Universidade de Brasília
Faculdade de Administração, Contabilidade, Economia e Gestão de Políticas Públicas
Departamento de Administração

CARLOS EDUARDO MANCINI QUEIROZ

ANÁLISE DAS ESTRUTURAS DE SEGURANÇA CIBERNÉTICA EM TRIBUNAIS DO DISTRITO FEDERAL: UM ESTUDO À LUZ DAS TRÊS LINHAS DE DEFESA

Brasília – DF
2022

CARLOS EDUARDO MANCINI QUEIROZ

ANÁLISE DAS ESTRUTURAS DE SEGURANÇA CIBERNÉTICA EM TRIBUNAIS DO DISTRITO FEDERAL: UM ESTUDO À LUZ DAS TRÊS LINHAS DE DEFESA

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

Professor Orientador:
Dr. Rafael Rabelo Nunes

Brasília – DF
2022

ANÁLISE DAS ESTRUTURAS DE SEGURANÇA CIBERNÉTICA EM TRIBUNAIS DO DISTRITO FEDERAL: UM ESTUDO À LUZ DAS TRÊS LINHAS DE DEFESA

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

Carlos Eduardo Mancini Queiroz

Dr. Rafael Rabelo Nunes
Professor-Orientador

Dr. Aldery Silveira Júnior
Professor-Examinador

Dr. José Humberto da Cruz Cunha
Professor-Examinador

Brasília, 05 de maio de 2022

AGRADECIMENTOS

Agradeço primeiramente ao Professor Dr. Rafael Rabelo Nunes, meu orientador, pelo constante apoio ao longo do desenvolvimento deste trabalho e pela sugestão do tema de pesquisa. Agradeço também aos amigos que fiz durante o curso de administração na UnB e aos meus familiares, que sempre me apoiaram no decorrer do curso.

“Your time is limited, so don't waste it living someone else's life. Don't be trapped by dogma – which is living with the results of other people's thinking.” – Steve Jobs

RESUMO

Ataques cibernéticos no setor público ganharam força nos últimos anos, impactando significativamente a disponibilidade de serviços providos pelo Estado. Dentro desse cenário, o Poder Judiciário tornou-se um alvo de grande destaque para os grupos *hackers*. Este trabalho teve como objetivo avaliar a existência de uma segunda linha de defesa dentro da estrutura de segurança cibernética dos órgãos do Poder Judiciário do Distrito Federal, baseado no Modelo das Três Linhas publicado pelo Instituto dos Auditores Internos. Para isso, foram levantados documentos tais como organogramas, portarias, atos normativos, planos estratégicos e demais documentos oficiais e realizada análise de conteúdo para comparar com a estrutura de segurança cibernética aplicada ao Modelo das Três Linhas. Os resultados demonstraram a existência da segunda linha de defesa nos órgãos analisados e em que forma está operando em cada tribunal. Este estudo oferece uma visão acerca da estrutura organizacional sobre segurança cibernética dos órgãos do Judiciário do Distrito Federal, elucidando recomendações para se adequarem à luz do Modelo das Três Linhas e propondo uma possível avaliação futura referente à adequação à Estratégia Nacional de Segurança Cibernética do Poder Judiciário.

Palavras-chave:
Modelo das Três Linhas, Segurança Cibernética, Segurança da Informação, Tribunais, Judiciário.

LISTA DE ILUSTRAÇÕES FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

ABNT – Associação Brasileira de Normas Técnicas

AECI – Assessores e Assessorias Especiais de Controle Interno

ENSEC-PJ – Estratégia Nacional de Segurança Cibernética do Poder Judiciário

IIA – Instituto dos Auditores Internos

ISSO – International Organization for Standardization

ITU – International Communication Union

LGDP – Lei Geral de Proteção de Dados Pessoais

SI – Segurança da Informação

STF – Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

STM – Superior Tribunal Militar

TIC – Tecnologia da Informação e Comunicações

TJDFT – Tribunal de Justiça do Distrito Federal e dos Territórios

TRF1 – Tribunal Regional Federal da 1ª Região

TST – Tribunal Superior do Trabalho

Sumário

1. INTRODUÇÃO

Com o passar dos anos, organizações públicas e privadas vêm se atualizando com cada vez mais sofisticação, buscando as melhores práticas de segurança e otimização de negócio de acordo com seu nível de complexidade e área de atuação. Serviços ficaram mais acessíveis à população, a criação de novos negócios ficou mais ágil e a competitividade no mundo das corporações aumentou de forma excepcional.

