REVISTA CEJ

ISSN 1414-008X
Ano XXVII
n. 86, jul./dez. 2023

Centro de Estudos Judiciários
Conselho da Justiça Federal

86

JUSTIÇA FEDERAL
Conselho da Justiça Federal
Centro de Estudos Judiciários

OS TRIBUNAIS TÊM ESTRUTURA PARA GERENCIAR RISCOS DE SEGURANÇA DA INFORMAÇÃO? Um estudo à luz das Três Linhas*

DOES THE COURTS HAVE STRUCTURES TO MANAGE INFORMATION SECURITY RISKS? A study considering the Three Lines

Renato Solimar Alves
Carlos Eduardo Mancini Queiroz
Rafael Rabelo Nunes

RESUMO
Este trabalho avalia a presença de uma 2ª linha de defesa na estrutura de segurança da informação dos órgãos do Poder Judiciário do Distrito Federal, fundamentando-se no Modelo das Três Linhas do Instituto dos Auditores Internos.

PALAVRAS-CHAVE
Segurança da informação; estratégias de mitigação de risco cibernético; medidas de segurança cibernética; estruturas de governança; cenários de ameaça digital.

ABSTRACT
This study aims to assess the presence of a second line of defense in the cybersecurity structure of the organs of the Federal District Judiciary, based on the Three Lines Model published by the Institute of Internal Auditors.

KEYWORDS
Cybersecurity; cybersecurity risk mitigation strategies; cybersecurity measures; governance structures; digital threat scenarios.

* Trabalho apresentado no Encontro de Administração da Justiça (EnAJUS 2022, ocorrido em Curitiba-PR entre 24 e 27 de outubro de 2022, e resumo expandido publicado nos anais do evento).

1 INTRODUÇÃO

No atual cenário da transformação digital, as companhias devem desenvolver ações organizacionais, visando à redução dos prejuízos operacionais a partir do investimento na melhoria das capacidades de identificação e respostas a riscos, enfatizando a importância da presença da gestão de riscos em todas as atividades da organização (Araújo, 2021). Como consequência da evolução dos riscos no ambiente cibernético, o tema de segurança cibernética ganhou força e a necessidade de ação para a prevenção a ataques e resposta a incidentes tornou-se altamente relevante para o mundo corporativo.

Um levantamento feito pela Kaspersky em 2020 demonstrou que o Brasil é o País com o maior número de vítimas de *phishing* no mundo (Valente, 2021). Já em 2021, a Roland Berger demonstrou que o Brasil foi o quinto País que mais sofreu crimes cibernéticos, sendo que no primeiro trimestre do ano já havia mais ocorrências que no ano de 2020 inteiro (Prado, 2021).

Organizações que têm as três linhas bem estabelecidas geralmente são mais inteligentes em relação aos riscos. Elas são capazes de identificar e reagir rapidamente a eles, implementam de forma mais eficiente recursos escassos [...]

Ataques cibernéticos ao Governo Federal são naturalmente esperados, visto que os órgãos da Administração Pública tratam dados sensíveis de milhares de brasileiros a todo momento. O Poder Judiciário é responsável por resolver conflitos entre cidadãos, entidades e Estado, administrando uma grande quantidade de dados sigilosos de diversos processos judiciais. Desse modo, a segurança dessas informações é de crítica importância. Em novembro de 2020, o Superior Tribunal de Justiça (STJ) foi alvo do maior ataque de *ransomware* contra um órgão público do Brasil, resultando no bloqueio de e-mails de servidores e casos sigilosos que envolviam grandes facções (Moura, 2022). No que tange às atividades de tribunais, Alves, Georg e Nunes (2022) listaram dez riscos na atividade de produção de despachos e decisões, aos quais os tribunais brasileiros estão submetidos. Os autores não só listam os que parecem mais óbvios, tais como a interrupção da prestação jurisdicional ou perda de informações, mas também ressaltam que a falta de segurança da informação implica riscos de previsão e manipulação da distribuição de processos; de parcialidade e favorecimentos pessoais; e de que o Estado brasileiro seja alvo de espionagem de outras nações e/ou grupos de interesse.

Considerando esse cenário, e que os sistemas seguros ou inseguros se apresentam da mesma forma para usuários finais, esta pesquisa buscou avaliar se órgãos do Poder Judiciário do Distrito Federal (DF) têm estruturas de segurança cibernética adequadas à luz de um modelo de gestão de riscos comumente utilizado, o modelo das Três Linhas. A divisão da estrutura de gestão de riscos em três linhas de defesa tem, por natureza, uma alta aplicabilidade, podendo ser considerada na segurança cibernética para a análise realizada neste trabalho. Outro fator que se busca abordar é a avaliação da existência da 2ª linha de defesa descrita no modelo, visto que uma eventual mistura entre a 1ª e 2ª linha pode não ser ideal para algumas organizações.

Este trabalho segue a seguinte estrutura: na seção 2, são indicados os principais conceitos bibliográficos sobre o tema; na seção 3, é evidenciada a metodologia utilizada; na seção 4, são apresentados e discutidos os resultados; e na seção 5, são abrangidas as conclusões obtidas e propostos trabalhos futuros.

2 REFERENCIAL TEÓRICO

2.1 RISCO E GESTÃO DE RISCOS

Segundo a Associação Brasileira de Normas Técnicas (2018), "risco é o efeito das incertezas nos objetivos". Risco geralmente é atribuído a um resultado ruim, ou à incerteza quanto à ocorrência de possíveis impedimentos; entretanto, essa atribuição veio sofrendo alterações, de forma que risco pode ser atribuído a um resultado positivo. Quando se pensa em instituições financeiras, geralmente aplicações mais arriscadas podem gerar resultados maiores. As organizações que evitam correr riscos provavelmente não irão gerar bons resultados para seus acionistas (Damodaran, 2009).

Whitman e Mattord (2018) definem gestão de riscos como o processo de identificação do risco, avaliação de sua magnitude relativa e a tomada de decisão para mitigá-lo a um nível aceitável. O gerenciamento de riscos pode ser definido como o processo de compreender e gerenciar incertezas internas e externas, reduzindo e controlando efetivamente os riscos e evitando os detrimentos das exposições especulativas (Anderson; Terp, 2016).

A eficácia da gestão de riscos está diretamente ligada à integração na governança e demais atividades da organização, sendo necessário o apoio de todas as partes interessadas, em particular da alta direção, que deve demonstrar comprometimento com a gestão de riscos, assegurando sua total integração em todas as atividades da organização (Associação Brasileira de Normas Técnicas, 2018). A efetiva cultura de riscos em órgãos públicos vem sendo estudada pela Administração Pública (Montezano; Da Costa Júnior; Ramos; Melchiades, 2019) (Ollaik, 2018), sendo já elencada como um instrumento de aplicação do princípio constitucional da eficiência, da mesma forma que a própria lei o é para o princípio da legalidade (Nunes; Perini; Pinto, 2021).

2.2 SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Segurança da informação é a "preservação da confidencialidade, integridade e disponibilidade da informação" (International Organization for Standardization, 2018a) por meio da aplicação de políticas, educação, treinamentos, conscientização e tecnologia (Whitman; Mattord, 2018).

Já a segurança cibernética é uma ramificação da segurança da informação, que envolve a metodologia utilizada para proteger a informação no espaço cibernético, buscando evitar o furto ou alterações de dados (Nunes, 2012). Para alcançar esse objetivo, deve-se criar estratégias de segurança cibernética, a fim de gerenciar riscos, identidades e incidentes e garantir uma reação eficiente contra os diversos sinistros que podem ocorrer (Nunes, 2012).

"Segurança cibernética é a organização e coleção de recursos, processos e estruturas usadas para proteger o ciberespaço e

os sistemas habilitados para o espaço cibernético de ocorrências que desalinham os direitos de propriedade de *jure* com de *facto*" (Craigen; Diakun-Thibault; Purse, 2014, p. 57). Essa definição tem como base o que os autores classificam como os cinco temas dominantes dentro de segurança cibernética, que são: I) soluções tecnológicas; II) eventos; III) estratégias, processos e métodos; IV) engajamento humano; e V) objetos de referência (de segurança) (Craigen; Diakun-Thibault; Purse, 2014).

As principais atividades da segurança cibernética são: monitorar, prevenir e responder ameaças capazes de colocar em risco o espaço de liberdade coletiva ou individual. Essas funções ficam sob a responsabilidade das forças de segurança e serviço de informações (Ralo, 2018).

Um ataque cibernético de grande envergadura e que não foi adequadamente tratado pode afetar profundamente a reputação da organização, impactar gravemente as receitas e levar a graves prejuízos, incluindo a perda de informações e sanções legais e administrativas (Laginestra, 2021).

De acordo com a International Telecommunication Union (ITU) (2009), denominam-se ativos todos os dispositivos que estão conectados à rede, aos serviços e às aplicações, assim como os demais sistemas de telecomunicações e informação transmitida e armazenada no ambiente virtual. A partir disso, torna-se a finalidade principal da segurança cibernética garantir a integridade e confidencialidade desses ativos contra os riscos existentes no mundo cibernético (ITU, 2009).

Outra mudança que o avanço do ambiente cibernético causou no mundo organizacional foi a forma como as organizações gerenciam os riscos cibernéticos. Uma estratégia que está ganhando espaço entre as grandes organizações é a parceria efetiva entre a gerência de risco e os times de segurança da informação, partindo da premissa de que nenhum time consegue obter a perspectiva completa necessária para tratar e gerir efetivamente os riscos no ambiente cibernético (Bevan *et al*., 2018).

Em 2021, o Conselho Nacional de Justiça (CNJ), por meio da Resolução n. 396, de 7 de junho de 2021, instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (Ensec-PJ), que buscou aumentar a resiliência às ameaças cibernéticas do Judiciário. No contexto desta pesquisa, destacam-se duas obrigações definidas pela Ensec-PJ para cada órgão do Judiciário, exceto o Supremo Tribunal Federal. O CNJ determina que os tribunais instituam um Comitê de Governança de Segurança da Informação (CGSI) com funções de assessorar diretamente a alta administração do órgão, de propor alterações em políticas e normas internas de segurança da informação e de supervisionar trabalhos de auditoria dessa área. Além disso, é determinado que exista estrutura organizacional de segurança da informação apartada do setor de Tecnologia da Informação (TI) e subordinada diretamente à alta administração (Conselho Nacional de Justiça, 2021a). Este artigo se concentrará nesses dois pontos relatados pela Ensec-PJ.

Apesar de terem sido normatizadas, as estruturas de governança são apontadas como desafios à gestão da segurança da informação na ótica de gestores de TI de órgãos públicos. Segundo eles, alguns pontos são importantes nesse quesito, a saber: áreas estratégicas não percebem a segurança cibernética como elementar; a governança costuma ser incipiente ou inexistente; o controle de processos de TI não é efetivo; há distanciamento entre gestores e a alta administração; há falta de política específica e/ou modelo de governança de segurança cibernética (Georg; Rodrigues; Alves; Silveira Jr.; Nunes, 2022).

2.3 MODELO DAS TRÊS LINHAS

O Modelo das Três Linhas, assim como é chamado hoje pelo Instituto dos Auditores Internos (IIA), tem como propósito "ajudar as organizações a identificar estruturas e processos que melhor auxiliam no atingimento de seus objetivos e facilitem uma forte governança e gerenciamento de riscos" (IIA, 2020). O Modelo das Três Linhas mobiliza gerentes de negócios (1ªlinha), equipes de gestão de riscos (2ª linha) e auditores internos (3ªlinha), de modo a trabalharem juntos, como um grupo de diferentes estágios, fornecendo maior proteção contra riscos cada vez mais complexos (Potter; Toburen, 2016). Ainda que, em teoria, as três linhas sejam distintas e separadas, ainda existem debates sobre os limites que devem ser aplicados entre elas e discussões divergentes no quesito de operacionalização do modelo (Davies; Zhivitskaya, 2018).

