos na Portaria CNJ

162/2022, está em processo de implementação, indicando uma trajetória de fortalecimento da postura de segurança cibernética da instituição.

As informações referentes ao Tribunal Estadual do Amapá foram fornecidas pela Secretaria de Estrutura de Tecnologia da Informação, mantém um comitê de segurança da informação formalmente designado. A avaliação da maturidade da segurança da informação é realizada com base na Resolução CNJ 396/2021 e na Portaria 162/2021, e mostra o compromisso do tribunal com a conformidade regulatória. A classificação de "maturidade média" sugere que o tribunal está ciente dos desafios que enfrenta e está trabalhando para melhorar sua postura de segurança.

O Tribunal de Justiça do Estado do Tocantins possui uma estrutura formal para abordar questões relacionadas à segurança da informação e proteção de dados determinada pela Resolução nº 22, de 16 de outubro de 2014, e pela Portaria 2755/2023 - PRESIDÊNCIA/ASPRE, de 13 de novembro de 2023. Apesar de adotar medidas específicas em relação à proteção de dados e possuir um Comitê Gestor de Proteção de Dados Pessoais e divulgar *online* seus Planos de Risco e Gestão de TI, não foi informada a sua aderência às metodologias de avaliação, *frameworks* ou sobre o processo de adesão às Resolução CNJ 396/2021 e à Portaria 162/2021, impossibilitando assim uma avaliação quanto à aderência.

O Tribunal de Justiça do Estado do Rondônia possui uma estrutura formal para abordar questões relacionadas à segurança da informação e proteção de dados que se reúne bimestralmente. O tribunal apresenta um comitê multidisciplinar, o comitê toma decisões considerando o processo de gestão de riscos e em relação a comunicação com os *stakeholders* o tribunal faz uso de atas, reuniões, e-mails, cartilhas e campanhas de conscientização. O tribunal não tem em sua estrutura um gerente de segurança e nem um encarregado de proteção de dados. Informações sobre a metodologia de avaliação/ *framework* , conformidade com a resolução CNJ 396/2021 e CNJ 162/2022 e equipe de tratamento de incidentes não foram informadas pelo tribunal

4.2 Tribunais da Região Centro-Oeste

Quadro 2: Resumo dos questionários da Região Centro-Oeste

		DF	GO	MT	MS
1	Comitê de Segurança da Informação	Sim, reúne-se mensalmente.	Sim, reúne-se a cada 45 dias.	Sim, reúne-se trimestralmente.	Sim, reúne-se semestralmente.
2	Qualificações e experiências dos membros	Membros da TI possuem mestrado e doutorado em segurança da informação.	Membros com experiência gerencial e o um membro da Diretoria de Tecnologia da Informação da Presidência e uma Diretora da Diretoria de Ciência de Dados e Estatística.	Membros com experiência gerencial e coordenadores de tecnologia.	Membros com experiência gerencial, assessora de inteligência, diretora de secretaria de segurança da informação, coordenador de segurança cibernética e um assessor de segurança da informação.
3	Gerente de segurança e alocação	Sim, alocado no Gabinete da Presidência.	Não existe	Não existe	Não informado
4/5	Encarregado de Proteção de Dados e alocação	Sim, alocado no Gabinete da Presidência.	Sim, alocado na Unidade de Atendimento aos Usuários de Sistemas.	Sim, alocado na Coordenadoria Judiciária.	Não informado
6	Tomada de decisão e Gestão de Riscos	Decisões baseadas em um processo de gestão e avaliação de riscos.	As decisões são tomadas com base na avaliação de riscos de TIC.	As decisões são baseadas em um processo de gestão de riscos.	Sim, porém não especificado.
7	Comunicação com *stakeholders*	Através da comunicação social, porém não especificada a forma.	Informações enviadas via e-mail, internamente.	Através de reuniões trimestrais e comunicação online.	Sim, porém não especificado.
8	Priorização de riscos pelo TI	São demandas prioritárias.	São demandas prioritárias solicitadas a partir de processos administrativos de incidentes de segurança formalizados.	São demandas prioritárias.	A partir de homologação do relatório de análise de risco as demandas são enviadas para tratamento.
9	Metodologia de Avaliação/*Framework*	CIS Controls v8.	NÃO INFORMADO.	NIST, CIS Controls e ISO 27001.	CIS Controls v8.

10	Conformidade com a CNJ 396/2021 e CNJ 162/2022	Alta aderência, detalhes disponíveis no site do TJDFT.	Seguem as diretrizes estabelecidas.	A conformidade às diretrizes é realizada por meio de avaliação interna e por consultoria da empresa Gartner.	Em andamento.
11	Equipe de Tratamento de Incidentes	Equipe designada e em funcionamento.	Não há.	Possui uma equipe desde 2021.	Sim.

Fonte: Elaborado pelo autor, 2023.

O Tribunal Estadual do Goiás possui um comitê formalmente designado para tratar de questões de segurança da informação, e é composto por diversos membros, incluindo juízes auxiliares, membros da presidência, diretores de tecnologia e recursos humanos, e profissionais de ciência de dados e estatística. Além disso, possui um servidor designado como encarregado de proteção de dados, o que é um requisito importante para cumprir com as regulamentações de proteção de dados. Não há uma metodologia formal para avaliar a maturidade da segurança da informação, nem uma equipe designada para tratamento de incidentes em redes de computador. O tribunal avalia seu nível de aderência à resolução CNJ 396/2021 e à portaria CNJ 162/2021 por meio de avaliações e questionamentos da Governança de TIC e da Controladoria Interna. Em resumo, apesar de demonstrar esforços para abordar a segurança da informação, existem áreas que podem ser aprimoradas, como a nomeação de um gerente de segurança da informação e a criação de uma equipe de tratamento de incidentes em redes de computador.

Por sua vez, o Tribunal Estadual do Mato Grosso demonstra compromisso com a proteção dos dados e sistemas da sua organização. Tem o Comitê Gestor de Segurança Cibernética e da Informação, criado pela Portaria 157/2023, e utiliza-se de metodologias reconhecidas, como NIST, CIS Control e ISO 27001, para avaliar a maturidade da segurança da informação. Isso proporciona uma abordagem estruturada e ampla para avaliar e melhorar a segurança. O tribunal avalia seu nível de aderência à Resolução CNJ 396/2021 e aos controles previstos na Portaria CNJ 162/2021 por meio de avaliação de conformidade interna, com o apoio da consultoria Gartner, o que garante o cumprimento das regulamentações do CNJ.

O Tribunal Estadual do Mato Grosso do Sul conta com um comitê de segurança da informação e possui um servidor designado como gerente de segurança da informação. Além disso, contam com comitê e o gerente de segurança que, além das decisões e ações prioritária de TI, mantém os *stakeholders* informados acerca dos ocorridos. Apesar do seu nível de aderência à resolução CNJ 396/2021 e aos controles previstos na portaria CNJ n. 162/2021 estar em adesão, utilizam-se do CIS Controls v8 como metodologia para avaliação de maturidade da segurança, e a presença de um comitê e de uma equipe de tratamento de incidentes reforçam a importância da segurança cibernética no funcionamento do tribunal.

É importante destacar que o TJDFT possui um Comitê de Segurança da Informação formalmente designado e os membros da equipe possuem mestrado e doutorado em segurança da informação, demonstrando um alto nível de expertise no campo. No que diz respeito à gestão de segurança. Uma das práticas adotadas pelo TJDFT é a tomada de decisões baseada em um processo estruturado de gestão de riscos e avaliação de riscos. Além disso, a comunicação eficaz

com os *stakeholders* e a alta administração é garantida por meio do assessoramento da área de comunicação social. O tribunal utiliza a metodologia CIS Controls v8 (Centro de Segurança da Internet) para avaliar a maturidade da segurança da informação, e possuem alta aderência à Resolução CNJ 396/2021 e aos controles previstos na portaria CNJ 162/2021.

4.3 Tribunais da Região Sudeste

Quadro 3: Resumo dos questionários da Região Sudeste

		ES	MG	SP	RJ
1	Comitê de Segurança da Informação	Não possui.	Sim, reúne-se bimestralmente	Sim, reúne-se semestralmente	Sim, reúnem-se mensalmente.
2	Qualificações e experiências dos membros	Não existe	Multidisciplinar	Multidisciplinar	O comitê tem uma composição multidisciplinar porém não divulgada.
3	Gerente de segurança e alocação	Sim, STI.	Não existe	Não existe	Não há um gerente designado.
4/5	Encarregado de Proteção de Dados e alocação	Não possui.	Não existe	Não existe	Sim, alocado na Presidência.
6	Tomada de decisão e Gestão de Riscos	Considera formalmente os riscos, porém não há especificação.	Considera formalmente os riscos, porém não há especificação	Considera formalmente os riscos, porém não há especificação	As decisões são tomadas com base em relatórios mensais apresentados nas reuniões do comitê.
7	Comunicação com *stakeholders*	E-mails, informações disponíveis no site, cartilhas	Relatórios regulares, campanhas de conscientização	E-mails, informações disponíveis no site, cartilhas	Através de Programa de Conscientização e Comunicação online.
8	Priorização de riscos pelo TI	São demandas prioritárias.	Sim, faz parte das atribuições do Comitê Gestor de Tecnologia da Informação e Comunicação (CGTIC).	São demandas prioritárias	São demandas prioritárias
9	Metodologia de Avaliação/*Framework*	Não informado	Não informado	Não informado	Sim, o tribunal utiliza metodologias como NIST, CIS Control e ISO 27001.
10	Conformidade com a CNJ 396/2021 e CNJ 162/2022	Baixa aderência.	Não informado	Não informado	O tribunal mantém um programa de melhoria contínua para garantir a aderência contínua aos normativos do CNJ.

11	Equipe de Tratamento de Incidentes	Não informado	Não informado	Não informado	Sim, possui uma equipe designada e em funcionamento.

Fonte: Elaborado pelo autor, 2023.

O Tribunal Estadual do Rio de Janeiro possui um Comitê de Segurança da Informação formalmente designado pela Resolução TJ/OE n.º 28/2022, que busca uma revisão contínua das práticas de segurança, além do Comitê Gestor de Proteção de Dados Pessoais. Além disso, possui um programa de conscientização e comunicação com páginas específicas no site do tribunal, dedicadas à segurança da informação e à Lei Geral de Proteção de Dados (LGPD), e utiliza *frameworks* como NIST (Instituto Nacional de Padrões e Tecnologia dos Estados Unidos), CIS Controls e ISO 27001. O tribunal também mantém um programa de melhoria contínua para garantir a aderência aos normativos do CNJ, como a Resolução CNJ 396/2021 e a Portaria CNJ 162/2022. Essas medidas garantem não apenas a conformidade com regulamentos, mas também a confiança da sociedade e a integridade do sistema judiciário do estado.