De acordo com Araújo (2021), no atual cenário da transformação digital, as companhias devem desenvolver ações organizacionais, visando a 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 todos as atividades da organização. O fácil acesso a dados estruturados e não estruturados é um dos principais benefícios da tecnologia para a gestão de riscos hoje, trazendo grande agilidade na elaboração de relatórios e qualidade para a tomada de decisão (COMO, 2017).

Como consequência da evolução dos riscos no ambiente cibernético, o tema de segurança cibernética ganhou força e a necessidade de ação para prevenção de ataques e resposta a incidentes tornou-se altamente relevante para o mundo corporativo. Como exemplos de movimentações internacionais, podemos citar a criação do *National Institute of Standards and Technlogy* pelos EUA, o Centro Nacional de Cibersegurança pelo Reino Unido e o Centro de Cibersegurança Australiano, todos focados em administrar a segurança cibernética (GUERRA, 2022).

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 5º país que mais sofreu crimes cibernéticos, sendo que o primeiro trimestre do ano já havia mais ocorrências de crimes cibernéticos que o ano de 2020 inteiro (PRADO, 2021).

Um acontecimento notório que aconteceu em fevereiro de 2022, foi o incidente de segurança da Americanas, que teve seus ambientes de e-commerce suspensos após a identificação de um “acesso não autorizado”, interrompendo a operação de suas outras marcas Submarino e Shoptime (AMERICANAS, 2022). Outro caso notável foi o ataque *ransomware* pelo grupo *hacker* Lapus$ ao site ConecteSUS e à página do Ministério da Saúde, que ocasionou na indisponibilidade do serviço de emissão do Certificado Nacional de Vacinação,

impactando cidades do país onde o comprovante de vacinação estava sendo exigido em locais de uso público (APLICATIVO, 2021)

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, então a necessidade de estratégias para garantir a segurança dessas informações tornou-se crítica. Em março de 2022, o Governo Federal lançou o Plano Tático de Combate a Crimes Cibernéticos, que une a Polícia Federal e a Federação Brasileira de Bancos em cooperação, buscando facilitar o compartilhamento de informações e tornar o espaço cibernético mais seguro (BRASIL, 2022a).

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).

Considerando esse cenário, esta pesquisa buscou comparar as estruturas de segurança cibernética dos órgãos do Poder Judiciário do Distrito Federal à luz de um modelo de gestão de riscos comumente utilizado, o Modelo das Três Linhas. A ideia da divisão da estrutura de gestão de riscos em três linhas de defesa possui por natureza uma alta aplicabilidade, podendo então ser considerada na segurança cibernética para a análise realizada neste trabalho. Outro fator que se busca abordar é a avaliação da existência da segunda linha de defesa descrita no modelo, visto que uma eventual mistura entre a primeira e segunda linha pode não ser ideal para algumas organizações.

O Modelo das Três Linhas, publicado pelo Instituto dos Auditores Internos, traz uma estrutura otimizada de gestão de riscos que se popularizou entre as organizações. O modelo traz três linhas de defesa, que são definidas por entidades da organização, de modo que cada entidade desempenha o papel de sua respectiva linha. A alta aplicabilidade do modelo permite contextualizá-lo dentro do contexto de segurança cibernética, consequentemente abrindo espaço para discussão e avaliação da estrutura de segurança cibernética dentro das organizações públicas e privadas.