Deve ser levado em conta também que, de acordo com o IIA (2020), o Modelo das Três Linhas pode ser aplicado em qualquer organização, independentemente da sua complexidade ou tamanho. Luburic *et al*. (2015) reforçam a aplicabilidade do modelo em qualquer organização e contexto. A partir do momento que uma organização estrutura adequadamente as três linhas, com elas operando de forma eficaz, não deve haver esforços desnecessários e o risco e o controle têm maior probabilidade de serem gerenciados com eficácia (Anderson; Eubanks, 2015).

O Instituto dos Auditores Internos (2020) detalha as funções de cada uma das três linhas. A 1ª controla os riscos diretamente; a 2ª supervisiona e faz a gestão da metodologia de controle sobre os riscos; e a 3ª é a auditoria interna, que fornece avaliações independentes sobre a organização e as outras duas linhas.

De forma mais detalhada, a 1ª linha inclui os profissionais que monitoram e controlam os processos de trabalho (Glynn *et al*., 2016). Essa linha também pode ser chamada de gerência operacional e está encarregada de identificar, avaliar, controlar e mitigar os riscos cotidianos da organização diretamente com seus funcionários (IIA, 2020).

É de grande importância destacar a responsabilidade dupla das unidades organizacionais responsáveis pela 1ª linha, uma vez que estão encarregadas da geração de receitas e ciência dos riscos e controles relacionados às atividades (Vousinas, 2021). No contexto de segurança cibernética, estão inclusas as linhas de frente do negócio e os empregados da organização, mas também tem foco em TI, que é responsável pela infraestrutura de dados, sistemas e processos nos quais os riscos são apresentados (Jamison; Morris; Wilkinson, 2018).

A 2ª linha de defesa serve como apoio para a 1ª linha, de modo a supervisionar e facilitar a implementação de práticas

de gerenciamento de riscos. Serve como uma linha supervisora, garantindo que a gerência operacional funcione conforme intencionado por políticas internas, ainda mantendo um certo nível de independência dentro do Modelo das Três Linhas (IIA, 2013). As funções gerenciais da 2ª linha normalmente são responsáveis pelo monitoramento contínuo de controle e risco e costumam trabalhar em colaboração direta com a gestão operacional para ajudar a definir estratégias de implementação, fornecer know-how em tratamento de riscos, implementar políticas e procedimentos e coletar informações para fornecer uma visão ampla acerca da organização sobre riscos e controles (Anderson; Eubanks, 2015).

Em resumo, a 2ª linha de defesa é encarregada, principalmente, de verificar a função adequada dos controles existentes da 1ª linha para lidar com os riscos enfrentados pela organização. Para funcionar de maneira eficaz, essa linha de defesa deve ser independente da 1ª, além de se basear em princípios claros de gestão e avaliação de riscos (Vousinas, 2021). "O papel da gestão de risco na segunda linha de defesa é dar uma opinião independente sobre os riscos identificados. A independência é muito importante porque a opinião é sem a influência da primeira linha ou da terceira linha" (Kumar, 2021, p. 1). Conforme Jamison *et al*. (2018), no contexto da segurança cibernética, a 2ª linha é de responsabilidade da equipe de segurança da informação, que instala e monitora diversos controles para elucidar atividades maliciosas.

De acordo com Anderson & Eubanks (2015), embora a 1ª e 2ª. linhas tenham responsabilidades diferentes por risco e controle, é essencial que ambas as linhas utilizem as mesmas ferramentas na gestão de riscos e trabalhem em conjunto, aproveitando processos e conhecimentos sempre que possível. Entretanto, ao exigir um nível de independência alto para cada uma das linhas, existem *trade offs* que podem afetar negativamente a eficácia do processo de gerenciamento de risco (Bantleon *et al*., 2020).

O IIA (2020) traz a possibilidade de combinação ou separação dos papéis das 1ªs e 2ªs linhas, considerando a chance de que alguns papéis de 2ª linha sejam atribuídos a especialistas para que, em troca, sejam fornecidos conhecimentos complementares, apoio, monitoramento e questionamento àqueles com papéis de 1ª linha. "Na medida em que o papel das funções da segunda linha exige que elas estejam diretamente envolvidas em uma atividade de primeira linha, essa função pode não ser totalmente independente dessa atividade de primeira linha de defesa" (Anderson; Eubanks, 2015, p. 6). As funções da 2ª linha podem focar em objetivos específicos, como a conformidade com leis, regulamentos e comportamento ético aceitável, controle interno, segurança da informação e tecnologia, sustentabilidade e avaliação da qualidade, além de poderem se estender às responsabilidades mais diretas dentro da gestão de riscos, como o *Enterprise Risk Management* (IIA, 2020).

A 3ª linha é a auditoria interna, que age independentemente das outras duas linhas, em caráter de supervisora delas, e reporta os dados à alta administração da organização (IIA, 2020). Kumar (2021) observa que, em muitos mercados, ocorre uma sobreposição entre a 2ª e 3ª linha, combinando as duas funções, e que essa integração invalida o propósito do modelo, pois essas linhas devem funcionar de forma independente.

A Figura 1 mostra um esquema do Modelo das Três Linhas, demonstrando os níveis de interação entre as entidades dentro e fora da organização:

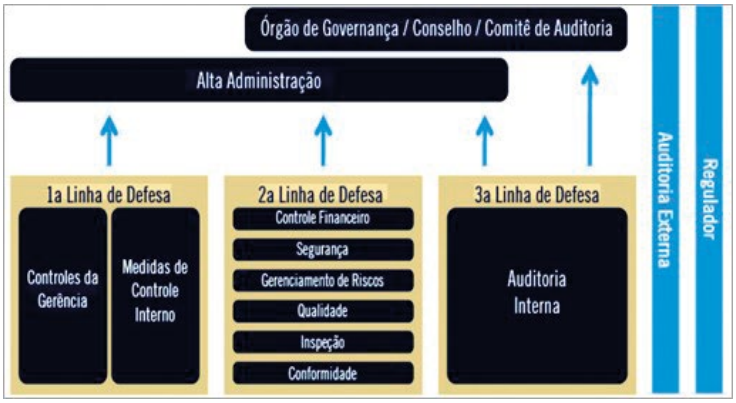

Figura 1 – Modelo de Três Linhas de Defesa. Fonte: As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles. IIA. São Paulo, 2013.

No contexto dos órgãos e entidades da Administração Pública Federal, o Modelo das Três Linhas é um modelo bem enraizado, visto que a alta administração desses órgãos e entidades tem a responsabilidade de manter, monitorar e aperfeiçoar os controles internos da gestão (Brasil, 2017a).

Já no contexto de risco cibernético, Bevan *et al*. (2018) propõem que o Modelo das Três Linhas pode ser visto nos papéis da segurança cibernética como a 1ª linha e a função de risco como a 2ª linha. Os autores também identificam que a segurança cibernética (geralmente como parte vinculada à TI) responsabiliza-se e gerencia os riscos provenientes das operações de TI. Já a função de risco trabalha com a 1ª linha para identificar e priorizar os riscos cibernéticos. Jamison, Morris e Wilkinson (2018) escrevem que, no caso de várias organizações, principalmente as que não têm um setor de segurança da informação dedicado, seu monitoramento e ação ficam sob responsabilidade do departamento de TI, resultando na desordem dos limites entre a 1ª e 2ª linhas.

Bevan *et al*. (2018) revelaram que, na prática, o fato de as organizações trabalharem coletivamente para identificar riscos e mitigar vulnerabilidades resulta numa incerteza dos limites entre as funções de risco e segurança cibernética. Entretanto, essa incerteza gera mais oportunidades à 2ª linha de questionar a 1ª linha em diálogo aberto, o que beneficia ambas, já que a 1ª linha fica apta a relacionar o risco cibernético dentro do gerenciamento de riscos corporativos e torna-se mais bem preparada para eventuais decisões de risco, enquanto a 2ª linha se adequa melhor com as capacidades e planos da 1ª (Bevan *et al*. 2018). Porém, a falta de coordenação é capaz de reduzir os benefícios das três linhas de defesa, já que as tarefas e recursos de cada linha não são independentes das outras linhas (Bantleon *et al*. 2020).

A Figura 2 ilustra, de forma simplificada, a disposição e atribuição das respectivas funções das três linhas, ilustrando também suas relações:

Figura 2 – O Modelo das Três Linhas do IIA. Fonte: Modelo das Três Linhas, IIA, 2020.

Organizações que têm as três linhas bem estabelecidas geralmente são mais inteligentes em relação aos riscos. Elas são capazes de identificar e reagir rapidamente a eles, implementam de forma mais eficiente recursos escassos para gerenciar o risco em uma base priorizada e têm maior transparência de risco interno, para que possam alavancar informações entre as linhas sem a necessidade de recriar relatórios ou realizar várias camadas de teste. Esses itens contribuem para evitar surpresas e perdas, diminuir custos de transferência de risco e favorecer que os objetivos da organização sejam alcançados (Potter; Toburen, 2016, p. 16).

Entre as críticas ao modelo, percebe-se que muitas se concentram no setor financeiro, que foi implementado em diversos países. Davies e Zhivitskaya (2018) discorrem que a separação de atividades entre as partes envolvidas reduz a responsabilidade das áreas e, por fim, diminui a efetividade do modelo, além de que a eficácia do modelo não é comprovada mesmo sendo utilizado em instituições financeiras de vários países. De acordo com Vousinas (2021), mesmo que a ideia original por trás do Modelo das Três Linhas seja de um modelo aplicável a todos os tipos de organizações, ele não reconhece as particularidades de setores específicos, principalmente de instituições financeiras e bancos, frisando a principal fraqueza do modelo, que é justamente a falta de uma análise ampla de toda a estrutura organizacional, resultando em controles ineficazes em diversos níveis da organização.

Chambers e Odar (2015) ressaltam que o modelo não foi totalmente eficaz e deu uma falsa sensação de segurança quando se analisa a crise financeira global de 2008. Após realizar uma pesquisa em bancos holandeses, Udding (2016) concluiu que o design do Modelo das Três Linhas é válido, entretanto vários problemas podem ser elucidados no processo de implementação e em sua operação. Segundo Bonisch (2013), devido à falta de uma definição universalmente aceita sobre o Modelo das Três Linhas, o descreve como uma "metáfora excessivamente usada".

2.4 CARACTERIZANDO A 2ª LINHA DE DEFESA

Esta subseção busca levantar as características que compõem a 2ª linha de defesa como um todo, levando em consideração suas funções, responsabilidades, nível de independência e relevância no setor público. As características evidenciadas servirão de base para a obtenção de informações por meio da pesquisa estruturada.

Ainda que não seja completamente independente, é de suma importância a existência de funções de 2ª linha bem capacitadas, pois é esperado um grau adequado de objetividade no fornecimento de informações críticas à alta administração e ao conselho de administração sobre a gestão de risco pela 1ª linha (Anderson; Eubanks, 2015). Considerando que deve haver uma interação regular entre a gestão e a auditoria interna, de forma que o trabalho da 3ª linha seja relevante e esteja alinhado às necessidades, torna-se necessária a colaboração entre as três linhas de defesa (IIA, 2020).

Conforme o posicionamento do IIA (2020), a 2ª linha tem funções típicas, presentes na maioria das organizações. Cada uma dessas funções engloba certo nível de independência da 1ª linha, mas, por natureza, são funções gerenciais. Em suma, espera-se da 2ª linha:

- Uma função (e/ou comitê) de gerenciamento de riscos que facilite e monitore a implementação de práticas eficazes de gerenciamento de riscos por parte da gerência operacional e auxilie os proprietários dos riscos a definir a meta de exposição ao risco e a reportar adequadamente informações relacionadas a riscos em toda a organização.
- Uma função de conformidade que monitore diversos riscos específicos, tais como a não conformidade com as leis e regulamentos aplicáveis (IIA, 2020).

Nesse quesito, a função separada reporta diretamente à alta administração e, em alguns setores do negócio, diretamente ao órgão de governança (IIA, 2020).