Quanto ao Tribunal Regional do Espírito Santo, pode-se considerar, de acordo com as informações recebidas, que este enfrenta um cenário desafiador em termos de segurança da informação, uma vez que não dispõe de um comitê formalmente designado para tratar dessas questões complexas. Esta ausência reflete diretamente na capacidade de avaliar a qualificação e experiência dos envolvidos, e o responsável de segurança lotado na Secretaria de Tecnologia da Informação não possui caráter gerencial. Isso indica uma lacuna na estrutura organizacional, uma vez que a abrangência do cargo é mais operacional do que tática ou estratégica. Ainda mais, a inexistência, até o momento, de um servidor designado como Encarregado de Proteção de Dados prejudica a conformidade com as demandas. Assim, no contexto normativo, observa-se uma baixa aderência à Resolução CNJ 396/2021 e aos controles estabelecidos pela Portaria CNJ 162/2022. Esta discrepância sugere uma necessidade de alinhamento com as diretrizes regulatórias estabelecidas.

Quanto ao Tribunal Estadual de São Paulo, possui um comitê de segurança cibernética que se reúne semestralmente, o comitê é multidisciplinar. Não existe um gerente de segurança e alocação e nem um encarregado de proteção de dados. Em relação a tomada de decisão o tribunal considera os riscos e a comunicação com *stakeholders* é feita através de e-mails, informações disponíveis no site e cartilhas. O tribunal prioriza a gestão de riscos pelo TI, porém não especifica a metodologia de avaliação/ *framework* e nem a conformidade com o CNJ

396/2021 e CNJ 162/2022. A equipe de tratamento de incidentes também não é especificada pelo tribunal.

O Tribunal Estadual de Minas Gerais, possui um comitê de segurança da informação que se reúne bimestralmente, o comitê é multidisciplinar. Não existe um gerente de segurança e alocação e nem um encarregado de proteção de dados. Em relação a tomada de decisão o tribunal considera os riscos e a comunicação com *stakeholders* é feita através de e-mails, informações disponíveis no site e cartilhas e e-mails. O tribunal prioriza a gestão de riscos pelo TI, porém não especifica a metodologia de avaliação/ *framework* e nem a conformidade com o CNJ 396/2021 e CNJ 162/2022. A equipe de tratamento de incidentes também não é especificada pelo tribunal.

4.4 Tribunais da Região Sul

Quadro 4: Resumo dos questionários da Região Sul

		PR	SC	RS
1	Comitê de Segurança da Informação	Sim, reúne-se mensalmente.	Sim, reúne-se mensalmente.	Sim, reúnem-se conforme necessidade.
2	Qualificações e experiências dos membros	Encarregado de Proteção de Dados, Núcleo de Inteligência e Segurança Institucional, Núcleo de Governança, Riscos e Compliance, e Departamento de Tecnologia da Informação e Comunicação.	Membros altamente qualificados em segurança cibernética, TI, gestão de riscos.	Não informado
3	Gerente de segurança e alocação	Sim, alocado na Divisão de Gestão de Segurança de TIC.	Sim, alocado na área de Tecnologia da Informação.	Sim, alocado na Corregedoria Geral de Justiça.
4/5	Encarregado de Proteção de Dados e alocação	Sim, alocado em Unidade Especial.	Sim, alocado na área de Compliance, Encarregado de Proteção de Dados.	Não informado
6	Tomada de decisão e Gestão de Riscos	Adoção de processos similares aos da Gartner.	Decisões baseadas em processo contínuo de gestão e avaliação de riscos.	Considera os riscos em sua tomada de decisões.
7	Comunicação com *stakeholders*	Há um comitê responsável em manter as partes interessadas informadas.	Divulgação de relatórios periódicos, apresentações em reuniões de diretoria e	De responsabilidade da Direção de Comunicação.

			comunicações diretas.	
8	Priorização de riscos pelo TI	Consideração formal dos riscos e vulnerabilidades.	Formalmente considerados na priorização das demandas de TI.	Formalmente priorizados nas demandas de TI, conforme Ordem de Serviço.
9	Metodologia de Avaliação/*Framework*	Realizada anualmente, seguindo o CIS Controls v8 *framework*.	Baseada no ISO 27001.	Realizada nacionalmente pelo iGovTIC-JUD, além de medições anuais por meio dos ITKeyMetrics do Gartner.
10	Conformidade com a CNJ 396/2021 e CNJ 162/2022	Plano de implementação de longo prazo.	Realiza avaliações regularmente.	Avaliação realizada pelo CNJ e auditoria interna.
11	Equipe de Tratamento de Incidentes	Em implementação.	Sim, possui equipe designada.	Sim, possui equipe designada.

Fonte: Elaborado pelo autor, 2023.

O Tribunal Regional do Paraná possui um Comitê de Governança de Segurança da Informação respaldado pela atual Política de Segurança da Informação (PSI) e regulamentado pelo Decreto 560/2022 P-GP. Além disso, possui um Núcleo de Inteligência e Segurança Institucional, o Núcleo de Governança, Riscos e *Compliance*, e o Departamento de Tecnologia da Informação e Comunicação. Dentro desse contexto, a gestão de segurança da informação é liderada pelo Gestor de Segurança da Informação. Possui também um encarregado de Proteção de Dados, destacando o comprometimento com a conformidade legal. O Comitê e o Gestor de Segurança da Informação adotam um processo estruturado de gestão de riscos, incorporando análises de riscos utilizadas por empresas de renome, como a Gartner. A avaliação da maturidade da segurança da informação é conduzida anualmente, seguindo o CIS Controls v8 *Security Framework*, em parceria com um parceiro tecnológico. A aderência à Resolução CNJ 396/2021 e aos controles da Portaria CNJ 162/2022 é considerado um compromisso de longo prazo. Um plano de ação já está em execução para a implantação desses controles.

No que diz respeito ao Tribunal de Justiça de Santa Catarina, a segurança da informação é uma preocupação fundamental, e a instituição implementou diversas medidas e estruturas especializadas para garantir sua prática. O TJSC conta com um Comitê de Segurança da Informação formalmente designado, e também um Gerente de Segurança da Informação e um Encarregado de Proteção de Dados. O tribunal adota uma metodologia estruturada para avaliação da maturidade da segurança da informação, baseada no renomado *framework* ISO 27001. Essa abordagem oferece uma estrutura sólida para avaliar e melhorar continuamente as práticas de segurança. Finalmente, o TJSC realiza avaliações regulares de aderência à

Resolução CNJ 396/2021 e à Portaria CNJ 162/2022, garantindo que a instituição esteja em conformidade com as regulamentações mais recentes.

Em resposta às perguntas apresentadas, o Tribunal de Justiça do Rio Grande do Sul informou possuir um Comitê de Segurança da Informação formalmente designado, conforme estabelecido no Ato 37/2018-P. Porém o tribunal não possui um servidor designado como Gerente de Segurança da Informação, mas mantém a Seção de Segurança da Informação, que está subordinada à Direção de Tecnologia da Informação e Comunicação. Essa estrutura indica uma abordagem centralizada para lidar com questões de segurança da informação. Além disso, o tribunal tem um Encarregado de Proteção de Dados, o que demonstra compromisso com a Lei Geral de Proteção de Dados (LGPD). Quanto à avaliação da maturidade da segurança da informação, o tribunal utiliza o iGovTIC-JUD (Índice de Governança, Gestão e Infraestrutura de Tecnologia da Informação e Comunicação do Poder Judiciário)e os ITKeyMetrics do Gartner (*framework*), bem como indicadores estratégicos do PDTIC (Plano Diretor de Tecnologia da Informação e Comunicação). Por fim, o tribunal acompanha sua aderência à resolução CNJ 396/2021 e aos controles previstos na portaria CNJ 162/2022 através de processos de acompanhamento realizados pelo CNJ e pela auditoria interna do TJRS, contando com uma estrutura organizacional bem definida, práticas de gestão de riscos, e conformidade com regulamentações relevantes.

4.5 Tribunais da Região Nordeste

Quadro 5: Resumo dos questionários da Região Nordeste

		AL	BA	CE	MA	PB	PE	PI	RN	SE
1	Comitê de Segurança da Informação	Sim, porém as reuniões não foram informadas.	Sim, as reuniões não foram informadas	Sim, reúne-se bimestralmente	Sim, reúne-se bimestralmente.	Sim, reúne-se semestralmente.	Sim, reúne-se bimestralmente.	Sim. A informação é tratada como sigilosa, devido a riscos de segurança cibernética.	Sim, reúne-se bimestralmente	Sim, mas não foi informado de quanto em quanto tempo se reúne
2	Qualificações e experiências dos membros	Multidisciplinar	Multidisciplinar	Multidisciplinar	Equipe multidisciplinar; qualificações e experiências em construção.	Além de membros com qualificações multidisciplinares, assessora de inteligência, diretor de auditoria interna, diretor de secretaria de segurança da informação, coordenador de segurança cibernética e um assessor de segurança da informação.	Multidisciplinar	A informação é tratada como sigilosa, devido a riscos de segurança cibernética.	Multidisciplinar	Multidis-ciplinar
3	Gerente de segurança e alocação	Não informado	Não existe	Não informado	Em criação	Sim, alocado na Coordenadoria	Não existe	Sim. A informação é	Não informado	Não existe

						de Segurança Cibernética.		tratada como sigilosa, devido a riscos de segurança cibernética.		
4/5	Encarregado de Proteção de Dados e alocação	Não informado	Não informado	Não informado	O ouvidor atua como Encarregado de Proteção de Dados, alocado na vice-presidência.	Não informado	Não existe	Sim.	Não informado	Não existe
6	Tomada de decisão e Gestão de Riscos	Seguem processo de gestão de riscos	Seguem processo de gestão de riscos	Não informado	Decisões fundamentadas em processo de gestão de riscos.	Seguem processo de gestão de riscos.	Seguem processo de gestão de riscos. Não especificado.	A informação é tratada como sigilosa, devido a riscos de segurança cibernética.	Seguem processo de gestão de riscos	Seguem processo de gestão de riscos
7	Comunicação com *stakeholders*	Comunicados via sítio eletrônico, e-mail e sistemas de informação	Comunicados via sítio eletrônico, e-mail e sistemas de informação	Comunicados via sítio eletrônico, e-mail e sistemas de informação	Comunicados via sítio eletrônico, e-mail e sistemas de informação.	Confirmaram a comunicação, porém não especificaram.	Comunicados via sítio eletrônico, e-mail e sistemas de informação.	A informação é tratada como sigilosa, devido a riscos de segurança cibernética.	Comunicados via sítio eletrônico, e-mail e sistemas de informação.	Comunicados via sítio eletrônico, e-mail e sistemas de informação

8	Priorização de riscos pelo TI	Sim, o CGSI terá a atribuição de priorizar ações e gerenciar riscos de segurança.	São demandas prioritárias	São demandas prioritárias.	Riscos e vulnerabilidades considerados formalmente na priorização de demandas.	Riscos e vulnerabilidades considerados formalmente na priorização de demandas	São demandas prioritárias	São demandas prioritárias	São demandas prioritárias	São demandas prioritárias
9	Metodologia de Avaliação/*Framework*	Não informado	Não informado	Não informado	CIS Controls v8 e NIST; diretrizes das Resoluções do CNJ e orientações da NBRs 27000.	Metodologia CIS Controls v8.	Não informado	A informação é tratada como sigilosa, devido a riscos de segurança cibernética.	Não informado	Não informado
10	Conformidade com a CNJ 396/2021 e CNJ 162/2022	Não informado	Não informado	Não informado	Nível de aderência satisfatório; resultados aprimorados no iGovTIC-JUD (2021-2026).	Em processo de implementação.	Não informado	A informação é tratada como sigilosa, devido a riscos de segurança cibernética.	Não informado	Não informado
11	Equipe de Tratamento de Incidentes	Não informado	Não informado	Não informado	Sim, designada e operante.	Sim, o designada e em funcionamento.	Não informado	A informação é tratada como sigilosa, devido a riscos de segurança	Não informado	Não informado

								cibernética.		