A 2ª linha de defesa possui o papel de definir políticas de gestão de riscos e supervisionar a operação da 1ª linha, portanto, uma das recomendações para a implementação do Modelo das

Três Linhas é a separação das 1ª e 2ª linhas de defesa, tanto em sua função quanto em estrutura dentro da organização. Em prática, algo que pode acontecer é a fusão da 1ª com a 2ª linha, podendo resultar no baralhamento das funções de operação e supervisão.

A partir do ataque ao STJ e as crescentes ameaças na Era dos Dados, surgiu a motivação desta pesquisa. Os órgãos do poder Judiciário do Distrito Federal são alvos de constantes ataques cibernéticos, portanto, cabe a avaliação se existe uma gerência de segurança da informação ou segurança cibernética apartada do setor de Tecnologia da Informação e Comunicações, atuando como 2ª linha de defesa para definição de políticas de segurança da informação e normas de respostas a incidentes.

Esta motivação justifica-se ao considerar o contexto atual de segurança cibernética do Poder Judiciário e a relevância atual do tema de pesquisa de segurança da informação. Uma avaliação das estruturas de segurança cibernética dos órgãos do Judiciário pode trazer contribuições relevantes para o tema e sugerir pesquisas futuras relacionadas, de forma a complementar a análise realizada.

1.1. Objetivo Geral

Esta pesquisa tem como objetivo geral avaliar a existência da segunda linha de defesa no âmbito de segurança cibernética em tribunais do poder Judiciário com sede no Distrito Federal considerando as definições estabelecidas no Modelo das Três Linhas do Instituto dos Auditores Internos.

1.2. Objetivos Específicos

a) Evidenciar o conceito do Modelo das Três Linhas, elucidando sua origem, eficácia, aplicabilidade, riscos inerentes à sua implementação e boas práticas do modelo em organizações públicas e privadas;
b) Contextualizar o Modelo das Três Linhas em segurança cibernética, de acordo com as características de cada linha de defesa;
c) Identificar, a existência ou ausência da 2ª linha de defesa nos tribunais do setor Judiciário do Distrito Federal, dentro do contexto de segurança cibernética;

d) Avaliar, com base na análise dos resultados, o nível de difusão das responsabilidades do setor de Tecnologia em tribunais do setor Judiciário, com base no Modelo das Três Linhas;

2. REFERENCIAL TEÓRICO

2.1. Risco

Segundo a Associação Brasileira de Normas Técnicas (2018), “risco é o efeito das incertezas nos objetivos”. O risco faz parte do cotidiano de pessoas e organizações e é comumente posto ao lado dos resultados prováveis de um projeto, mesmo nos processos iniciais. “O risco pode ser simplesmente definido como a exposição à mudança. É a probabilidade de que algum evento futuro, ou conjunto de eventos, ocorra” (PAXSON & WOOD, 1998, p. 306). A existência de um objetivo a se alcançar é fundamental para a existência do risco implícito para o sucesso desse objetivo.

Com o intenso avanço de novas tecnologias, as organizações precisam se adaptar com cada vez mais sofisticação e agilidade, e isso consequentemente traz mais riscos. Gregorio, (2005), traz que à medida que novas tecnologias vêm surgindo na atualidade, novos riscos relacionados à essas tecnologias surgem na mesma proporção. Fatos novos e surpresas sempre podem acontecer, portanto o risco está atrelado às leis da probabilidade e por isso deve ser algo possível de acontecer (ASSI, 2021).

Risco geralmente é atribuído a um resultado ruim, ou à incerteza de que algo que impeça o objetivo de acontecer, entretanto, esta atribuição veio sofrendo alterações conforme o passar dos tempos, podendo ser atribuído a um resultado positivo. Quando pensamos em instituições financeiras, geralmente aplicações mais arriscadas geram resultados maiores. As organizações que evitam correr riscos, provavelmente não irão gerar bons resultados para seus acionistas (DAMODARAN, 2009).