Sob a ótica da segurança cibernética, a função de gestão de risco fica atribuída à 2ª linha, apoiando e monitorando as atividades de segurança cibernética atreladas à 1ª linha (Bevan *et al*. 2018). Mabwe, Ring e Webb (2017) realizaram um estudo baseado no Modelo das Três Linhas, em que muitos entrevistados comentaram sobre a indefinição inerente às duas 1ªs linhas, além de identificar que o papel de supervisão da 2ª linha sobre a 1ª acaba removendo o conceito da independência da 2ª linha e cria lacunas entre teoria e prática.

Sob o contexto de controles internos dos órgãos e entidades da Administração Pública Federal, a estrutura desses controles deve pertencer ao Modelo das Três Linhas, com o objetivo de operar de forma eficaz e coordenada (Brasil, 2017a). Nesse cenário, a 1ª linha, dependente da 2ª, recebe as seguintes responsabilidades:

- A 1ª linha é responsável por identificar, avaliar, controlar e mitigar os riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos

destinados a garantir que as atividades sejam realizadas de acordo com as metas e objetivos da organização.
- A 1ª linha contempla os controles primários, que devem ser instituídos e mantidos pelos gestores responsáveis pela implementação das políticas públicas durante a execução de atividades e tarefas, no âmbito de seus macroprocessos finalísticos e de apoio (Brasil, 2017a, p. 3).

Seguindo a função de supervisora apartada da 1ª linha, são atribuídas à 2ª linha as funções a seguir:

- As instâncias de 2ª linha de defesa estão situadas no nível de gestão e objetivam assegurar que as atividades realizadas pela 1ª linha sejam desenvolvidas e executadas de forma apropriada.
- Essas instâncias são destinadas a apoiar o desenvolvimento dos controles internos da gestão e realizar atividades de supervisão e de monitoramento das atividades desenvolvidas no âmbito da 1ª linha de defesa, que incluem gerenciamento de riscos, conformidade, verificação de qualidade, controle financeiro, orientação e treinamento.
- Os Assessores e Assessorias Especiais de Controle Interno (AECI) nos ministérios integram a 2ª linha de defesa e podem ter sua atuação complementada por outras estruturas específicas definidas pelas próprias organizações (Brasil, 2017a, p. 3).

Percebe-se que a 2ª linha é responsável por funções gerenciais, de modo a garantir a operação da 1ª linha, e tem independência na gestão dos riscos dentro do modelo, mesmo que em grau reduzido, pois está sob o comando da alta administração da organização.

3 METODOLOGIA

Esta pesquisa classifica-se como de natureza aplicada, com objetivos exploratórios sob a perspectiva qualitativa. Pode ser classificada como exploratória, pois tem como objetivo desenvolver, esclarecer e modificar conceitos e ideias, buscando a formulação de problemas de pesquisa mais específicos para estudos futuros (Gil, 2008). Além disso, esse tipo de pesquisa é desenvolvido com o objetivo de proporcionar uma visão ampla sobre um fato e envolve um levantamento bibliográfico e documental, o que reforça essa classificação (Gil, 2008).

Foi utilizada a perspectiva essencialmente qualitativa para a elaboração desta pesquisa, pois busca elucidar o sentido dos fenômenos do mundo social e reduzir a distância entre indicador e indicado, entre teoria e dados, entre contexto e ação (Van Maanen, 1979). De acordo com Minayo (2009, p. 21), a pesquisa qualitativa conta com o "universo dos significados, dos motivos, das aspirações, das crenças, dos valores e das atitudes".

O procedimento de coleta de dados ocorreu por meio da pesquisa documental, com os dados tratados via análise de conteúdo. A coleta dos dados foi realizada em pesquisa documental entre fevereiro e abril de 2022, utilizando-se principalmente de organogramas, portarias, resoluções, atas de reuniões e documentos oficiais disponibilizados publicamente nos *websites* dos respectivos tribunais investigados, ou por dados obtidos por meio de pedidos de acesso à informação via canais disponibilizados por ouvidorias e canais oficiais dos órgãos. Cellard (2008) diz que a pesquisa documental utiliza o documento que pode ser definido como instrumento escrito que faz fé daquilo que atesta. De acordo com Flick (2004), é caracterizada como documental a pesquisa de abordagem unicamente qualitativa, sendo usada como método independente.

Baseando-se no cenário atual de segurança cibernética do Poder Judiciário e no potencial impacto de um ataque cibernético bem-sucedido aos órgãos, esta pesquisa delimitou o escopo para seis tribunais sediados em Brasília-DF – dos quais foi possível obter informações –, buscando analisar suas estruturas de segurança cibernética. Os tribunais analisados foram: Supremo Tribunal Federal (STF), Superior Tribunal de Justiça (STJ), Superior Tribunal Militar (STM), Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT), Tribunal Regional Federal da 1ª Região (TRF1) e Tribunal Superior do Trabalho (TST).

Os pedidos de acesso à informação foram abertos de forma exclusivamente eletrônica, via formulário virtual ou e-mail. Foram solicitadas duas informações nos pedidos, ambas referentes aos comitês de segurança da informação dos tribunais identificados por meio da análise documental. A primeira solicitação buscava confirmar a existência dos comitês e se, porventura, existiam outros comitês de segurança da informação no respectivo órgão. A 2ª solicitação buscava confirmar a situação desses comitês e se continuavam se reunindo de forma regular.

No tratamento dos dados, foi utilizada a análise de conteúdo sobre os documentos governamentais obtidos, relacionando as informações apresentadas nos documentos com as definições do Modelo das Três Linhas em conjunto ao contexto de segurança cibernética, de modo a alcançar os objetivos desta pesquisa. A análise documental, como forma de tratamento de dados, busca "a facilitação do acesso ao observador, de tal forma que esta obtenha o máximo de informação (aspecto quantitativo) com o máximo de pertinência (aspecto qualitativo)" (Bardin, 2016, p. 51).

Conforme Gil (2008), fontes documentais podem, muitas vezes, proporcionar ao pesquisador dados suficientes e ricos, proporcionando economia de tempo na pesquisa, e, em muitos casos, a investigação social só é possível por meio de documentos. Gil (2008) também discorre que registros escritos fornecidos por instituições governamentais podem ser úteis para a pesquisa social, como projetos de lei, relatório de órgãos governamentais, entre outros. Baseada nessas afirmações, foi definida a metodologia desta pesquisa.

4 RESULTADOS E DISCUSSÃO

Nesta seção são apresentados os resultados dos dados coletados de seis tribunais do Poder Judiciário do DF, disponíveis em seus respectivos sites oficiais e em ouvidorias

abertas por meio da lei de acesso à informação. Mediante análise de conteúdos, buscou-se mostrar como estão organizadas as estruturas dos tribunais sob a ótica de segurança cibernética, como essas estruturas funcionam e contextualizá-las com o Modelo das Três Linhas do IIA.

4.1 SUPREMO TRIBUNAL FEDERAL

A estrutura organizacional do STF, apresentada no organograma nas Figuras 3 e 4, possibilitou a tirada de conclusões quanto à divisão de corpos funcionais que tratam de segurança cibernética. No documento, fica disposta a Secretaria de Tecnologia da Informação (STI), destacando suas coordenadorias de Gestão de TI, de Infraestrutura Tecnológica e seu Núcleo de Prevenção, Tratamento e Respostas a Incidentes. O documento também revela, em especial, a Assessoria de Segurança da Informação (ASI) e a Auditoria Interna, apontando que ambas as estruturas estão apartadas da STI e são hierarquicamente superiores.

A partir dessas informações, considera-se que a STI, em suas atribuições, conjunta de suas coordenadorias e núcleo, representa a 1ª linha de defesa no campo de segurança cibernética. A STI é responsável pelo tratamento, prevenção e respostas a incidentes dentro do campo da TI, justificando sua classificação dentro do modelo.

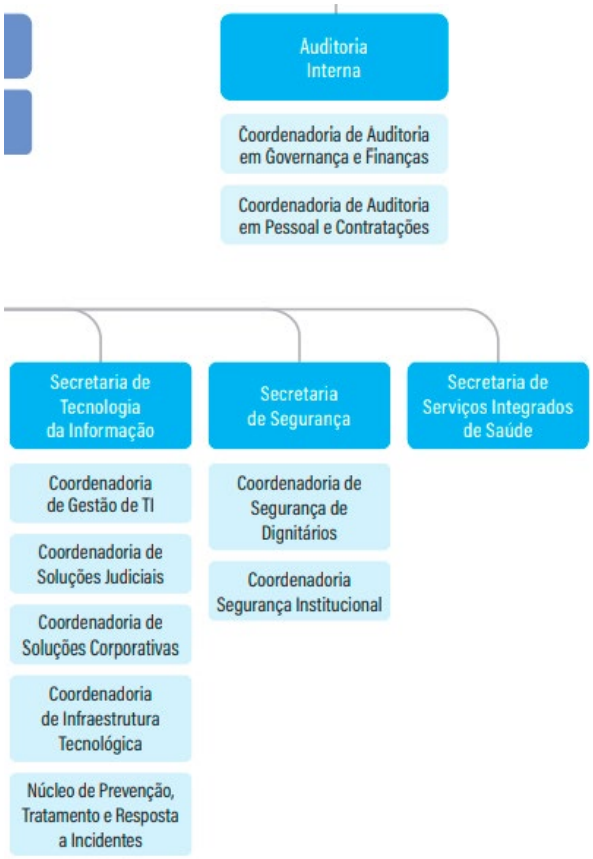

Figura 3 – Organograma do STF – STI e AI. Fonte: Organograma Supremo Tribunal: Ato Regulamentar n. 25, de 29 de novembro de 2021. Supremo Tribunal Federal. Brasília (DF), 2021. Disponível em: <https://portal.stf.jus.br/textos/verTexto.asp?servico=sobreStfOrganograma>. Acesso em: 2 mar. 2022.

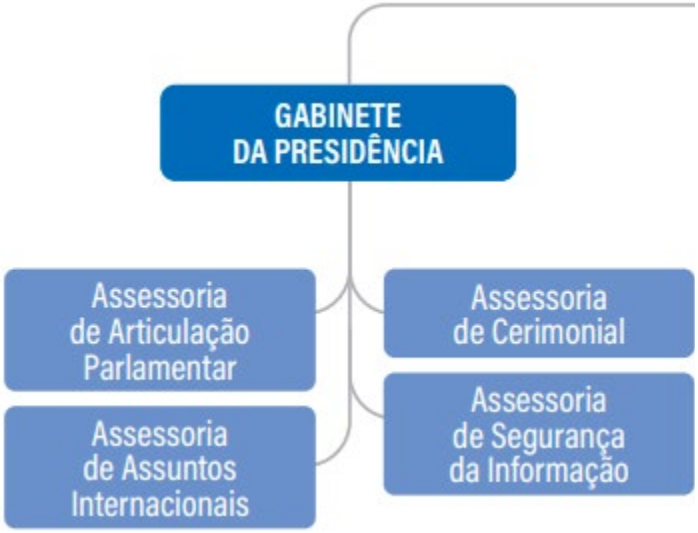

Figura 4 – Organograma do STF – ASI. Fonte: Organograma Supremo Tribunal: Ato Regulamentar n. 25, de 29 de novembro de 2021. Supremo Tribunal Federal. Brasília (DF), 2021. Disponível em: <https://portal.stf.jus.br/textos/verTexto.asp?servico=sobreStfOrganograma>. Acesso em: 2 mar. 2022.

Representando a 2ª linha, considerou-se a ASI, pois é uma estrutura organizacional apartada da STI com funções de supervisão e assessoramento. Em conjunto com a ASI, o STF conta com comitês de segurança da informação, em especial o Comitê Corporativo de Segurança da Informação (CCSI), instituído pela Resolução n. 612, de 23 de abril de 2018, que define atribuições diretamente relacionadas à 2ª linha de defesa.