Fonte: Elaborado pelo autor, 2023.

O Tribunal de Justiça do Estado de Alagoas alterou recentemente suas políticas de proteção de dados baseando-se em considerações legais, destacando a Lei Federal nº. 13.709, de 14 de agosto de 2018, que trata da Proteção de Dados Pessoais, e a Resolução CNJ 363/2021, que estabeleceu medidas para a adequação à Lei Geral de Proteção de Dados Pessoais pelos Tribunais, instituindo assim a Estratégia de Segurança da Informação e Cibernética do Poder Judiciário de Alagoas. Demais informações, porém, não foram disponibilizadas pelo tribunal, impossibilitando uma análise mais detalhada.

No Tribunal de Justiça do Maranhão a segurança da informação é tratada com seriedade, refletida pela presença do Comitê de Gestão de Segurança da Informação (CGSI). Este comitê reúne-se bimestralmente, proporcionando uma abordagem regular e sistemática para a avaliação contínua de questões relacionadas à segurança. O tribunal adota uma postura proativa na conformidade com normas de proteção de dados, e as decisões relacionadas à segurança da informação no comitê, assim como na gestão de riscos, são fundamentadas em processos estruturados. A metodologia utilizada para a avaliação da maturidade da segurança da informação é baseada nos *frameworks* CIS Controls v8 e NIST, além de seguir as diretrizes das Resoluções do CNJ e as orientações das NBRs da família 27000 como referências balizadoras para seu Sistema de Gestão de Segurança da Informação. Quanto à conformidade com a Resolução CNJ n. 396/2021 e à Portaria CNJ n. 162/2021, mantém um nível de aderência satisfatório, conforme atestado pelos resultados aprimorados no iGovTIC-JUD (2021-2026).

Um da transparência e governança de dados do Tribunal Estadual da Paraíba é o Comitê Executivo de Proteção de Dados Pessoais, que proporciona a base necessária para a tomada de decisões informadas relacionadas à segurança cibernética da organização. A presença de um gerente de segurança da informação e de um Encarregado de Proteção de Dados demonstra a importância dada à proteção de dados pessoais e à segurança da informação. Além disso, o tribunal possui uma metodologia para avaliação da maturidade da segurança da informação pela metodologia CIS Controls v8, aderindo aos padrões e *frameworks* recomendados. O TJPB avalia seu nível de aderência à Resolução CNJ 396/2021 e aos controles previstos na Portaria CNJ n. 162/2021. Sua estrutura organizacional e práticas refletem um empenho em atender aos padrões regulatórios e garantir a proteção dos dados pessoais.

A segurança da informação é de extrema importância em qualquer organização, especialmente em ambientes governamentais onde dados sensíveis são manipulados. Ao analisar as respostas fornecidas por um determinado Tribunal a perguntas específicas relacionadas à segurança da informação, fica evidente a preocupação com a confidencialidade e a proteção de informações críticas.

O Tribunal Estadual do Piauí, por sua vez, confirma a existência de um comitê de segurança da informação, porém, devido a preocupações com segurança cibernética, a frequência de suas reuniões não é divulgada. Da mesma forma, as qualificações e experiências dos membros desse comitê são consideradas informações sigilosas, destacando a necessidade de profissionais altamente qualificados e experientes na gestão da segurança da informação.

Um aspecto notável é a designação de um Encarregado de Proteção de Dados, conforme a Portaria n. 3735/2023, embora a localização deste Encarregado também seja mantida em sigilo. A comunicação com *stakeholders*, incluindo a alta administração e a sociedade, é fundamental em questões de segurança cibernética. No entanto, os detalhes sobre como o comitê mantém esses grupos informados não foram revelados por razões de segurança. Os riscos e vulnerabilidades de segurança cibernética são formalmente considerados na priorização das demandas de TI pelo comitê gestor de TI, demonstrando a integração da segurança da informação em todos os aspectos da tecnologia da informação. No que diz respeito à avaliação da maturidade da segurança da informação, o Tribunal adota uma metodologia, embora os detalhes específicos e o *framework* utilizado não tenham sido divulgados também por razões de segurança.

O Tribunal Estadual da Bahia, por sua vez, confirma a existência de um comitê de segurança da informação, porém o período em que o tribunal se reúne não foi informado. As qualificações e experiências dos membros são consideradas de forma multidisciplinar. O Tribunal não apresenta um encarregado de proteção de dados, assim como, também não apresenta um gerente de segurança e alocação. A tomada de decisão e gestão de riscos são consideradas pelo tribunal e a comunicação com os *stakeholders* é realizada através de comunicados, e-mails e sistemas de informação. O tribunal prioriza os riscos pela TI, porém não informa a metodologia de avaliação/ *framework*.

O Tribunal Estadual do Rio Grande do Norte, por sua vez, confirma a existência de um comitê de segurança cibernética e ele se reúne bimestralmente. As qualificações e experiências dos membros são consideradas de forma multidisciplinar. No tribunal não existe um gerente de segurança e nem um encarregado de proteção de dados, mas seguem o processo de gestão de riscos. A comunicação com os *stakeholders* é feita através de comunicados via sítio eletrônico, e-mails. O tribunal prioriza demandas relacionadas aos riscos pela TI, porém não informa a metodologia de avaliação/*framework* e nem informações sobre a equipe de tratamento e incidentes.

O Tribunal Estadual de Sergipe, por sua vez, confirma a existência de um comitê de segurança da informação, mas não especifica de quanto em quanto tempo se reúne. As

qualificações e experiências dos membros são consideradas de forma multidisciplinar. No tribunal não existe um gerente de segurança e nem um encarregado de proteção de dados, mas seguem o processo de gestão de riscos. A comunicação com os *stakeholders* é feita através de comunicados via sítio eletrônico, e-mails. O tribunal prioriza demandas relacionadas aos riscos pela TI, porém não informa a metodologia de avaliação/*framework* e nem informações sobre a equipe de tratamento e incidentes.

O Tribunal Estadual do Ceará, por sua vez, confirma a existência de um comitê de segurança da informação, que se reúne bimestralmente. As qualificações e experiências dos membros são consideradas de forma multidisciplinar. No tribunal não existe um gerente de segurança e nem um encarregado de proteção de dados, mas seguem o processo de gestão de riscos. A comunicação com os *stakeholders* é feita através de comunicados via sítio eletrônico, e-mails. O tribunal prioriza demandas relacionadas aos riscos pela TI, porém não informa a metodologia de avaliação/*framework* e nem informações sobre a equipe de tratamento e incidentes.

O Tribunal Estadual de Pernambuco, por sua vez, confirma a existência de um comitê de segurança da informação, que se reúne bimestralmente. As qualificações e experiências dos membros são consideradas de forma multidisciplinar. No tribunal não existe um gerente de segurança e nem um encarregado de proteção de dados, mas seguem o processo de gestão de riscos. A comunicação com os *stakeholders* é feita através de comunicados via sítio eletrônico, e-mails. O tribunal prioriza demandas relacionadas aos riscos pela TI, porém não informa a metodologia de avaliação/*framework* e nem informações sobre a equipe de tratamento e incidentes.

4.6 Indicador de respostas

No âmbito de uma análise abrangente sobre a Lei de Acesso à Informação nos Tribunais Estaduais do Brasil, foi realizado um processo de solicitação de acesso à informação em setembro de 2023. O objetivo foi avaliar a prontidão e transparência dessas instituições em compartilhar informações cruciais dentro dos prazos estabelecidos pela legislação.

Quadro 6: 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	11/10/2023	Sim
Alagoas	1	15/09/2023	06/11/2023	Não
Amapá	0	15/09/2023	16/10/2023	Sim

Amazonas	1	15/09/2023	03/11/2023	Não
Bahia	6	15/09/2023	SEM RESPOSTA	Não
Ceará	4	15/09/2023	SEM RESPOSTA	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
Mato Grosso do Sul	3	15/09/2023	16/10/2023	Sim
Minas Gerais	7	15/09/2023	SEM RESPOSTA	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 RESPOSTA	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 RESPOSTA	Não
Rio Grande do Sul	0	15/09/2023	16/10/2023	Sim
Rondônia	4	15/09/2023	SEM RESPOSTA	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 RESPOSTA	Não
Sergipe	4	15/09/2023	SEM RESPOSTA	Não
Tocantins	4	15/09/2023	23/11/2023	Não

Fonte: Elaborado pelo autor, 2023.

No dia 15 de setembro de 2023, deu-se início o processo de solicitação de acesso à informação em relação à segurança da informação nos tribunais de 26 estados brasileiros e o Distrito Federal. O objetivo era obter informações relevantes sobre como essas instituições estão estruturadas nesses aspectos, considerando a importância desses temas no cenário atual.

Conforme estabelecido pela Lei nº 12.527/2011, definiu-se um prazo de 20 a 40 dias para que os tribunais fornecessem as respostas necessárias. O intuito era avaliar a transparência e prontidão dessas instituições em compartilhar informações relacionadas à segurança da informação.

Os resultados das solicitações indicaram diferentes cenários, e esses resultados levantam importantes considerações sobre a transparência e prontidão dos tribunais em abordar questões críticas de segurança da informação. A análise detalhada dessas respostas, ou da falta delas, será essencial para avaliar o compromisso dessas instituições com a segurança da informação e a transparência no fornecimento de informações solicitadas dentro dos prazos estabelecidos por lei.

Em dezembro de 2023, foram realizadas apurações nos sites dos oito tribunais que não responderam a pesquisa em tempo hábil, são eles: Bahia, Ceará, Minas Gerais, Pernambuco Rio Grande do Norte, Rondônia, São Paulo e Sergipe. Porém só foram alcançadas respostas para questões sobre a existência do comitê de segurança cibernética, de quanto tempo ele se reúne, qualificações e experiências dos membros do comitê, tomada de decisão e gestão de riscos, comunicação com os *stakeholders*, priorização de riscos pela TI. As demais perguntas só são passíveis de informação enviando o pedido de acesso à informação para os tribunais em questão pois são questões específicas.