2.2. Gestão de Riscos

A gestão de riscos veio crescendo ao longo dos anos como um importante recurso para as organizações, principalmente quando inserida na era digital. Alguns modelos de gestão de riscos foram desenvolvidos e são amplamente aceitos hoje em dia, em especial o modelo proposto na ISO 31000, desenvolvida pela *International Organization for Standardization* (ISO) e publicada no Brasil pela Associação Brasileira de Normas Técnicas (ABNT).

“O processo de gestão de riscos envolve a aplicação sistemática de políticas, procedimentos e práticas para as atividades de comunicação e consulta, estabelecimento do contexto e avaliação, tratamento, monitoramento, análise crítica, registro e relato de riscos”

(ABNT, 2018). Whitman & Mattord (2018), definem gestão de riscos como o processo de identificação do risco, avaliação de sua magnitude relativa e a tomada de decisão para mitigar o risco a um nível aceitável. O processo de 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).

De acordo com a ABNT (2018) o processo de gestão de riscos eficaz, descrito na ISO 31000, deve ser norteada pelos princípios apresentados na norma, que por sua vez servem como base para o desenvolvimento da estrutura e processos de gestão de riscos e baseados neles a gestão de riscos deve ser:

- Integrada em todas as atividades;
- Estruturada e abrangente;
- Personalizada aos contextos internos e externos;
- Inclusiva às partes interessadas,
- Dinâmica às mudanças e eventos;
- Trazer a melhor informação possível;
- Considerar os fatores humanos e culturais; e
- Aprimorável.

A ABNT (2018) apresenta na ISO 31000 a estrutura da gestão de riscos (Figura 1), que tem como principal objetivo apoiar a organização na integração da gestão. 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.

Figura 1 – Estrutura de gestão de riscos da ISO 31000. Fonte: Gestão de riscos – Diretrizes. ABNT. Rio de Janeiro, 2018

A ABNT (2018), discorre que, no que tange à Alta Direção e os órgãos de supervisão, é fundamental que assegurem a total integração da gestão de riscos em todas as atividades da organização, assegurando recursos para a gestão de riscos, atribuindo estratégias, objetivos, políticas e implementando a cultura da organização e normas. A Alta Direção também deve demonstrar comprometimento com a gestão de riscos por qualquer meio que transmita de maneira clara seus objetivos com a gestão de riscos, além de atribuir autoridade, responsabilidade e responsabilizações para os papéis da gestão de riscos (ABNT, 2018).

Por fim, a Figura 2 ilustra o processo de gerenciamento de riscos descrito na ISO 31000. O processo traz as etapas que devem ser seguidas para gerir os riscos de forma efetiva, que devem compor partes integrantes da gestão e tomada de decisão, atuando nas operações e processos da organização.

Figura 2 – Processo de gestão de riscos da ISO 31000. Fonte: Gestão de riscos – Diretrizes. ABNT. Rio de Janeiro, 2018.

Tranchard (2018), discorre que a ISO 31000 fornece um guia claro, curto e conciso, que auxilia as organizações a utilizar princípios da gestão de riscos para melhorar o planejamento e tomada de decisão. A norma é aplicável em todos os tipos de organizações e cobre todos os tipos de risco, além de melhorar a probabilidade de atingirem seus objetivos estratégicos (ISO, 2018).

2.3. Gestão de Riscos de Segurança da Informação

À medida que avançamos na era da transformação digital, tornaram-se críticas a gestão, manutenção e tratamento de dados pessoais e sensíveis de todos os indivíduos, internos e externos, envolvidos no ciclo operacional da empresa. A interconectividade existente hoje entre organizações e pessoas trouxe eficiência para a operação de vários negócios, mas também trouxe riscos vinculados à exposição desses dados.