Complementando as atividades da ASI e do CCSI, existe também o Comitê Executivo de Segurança da Informação (Cesi), que tem o papel de monitorar a implantação e gerenciar o funcionamento do Sistema de Gestão de Segurança da Informação do STF (SGSI/STF). De acordo com a Resolução n. 612/2018, o SGSI/STF "é um conjunto de elementos organizados para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação" (Brasil, 2018, p. 3).

A 3ª linha de defesa fica atrelada à Auditoria Interna, estando apartada dos demais setores do STF e respondendo diretamente à Presidência do Tribunal, realizando atividades de auditoria em governança, possivelmente incluindo a governança de TI.

De acordo com a resposta obtida na solicitação de acesso à informação, o CCSI continua ativo, realizando suas reuniões ordinárias semestralmente e extraordinárias quando convocadas. O Cesi também continua ativo e realiza suas reuniões ordinárias mensalmente e as extraordinárias quando convocadas; entretanto, não existem registros das atas das reuniões.

4.2 SUPERIOR TRIBUNAL DE JUSTIÇA

A partir da estrutura organizacional disposta no organograma do STJ, nas figuras 5 e 6, disponibilizado publicamente em seu website oficial, realizou-se a interpretação relacionada à estrutura organizacional sob a ótica de segurança cibernética. No documento, é apresentada a Secretaria de Tecnologia da Informação e Comunicação (STI), que tem seis coordenadorias, no total, destacando as coordenadorias de Tecnologia da Informação, a de apoio à Governança e Gestão de Tecnologia

da Informação e Comunicação (CGOT) e a de Segurança da Informação e Defesa Cibernética (CSID). O documento apresenta, também, a Secretaria de Auditoria Interna, que funciona como área independente das demais secretarias do Tribunal.

Figura 5 – Organograma do STJ – STI. Fonte: Organograma: Estrutura Básica. Superior Tribunal de Justiça. Brasília (DF), 2018. Disponível em: <https://www.stj.jus.br/static_files/STJ/Midias/arquivos/2482_Org_Estrutura_Basica.pdf>. Acesso em: 2 mar. 2022.

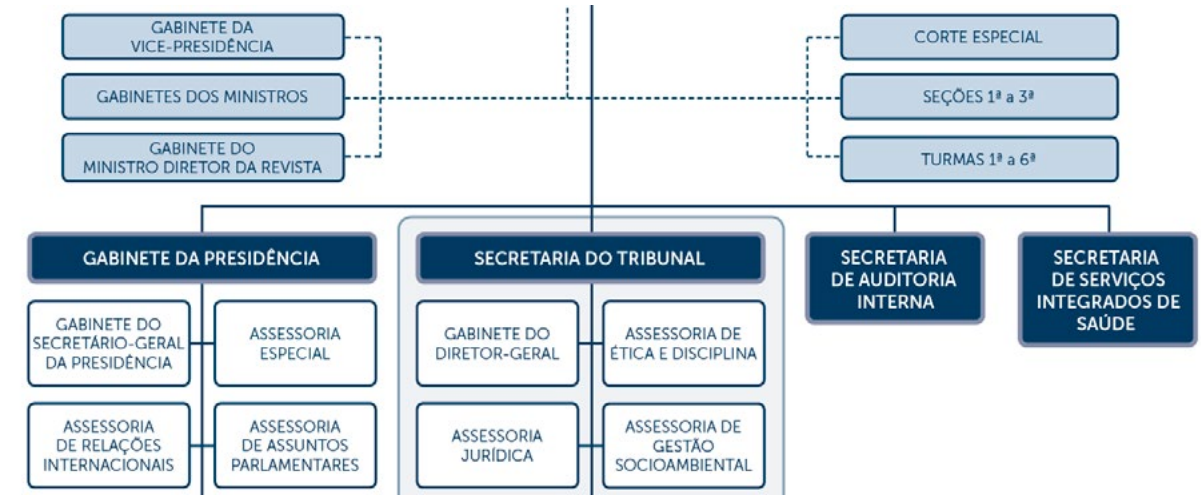

Figura 6 – Organograma do STJ – SAI. Fonte: Organograma: Estrutura Básica. Superior Tribunal de Justiça. Brasília (DF), 2018. Disponível em: <https://www.stj.jus.br/static_files/STJ/Midias/arquivos/2482_Org_Estrutura_Basica.pdf>. Acesso em: 2 mar. 2022.

Convém apontar que as coordenadorias do STJ contêm suas respectivas seções subordinadas, conforme demonstrado no organograma da STI (Brasil, 2021). A CSID tem duas seções: a de Segurança da Informação e Proteção de Dados e a de Operação de Segurança de Tecnologia da Informação e Comunicação, que obteve destaque nesta pesquisa. Outra informação relevante é que a CSID engloba um gestor responsável pela segurança da informação.

Sobre uma das atribuições da STI, a Resolução STJ/GP n. 11, de 12 de novembro de 2015, determina: "Compete à Secretaria de Tecnologia da Informação e Comunicação – STI prover e controlar o uso dos recursos de tecnologia da informação, tendo em vista os requisitos de segurança, estabilidade, confiabilidade e padronização do ambiente computacional" (Brasil, 2015, p. 2)

Quando comparada com o Modelo das Três Linhas, interpreta-se que a estrutura organizacional do STJ atribui a Secretaria de Tecnologia da Informação e Comunicação à 1ª linha de defesa, por realizar operações de segurança de tecnologia de informação e comunicação (TIC). A CSID fica apartada das demais coordenadorias do STI e tem um coordenador específico em segurança da informação enquanto está subordinada ao secretário de tecnologia da informação em conjunto com as outras coordenadorias.

Com o objetivo de apoiar o funcionamento da segurança cibernética e da informação do STJ, existem três comitês ativos no tribunal, sendo eles: o Comitê Gestor de Proteção de Dados Pessoais (CGPD); o Comitê Gestor de Tecnologia da Informação e Comunicação (CGeTIC); e o Comitê de Governança de Tecnologia da Informação e Comunicação (CGovTIC).

De acordo com a Portaria STJ/GDG n. 178, de 12 de março de 2021, que institui o CGPD, o comitê é responsável pela implementação da Lei Geral de Proteção de Dados no STJ (Brasil, 2021c). Cabe ao CGeTIC a elaboração do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) e ao CGovTIC a análise, aprovação e acompanhamento do PDTIC do STJ, levando em consideração que, no plano, estão dispostas atividades de segurança da informação (Brasil, 2017b).

Com base nessas atividades e no contexto de segurança cibernética, a 2ª linha de defesa do STJ é composta pelo CGPD, CGeTIC e CGovTIC. De acordo com resposta obtida pela ouvidoria do STJ, por meio de pedido de acesso à informação, os três comitês mencionados continuam se reunindo de maneira rotineira ou extraordinária via convocação dos seus respectivos presidentes.

Fica atribuída à 3ª linha de defesa a Secretaria de Auditoria Interna (SAI), que está apartada das outras secretarias e responde

diretamente ao ministro presidente do STJ. Complementando essa afirmação, de acordo com a Resolução STJ/GP n. 11/2015, "Todas as operações realizadas com uso dos recursos de tecnologia da informação serão registradas para fins de auditoria" (Brasil, 2015, p. 2).

4.3 SUPERIOR TRIBUNAL MILITAR

Por meio do organograma obtido no website oficial do STM (figuras 7 e 8), obtiveram-se conclusões referentes à segurança cibernética do órgão. O organograma dispõe a Diretoria de Tecnologia da Informação (DITIN), que tem quatro coordenadorias e dois núcleos sob sua gestão. No contexto desta pesquisa, destacam-se a Coordenadoria de Tecnologia, que controla três seções, em especial a Seção de Administração e Gerência de Redes e Segurança da Informação (SAGRE) e a Seção de Bancos e Armazenamento de Dados (SEBAD). Está exposta, também, a Secretaria de Auditoria Interna, operando independentemente das outras duas secretarias do STM.

De acordo com a Resolução n. 222, de 3 de fevereiro de 2016, a Secretaria de Segurança Institucional (SESEG) é a responsável por "propor as medidas e processos específicos para a Segurança da Informação e Comunicação (SIC) com base na avaliação de risco apresentada nos Planos de Segurança das unidades da JMU [Justiça Militar da União]" (Brasil, 2016, p. 8). A SESEG não é exibida no atual organograma do STM, portanto, interpreta-se que sua responsabilidade foi transferida à SAGRE.

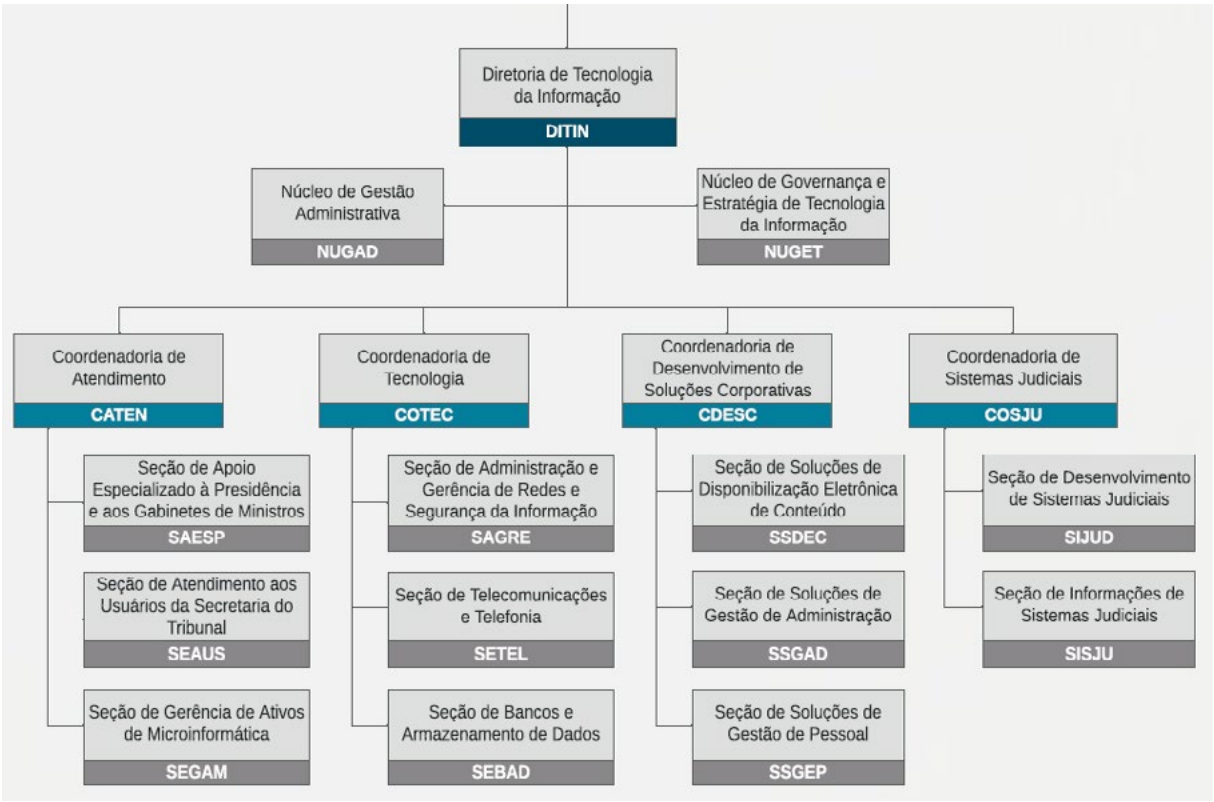

Figura 7 – Organograma do STM – DITIN. Fonte: Estrutura Organizacional: Resolução n. 306, de 16 de fevereiro de 2022. Superior Tribunal Militar. Brasília (DF), 2022. Disponível em: <https://www.stm.jus.br/images/arquivos/institucional/Organograma_estrutura%20organizacional_v10.pdf>. Acesso em: 9 mar. 2022

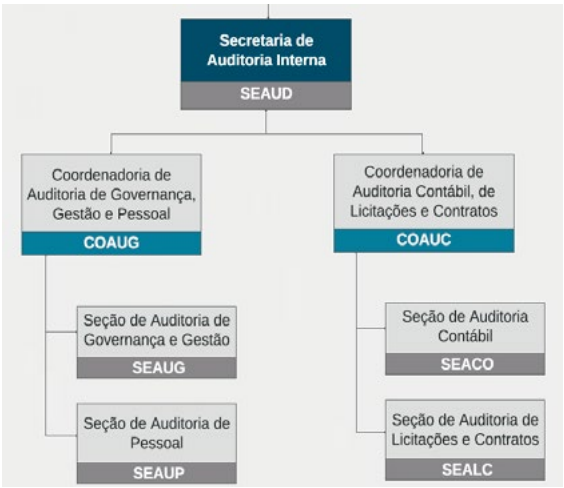

Figura 8 – Organograma do STM – SEAUD. Fonte: Estrutura Organizacional: Resolução n. 306, de 16 de fevereiro de 2022. Superior Tribunal Militar. Brasília (DF), 2022. Disponível em: <https://www.stm.jus.br/images/arquivos/institucional/Organograma_estrutura%20organizacional_v10.pdf>. Acesso em: 9 mar. 2022

A Resolução n. 298, de 4 de agosto de 2021, estabelece: "Detectados eventuais incidentes cibernéticos que coloquem em risco a segurança cibernética, fica a Diretoria de Tecnologia da Informação autorizada a desligar todos os serviços de tecnologia da informação e comunicação" (Brasil, 2021d, p. 9).