5 ANÁLISE E DISCUSSÕES

Neste capítulo, apresentamos os desdobramentos dos dados coletados de vinte e sete cortes do sistema judiciário brasileiro, obtidos tanto por meio de seus portais oficiais quanto por canais de comunicação abertos pela Lei de Acesso à Informação. A análise de conteúdo teve como objetivo destacar a estrutura das cortes sob a perspectiva da segurança da informação, examinando como essas estruturas operam e contextualizando-as conforme o Modelo das Três Linhas do IIA.

É relevante destacar que alguns tribunais enfrentam desafios na atualização de seus organogramas e sites, o que dificulta a obtenção de informações claras, atualizadas e precisas no momento desejado. Além disso, observamos que, em determinados casos, como nos tribunais do Amapá e do Mato Grosso do Sul, houve falta de resposta a algumas perguntas. No caso do Mato Grosso do Sul, a omissão na resposta à pergunta sete, que questionava como o comitê de segurança da informação mantém os *stakeholders* ou a alta administração informados sobre segurança cibernética, levanta dúvidas sobre a transparência ou possíveis problemas no órgão em relação a esse tema.

No tribunal do Amapá, as respostas foram breves, não permitindo um entendimento adequado da solicitação de acesso à informação. Além disso, as respostas levantaram suspeitas quanto à veracidade da resposta à pergunta 10, que indagava como o tribunal avalia seu nível de aderência à Resolução CNJ n. 396/2021 (ENSEC-PJ) e aos controles previstos na Portaria CNJ n. 162/2021. A resposta indicando uma maturidade média entra em contradição com as informações anteriores fornecidas. O tribunal estadual do Piauí, por exemplo, alegou que as perguntas do pedido de acesso à informação são perguntas sigilosas que não compete a terceiros saber uma vez que pode deixar o tribunal em risco. Porém, não há sentido nesse o argumento, pois as perguntas eram simples e tinham o objetivo saber se o tribunal possuía um comitê de segurança da informação e estudar a estrutura do órgão em relação a segurança da informação, que de modo algum colocaria o tribunal em risco.

Uma problemática identificada neste estudo refere-se à falta de disponibilidade de organogramas e informações relacionadas à existência e atividades do comitê de segurança cibernética em certos tribunais estaduais. Como medida corretiva, foi necessário criar um formulário para formalizar pedidos de acesso à informação, seguido de uma espera pela resposta da entidade em questão. Importante destacar que, de acordo com a Lei nº 12.527/2011, o órgão é obrigado a responder dentro de um prazo estipulado, variando entre 30 e 40 dias, sendo vedada a recusa desse pedido. Entretanto, alguns órgãos demonstraram despreocupação ao não

responder dentro do prazo estabelecido, desrespeitando a legislação que regula o direito ao acesso a informações públicas.

Embora em alguns casos a presença da segunda linha de defesa e do comitê de segurança cibernética seja claramente delineada nos organogramas, identificamos situações em que a existência dessas estruturas não estava explicitamente indicada. Nesse contexto, o formulário utilizado para solicitar acesso à informação desempenhou um papel crucial em esclarecer tais ambiguidades.

Por fim, é notório que o processo burocrático subjacente ao pedido de acesso à informação constituiu um entrave à condução deste estudo, introduzindo complexidades que impactaram negativamente a transparência e a participação cidadã.

Assim, de maneira a facilitar a visualização das informações, segue abaixo uma tabela resumo com todos os estados que enviaram as informações solicitadas, bem como com as informações que puderam ser reunidas nos sites dos tribunais. Vale ressaltar que até o momento, mesmo com as orientações da Lei de Acesso à Informação, os tribunais dos estados do Rio Grande do Norte, Sergipe, Bahia, Ceará, Pernambuco, Minas Gerais e São Paulo não enviaram respostas ao questionário, portanto não constam na tabela resumo.

Quadro 7: Tabela resumo dos questionários recebidos

		AC	AL	AM	AP	DF	ES	GO	MA	MS	MT	PA	PB	PI	PR	RS	RJ	RR	SC	TO
1	Comitê de Segurança da Informação	SIM	SIM	SIM	SIM	SIM	NÃO	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM
2	Qualificações e experiências dos membros	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM
3	Gerente de segurança e alocação	SIM	NÃO	NÃO	SIM	SIM	SIM	NÃO	NÃO	NÃO	NÃO	SIM	NÃO	SIM	SIM	SIM	NÃO	NÃO	SIM	NÃO
4/5	Encarregado de Proteção de Dados	SIM	-	SIM	SIM	SIM	NÃO	SIM	SIM	-	SIM	SIM	-	SIM	SIM	-	SIM	NÃO	SIM	SIM
6	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
7	Comunicação com *stakeholders*	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	NÃO	SIM	SIM	SIM	SIM	SIM	SIM
8	Priorização de riscos pelo TI	SIM	SIM	-	SIM	SIM	-	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM
9	Metodologia de Avaliação/*Framework*	NÃO	NÃO	SIM	SIM	SIM	NÃO	-	SIM	SIM	SIM	NÃO	SIM	-	SIM	SIM	SIM	NÃO	SIM	-
10	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	-
11	Equipe de Tratamento de Incidentes	NÃO	-	-	-	SIM	NÃO	NÃO	SIM	SIM	SIM	SIM	SIM	NÃO	-	SIM	SIM	NÃO	SIM	NÃO

Fonte: Elaborado pelo autor, 2023.

Quadro 8: Tabela resumo dos questionários não recebidos

		BA	CE	MG	PE	RN	RO	SE	SP
1	Comitê de Segurança da Informação	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM
2	Qualificações e experiências dos membros	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM
3	Gerente de segurança e alocação	-	-	-	-	-	-	-	NÃO
4/5	Encarregado de Proteção de Dados	-	-	-	-	-	-	-	NÃO
6	Tomada de decisão e Gestão de Riscos	SIM	NÃO	SIM	SIM	SIM	NÃO	SIM	SIM
7	Comunicação com *stakeholders*	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM
8	Priorização de riscos pelo TI	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM
9	Metodologia de Avaliação/*Framework*	-	-	-	-	-	-	-	-
10	Conformidade com a CNJ 396/2021 e CNJ 162/2022	-	-	-	-	-	-	-	-
11	Equipe de Tratamento de Incidentes	-	-	-	-	-	-	-	-

Fonte: Elaborado pelo autor, 2023

CONCLUSÃO

Com base nas informações fornecidas sobre os tribunais estaduais em relação à segurança da informação, pode-se observar que há uma variedade de abordagens e práticas em vigor. Alguns tribunais possuem comitês de segurança da informação formalmente designados, enquanto outros ainda estão em processo de criação ou não têm essa estrutura específica. A frequência das reuniões desses comitês também varia, indo desde encontros mensais até reuniões semestrais ou conforme a necessidade.

Quanto às qualificações e experiências dos membros desses comitês, há uma diversidade significativa. Alguns tribunais enfatizam a experiência gerencial, enquanto outros buscam membros com experiências diversas em áreas como inteligência, auditoria interna e segurança da informação. A presença de um Gerente de Segurança da Informação e Encarregado de Proteção de Dados é comum em muitos tribunais, mas suas atribuições e funções podem variar.

Os tribunais demonstram utilizar processos estruturados de gestão de riscos ou avaliação de riscos, refletindo um comprometimento com a segurança da informação. Alguns adotam metodologias específicas, como o *framework* ISO 27001, CIS Controls v8 ou referências como ISO 27.005 e ISO 31000.

A avaliação da conformidade com a Resolução CNJ n. 396/2021 e aos controles da Portaria CNJ n. 162/2021 revela que alguns tribunais estão empenhados em atingir altos níveis de aderência, enquanto outros têm uma aderência mais baixa.

Quanto à existência de uma Equipe de Tratamento de Incidentes em Redes de Computador (ETIR), a presença é afirmativa em alguns tribunais, enquanto outros estão em processo de implementação ou não especificam claramente a existência dessa equipe.

Em resumo, a análise das práticas de segurança da informação nos tribunais estaduais indica uma variedade de abordagens e níveis de maturidade, refletindo a complexidade e diversidade dessas instituições no Brasil. A atenção à conformidade com regulamentações e a implementação de processos estruturados indicam uma preocupação crescente com a segurança cibernética no âmbito judiciário.

REFERÊNCIAS

ABNT NBR ISO 31000:2018. Gestão de riscos - **Princípios e diretrizes**. Rio de Janeiro: ABNT, 2018.

Aguiar, A. S. **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, D. et al. **Gestão de riscos no setor público: revisão bibliométrica e proposta de agenda de pesquisa**. Revista do Serviço Público (RSP), 72(4), 824-854, 2021.

Anderson, D. J.; EUBANKS, G. **Leveraging COSO Across the Three Lines of Defense**. Committee of Sponsoring Organizations of the Treadway Commission, 2015.

Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27001**. Tecnologia da informação: técnicas de segurança: sistemas de gestão da segurança da informação: requisitos. Rio de Janeiro, 2018.

Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27002**. Tecnologia da informação: técnicas de segurança: código de prática para controles de segurança da informação. Rio de Janeiro, 2013.

Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27035-3**. Tecnologia da informação: Gestão de incidentes de segurança da informação, parte 3: diretrizes para operações de resposta a incidentes de TIC. Rio de Janeiro, 2013.

Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27037**. Tecnologia da informação: técnicas de segurança: diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Rio de Janeiro, 2021.

Awang, N. et al. Identification of Information Security Threats Using Data Mining Approach in Campus Network. **Journal of Physics**: Conference Series, n. 1551, v. 1, p. 12, 2020. DOI: https://doi.org/10.1088/1742-6596/1551/1/01, 2006.

Bardin, L. **Análise de Conteúdo**. São Paulo, Almedina Brasil, 2016.

Bermejo, P. H. de; Sant'ana, T. D.; Salgado, E. G. et al. **ForRisco**: **gerenciamento de riscos em instituições públicas na prática**. São Paulo: FDSMPRESS, 2016.

Bevan, O. *et al*. **Cybersecurity and the risk function**. McKinsey&Company, 2018.

Borges, L. F. X.; Serrão, C. F. **Aspectos de Governança Corporativa Moderna no Brasil**. 2005.

Brasil. **Decreto de 15 de dezembro de 2017**. Aprova a Estratégia Nacional de Inteligência. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/dsn/Dsn14503.htm. Acesso em: 22 jun. 2023.

Canongia, C.; Mandarino Junior, R. Segurança cibernética: o desafio da nova sociedade de informação. Revista da SEF. Gestão de riscos. **Revista da SEF**, 1(1), 10-18, 2018. Disponível em: http://biblioteca.ijsn.es.gov.br/Record/18438. Acesso em: 24 jun. 2023.

Cellard, A. **A pesquisa qualitativa: enfoques epistemológicos e metodológicos**. Petrópolis, RJ, 2008.

Chauk, C.; Galvão, A. **Parcerias Estratégicas**. Brasília, v. 14, n. 29, dezembro de 2009.

Conselho Nacional de Justiça. **Três em cada quatro tribunais já se integraram à plataforma** digital. Disponível em: https://www.cnj.jus.br/tres-em-cada-quatro-tribunais-ja-se-integraram-a-plataforma-digital/. Acesso em: 15 ago. 2023.