De acordo com a *International Organization For Standardization* (2018, p. 4), segurança da informação é definida como a "preservação da confidencialidade, integridade e disponibilidade da informação". Whitman & Mattord (2018), definem segurança da informação como a proteção da confidencialidade, integridade e disponibilidade de ativos de informação, através da aplicação de políticas, educação, treinamentos, conscientização e tecnologia. De acordo com Bevan et al. (2018), caso a segurança cibernética, que é uma ramificação da segurança da informação, não possua foco em risco, as ogranizações geralmente ignoram os verdadeiros fatores de risco, podendo levar à crises e grandes perdas comerciais.

Em outra norma, a Associação Brasileira de Normas Técnicas (2013), traz que a partir da implementação de um conjunto de controles selecionados dentro de um processo de gerenciamento de riscos e gerenciados por um Sistema de Gestão de Segurança da Informação (SGSI), obtém-se a segurança efetiva das informações. Conforme Whitman & Mattord (2018), os corpos funcionais da organização devem ter políticas como base para toro o planejamento, projeto e implantação de segurança da informação, com objetivo de direcionar como cada caso deve ser abordado e como as tecnologias devem ser usadas. A proteção dos ativos de informações identificados é realizada através de políticas, processos, procedimentos, estruturas organizacionais, *software* e *hardware* (ABNT, 2006).

Segundo a ABNT (2019) a gestão de riscos de segurança da informação pode ser aplicada em todo o escopo da organização, áreas específicas, em controles já existentes e contribui para:

- A identificação de riscos;
- O processo de avaliação de riscos em função das consequências e da probabilidade de sua ocorrência;
- A comunicação e entendimento da probabilidade e das consequências destes riscos;
- O estabelecimento da ordem prioritária para tratamento do risco;
- A priorização das ações para reduzir a ocorrência dos riscos;
- O envolvimento das partes interessadas quando as decisões de gestão de riscos são tomadas e para que elas sejam mantidas informadas sobre a situação da gestão de riscos;
- A eficácia do monitoramento do tratamento dos riscos;
- O monitoramento e análise crítica periódica dos riscos e do processo de gestão de riscos;
- A coleta de informações de forma a melhorar a abordagem da gestão de riscos;
- O treinamento de gestores e pessoal a respeito dos riscos e das ações para mitigá-los (ABNT, 2019, p. 3)

2.4. Segurança Cibernética

É possível definir segurança cibernética como 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, garantindo uma reação eficiente contra os diversos sinistros que podem ocorrer (NUNES, 2012). Atualmente as tecnologias da informação estão em constante crescimento, assim a segurança dessas informações obteve seu destaque (LAUDON & LAUDON, 2014).

"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 com os 5 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). No ano de 2021, o Brasil foi considerado um dos países líderes no ranking mundial de ataques cibernéticos (THE HARRIS POLL, 2022).

Conforme Ralo (2013), as principais atividades da segurança cibernética são: monitorar, prevenir e responder ameaças capazes de colocar em risco o espaço de liberdade coletiva ou individual, essa função fica sob a responsabilidade das forças de segurança e serviço de informações.

> Um ataque cibernético de grande envergadura, caso não seja adequadamente tratado, pode afetar profundamente a reputação da organização, ocasionar perda de receitas, levar a prejuízos operacionais com a paralisação dos serviços, resultar em perda de informações e ainda levar à aplicação de sanções legais e administrativas (LAGINESTRA, 2021, p. 25).

De acordo com a *International Telecommunication Union* (ITU) (2009), denominam-se os ativos todos os dispositivos que estão conectados à rede, serviços e 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). Conforme Couto (2018), as tecnologias podem se tornar vulneráveis, mesmo com os benefícios proporcionados, o que resulta na formação de riscos sociais e materiais. A conexão à uma rede global resulta na exposição a ameaças constante e roubo de dados e informações sensíveis, estando em risco eminente e tornando-se alvo para ataque de hackers e possíveis fraudes (ABU-MUSA, 2003).