Contextualizando a estrutura do STM no Modelo das Três Linhas dentro de segurança cibernética, pode-se considerar a DITIN como a 1ª linha de defesa, pois é responsável pelo gerenciamento de redes e armazenamento de dados do STM, por meio das SAGRE e SEBAD, respectivamente.

Ainda no âmbito da 1ª linha de defesa, o STM tem o Comitê de Crises e Incidentes Cibernéticos (CCIC), que deve reportar eventuais incidentes de segurança cibernética para o Comitê Executivo de Privacidade, Segurança Cibernética e Dados Abertos (CESDA) e deve colaborar com a identificação e tratamento de incidentes de segurança da informação (BRASIL, 2021d).

Analisando o CESDA, entende-se que ele atua na 2ª linha do STM em segurança cibernética, levando em conta que compete ao comitê as seguintes funções:

V – Formular e conduzir diretrizes para o Sistema de Gestão de Segurança Cibernética e da Informação, considerando as disposições da Lei Geral de Proteção de Dados Pessoais (LGPD);

XII – Assessorar o Comitê de Governança de Tecnologia da Informação e Comunicação em matéria correlata à segurança cibernética;

XIV – Promover, coordenar e acompanhar as ações relacionadas à segurança cibernética e da informação;

XVIII – Elaborar o protocolo de prevenção a incidentes cibernéticos;

XIX – Elaborar o plano de ação do protocolo de gerenciamento de crise cibernética (Brasil, 2021d, p. 12).

De modo a atender a ENSEC-PJ, a Resolução n. 301, de 8 de setembro de 2021, institui o Comitê de Governança de Tecnologia da Informação e Comunicação da Justiça Militar da União (CGovTIC) que tem as seguintes competências:

1. Promover diretivas e ações referentes a segurança da informação e segurança cibernética, no que cabe à ENSEC-PJ;

2. Avaliar normas e mecanismos institucionais de modo a melhorar serviços de segurança cibernética (Brasil, 2021e).

A SEAUD é responsável pela 3ª linha, por estar apartada das demais secretarias e responder diretamente à presidência do STM. De acordo com a Resolução n. 298, de 4 de agosto de 2021, "As violações de segurança devem ser comunicadas e registradas, e esses registros analisados periodicamente, com o propósito de caráter corretivo, legal e de auditoria" (Brasil, 2021d, p. 9).

Em resposta obtida pela ouvidoria, por meio da Lei de Acesso à Informação, o CGovTIC não tem registro de reunião, porém a primeira reunião semestral estava prevista para junho de 2022.

4.4 TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS

Por meio do organograma do TJDFT (figuras 9 e 10), foi realizada a interpretação da estrutura organizacional do órgão, sob o contexto de segurança cibernética. O documento apresenta a Secretaria Geral do Tribunal (SEG), que engloba, em especial, a Secretaria de Tecnologia da Informação (Seti). Existe, também, a Secretaria de Segurança e Inteligência (Sesi), entretanto, não foram encontradas evidências de que a Sesi atua no campo de segurança cibernética. A Secretaria de Auditoria Interna (Seai) está separada das demais secretarias e áreas funcionais, operando de forma independente.

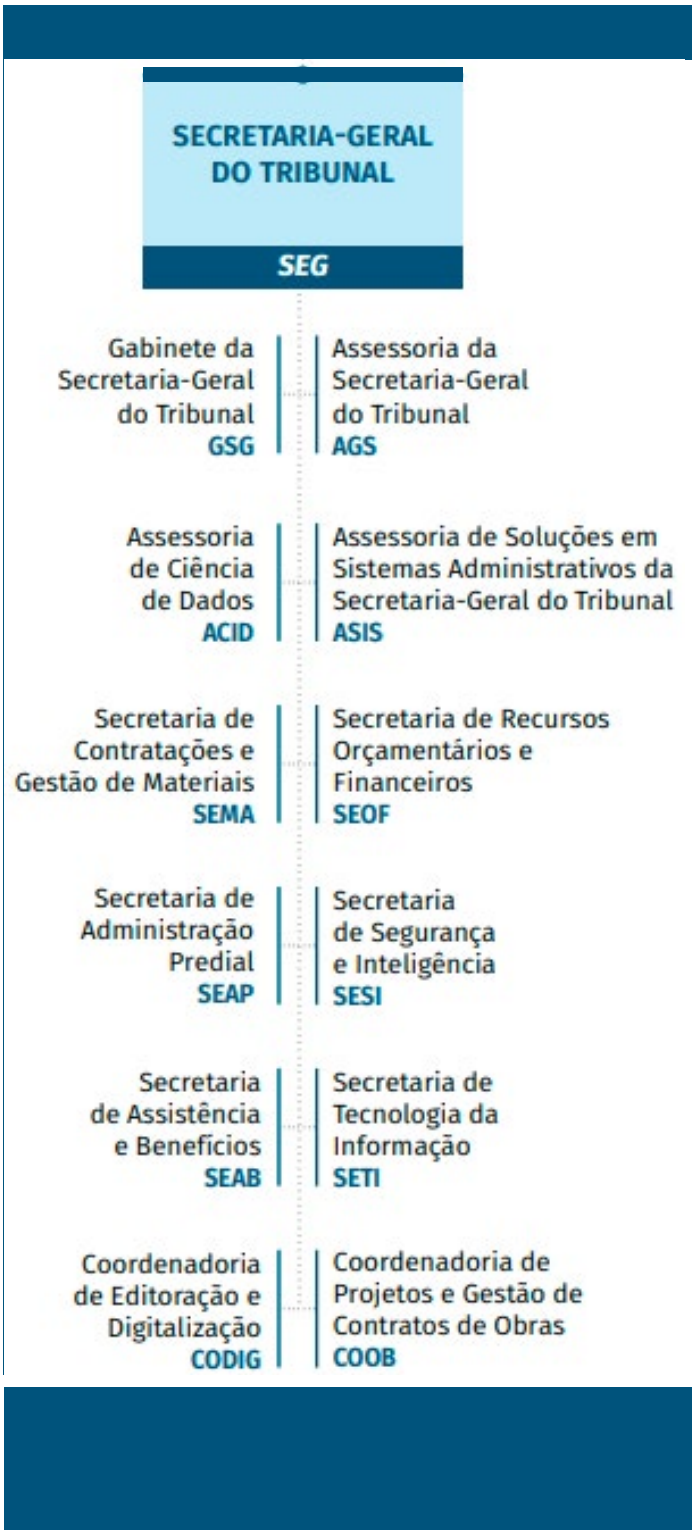

Figura 9 – Organograma do TJDFT – SEG. Fonte: Estrutura Organizacional. Tribunal de Justiça do Distrito Federal e dos Territórios. Brasília (DF), 2022. Disponível em: <https://www.tjdft.jus.br/transparencia/estrutura-organizacional>. Acesso em: 9 mar. 2022.

Figura 10 – Organograma do TJDFT – SEAI. Fonte: Estrutura Organizacional. Tribunal de Justiça do Distrito Federal e dos Territórios. Brasília (DF), 2022. Disponível em: <https://www.tjdft.jus.br/transparencia/estrutura-organizacional>. Acesso em: 9 mar. 2022.

Tendo como base o Modelo das Três Linhas e o tema de segurança cibernética, cabe a interpretação que a SETI representa a 1ª linha de defesa, pois, de acordo com o Plano Diretor de Tecnologia da Informação e de Comunicação de 2022 do TJDFT, "Em caso de incidentes graves e potenciais ameaças de segurança cibernética, a SETI deverá atuar imediatamente em ações preventivas ou resposta a incidentes" (Brasil, 2022e, p. 16).

Representando a 2ª linha de defesa, o TJDFT tem o Comitê Gestor de Segurança da Informação e Proteção de Dados Pessoais (CGSI), que tem como finalidade a garantia da integridade dos sistemas e procedimentos e a promoção da cultura de segurança da informação do tribunal (Distrito Federal, 2022e). Também compete ao CGSI "propor a elaboração e a revisão de normas e de procedimentos relativos à segurança da informação e ao tratamento de dados pessoais; promover, coordenar e acompanhar as ações relacionadas à segurança da informação e à proteção de dados pessoais" (Distrito Federal, 2020a, p. 3).

A responsabilidade da 3ª linha de defesa fica a cargo da SEAI, por operar de forma independente das outras linhas e responder diretamente à alta administração do TJDFT.

Não foi recepcionado despacho da ouvidoria confirmando que o CGSI continua ativo, porém, no site do TJDFT não é informada a revogação do comitê. Dessa forma, não é possível confirmar a ocorrência de reuniões regulares.

4.5 TRIBUNAL REGIONAL FEDERAL DA 1ª REGIÃO

A partir da estrutura disposta no organograma do TRF1 nas figuras 11 e 12, foi possível tirar conclusões sobre a estrutura organizacional do órgão sob o contexto de segurança cibernética. O organograma apresenta o Núcleo de Tecnologia da Informação (Nutec), que pertence à Secretaria Administrativa (Secad). O Nutec é composto pela Seção de Sistemas, Suporte Técnico e Infraestrutura (Sesis), que, por sua vez, é dividida em três setores. O Núcleo de Auditoria Interna (Nuaud) é apresentado separado das demais secretarias e núcleos.