Fernandes, M. P. **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: 4 nov. 2023.

Flick, U. **Uma Introdução à Pesquisa Qualitativa**. Porto Alegre, Bookman, 2004.

Fortinet. **Brasil sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos em 2021**. 2022. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021. Acesso em: 4 out. 2023.

Gil, A. C. **Métodos e Técnicas de Pesquisa Social**. São Paulo, Atlas S.A., 2008.

Glynn, C. *et al*. **Internal Audit and the Second Line of Defense**. 2016.

Hosang, A. **Política Nacional de Segurança Cibernética:** uma necessidade para o Brasil. Caepe, 2010.

Instituto Brasileiro de Governança Corporativa. **Governança Corporativa**. 2017. Disponível em: https://www.ibgc.org.br/conhecimento/governanca-corporativa. Acesso em: 11 nov. 2023.

Instituto dos Auditores Internos. **Declaração de Posicionamento do IIA:** As três linhas de defesa no gerenciamento eficaz de riscos e controles. São Paulo, 2013.

Instituto dos Auditores Internos. **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: 10 out. 2022.

Jamison, J.; Morris, L.; Wilkinson, C. **The Future of Cybersecurity in Internal Audit**. Internal Audit Foundation, 2018.

Karanja, E.; Rosso, M. A. **The Chief Information Security Officer:** An Exploratory Study. North Carolina Central University, 2017.

Laudon, K. C.; Laudon, J. P. **Sistemas de informação gerenciais**. México, Pearson Education, 2014.

Lobato; Huriel. **Uma Estratégia para a Governança da Segurança Cibernética no Brasil**, Instituto Iguarapé, 2028.

Maamen, J. V. Reclaiming qualitative methods for organizational research: a preface. **Administrative Science Quarterly**, 1979, p. 520-526. Disponível em: https://www.jstor.org/stable/2392358. Acesso em: 7 abr. 2023.

Mabwe, K.; Ring, P.; Webb, R. Operational risk and the three lines of defense in UK financial institutions: is three really the magic number? **Journal of Operational** Risk. 2017. Disponível em: https://researchonline.gcu.ac.uk/ws/portalfiles/portal/24077798/Submitted_version.pdf. Acesso em: 01. Dez 2023.

Magalhães, I. L.; Pinheiro, W. B.; Minayo, M. **Pesquisa Social:** teoria, método e criatividade. Rio de Janeiro, Vozes, 2009.

Nunes, P. V. **A definição de uma estratégia nacional de cibersegurança:** cibersegurança. Lisboa, 2012.

Pereira, M. R. **O Gerenciamento de Riscos Empresariais como Forma de Agregar Valor às Organizações.** Rio de Janeiro: Universidade Federal do Rio de Janeiro, Instituto de Economia, 2014.

Potter, P.; Toburen, M. **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.

Ramos, G. M.; Martinez, A. L. **Governança Corporativa**. Fundação Visconde de Cairu - FVC, Universidade Federal da Bahia - UFBA, Brasil.

Reina. E. C. **Em 18 meses, hackers violaram sistemas de tribunais no Brasil a cada 41 dias**. 2022. Disponível em: https://www.conjur.com.br/2022-abr-15/onda-invasoes-hackers-estruturas-tecnologicas-tribunais/. Acesso em: 12 jun. 2023.

Shayo, C.; Lin, F. 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, M. R. C. **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, SP, 2018.

Sociedade da Informação. Parc. Estrat. Brasília, v. 14, n. 19, p. 21-46, jul-dez 2009. Disponível em: https://cdi.mecon.gob.ar/bases/doc/parceriasest/29.pdf#page=23. Acesso em: 22 abr. 2023.

Tarantino, A. **Governance, risk, and compliance handbook**: technology, finance, environmental, and international guidance, and best practices. John Wiley & Sons, 2008.

Tribunal Regional Federal da 1ª Região. **Segurança da Informação é prioridade no Plano de Contratações de Soluções de TI 2022 do TRF1**. Tribunal Regional Federal da 1ª Região, 25 nov. 2021. Disponível em: https://portal.trf1.jus.br/. Acesso em: 05 dez. 2022.

Tribunal Superior do Trabalho. **Justiça do Trabalho**, s.d. Disponível em: https://www.tst.jus.br/web/gestaoestrategica/processos-conceitos. Acesso em: 09 dez. 2022.

Tribunal Superior do Trabalho. **Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC)**. Brasília, 2020.

Rezende, Mauricio Vianna de. **Avaliação de segurança cibernética no desenvolvimento de software embarcado automotivo**: uma abordagem ontológica. 2020. Tese (Doutorado em Sistemas de Informação e Gestão do Conhecimento) - Universidade FUMEC, Faculdade de Ciências Empresariais - FACE, Belo Horizonte.

ANEXOS

Levantamento dos questionários de cada estado

Tribunal de Justiça do Distrito Federal e Territórios

ASPECTO DE SEGURANÇA CIBERNÉTICA	PRÁTICAS DO TJDF
Comitê de Segurança da Informação	Designado formalmente, reuniões mensais, composto por especialistas multidisciplinares em diversas áreas.
Expertise em Segurança da Informação	Membros da equipe de TI possuem mestrado e doutorado em segurança da informação.
Gestão de Segurança	Gerente de Segurança da Informação designado, localizado no Gabinete da Presidência.
Encarregado de Proteção de Dados	Presidente do Comitê de Segurança da Informação assume o papel, também localizado no Gabinete da Presidência.
Gestão de Riscos	Tomada de decisões baseada em um processo estruturado de gestão de riscos e avaliação de riscos.
Comunicação Eficaz	Comunicação eficaz com *stakeholders* e alta administração garantida por meio do assessoramento da área de comunicação social.
Priorização de TI	Reconhecimento dos riscos e vulnerabilidades de segurança cibernética na priorização das demandas de TI.
Metodologia de Avaliação	Utilização da metodologia CIS Controls v8 para avaliar a maturidade da segurança da informação.
Conformidade com Resoluções	Alta aderência à Resolução CNJ n. 396/2021 (ENSEC-PJ) e à Portaria CNJ n. 162/2021. Detalhes de implementação disponíveis no site do TJDFT.
Equipe de Tratamento de Incidentes	Equipe de Tratamento de Incidentes em Redes de Computador (ETIR) devidamente designada e em funcionamento.

Fonte: Elaborado pelo autor, 2023.

Tribunal Estadual do Amapá

ASPECTOS DE SEGURANÇA CIBERNÉTICA	PRÁTICAS DO TJAP
Comitê de Segurança da Informação	Existe um comitê de segurança da informação formalmente designado que se reúne bimestralmente.
Expertise em segurança da informação	O comitê é formado por representantes da Administração do Tribunal, Corregedoria, Secretarias de Sistemas e Infraestrutura, e Coordenadoria de Segurança da Informação.
Gestão de segurança	Sim, há um gerente de segurança da informação alocado na Secretaria de Estrutura de Tecnologia da Informação.
Encarregado de Proteção de Dados	O Encarregado de Proteção de Dados está lotado na Secretaria de Gestão de Sistemas.
Gestão de Riscos	O comitê de segurança da informação toma decisões considerando um processo estruturado de gestão de riscos ou avaliação dos riscos.
Comunicação eficaz	Os *stakeholders* são mantidos informados por meio de relatórios e reuniões.
Priorização de TI	Os riscos e vulnerabilidades de segurança cibernética são formalmente considerados na priorização das demandas de TI pelo comitê gestor de TI.

Metodologia de avaliação	Utilização da Resolução CNJ 396/2021 e Portaria 162/2021 e seus anexos como metodologia para avaliação da maturidade da segurança da informação.
Conformidade com resoluções	O tribunal avalia seu nível de aderência como "maturidade média".
Equipe de tratamento de incidentes	Não informado

Fonte: Elaborado pelo autor, 2023.

Quadro 8: Tribunal Estadual do Rio Grande do Sul

ASPECTOS DA SEGURANÇA CIBERNÉTICA	**PRÁTICAS DO TJRS**
Existência de um comitê de segurança de informações formalmente designado e frequência das reuniões	Sim, conforme Ato 37/2018-P. As reuniões são realizadas conforme necessidade e convocação do Presidente do comitê.
Qualificações e experiências dos membros do comitê de segurança da informação	Não há um gerente de segurança da informação. Em vez disso, existe a Seção de Segurança da Informação, subordinada à Direção de Tecnologia da Informação e Comunicação.
Existência de um gerente de segurança da informação e sua alocação	O Encarregado de Proteção de Dados está lotado na Corregedoria Geral de Justiça.
Tomada de decisões considerando gestão de riscos ou avaliação de riscos	A Seção de Segurança da Informação, assim como a Direção de Tecnologia da Informação e Comunicação, considera os riscos em sua tomada de decisões.
Comunicação com os *stakeholders* sobre segurança cibernética	A comunicação com os *stakeholders* é coordenada pela Direção de Comunicação do TJRS.
Consideração de riscos e vulnerabilidades na priorização das demandas de TI	Sim, os riscos e vulnerabilidades de segurança cibernética são formalmente considerados na priorização das demandas de TI, conforme a Ordem de Serviço 005/2023-DITIC.
Metodologia para avaliação da maturidade da segurança da informação e *framework* utilizado	A avaliação da maturidade da segurança da informação é realizada nacionalmente pelo iGovTIC-JUD, que inclui a dimensão "Riscos, Segurança da Informação e Proteção de Dados". Além disso, há medições anuais por meio dos ITKeyMetrics do Gartner, mapeados em indicadores estratégicos do PDTIC.
Avaliação do nível de aderência à Resolução CNJ n. 396/2021	A avaliação é realizada pelo CNJ e também por meio de auditoria interna do TJRS
Equipe de tratamento de incidentes em redes de computador (ETIR)	Sim, o tribunal possui uma equipe de tratamento de incidentes em redes de computadores designada e em funcionamento, conforme a Ordem de Serviço 001/2023-DITIC.

Fonte: Elaborado pelo autor, 2023.

Quadro 9: Tribunal Estadual do Mato Grosso do Sul

ASPECTOS DE SEGURANÇA CIBERNÉTICA	**PRÁTICAS DO TJMS**
Qualificações e experiências dos membros do comitê de segurança da informação	Sim, semestralmente ou quando há necessidade.
Existência de um servidor designado como gerente de segurança da informação e alocação	Um juiz auxiliar da presidência, uma diretora geral da secretaria, uma assessora de inteligência, diretora de auditoria interna, diretora de secretaria de gestão de pessoas, diretora de secretaria de magistratura, diretora de secretaria de segurança da informação, coordenador de segurança cibernética e um assessor de segurança da informação.