Outra mudança que o avanço do ambiente cibernético trouxe para o mundo organizacional é 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 sua essência, a segurança da informação é o processo de entender, gerenciar e mitigar riscos. Em última análise, esse foco no risco pode ajudar a equipe de gerenciamento de risco de uma organização a desenvolver relacionamentos críticos com a segurança da informação e a auditoria interna.” (JAMISON, MORRIS, & WILKINSON, 2018, p. 10).

Em 2021, o Conselho Nacional de Justiça (CNJ) por meio da Resolução Nº 396, de 7 de junho de 2021, instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), que busca 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 traz:

1. Instituir o Comitê de Governança de Segurança da Informação (CGSI), que:
    a. assessora diretamente a alta administração do órgão;
    b. propõe alterações em políticas de segurança da informação;
    c. propõe normas internas de segurança da informação; e
    d. supervisiona trabalhos de auditoria de segurança da informação
2. Constituir a estrutura de segurança da informação, apartada do setor de TI e subordinado diretamente à alta administração (BRASIL, 2021a)

O funcionamento dos CGSIs é definido pelos seus respectivos órgãos do Judiciário e são coordenados por uma autoridade responsável por segurança da informação, nomeado pelos presidentes dos órgãos (BRASIL, 2021a).

A ENSEC-PJ orienta e determina as estratégias de segurança da informação dos órgãos do poder Judiciário, sendo fortemente relevante para este trabalho. A avaliação do cumprimento das obrigações declaradas na resolução torna-se um ponto de referência para a análise de resultados desta pesquisa.

2.4.1. Incidentes Cibernéticos no Poder Judiciário

Em 2020, o Superior Tribunal de Justiça foi vítima de um ataque *hacker*, que causou a interrupção de diversos julgamentos que ocorriam simultaneamente via videoconferência, resultando no adiamento de vários casos, além de deixar os sistemas do tribunal indisponíveis e resultaram na suspensão de todos os prazos processuais por alguns dias (PONTES, 2020). Este caso gerou grande repercussão nacional, visto que a escala deste ataque tomou proporções gigantescas e impactou diversos processos do Poder Judiciário.

Entretanto, esse não foi o único ataque cibernético em um órgão do Judiciário. Em novembro de 2020, durante o período eleitoral, o Tribunal Superior Eleitoral sofreu tentativas de ataques cibernéticos que buscavam derrubar o sistema online do tribunal por meio de milhares de acessos simultâneos, atingindo picos de 486 mil conexões (AMORIM, 2020).

Em 2022, foram registrados casos de ataques cibernéticos em órgãos do Judiciário. alguns deles sendo bem-sucedidos em impactar o funcionamento dos sistemas dos tribunais atacados. Em fevereiro, o Tribunal Regional do Trabalho do Espírito Santo identificou atividades maliciosas em sua infraestrutura tecnológica, entretanto não houve indícios de comprometimento da integridade dos sistemas ou vazamento de dados graças às medidas de isolamento e contenção adotadas (TRIBUNAL, 2022).

No mês de março, o Tribunal Regional Federal da 3ª Região suspendeu suas atividades por consequência de um ataque cibernético e, até a data de publicação desta pesquisa, não há previsão de retorno do atendimento e funcionamento do tribunal (MACIEL, 2022). Já em abril, a Justiça Federal em Pernambuco sofreu um ataque por *hackers*, que levou à indisponibilidade do site e de praticamente todos os sistemas da seção judiciária, restando apenas 1 sistema em funcionamento (JUSTIÇA, 2022).

Considerando os recentes casos de ataques cibernéticos aos órgãos do Poder Judiciário indicam a necessidade de revisão e sofisticação de seus modelos de segurança da informação e gestão de riscos de segurança da informação.