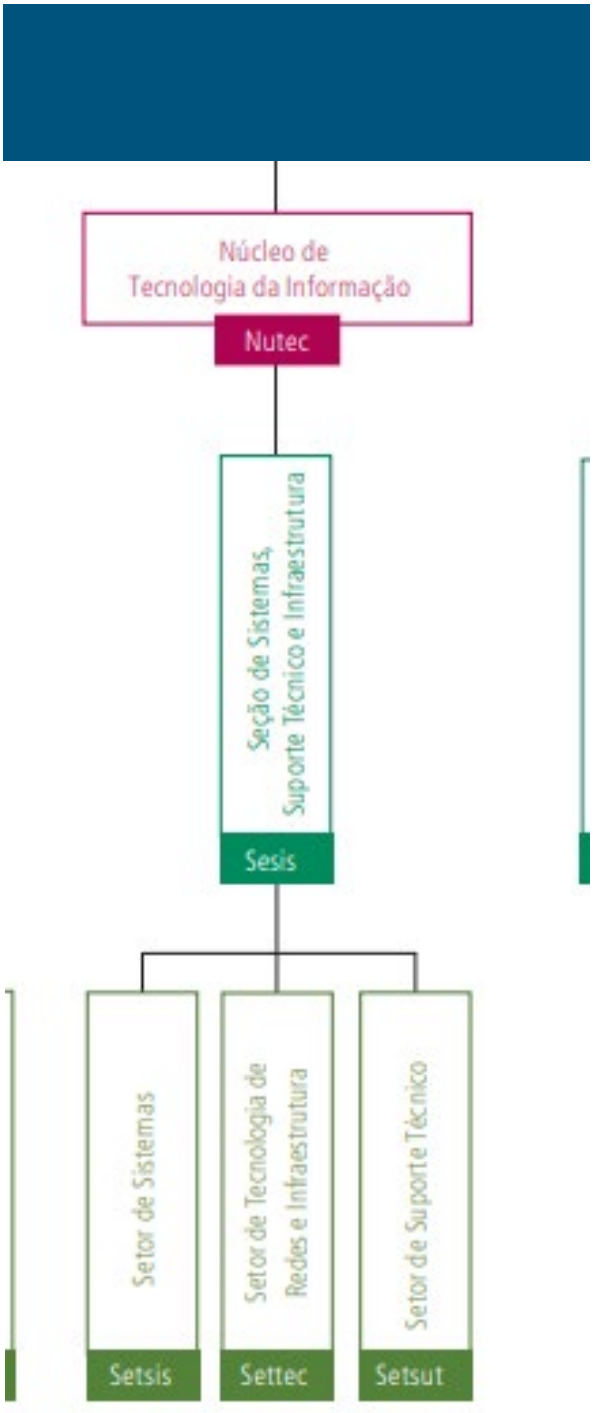

Figura 11 – Organograma do TRF1 – Nutec. Fonte: Área Administrativa: De acordo com a Portaria Diref 636, de 3 de novembro de 2021. Seção Judiciária do Distrito Federal. Brasília (DF), 2021. Disponível em: <https://portal.trf1.jus.br/portaltrf1/institucional/organizacao/organograma/organograma.htm>. Acesso em: 9 mar. 2022.

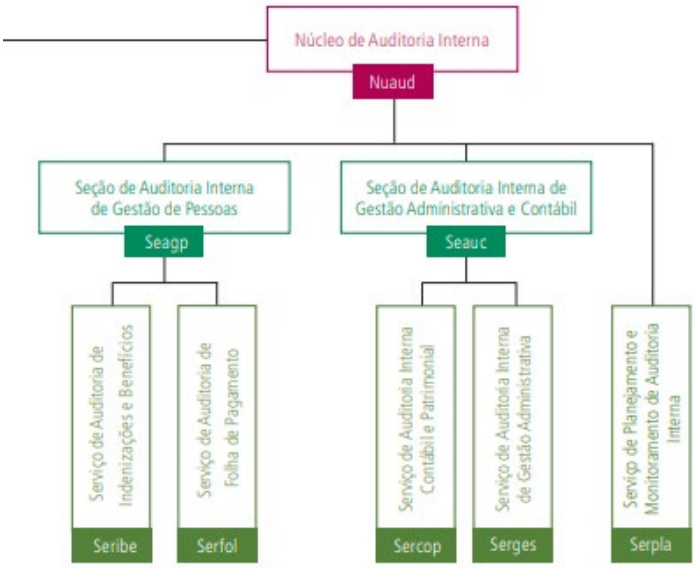

Figura 12 – Organograma do TRF1 – Nuaud. Fonte: Área Administrativa: De acordo com a Portaria Diref 636, de 3 de novembro de 2021. Seção Judiciária do Distrito Federal. Brasília (DF), 2021. Disponível em: <https://portal.trf1.jus.br/portaltrf1/institucional/organizacao/organograma/organograma.htm>. Acesso em: 9 mar. 2022.

No que tange ao Modelo das Três Linhas e segurança cibernética, interpreta-se como a 1ª linha de defesa do TRF1 a Nutec, considerando que, conforme a Portaria Diref n. 11858602, suas seções desempenham papéis de implementação e suporte dos sistemas, bem como outras competências típicas da unidade (Brasil, 2020b). Ademais, pode-se interpretar a Nutec também como 2ª linha, tendo como base que suas seções desempenham papéis de planejamento e supervisão dos sistemas do TRF1 (Brasil, 2020b).

O TRF1 é apoiado pelo Comitê de Governança e Tecnologia da Informação da Justiça Federal da 1ª Região (CGTI-JF1), que, em suas reuniões, aborda planos referentes à segurança da informação, como o Plano de Contratações de Soluções de Tecnologia da Informação e Comunicação (PCSTIC) de 2022, que teve como enfoque a segurança dos dados do Tribunal (Brasil, 2021). O CGTI-JF1, por ser apartado da estrutura organizacional do TRF1 e desempenhar esse tipo de função, também pode ser caracterizado como 2ª linha de defesa no contexto desta pesquisa.

A 3ª linha de defesa permanece atribuída à Nuaud, já que está apartada da Nutec e dos demais corpos funcionais do TRF1 e responde diretamente à alta administração. Complementando essa interpretação, a Portaria Diref n. 11858602 expressa que a Nuaud promove, coordena e orienta trabalhos de auditoria para avaliação da gestão de riscos (Brasil, 2020b).

Em despacho recebido da ouvidoria do TRF1, via pedido de acesso à informação, o CGTI-JF1 continua se reunindo regularmente.

4.6 TRIBUNAL SUPERIOR DO TRABALHO

O organograma do TST (figuras 13 e 14), disponibilizado em seu website oficial, possibilitou a análise de sua estrutura organizacional referente à segurança cibernética. É evidenciada a Secretaria de Tecnologia da Informação e Comunicação (SETIN), subordinada à Secretaria Geral da Presidência (SEGP). O organograma apresenta a Secretaria de Auditoria (SEAUD), composta por duas coordenadorias, em destaque a Coordenadoria de Auditoria de Gestão Administrativa (CAUGE), que engloba a Seção de Auditoria de Tecnologia da Informação e Comunicação (SAUTIC).

A SETIN, é composta de quatro coordenadorias, em destaque a Coordenadoria de Apoio à Governança e Gestão de Tecnologia da Informação e Comunicação (CGOV) e a Coordenadoria de Infraestrutura Tecnológica (CITEC). A CGOV é composta por quatro seções, uma delas sendo a Seção de Segurança da Informação e Proteção de Dados (SIPD), enquanto a CITEC tem seis seções, em destaque a Seção de Gerenciamento de Redes (SGRE).

Caracterizando a estrutura organizacional do TST no Modelo das Três Linhas e contextualizando-a em segurança cibernética, cabe à SETIN o papel de 1ª linha de defesa, executado pela CITEC e CGOV. A CITEC implementa melhorias na rede do TST, sendo um de seus objetivos a melhoria na segurança. Já a CGOV propõe modernizações do sistema de gestão da segurança da informação, por meio de compras e contratações de ativos de segurança e revisões nos processos de segurança da informação.

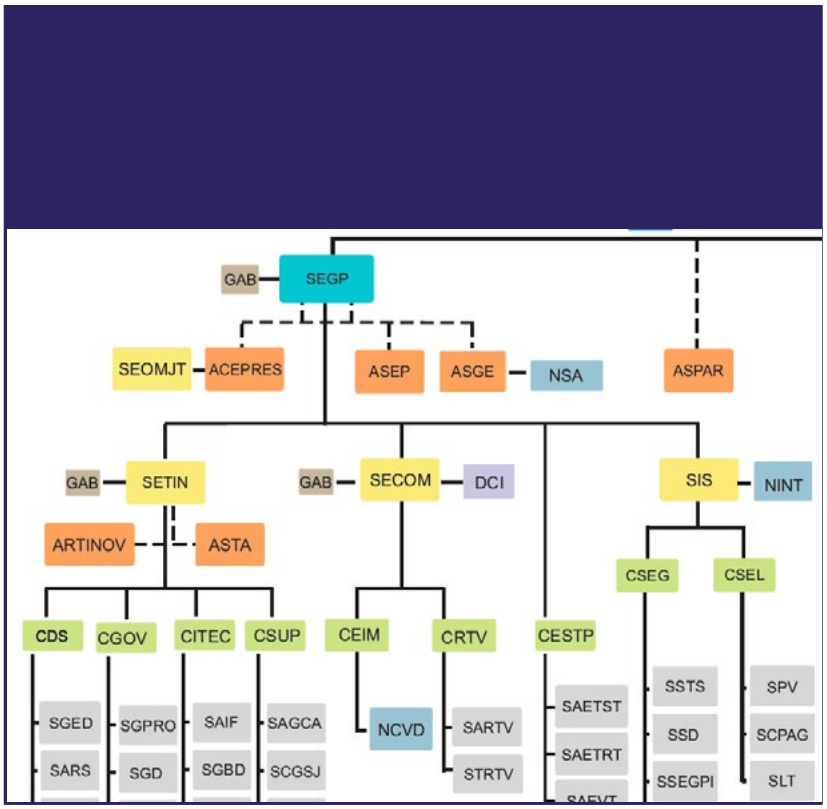

Figura 13 – Organograma do TST – SETIN. Fonte: Estrutura Organizacional. Tribunal de Justiça do Distrito Federal e dos Territórios. Brasília (DF), 2022. Disponível em: <https://www.tst.jus.br/web/acesso-a-informacao/organograma>. Acesso em: 9 mar. 2022.

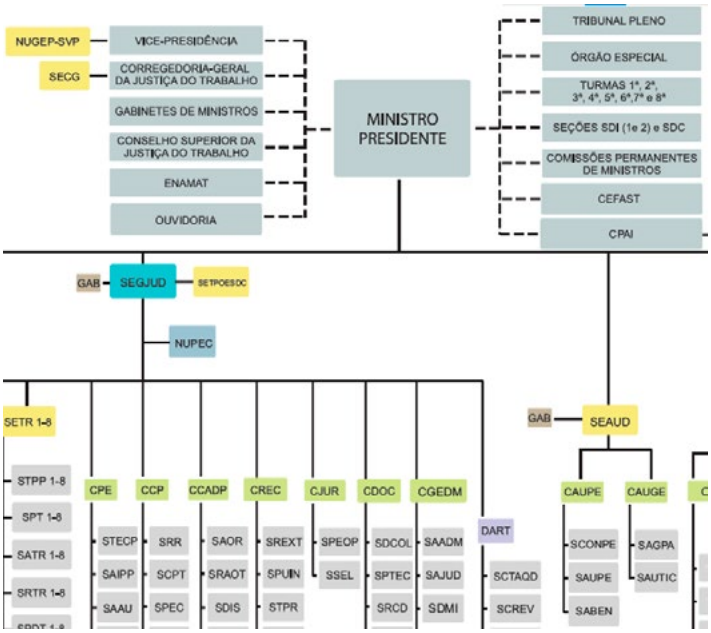

Figura 14 – Organograma do TST – SEAUD. Fonte: Estrutura Organizacional. Tribunal de Justiça do Distrito Federal e dos Territórios. Brasília (DF), 2022. Disponível em: <https://www.tst.jus.br/web/acesso-a-informacao/organograma>. Acesso em: 9 mar. 2022.

No Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC 2020), as soluções e melhorias propostas pela CITEC esperam gerar, em seus benefícios esperados, maior segurança às soluções para os usuários do TST (Brasil, 2020). Os projetos da CGOV, dispostos no PDTIC 2020, incluem propostas de aprimoramento de maturidade em relação à segurança da informação e modernização do sistema de gestão de segurança da informação do TST, visando atender à ENSEC-PJ (Brasil, 2020).

No âmbito da 2ª linha de defesa, pode-se interpretar que a CGOV tem funções de planejamento e supervisão em relação à segurança da informação do TST, entretanto, não estaria apartada da 1ª linha, pois compõe a SETIN. Já o Comitê de Governança de Tecnologia da Informação e Comunicação (CGTI) tem atribuições que justificariam sua classificação como 2ª linha, além de não integrar diretamente à SETIN. De acordo com o Ato n. 65/TST.GP, de 6 de abril de 2021, que institui o CGTI, destacam-se as seguintes competências do comitê:

> VIII – Formular propostas de políticas, objetivos, estratégias, indicadores e metas institucionais, investimentos e prioridades de TIC; […]
>
> XIV – Avaliar e monitorar a execução do PDTIC, do PCSTIC e demais instrumentos estratégicos de TIC, recomendando, quando couber, ações de aperfeiçoamento; […]
>
> XVI – Recomendar e acompanhar a adoção de boas práticas de governança de TIC, assim como a eficácia e a efetividade de seus processos, propondo atualizações e melhorias quando necessário (Brasil, 2021f, p. 2).