Alocação do Encarregado de Proteção de Dados	Sim. Coordenadoria de segurança cibernética
Tomada de decisões considerando um processo estruturado de gestão de riscos ou avaliação dos riscos	Sim
Comunicação com os *stakeholders* sobre segurança cibernética	Sim (Mas nada informado pelo tribunal)
Consideração de riscos e vulnerabilidades na priorização das demandas de TI	Sim, a partir de homologação do relatório de análise de risco, a assessoria da informação abre as demandas de TIC para o tratamento
Metodologia para avaliação da maturidade da segurança da informação	Sim, CIS Controls v8
Avaliação do nível de aderência à Resolução CNJ n. 396/2021	Em implantação
Equipe de tratamento de incidentes em redes de computador (ETIR)	Sim, política de gerenciamento de incidentes cibernéticos

Fonte: Elaborado pelo autor, 2023.

Quadro 10: Tribunal Estadual do Goiás

ASPECTOS DE SEGURANÇA CIBERNÉTICA	**PRÁTICAS DO TJGO**
Existência de um comitê de segurança de informações formalmente designado e frequência das reuniões	Sim, o comitê se reúne a cada 45 dias ou, excepcionalmente, quando necessário.
Qualificações e experiências dos membros do comitê de segurança da informação	2 Juízes Auxiliares da Presidência - 1 Juiz Auxiliar da CGJ - 1 Secretaria-Geral da Presidência - 1 Diretor da Diretoria de Tecnologia da Informação da Presidência - 1 Diretora da Diretoria de Ciência de Dados e Estatística - 1 Diretora de Recursos Humanos
Existência de um servidor designado como gerente de segurança da informação e alocação	Não há um gerente de segurança da informação no tribunal.
Alocação do Encarregado de Proteção de Dados	O Encarregado de Proteção de Dados está lotado na Unidade de Atendimento aos Usuários de Sistemas (departamento de gerenciamento e suporte aos usuários).
Tomada de decisões considerando um processo estruturado de gestão de riscos ou avaliação dos riscos	Sim, as decisões são tomadas com base na avaliação de riscos de TIC.
Comunicação com os *stakeholders* sobre segurança cibernética	A comunicação com os *stakeholders* é feita através de processos administrativos de incidentes de segurança e informações via e-mail, com referência ao Processo PROAD: 202309000444103.
Consideração de riscos e vulnerabilidades na priorização das demandas de TI	Sim, os riscos e vulnerabilidades de segurança cibernética são formalmente considerados na priorização das demandas de TI a partir de processos administrativos de incidentes de segurança formalizados.
Metodologia para avaliação da maturidade da segurança da informação	Não há uma metodologia específica para a avaliação da maturidade da segurança da informação mencionada.
Avaliação do nível de aderência à Resolução CNJ n. 396/2021	A avaliação é feita por meio de avaliações e questionamentos da Governança de TIC e Controladoria Interna, seguindo as diretrizes e controles estabelecidos nas Resoluções e portarias do CNJ.
Equipe de tratamento de incidentes em redes de computador (ETIR)	Não há uma equipe de tratamento de incidentes em redes de computador (ETIR) designada e em funcionamento no tribunal.

Fonte: Elaborado pelo autor, 2023.

Quadro 11: Tribunal do Rio de Janeiro

ASPECTOS DE SEGURANÇA CIBERNÉTICA	PRÁTICAS DO TJRJ
Existência de um comitê de segurança de informações formalmente designado e frequência das reuniões	Sim, o comitê de segurança da informação existe, e as reuniões ocorrem mensalmente, conforme estabelecido na Resolução TJ/OE n.o 28/2022.
Qualificações e experiências dos membros do comitê de segurança da informação	O comitê tem uma composição multidisciplinar, de acordo com o artigo 14 da Resolução TJ/OE n.o 28/2023
Existência de um servidor designado como gerente de segurança da informação e alocação	Existe um Departamento de Segurança da Informação vinculado diretamente à Presidência do TJRJ, conforme a Resolução TJ/OE n.o 04/2023. Não há um gerente de segurança de informação designado.
Existência de um servidor designado como Encarregado de Proteção de Dados	O Encarregado de Proteção de Dados está vinculado à Presidência do TJRJ.
Tomada de decisões considerando um processo estruturado de gestão de riscos ou avaliação dos riscos	Sim, as decisões são tomadas com base em relatórios mensais apresentados nas reuniões do comitê.
Comunicação com os *stakeholders* sobre segurança cibernética	Há um Programa de Conscientização e Comunicação com páginas específicas no site do TJRJ para segurança da informação e LGPD
Consideração de riscos e vulnerabilidades na priorização das demandas de TI	Sim, a consideração de riscos e vulnerabilidades de segurança cibernética faz parte das atribuições do Comitê Gestor de Tecnologia da Informação e Comunicação (CGTIC).
Metodologia para avaliação da maturidade da segurança da informação	Sim, o tribunal utiliza metodologias como NIST, CIS-Control e ISO 27001 para avaliar a maturidade da segurança da informação.
Avaliação do nível de aderência à Resolução CNJ n.o 396/2021	O tribunal mantém um programa de melhoria contínua para garantir a aderência contínua aos normativos do CNJ.
Equipe de tratamento de incidentes em redes de computador (ETIR)	Sim, o tribunal possui uma equipe de tratamento de incidentes em redes de computador designada e em funcionamento, de acordo com o Ato Normativo TJ n.o 11/2022.

Fonte: Elaborado pelo autor, 2023.

Quadro 12: Tribunal Estadual do Mato Grosso

ASPECTO DE SEGURANÇA CIBERNÉTICA	PRÁTICAS DO TRIBUNAL ESTADUAL DO MATO GROSSO
Existência de um comitê de segurança de informações formalmente designado e frequência das reuniões	Sim, o Comitê Gestor de Segurança Cibernética e da Informação foi instituído pela Portaria 157 de 25 de janeiro de 2023, com reuniões trimestrais, de acordo com o art. 12 da Portaria.
Qualificações e experiências dos membros do comitê de segurança da informação	O comitê é composto por membros com qualificações multidisciplinares, incluindo juízes, coordenadores de tecnologia, diretores e outros profissionais experientes.
Existência de um servidor designado como gerente de segurança da informação e alocação	Não há um gerente de segurança da informação designado, mas existe um Departamento de Segurança da Informação vinculado diretamente à Presidência do tribunal.

Existência de um servidor designado como Encarregado de Proteção de Dados	O Encarregado de Proteção de Dados está lotado na Coordenadoria Judiciária.
Tomada de decisões considerando um processo estruturado de gestão de riscos ou avaliação dos riscos	Sim, as decisões são baseadas em um processo estruturado de gestão de riscos, conforme estabelecido pelas Portarias TJMT N. 1247/2023 e 1248/2023.
Comunicação com *stakeholders* sobre segurança cibernética	Os *stakeholders* são mantidos informados por meio de reuniões trimestrais definidas pela Portaria 157/2023 e comunicação online.
Consideração de riscos e vulnerabilidades na priorização das demandas de TI	Sim, os riscos e vulnerabilidades de segurança cibernética são formalmente considerados na priorização das demandas de TI.
Metodologia de avaliação da maturidade da segurança da informação	O tribunal utiliza metodologias reconhecidas, como NIST, CIS-Control e ISO 27001, para avaliar a maturidade da segurança da informação.
Avaliação da aderência à Resolução CNJ n. 396/2021	A aderência à Resolução CNJ n. 396/2021 e aos controles da Portaria CNJ n. 162/2021 é avaliada por meio de uma avaliação de conformidade interna e com o apoio da consultoria Gartner.
Equipe de tratamento de incidentes em redes de computador (ETIR)	O tribunal possui uma equipe de tratamento de incidentes em redes de computador designada e em funcionamento desde 2021, de acordo com a Portaria N. 1167/2022.

Fonte: Elaborado pelo autor, 2023.

Quadro 13: Tribunal Estadual do Pará

ASPECTO DE SEGURANÇA CIBERNÉTICA	**PRÁTICAS DO TRIBUNAL ESTADUAL DO PARÁ**
Existência de um comitê de segurança de informações formalmente designado e frequência das reuniões	Estabelecido pela Resolução 016/2022. - Reúne-se ordinariamente a cada 60 dias.
Qualificações e experiências dos membros do comitê de segurança da informação	Membros designados pela Portaria 847/2023. - Inclui uma Desembargadora, um Juiz Auxiliar, Secretários, Diretores, Coordenador Militar e Coordenador da Estrutura de Segurança da Informação (CISO). - A maioria dos membros possui experiência gerencial, com exceção do Secretário de Informática e do CISO, que têm experiência direta em Segurança da Informação.
Existência de um servidor designado como gerente de segurança da informação e alocação	Lotado na Secretaria de Informática.
Existência de um servidor designado como Encarregado de Proteção de Dados	Gerenciado por um comitê composto por quatro pessoas (Desembargador, Juiz Auxiliar, representante da Secretaria de Administração e da Secretaria de Informática), conforme a Portaria 2644/2023.
Tomada de decisões considerando um processo estruturado de gestão de riscos ou avaliação dos riscos	Processo estruturado de gestão de riscos.
Comunicação com *stakeholders* sobre segurança cibernética	Atas das reuniões do Comitê de Segurança da Informação são publicadas no Portal Institucional.
Consideração de riscos e vulnerabilidades na priorização das demandas de TI	Riscos de segurança cibernética são considerados na priorização das demandas de TI pelo Comitê Gestor de TI.
Metodologia de avaliação da maturidade da segurança da informação	Avaliação de *frameworks* em andamento
Avaliação da aderência à Resolução CNJ n. 396/2021	Por meio de questionários fornecidos pelo CNJ.

Equipe de tratamento de incidentes em redes de computador (ETIR)	Comitê de Crise Cibernética, estabelecido pela Resolução 017/2022.

Fonte: Elaborado pelo autor, 2023.

Quadro 14: Tribunal Estadual da Paraíba

ASPECTO DE SEGURANÇA CIBERNÉTICA	**PRÁTICAS DO TRIBUNAL ESTADUAL DA PARAÍBA**
Existência de um comitê de segurança de informações formalmente designado e frequência das reuniões	Sim, existe um comitê de segurança da informação. As reuniões são realizadas semestralmente ou quando há necessidade.
Qualificações e experiências dos membros do comitê de segurança da informação	Os membros do comitê possuem qualificações e experiências em diversas áreas, incluindo uma diretora geral da secretaria, uma assessora de inteligência, diretor de auditoria interna, diretor de secretaria de gestão de pessoas, diretor de secretaria de magistratura, diretor de secretaria de segurança da informação, coordenador de segurança cibernética e um assessor de segurança da informação.
Existência de um servidor designado como gerente de segurança da informação e alocação	Sim, o Encarregado de Proteção de Dados está alocado na Coordenadoria de Segurança Cibernética.
Existência de um servidor designado como Encarregado de Proteção de Dados	Sim, o tribunal considera os riscos em suas decisões, seguindo um processo estruturado de gestão de riscos.
Tomada de decisões considerando um processo estruturado de gestão de riscos ou avaliação dos riscos	Sim, o tribunal considera os riscos em suas decisões, seguindo um processo estruturado de gestão de riscos.
Comunicação com *stakeholders* sobre segurança cibernética	Sim, há comunicação com os *stakeholders* sobre segurança cibernética, embora nenhum detalhe específico tenha sido fornecido na tabela.
Consideração de riscos e vulnerabilidades na priorização das demandas de TI	Sim, os riscos e vulnerabilidades de segurança cibernética são formalmente considerados na priorização das demandas de Tecnologia da Informação (TI).
Metodologia de avaliação da maturidade da segurança da informação	Sim, o tribunal utiliza a metodologia CIS Controls v8 para avaliação da maturidade da segurança da informação.
Avaliação da aderência à Resolução CNJ n. 396/2021	Em implantação, o tribunal está em processo de avaliação da aderência à Resolução CNJ n. 396/2021.
Equipe de tratamento de incidentes em redes de computador (ETIR)	Sim, o tribunal possui uma equipe de tratamento de incidentes em redes de computador designada e em funcionamento, conforme a política de gerenciamento de incidentes cibernéticos.