2.5. Modelo das Três Linhas

À medida que as organizações vêm se tornando cada vez mais competitivas em seus mercados, a adoção de modelos de segurança organizacional reconhecidos internacionalmente vem se tornando mais crítica. As organizações modernas, buscando garantir seu

desenvolvimento e sobrevivência dentro do mercado competitivo, torna-se necessária a adoção de medidas mais arriscadas para que seja possível atender as necessidades dos *stakeholders* e usuários (LUBURIC, PEROVIC, & RAJKO, 2015). Anderson & Eubanks (2015) discorrem que a busca dos objetivos organizacionais de qualquer organização envolve a adoção de oportunidades, busca de crescimento, assumir e gerenciar os riscos conforme o crescimento e desenvolvimento da organização, sabendo que a conquista desses objetivos pode ser impedida pela falha da gestão apropriada dos riscos.

O Modelo das Três Linhas, assim como é chamado hoje pelo Instituto dos Auditores Internos (IIA), traz a ideia de que, dentro da organização, cada área organizacional enquadrada nas três linhas possui um papel bem definido e tenha a total capacidade de agir sobre determinadas situações quando é requisitada. De acordo com Potter & Toburen (2016) o Modelo das Três Linhas mobiliza gerentes de negócios, equipes de gestão de ricos e auditores internos, de modo a trabalharem juntos como um grupo de diferentes estágios, fornecendo maior proteção contra riscos cada vez mais complexos. 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 (2013) o Modelo das Três Linhas pode ser aplicado em qualquer organização, independente da sua complexidade ou tamanho. Luburic, Perovic, & Rajko (2015) reforçam que uma das grandes qualidades do modelo é ser aplicável em qualquer organização, independente do seu tamanho e atividade. Essa afirmação possui um peso considerável no tema abordado neste estudo, principalmente quando analisamos a relação entre a primeira e segunda linha. Conforme Anderson & Eubanks (2015), 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 controle têm maior probabilidade de serem gerenciados com eficácia.

Segundo o IIA (2013), o Modelo das Três Linhas baseia-se em seis princípios:

1. Governança
2. Papéis do órgão de segurança
3. Gestão e os papéis da primeira e segunda linhas
4. Papéis da terceira linha
5. A independência da terceira linha

6. Criando e protegendo valor

A partir desses princípios, as três linhas de defesa devem ser bem definidas, cada uma com responsabilidades específicas de acordo com o modelo. A coerência e pleno funcionamento do modelo depende do alinhamento das atividades com os objetivos da organização (IIA, 2020).

O Instituto dos Auditores Internos (2013), detalha as três linhas:

1. Primeira linha: funções que controlam os riscos diretamente;
2. Segunda linha: funções que supervisionam e fazem a gestão da metodologia de controle sobre os riscos; e
3. Terceira linha de defesa: a auditoria interna, que fornece avaliações independentes sobre a organização e as outras duas linhas.

A primeira linha engloba os profissionais que monitoram e controlam os processos de trabalho (GLYNN et al, 2016). Esta linha também pode ser chamada de gerência operacional e está encarregada de identificar, avaliar, controlar e mitigar os riscos cotidianos da organização, em nível direto com seus funcionários (IIA, 2013). Vousinas (2021), traz que os processos de controle interno de gestão de riscos na primeira linha já foram altamente automatizados nos dias de hoje, o que facilitou a identificação de fraquezas operacionais e obtenção das informações necessárias assim que possível de modo a aplicar todas as medidas necessárias e informar o corpo funcional responsável.

É de grande importância destacar a responsabilidade dupla das unidades organizacionais responsáveis pela primeira 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 tecnologia da informação, que é responsável pela infraestrutura dos dados, sistemas e processos nos quais os riscos são apresentados (JAMISON, MORRIS, & WILKINSON, 2018).

A segunda linha de defesa serve como apoio para a primeira linha, de modo 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 meio de políticas internas, ainda mantendo um certo nível de independência dentro do Modelo das Três Linhas (IIA, 2013). Conforme Anderson & Eubanks (2015), 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.

Em resumo, a segunda linha de defesa é encarregada principalmente de verificar a função adequada dos controles existentes da primeira linha para lidar com os riscos enfrentados pela organização e para funcionar de maneira eficaz, essa linha de defesa deve ser independente da primeira, 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, Morris, & Wilkinson (2018), no contexto da segurança cibernética, a segunda 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), enquanto a primeira e segunda linha 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 *tradeoffs* que podem afetar negativamente a eficácia do processo de gerenciamento de risco (BANTLEON, et al., 2020).