A CAUGE, por responder diretamente à alta administração do TST e atuar de forma independente das demais secretarias, encaixa-se no papel de 3ª linha de defesa do Tribunal. A partir do organograma, é válida a interpretação de que a SAUTIC é diretamente responsável por auditar os processos relacionados à segurança da informação.

O último registro de reunião do CGTI foi publicado em 7 de outubro de 2021, porém não foi recepcionado despacho da ouvidoria confirmando se essa foi a reunião mais recente. Considerando o ato que institui o CGTI, as reuniões ocorrem trimestralmente, portanto, infere-se que o comitê continua se reunindo.

4.7 TABELA RESUMO E DISCUSSÃO

A Tabela 1 mostra a síntese dos resultados obtidos pela análise documental sobre os tribunais do Poder Judiciário do DF, e busca destacar as principais diferenças entre eles. Foi analisado se o tribunal tem um setor específico de segurança da informação (SI), se esse setor fica apartado do setor de tecnologia da informação e comunicações (TIC), se existe um comitê de segurança da informação ativo e se esse comitê se reúne regularmente.

TABELA 1 – **SÍNTESE DOS RESULTADOS OBTIDOS**

Tribunal	Setor específico de SI	Setor de SI apartado da TIC	Comitê de SI	Comitê se reúne
STF	SIM	SIM	SIM	SIM
STJ	SIM	NÃO	SIM	SIM
STM	SIM	NÃO	SIM	NÃO
TJDFT	NÃO	NÃO	SIM	NÃO
TRF1	NÃO	NÃO	SIM	SIM
TST	SIM	NÃO	SIM	SIM

Fonte: Elaboração própria

Percebe-se que o STF se destaca entre os demais tribunais por ser o único a ter, dentro do Gabinete da Presidência, um setor de assessoria de segurança da informação apartado do setor de TI, que é a STI. Além de apresentar essa estrutura interna, ele também conta com um comitê focado em segurança da informação ativo.

A estrutura organizacional apresentada no STF propõe um cenário ótimo na ótica de gestão de riscos, considerando que as três linhas estão dispostas de forma adequada para o modelo, gerando maior probabilidade de os riscos e controles serem gerenciados com eficiência (Anderson; Eubanks, 2015). Com base no cenário observado, e conforme Potter e Toburen (2016), o STF reage com mais eficácia às ameaças e o órgão como um todo tem a tendência de ser mais inteligente perante os riscos.

Constatou-se que o STJ, o TST e o STM têm coordenadorias específicas de segurança da informação dentro de sua estrutura organizacional, a CSID, CGOV, e COTEC respectivamente. Entretanto, são integrantes do setor de TIC e não estão apartadas da 1ª linha de defesa. De acordo com o IIA (2020), a combinação dos papéis da 1ª e da 2ª linha é possível dentro do modelo, permitindo a atribuição de funções de supervisão para especialistas dentro das coordenadorias.

Os dados obtidos não foram suficientes para comprovar a existência de um setor focado em segurança da informação no TJDFT e no TRF1, que, por consequência, têm apenas comitês que desenvolvem políticas e ações relacionadas ao tema. Jamison et al. (2018) discorrem sobre a possível desordem causada pela mistura dos papéis da 1ª e 2ª linha em organizações que não têm um setor específico de segurança da informação. No cenário analisado, apenas o STF tem esse setor efetivamente apartado do setor de TIC, então pode-se interpretar que o STJ, o STM e o TST não estão em condições ideais para segurança cibernética de acordo com o Modelo das Três Linhas.

No que tange às semelhanças entre os tribunais, a principal é a existência de comitês de segurança da informação em todos eles, conforme previsto na ENSEC-PJ. Os dados obtidos endossam a ideia de que os comitês estão ativos, apoiando e desenvolvendo políticas de segurança da informação nos órgãos analisados. O IIA (2013) admite a 2ª linha na forma de comitê, com o objetivo de facilitar e monitorar práticas de gestão de riscos e auxiliar a gestão operacional no tratamento direto dos riscos.

Observou-se, também, que todos os órgãos analisados têm o setor de auditoria interna independente das demais secretarias e coordenadorias e diretamente subordinada à alta administração do tribunal, encaixando-se com facilidade na função de 3ª linha de defesa.

Por mais que seja admitida a presença de um comitê como 2ª linha de defesa, o fato de não ser um corpo efetivamente integrante da estrutura organizacional do tribunal pode resultar na mesclagem das responsabilidades da 2ª e 3ª linha, o que invalidaria o propósito do modelo, visto que ambas as linhas não seriam independentes (Kumar, 2021). Bantleon *et al*. (2020) complementam essa afirmação ao dizer que os recursos de cada linha não são intrinsecamente independentes, podendo causar a perda de benefícios do modelo por falta de coordenação entre as linhas.

A existência do comitê de segurança da informação é predominante nos tribunais, de modo a atender à ENSEC-PJ; porém, não foi possível comprovar que todos os comitês se reúnem regularmente pelo despacho das ouvidorias. O IIA (2020) discorre que é necessária a colaboração entre todas as linhas de defesa, pois deve haver uma interação regular entre a gestão e a auditoria interna. Portanto, o STM e o TJDFT podem não atender essa orientação do IIA, pois não foi confirmada a existência das reuniões regulares de seus respectivos comitês.

5 CONCLUSÕES

A análise de conteúdo realizada nos tribunais do Poder Judiciário do DF demonstrou que, partindo dos conceitos do Modelo das Três Linhas do IIA, a 2ª linha de defesa dentro de segurança cibernética está presente predominantemente na forma de comitês de segurança da informação. Considerando a definição da ENSEC-PJ da obrigatoriedade da existência de um Comitê de Governança de Segurança da Informação e suas respectivas funções, justifica-se a atribuição de 2ª linha de defesa a esses comitês.

Verificou-se, ainda, o não cumprimento do art. 21 da ENSEC-PJ pelos tribunais subordinados a ela, que afirma: "Cada órgão do Poder Judiciário, com exceção do STF, deverá constituir estrutura de segurança da informação, subordinada diretamente à alta administração do órgão e desvinculada da área de TIC" (Conselho Nacional de Justiça, 2021a). A partir da documentação analisada, não foram encontradas evidências de que os tribunais subordinados à ENSEC-PJ atendem essa exigência.

Considerando o cenário dos recentes ataques cibernéticos aos órgãos do Poder Judiciário, fica evidente a necessidade de constante modernização da estrutura de segurança da informação, de modo a evitar a indisponibilidade dos sistemas dos tribunais e a perda ou vazamento de dados de cidadãos e entidades brasileiras. A adequação ao Modelo das Três Linhas para a estrutura de segurança cibernética dentro dos tribunais pode reforçar as políticas de segurança e prevenir a incidência dos riscos cibernéticos, entretanto, seriam necessárias mudanças na própria estrutura organizacional dos órgãos.

Esta pesquisa buscou fontes de documentos oficiais disponibilizados nas páginas web dos tribunais e utilizou a solicitação de acesso à informação para realizar a análise de suas estruturas e contextualizá-las no Modelo das Três Linhas, dentro de segurança cibernética. Por consequência, foram encontradas limitações, sendo elas a ausência de respostas das ouvidorias do TJDFT e do TST, além da eventual indisponibilidade de documentos atualizados nas páginas oficiais dos tribunais.

Como sugestão para trabalhos futuros, propõe-se avaliar, em função de uma eventual carência de profissionais habilitados na área de segurança da informação, em que medida os integrantes dos comitês de gestão de segurança atuam concomitantemente na 1ª linha de defesa, caracterizando a sobreposição entre a 1ª e a 2ª linha e uma possível descaracterização da aplicação do modelo. Ademais, pode-se analisar outros órgãos do Poder Judiciário, fora do DF, e pela perspectiva de outros modelos e *frameworks* de gestão de riscos aplicáveis à segurança cibernética. Pode-se pesquisar, também, a existência de planos futuros de adequação da estrutura organizacional dos tribunais analisados, de modo a atender integralmente a Ensec-PJ.

REFERÊNCIAS

ALVES, R.S; GEORG, M. A. C; NUNES, R. R. Judiciário sob ataque hacker: riscos de negócio para a segurança cibernética em tribunais brasileiros. *Revista Ibérica de Sistemas e Tecnologias de Informação*: RISTI, Porto, n. E56, p. 344-357, 2023.

ANDERSON, D. J.; EUBANKS, G. *Leveraging COSO across*: the three lines of defense. Carolina do Norte, US: Committee of Sponsoring Organizations of the Treadway Commission, July 2015. Disponível em: https://riskcue.id/uploads/ebook/20211013105542-2021-10-13ebook105459.pdf. Acesso em: 26 abr. 2022.

ANDERSEN, T.J. (ed.). P*erspectives on strategic risk management*: risk management. Copenhagen: Copenhagen Business School Press, 2016.

ARAÚJO, M. de. A gestão de riscos no **âmbito** da transformação digital. *TI INSIDE*, Transformação Digital, São Paulo, 15 set. 2021. Disponível em: https://tiinside.com.br/15/09/2021/a-gestao-de-riscos-no-ambito-da-transformacao-digital/. Acesso em: 26 abr. 2022.

ASSI, M. *Gestão de riscos com controles internos.* São Paulo: Saint Paul, 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *Norma brasileira ABNT ISO/IEC 31000*: gestão de riscos: diretrizes. Rio de Janeiro: ABNT, 2018.

BANTLEON, U.; D'ARCY, A.; EULERICH, M.; HUCKE, A.; PEDELL, B.; RATZINGER-SAKEL, N.V.S. Coordination challenges in implementing the three lines of defense model. *International Journal of Auditing*: IJA, [London], v. 25, n. 1, p. 59-74, Mar. 2021. Disponível em: https://onlinelibrary.wiley.com/doi/full/10.1111/ijau.12201. Acesso em: 23 fev. 2022.

BARDIN, L. *Análise de conteúdo*. São Paulo: Almedina Brasil, 2016.

BEVAN, O.; BOEHM, J.; MANOCARAN, M.; RIEMENSCHNITTER, R. *Cybersecurity and the risk function.* [Washington, D.C.]: McKinsey&Company, 2018.

BONISCH, P. Excuse me, how many lines of defence?: the new financial Maginot lines. *Thinking about Strategy & Uncertainty*, [*S.l.*], 18 mar. 2013. Disponível em: https://paradigmrisk.wordpress.com/2013/03/18/excuse-me-how-many-lines-of-defence-the-new-financial-maginot-lines/. Acesso em: 5 abr. 2022.

BRASIL. Ministério da Transparência; CONTROLADORIA-GERAL DA UNIÃO. *Instrução normativa nº 3, de 9 de junho de 2017.* Brasília, DF: Diário Oficial da União, 2017a.

BRASIL. Superior Tribunal de Justiça. *Instrução normativa STJ/GP n. 5, de 28 de março de 2017.* Brasília, DF: Superior Tribunal de Justiça, 2017b.

BRASIL. Superior Tribunal de Justiça. *Plano Diretor de Tecnologia da Informação e Comunicação*. Brasília, DF, 2021. Disponível em: https://www.stj.jus.br/publicacaoinstitucional/index.php/PDTIC/issue/archive. Acesso em: 03 mar. 2022.

BRASIL. Superior Tribunal de Justiça. *Portaria STJ/GDG n. 178, de 12 de março de 2021*. Brasília, DF: Superior Tribunal de Justiça, 2021c.

BRASIL. Superior Tribunal de Justiça. *Resolução STJ/GP n. 11, de 12 de novembro de 2015.* Brasília, DF: Superior Tribunal de Justiça, 2015.