Fonte: Elaborado pelo autor, 2023.

Quadro 15: Tribunal Estadual do Acre

ASPECTO DE SEGURANÇA CIBERNÉTICA	**PRÁTICAS DO TRIBUNAL ESTADUAL DO ACRE**
Existência de um comitê de segurança de informações formalmente designado e frequência das reuniões	Criado recentemente pela Portaria Nº 2997/2023. Em processo de elaboração do plano de ação de segurança da informação.
Qualificações e experiências dos membros do comitê de segurança da informação	Regulamentadas na Resolução TPADM 291/2023. Outras qualificações sugeridas podem ser consideradas.
Existência de um servidor designado como gerente de segurança da informação e alocação	Designado e lotado na Gerência de Segurança. da Informação (Portaria 2997/2023).

Existência de um servidor designado como Encarregado de Proteção de Dados	Comitê LGPD com Victor Hugo Lima de Sousa como especialista e representante da DITEC Juiz auxiliar da Presidência, Giordane de Souza Dourado atua como o Encarregado de Proteção de Dados.
Tomada de decisões considerando um processo estruturado de gestão de riscos ou avaliação dos riscos	Conforme a Resolução 396/2021, os procedimentos estão sendo reavaliados para atender à gestão e avaliação dos riscos.
Comunicação com *stakeholders* sobre segurança cibernética	Utilização de comunicações, reuniões e processos internos para manter a alta administração informada sobre segurança cibernética.
Consideração de riscos e vulnerabilidades na priorização das demandas de TI	Formalização e tratamento imediato de vulnerabilidades; mapeamento no Plano de Gestão de Risco e Plano de Contratações de TIC.
Metodologia de avaliação da maturidade da segurança da informação	Ainda não implementada, estão realizando estudos para adotar uma metodologia/*framework* no futuro.
Avaliação da aderência à Resolução CNJ n. 396/2021	Adesão inicial, com o recente comitê de segurança, estão iniciando ações para cumprir a Resolução.
Equipe de tratamento de incidentes em redes de computador (ETIR)	Em tratativa de implementação de acordo com a Resolução 291/2023.

Fonte: Elaborado pelo autor, 2023.

Quadro 16: Tribunal Estadual de Roraima

ASPECTO DE SEGURANÇA CIBERNÉTICA	**PRÁTICAS DO TRIBUNAL ESTADUAL DE RR**
Existência de um comitê de segurança de informações formalmente designado e frequência das reuniões	Sim, o comitê se reúne bimestralmente.
Qualificações e experiências dos membros do comitê de segurança da informação	Juiz(a) Auxiliar da Presidência, representantes do Corregedor Geral de Justiça, Comissão Permanente de Sindicância, Gabinete Militar, Secretário-Geral, Secretário de Gestão Administrativa, Secretário de Gestão Estratégica, Secretário de Gestão de Pessoas, Secretário de Infraestrutura e Logística, Secretário de Orçamento e Finanças, Secretário de Tecnologia da Informação, Servidor da Secretaria de Tecnologia da Informação, Assessor Jurídico do Núcleo Jurídico Administrativo, e Analista de Sistemas Especialista em Segurança da Informação são membros do comitê.
Existência de um servidor designado como gerente de segurança da informação e alocação	Não foi designado um Gerente de Segurança da Informação.
Existência de um servidor designado como Encarregado de Proteção de Dados	Não foi designado um Gerente de Segurança da Informação.
Tomada de decisões considerando um processo estruturado de gestão de riscos ou avaliação dos riscos	O comitê toma decisões considerando o processo de gestão de riscos.
Comunicação com *stakeholders* sobre segurança cibernética	Realização de campanhas de conscientização e elaboração de cartilhas de orientação para Magistrados, Servidores e Estagiários para manter as partes interessadas informadas.
Consideração de riscos e vulnerabilidades na priorização das demandas de TI	Sim, demandas de TI são priorizadas com base em riscos e vulnerabilidades identificados.
Metodologia de avaliação da maturidade da segurança da informação	Atualmente, não há uma metodologia formal para avaliação da maturidade da segurança da informação em vigor.
Avaliação da aderência à Resolução CNJ n. 396/2021	O tribunal está em processo de adesão à Resolução CNJ n. 396/2021 e à Portaria CNJ n. 162/2021.

Equipe de tratamento de incidentes em redes de computador (ETIR)	A implementação de uma Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) está em andamento.

Fonte: Elaborado pelo autor, 2023.

Quadro 17: Tribunal Estadual do Amazonas

ASPECTO DE SEGURANÇA CIBERNÉTICA	**PRÁTICAS DO TRIBUNAL ESTADUAL DO AM**
Existência de um comitê de segurança de informações formalmente designado e frequência das reuniões	Sim, existe. O comitê reúne-se regularmente, de forma presencial e/ou por vídeo conferência.
Qualificações e experiências dos membros do comitê de segurança da informação	Profissionais com formação acadêmica na área de Segurança da Informação e Proteção de Dados, com certificações internacionais na área e experiência no mercado.
Existência de um servidor designado como gerente de segurança da informação e alocação	Não, existe uma Assessoria de Segurança da Informação e Proteção de Dados lotada na SETIC.
Existência de um servidor designado como Encarregado de Proteção de Dados	Existe.
Tomada de decisões considerando um processo estruturado de gestão de riscos ou avaliação dos riscos	O Encarregado está lotado na Presidência.
Comunicação com *stakeholders* sobre segurança cibernética	Todas as decisões são tomadas baseadas na Gestão de Riscos, utilizando como referência a ISO 27.005 e ISO 31000.
Consideração de riscos e vulnerabilidades na priorização das demandas de TI	A alta administração recebe atualizações sobre segurança a partir do acompanhamento dos Projetos de Segurança, além disso, repassa as informações para o Comitê Gestor de TIC e o mesmo tem contato direto com a Presidência.
Metodologia de avaliação da maturidade da segurança da informação	Sim. Este órgão faz a adoção aos *frameworks*, orientações e aos checklists definidos na resolução 396.
Avaliação da aderência à Resolução CNJ n. 396/2021	(Informação não fornecida)
Equipe de tratamento de incidentes em redes de computador (ETIR)	(Informação não fornecida)

Fonte: Elaborado pelo autor, 2023.

Quadro 18: Tribunal Estadual do Piauí

ASPECTO DE SEGURANÇA CIBERNÉTICA	**PRÁTICAS DO TRIBUNAL ESTADUAL DO PI**
Existência de um comitê de segurança de informações formalmente designado e frequência das reuniões	Sim. A informação é tratada como sigilosa, devido a riscos de segurança cibernética.
Qualificações e experiências dos membros do comitê de segurança da informação	A informação é tratada como sigilosa, devido a riscos de segurança cibernética.
Existência de um servidor designado como gerente de segurança da informação e alocação	Sim. A informação é tratada como sigilosa, devido a riscos de segurança cibernética.
Existência de um servidor designado como Encarregado de Proteção de Dados	Sim. Designado na Portaria Nº 3735/2023 - PJPI/TJPI/PRESIDENCIA/SEGES.
Tomada de decisões considerando um processo estruturado de gestão de riscos ou avaliação dos riscos	A informação é tratada como sigilosa, devido a riscos de segurança cibernética.
Comunicação com *stakeholders* sobre segurança cibernética	A informação é tratada como sigilosa, devido a riscos de segurança cibernética.

Consideração de riscos e vulnerabilidades na priorização das demandas de TI	Sim.
Metodologia de avaliação da maturidade da segurança da informação	A informação é tratada como sigilosa, devido a riscos de segurança cibernética.
Avaliação da aderência à Resolução CNJ n. 396/2021	A informação é tratada como sigilosa, devido a riscos de segurança cibernética.
Equipe de tratamento de incidentes em redes de computador (ETIR)	A informação é tratada como sigilosa, devido a riscos de segurança cibernética.

Fonte: Elaborado pelo autor, 2023.

Quadro 19: Tribunal Estadual de Santa Catarina

ASPECTO DE SEGURANÇA CIBERNÉTICA	**PRÁTICAS DO TRIBUNAL ESTADUAL DE SC**
Existência de um comitê de segurança de informações formalmente designado e frequência das reuniões	Formalmente designado e reuniões mensais para avaliação e discussão.
Qualificações e experiências dos membros do comitê de segurança da informação	Membros altamente qualificados em segurança cibernética, TI, gestão de riscos, e conformidade legal.
Existência de um servidor designado como gerente de segurança da informação e alocação	Designação de um Gerente de Segurança da Informação, integrado à área de Tecnologia da Informação.
Existência de um servidor designado como Encarregado de Proteção de Dados	Servidor designado na área de Compliance como Encarregado de Proteção de Dados.
Tomada de decisões considerando um processo estruturado de gestão de riscos ou avaliação dos riscos	Decisões baseadas em processo estruturado de gestão de riscos, reconhecendo a importância da avaliação contínua dos riscos.
Comunicação com *stakeholders* sobre segurança cibernética	Comitê de Segurança da Informação mantém *stakeholders* informados por meio de relatórios periódicos, apresentações em reuniões de diretoria e comunicações diretas.
Consideração de riscos e vulnerabilidades na priorização das demandas de TI	Riscos e vulnerabilidades de segurança cibernética são formalmente considerados na priorização das demandas de TI pelo Comitê Gestor de TI.
Metodologia de avaliação da maturidade da segurança da informação	Adoção de metodologia estruturada para avaliação da maturidade da segurança da informação, baseada no *framework* ISO 27001.
Avaliação da aderência à Resolução CNJ n. 396/2021	Realização de avaliações regulares para garantir a conformidade com a Resolução CNJ n. 396/2021.
Equipe de tratamento de incidentes em redes de computador (ETIR)	Existência de uma Equipe de Tratamento de Incidentes em Redes de Computador (ETIR) capacitada para lidar com incidentes de segurança cibernética.

Fonte: Elaborado pelo autor, 2023.

Quadro 20: Tribunal Estadual do Maranhão

ASPECTO DE SEGURANÇA CIBERNÉTICA	**PRÁTICAS DO TRIBUNAL ESTADUAL DO MA**
Existência de um comitê de segurança de informações formalmente designado e frequência das reuniões	Comitê formalmente designado chamado CGSI; reuniões bimestrais.
Qualificações e experiências dos membros do comitê de segurança da informação	Equipe multidisciplinar; qualificações e experiências em construção.
Existência de um servidor designado como gerente de segurança da informação e alocação	Cargo em análise para criação; presidente do CGSI desempenha papel próximo.