BRASIL. Supremo Tribunal Federal. *Resolução n. 612, de 23 de abril de 2018.* Brasília, DF: Supremo Tribunal Federal, 2018.

BRASIL. Superior Tribunal Militar. *Resolução n. 222, de 3 de fevereiro de 2016.* Brasília, DF: Superior Tribunal Militar, 2016.

BRASIL. Superior Tribunal Militar. *Resolução n. 298, de 4 de agosto de 2021.* Brasília, DF: Superior Tribunal Militar, 2021d.

BRASIL. Superior Tribunal Militar. *Resolução n. 301, de 8 de setembro de 2021.* Brasília, DF: Superior Tribunal Militar, 2021e.

BRASIL. Tribunal Regional Federal (1. Região). Seção Judiciária do Distrito Federal. *Regulamento de serviço das unidades administrativas da Diretoria do foro e da Secretaria administrativa da Seção Judiciária do Distrito Federal.* Brasília, DF: Seção Judiciária do Distrito Federal, 2020b.

BRASIL. Tribunal Regional Federal (1. Região). Institucional: segurança da informação é prioridade no Plano de Contratações de Soluções de TI 2022 do TRF1. *Tribunal Regional Federal da 1ª Região,* Brasília, DF, 25 nov. 2021. Disponível em: https://portal.trf1.jus.br/. Acesso em: 5 fev. 2022.

BRASIL. Tribunal Superior do Trabalho. *Ato n. 65/TST.GP, de 6 de abril de 2021*. Brasília, DF: Tribunal Superior do Trabalho, 2021f.

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

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

CHAMBERS, A. D.; ODAR, M. A new vision for internal audit. *Managerial Auditing Journal*, Bradford, GB, v. 30, n. 1, p. 34-55, 2015.

CONSELHO NACIONAL DE JUSTIÇA (Brasil). *Resolução n. 396, de 7 de junho de 2021.* Brasília, DF: Conselho Nacional de Justiça, 2021a.

CRAIGEN, D.; DIAKUN-THIBAULT, N.; PURSE, R. Defining cybersecurity. *Technology Innovation Management Review*, [Stanford], v. 4, n. 10, p. 13-21, Oct. 2014.

DAMODARAN, A. *Gestão estratégica do risco*: uma referência para a tomada de riscos empresariais. Porto Alegre: Bookman, 2009.

DAVIES, H.; ZHIVITSKAYA, M. Three lines of defence: a robust organising framework, or just lines in the sand? *Global Policy*, [Durham], Special Issue, v. 9, p. 34-42, 2018. Disponível em: https://onlinelibrary.wiley.com/doi/10.1111/1758-5899.12568. Acesso em: 10 ago. 2021.

DISTRITO FEDERAL (Brasil). Tribunal de Justiça do Distrito Federal e dos Territórios *Portaria GPR 1204, de 02 de julho de 2020*. Brasília, DF: Tribunal de Justiça do Distrito Federal e dos Territórios, 2020a.

DISTRITO FEDERAL (Brasil). Tribunal de Justiça do Distrito Federal e dos Territórios. *PDTIC 2022*: Plano Diretor de Tecnologia da Informação e de Comunicação. Brasília, DF: TJDFT, 2022e. Disponível em: https://www.tjdft.jus.br/transparencia/governanca-de-tic/planejamento-de-tic/pdtic/pdtic-2022.pdf. Acesso em: 3 mar. 2022.

FLICK, U. U*ma introdução à pesquisa qualitativa.* Porto Alegre: Bookman, 2004.

GEORG, Marcus Aurélio Carvalho; RODRIGUES, Walisson Magno Silva; ALVES, Carlos André de Melo; SILVEIRA, Aldery, Júnior; NUNES, Rafael Rabelo. Os desafios da segurança cibernética no setor público federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação. RISTI: Revista Ibérica de Sistemas e Tecnologias de Informação, Lousada, n.E54, p. 602-616, nov. 2022. Disponível em: https://www.proquest.com/openview/d9b50e81659401d470649f6580c8cf2a/1?pq-origsite=gscholar&cbl=1006393. Acesso em: 12 mar. 2024.

GIL, A. C. *Métodos e técnicas de pesquisa social.* São Paulo: Atlas, 2008.

GLYNN, C. *et al. Internal audit and the second line of defense*. Amsterdam, NL: Intituut van Internal Auditors, 2016.

INSTITUT OF INTERNAL AUDITORS (Brasil). *Modelo das três linhas do IIA 2020.* Florida, US: IIA, 2020. Disponível em: https://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/20200758glob-th-editorHTML-00000013-20072020131817.pdf. Acesso em: 30 abr. 2023.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 27000: Information technology – Security techniques – Information security management systems – Overview and vocabulary.* Vernier, CH: ISO/IEC, 2018.

INTERNATIONAL TELECOMMUNICATION UNION. Understanding cybercrime: a guide for developing countries. *Technical Report*, ITU-D ICT Applications and Cybersecurity Division, Geneva, CH, 2009. Disponível em: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf. Acesso em: 14 out. 2021.

JAMISON, J.; MORRIS, L.; WILKINSON, C. *The future of cybersecurity in internal audit.* [*S.l.*]: Internal Audit Foundation, 2018.

KUMAR, S. Overlap between second and third line of defense for risk management. *SSRN*, Oct. 7, 2021. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3938315. Acesso em: 9 fev. 2022.

LAGINESTRA, A.M.; OLIVEIRA, C.G.; BRAREN, I.; Freitas, J. *Cibersegurança no território brasileiro*: impacto da LGPD e normas de segurança da informação na defesa nacional. Abian Laginestra, Rio de Janeiro, 2021. Disponível em: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2022/01/ciberseguranca-no-territorio-brasileiro-impacto-da-lgpd-e-normas-de-seguranca-da-informacao-na-defesa-nacional.pdf. Acesso em: 10 ago. 2021.

LUBURIC, R.; PEROVIC, M.; RAJKO, S. Quality management in terms of strengthening the "three lines of defence" in risk management: process approach. *International Journal for Quality Research,* [Montenegro, RS], p. 243-250, 2015. Disponível em: https://www.researchgate.net/publication/279180559_Quality_Management_in_terms_of_strengthening_the_Three_Lines_of_Defence_in_Risk_Management_-_Process_Approach. Acesso em: 10 ago. 2021.

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,* [Glasgow, UK], v. 12, n. 1, p. 53-69, 2017. Disponível em: https://researchonline.gcu.ac.uk/ws/portalfiles/portal/24077798/Submitted_version.pdf. Acesso em: 9 fev. 2022.

MINAYO, M. *Pesquisa social*: teoria, método e criatividade. Rio de Janeiro: Vozes, 2009.

MONTEZANO, L.; DA COSTA JÚNIOR, R. L.; RAMOS, K. H. C; MELCHIADES, A. T. Percepção de servidores públicos quanto à implementação da gestão de riscos em uma secretaria do governo federal do Brasil. *Revista Economia & Gestão,* Belo Horizonte, p. 77-94, 2019. Disponível em: https://periodicos.pucminas.br/index.php/economiaegestao/article/view/19310. Acesso em: 11 abr. 2022.

MOURA, R. M. A impunidade dos hackers que colocaram o Judiciário de joelhos. *Veja,* Política, São Paulo, 28 mar. 2022. Disponível em: https://veja.abril.com.br/politica/a-impunidade-dos-hackers-que-colocaram-o-judiciario-de-joelhos/. Acesso em: 11 abr. 2022.

NUNES, P. F. V. A definição de uma estratégia nacional de cibersegurança: cibersegurança. *Nação e Defesa*, Lisboa, n. 133, 5. Série, p. 113-127, 2012. Disponível em: https://www.idn.gov.pt/pt/publicacoes/nacao/Documents/NeD133/NeD133_PauloFernandoViegasNunes_Resumo.pdf. Acesso em: 5 ago. 2021.

NUNES, R. R.; PERINI, M. T. B. S.; PINTO, I. E. M. M. A gestão de riscos como instrumento para a aplicação efetiva do princípio constitucional da eficiência. *Revista Brasileira de Políticas Públicas*, Brasília, DF, v. 11, n. 3, 2021. Disponível em: https://doi.org/10.5102/rbpp.v11i3.7903. Acesso em: 30 abr. 2022.

OLLAIK, L. G. *Táxigov*: inovando no serviço de mobilidade de servidores. Brasília, DF: ENAP; Secretaria de Gestão (SEGES/MP), 2018. (Coleção: Casos SEGES renovando a gestão pública). Disponível em: https://repositorio.enap.gov.br/handle/1/3454. Acesso em: 30 abr. 2022.

POTTER, P.; TOBUREN, M. The 3 lines of defense for good risk management. *Risk Management, New York,* p. 16. 2016, Disponível em: https://www.rmmagazine.com/articles/article/2016/06/01/-The-3-Lines-of-Defense-for-Good-Risk-Management-. Acesso em: 5 ago. 2021.

PRADO, F. Brasil foi 5º país com mais ataques cibernéticos no ano: relembre os principais. *Isto é Dinheiro,* São Paulo, 20 dez. 2021. Disponível em: https://www.istoedinheiro.com.br/brasil-foi-5o-pais-com-mais-ataques-ciberneticos-no-ano-relembre-os-principais/. Acesso em: 8 abr. 2022.

RALO, T. J. Artigo de opinião: cibersegurança e ciberdefesa, direção geral de política de defesa nacional. *Direção-Geral de Política de Defesa Nacional,* [Lisboa], 25 mar. 2013. Disponível em: http://dgpdn.blogspot.com/2013/03/artigo-de-opiniao-ciberseguranca-e.html. Acesso em: 10 out. 2021.

UDDING, A. Three lines of defence: a panacea? *AXVECO*, Utrecht, NL, 1 nov. 2016. Disponível em: https://axveco.com/three-lines-of-defence-a-panacea/. Acesso em: 10 fev. 2022.

VALENTE, J. Brasil é o país com maior número de vítimas de phishing na internet. *InfoMoney,* São Paulo, 4 mar. 2021. Disponível em: https://www.infomoney.com.br/consumo/brasil-e-o-pais-com-maior-numero-de-vitimas-de-phishing-na-internet/. Acesso em: 11 abr. 2022.

VAN MAANEN, J. Reclaiming qualitative methods for organizational research: a preface. *Administrative Science Quarterly,* [*S.l.*], v. 24, n. 4, p. 520-526, Dec. 1979. Disponível em: https://www.jstor.org/stable/2392358. Acesso em: 9 fev. 2022.

VOUSINAS, G. L. Beyond the three lines of defense: the five lines of defense model for financial institutions. *ACRN Journal of Finance and Risk Perspectives*, Oxford, p. 95-110, 2021.

WHITMAN, M. E.; MATTORD, H. J. *Principles of information security.* Georgia, US: Cengage Learning, 2018.

Artigo recebido em 11/5/2023.
Artigo aprovado em 27/10/2023.

Renato Solimar Alves é gestor de Segurança da Informação e Tecnologia da Informação com atuação na proteção dos recursos tecnológicos no Poder Judiciário há 15 anos. É membro ativo do Comitê Gestor de Segurança da Informação do Poder Judiciário, e contribuiu para a definição e implementação de políticas e diretrizes que fortalecem a postura de segurança cibernética e a resposta a incidentes de segurança no âmbito judiciário. Mestre em Engenharia Elétrica, com especialização em Engenharia de Sistemas, graduando-se previamente em Tecnologia de Telecomunicações Móveis.

Carlos Eduardo Mancini Queiroz é bacharel em Administração pela Universidade de Brasília (UnB) e atuante nas áreas de Tecnologia da Informação e Desenvolvimento de Software. Analista de Sistemas Pleno na BRB Seguros, desempenha um papel na implementação de soluções desde 2022.

Rafael Rabelo Nunes é Professor Adjunto da Universidade de Brasília (UnB), em regime parcial. Também atua na Gestão de Riscos de Segurança da Informação no Supremo Tribunal Federal, e como Professor no Centro Universitário UniAtenas. É Doutor em Engenharia Elétrica pela UnB.