Existência de um servidor designado como Encarregado de Proteção de Dados	O ouvidor atua como Encarregado de Proteção de Dados, lotado na 2a vice-presidência.
Tomada de decisões considerando um processo estruturado de gestão de riscos ou avaliação dos riscos	Decisões fundamentadas em processo estruturado de gestão de riscos.
Comunicação com *stakeholders* sobre segurança cibernética	Comunicados por meio do sítio eletrônico do CGSI, e-mail e sistemas de informação.
Consideração de riscos e vulnerabilidades na priorização das demandas de TI	Riscos e vulnerabilidades considerados formalmente na priorização de demandas de TI.
Metodologia de avaliação da maturidade da segurança da informação	Utilização dos *frameworks* CIS Controls v8 e NIST; diretrizes das Resoluções do CNJ e orientações da NBRs 27000.
Avaliação da aderência à Resolução CNJ n. 396/2021	Nível de aderência satisfatório; resultados aprimorados no iGovTIC-JUD (2021-2026).
Equipe de tratamento de incidentes em redes de computador (ETIR)	Existência de uma ETIR designada e operante.

Fonte: Elaborado pelo autor, 2023.

Quadro 21: Tribunal Estadual de Alagoas

ASPECTO DE SEGURANÇA CIBERNÉTICA	**PRÁTICAS DO TRIBUNAL ESTADUAL DE AL**
Existência de um comitê de segurança de informações formalmente designado e frequência das reuniões	Instituição do Comitê de Governança de Segurança da Informação (CGSI) do TJAL, com atribuições que incluem assessorar a alta administração, propor alterações na política de segurança da informação, deliberar sobre assuntos relacionados, priorizar ações e gerenciar riscos.
Qualificações e experiências dos membros do comitê de segurança da informação	Não especificado.
Existência de um servidor designado como gerente de segurança da informação e alocação	Não mencionado. A resolução sugere a criação do CGSI, mas não especifica um servidor designado como Gerente de Segurança da Informação.
Existência de um servidor designado como Encarregado de Proteção de Dados	Não mencionado diretamente. O Comitê Gestor Institucional de Proteção de Dados Pessoais (CGPD) irá receber atribuições do CGSI, mas a designação de um servidor específico como Encarregado de Proteção de Dados não é detalhada na resolução.
Tomada de decisões considerando um processo estruturado de gestão de riscos ou avaliação dos riscos	Sim, o CGSI terá a responsabilidade de deliberar sobre assuntos relacionados à segurança da informação, incluindo a gestão de riscos.
Comunicação com *stakeholders* sobre segurança cibernética	Não especificado, mas o CGSI, ao assessorar a alta administração em questões relacionadas à segurança da informação, sugere uma forma de comunicação com *stakeholders.*
Consideração de riscos e vulnerabilidades na priorização das demandas de TI	Sim, o CGSI terá a atribuição de priorizar ações e gerenciar riscos de segurança.
Metodologia de avaliação da maturidade da segurança da informação	Não especificado, mas a criação do CGSI indica uma estratégia mais robusta de segurança da informação, podendo envolver metodologias de avaliação da maturidade.
Avaliação da aderência à Resolução CNJ n. 396/2021	Não especificado, mas o CGSI do TJAL observará o disposto na Resolução CNJ n. 396/2021, indicando um compromisso com as diretrizes dessa resolução.
Equipe de tratamento de incidentes em redes de computador (ETIR)	Não mencionado diretamente. A resolução cria o CGSI, mas não detalha a existência ou função de uma ETIR.

Fonte: Elaborado pelo autor, 2023.

Quadro 22: Tribunal Estadual do Paraná

ASPECTO DE SEGURANÇA CIBERNÉTICA	PRÁTICAS DO TRIBUNAL ESTADUAL DO PR
Existência de um comitê de segurança de informações formalmente designado e frequência das reuniões	Formalmente designado, composto conforme a PSI e Decreto 560/2022 P-GP. Reuniões mensais realizadas no último ano.
Qualificações e experiências dos membros do comitê de segurança da informação	Representantes da alta cúpula e unidades estratégicas, como Encarregado de Proteção de Dados, Núcleo de Inteligência e Segurança Institucional, Núcleo de Governança, Riscos e Compliance, e Departamento de Tecnologia da Informação e Comunicação.
Existência de um servidor designado como gerente de segurança da informação e alocação	Reconhecido pela PSI como Gestor de Segurança da Informação, atualmente lotado na Divisão de Gestão de Segurança de TIC no Departamento de Tecnologia da Informação e Comunicação.
Existência de um servidor designado como Encarregado de Proteção de Dados	Designado pelo Desembargador Claudio Smirne Diniz conforme a Portaria Nº 3237/2022 - D.M., lotado em uma unidade especial abaixo do Órgão Especial.
Tomada de decisões considerando um processo estruturado de gestão de riscos ou avaliação dos riscos	Adoção de trabalhos e análises de riscos similares às de grandes empresas, como a Gartner, pelo Comitê e pelo Gerente de Segurança da Informação.
Comunicação com *stakeholders* sobre segurança cibernética	Representantes da alta administração designados como membros no Comitê para manter as partes interessadas informadas sobre segurança cibernética.
Consideração de riscos e vulnerabilidades na priorização das demandas de TI	Consideração formal dos riscos e vulnerabilidades, com aquisição de solução de gestão de vulnerabilidade para aprimoramento interno.
Metodologia de avaliação da maturidade da segurança da informação	Realizada anualmente em parceria com um parceiro tecnológico, seguindo o CIS Controls v8 *framework*.
Avaliação da aderência à Resolução CNJ n. 396/2021	Compromisso de longo prazo, com plano de ação em execução para a implementação dos controles exigidos.
Equipe de tratamento de incidentes em redes de computador (ETIR)	Definição de missão, escopo, modelo de trabalho, autonomia e integrantes, com ajustes necessários, como capacitação, para pleno funcionamento.

Fonte: Elaborado pelo autor, 2023.

Quadro 23: Tribunal Estadual do Tocantins

ASPECTO DE SEGURANÇA CIBERNÉTICA	PRÁTICAS DO TRIBUNAL ESTADUAL DO TO
Existência de um comitê de segurança de informações formalmente designado e frequência das reuniões	Sim, as reuniões são realizadas trimestralmente segundo a Resolução nº 22, de 16 de outubro de 2014, e a Portaria Nº 2755/2023 - PRESIDÊNCIA/ASPRE, de 13 de novembro de 2023, que designa os membros.
Qualificações e experiências dos membros do comitê de segurança da informação	Conforme Portaria Nº 2755/2023 - PRESIDÊNCIA/ASPRE, de 13 de novembro de 2023, que designa os membros que compõem o comitê, verifica-se que: Desembargadora Presidente do CGSI, Juiz Auxiliar da Corregedoria-Geral da Justiça, Juiz Auxiliar da Presidência, Juiz Coordenador do CGTIC, Diretora-Geral, Diretor Administrativo, Diretora de Tecnologia da Informação, Diretor Judiciário, Diretora de Gestão de Pessoas, Coordenador da COGES e o Assessor Militar.

Existência de um servidor designado como gerente de segurança da informação e alocação	Não existe este cargo específico atribuído no Tribunal, havendo a Divisão de Administração e Segurança de Redes.
Existência de um servidor designado como Encarregado de Proteção de Dados	Conforme Resolução Nº 17, de 23 de junho de 2021, que instituiu o Comitê Gestor de Proteção de Dados Pessoais - CGPDP, em seu Art 3º estabelece que o CGPDP é o órgão Encarregado pelo Tratamento de Dados Pessoais do Poder Judiciário do Estado do Tocantins. Se tratando de um Comitê Multidisciplinar, conta com um gabinete para acompanhamento das deliberações.
Tomada de decisões considerando um processo estruturado de gestão de riscos ou avaliação dos riscos	Sim, o CGSI atuam no processo de tomada de decisões considerando o processo de Gestão de Riscos do Tribunal de Justição, bem como o Plano de Gestão de Riscos e Plano de Continuidade de Negócio e Serviços de TIC do TJTO, podendo ser acessados por meio do endereço eletrônico: *https://www.tjto.jus.br/tic/base-de-arquivos/planos* e *https://www.tjto.jus.br/component/edocman/21192-aqui-2/download?Itemid=0*.
Comunicação com *stakeholders* sobre segurança cibernética	O Comitê realiza reuniões sendo registradas em atas, no qual são deliberadas questões atinentes a sua temática, sendo encaminhadas as unidades responsáveis pela execução e operacionalização das decisões, como unidades organizacionais e grupos de trabalhos, além de quando necessário demandado junto a Diretoria de Comunicação - CECOM, campanhas de conscientização e divulgação de instruções.
Consideração de riscos e vulnerabilidades na priorização das demandas de TI	Sim, conforme Plano de Gestão de Riscos de TIC do TJTO e Plano de Gestão da Continuidade do Negócio e Serviços de TIC do TJTO, disponíveis no endereço *https://www.tjto.jus.br/tic/base-de-arquivos/planos*.
Metodologia de avaliação da maturidade da segurança da informação	NÃO INFORMADO
Avaliação da aderência à Resolução CNJ n. 396/2021	NÃO INFORMADO
Equipe de tratamento de incidentes em redes de computador (ETIR)	NÃO INFORMADO

Fonte: Elaborado pelo autor, 2023.

Quadro 24: Tribunal Estadual do Espírito Santo

ASPECTO DE SEGURANÇA CIBERNÉTICA	**PRÁTICAS DO TRIBUNAL ESTADUAL DO ES**
Existência de um comitê de segurança de informações formalmente designado e frequência das reuniões	Não formalmente designado até o momento.
Qualificações e experiências dos membros do comitê de segurança da informação	Não informado
Existência de um servidor designado como gerente de segurança da informação e alocação	Responsável pela área de segurança lotado na STI, sem cargo gerencial.
Existência de um servidor designado como Encarregado de Proteção de Dados	Não designado até o momento, prejudicando a conformidade com regulações.
Tomada de decisões considerando um processo estruturado de gestão de riscos ou avaliação dos riscos	O Comitê Gestor de TI considera formalmente os riscos de segurança cibernética.

Comunicação com *stakeholders* sobre segurança cibernética	Ausência atual de uma metodologia formal para avaliação de maturidade.
Consideração de riscos e vulnerabilidades na priorização das demandas de TI	Não informado
Metodologia de avaliação da maturidade da segurança da informação	Ausência atual de uma metodologia formal para avaliação de maturidade.
Avaliação da aderência à Resolução CNJ n. 396/2021	Baixa aderência ao cenário regulatório.
Equipe de tratamento de incidentes em redes de computador (ETIR)	Ausência de uma equipe formalmente constituída para tratamento de incidentes.

Fonte: Elaborado pelo autor, 2023.