O Instituto dos Auditores Internos (2020) traz a possibilidade de combinação ou separação dos papeis das primeiras e segundas linhas, considerando a possiblidade de que alguns papéis de segunda linha sejam atribuídos a especialistas para que em troca sejam fornecidos conhecimentos complementares, apoio, monitoramento e questionamento àqueles com papéis de primeira 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 segunda linha de defesa 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 à responsabilidades mais diretas dentro da gestão de riscos, como o *Enterprise Risk Management* (IIA, 2020).

A terceira linha engloba a auditoria interna, que age de forma independente das outras duas linhas, em caráter de supervisor delas e reporta os dados à alta administração da organização (IIA, 2013). A Instrução Normativa Nº 3, de 09/06/2017 traz as principais diretrizes, boas práticas, princípios e requisitos para a atuação da auditoria interna governamental, no âmbito do Poder Executivo Federal, que é exercida pelo conjunto de Unidades de Auditoria Interna Governamental (UAIG). O documento destaca as responsabilidades das UAIG, dentre elas destaca-se o apoio aos órgãos e entidades do Poder Executivo Federal, de modo a garantir a efetiva operação da primeira e segunda linha de defesa, via serviços de consultoria, avaliação de processos de governança, gestão de riscos e controles internos (BRASIL, 2017a).

> Tem sido observado em muitos mercados que existe uma sobreposição entre a segunda e a terceira linhas de defesa, combinando as duas funções. A integração da segunda e terceira linha invalida o propósito do modelo de três linhas de defesa porque tanto a segunda quanto a terceira linha não podem funcionar de forma independente (KUMAR, 2021, p. 1).

Kumar (2021) aplicou uma enquete em agosto de 2021 para profissionais seniores Chefe de Auditoria Interna, Diretores de Risco, Diretores de Conformidade, Chefe de Segurança da Informação, Diretor, Atuário Chefe etc., buscando investigar se as empresas combinam funções de risco e auditoria, objetivo que se assemelha ao desta pesquisa. A enquete avaliou a aceitação de um modelo separado de três linhas ou função de garantia integrada por meio de uma única pergunta: “Sua organização tem uma função de risco e auditoria separada ou uma função combinada de risco e auditoria?” No total foram obtidas 205 respostas sendo que 85% responderam que suas empresas têm as funções de risco e auditoria separadas e 15% responderam que em suas empresas as funções são combinadas.

A Figura 3 traz a distribuição visual do Modelo das Três Linhas, demonstrando os níveis de interação entre as entidades dentro e fora da organização:

Figura 3 – 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 possuem a responsabilidade de manter, monitorar e aperfeiçoar os controles internos da gestão (BRASIL, 2017a).

> A estrutura de controles internos dos órgãos e entidades da Administração Pública Federal deve contemplar as três linhas de defesa da gestão ou camadas, a qual deve comunicar, de maneira clara, as responsabilidades de todos os envolvidos, provendo uma atuação coordenada e eficiente, sem sobreposições ou lacunas. (BRASIL, 2017a, p. 3).

Já no contexto de risco cibernético, Bevan et al. (2018) trazem que o Modelo das Três Linhas pode ser visto nos papéis da segurança cibernética como a primeira linha e a função de risco como a segunda linha. Os autores supracitados 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 primeira linha para identificar e priorizar os riscos cibernéticos. Jamison, Morris, & Wilkinson (2018), escrevem que, no caso de várias organizações, principalmente as que não possuem um setor de segurança da informação dedicado, o monitoramento e ação da segurança da informação ficam sob responsabilidade do departamento de TI, resultando na desordem dos limites entre a primeira e segunda linha de defesa.

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 segunda linha de questionar a primeira linha em diálogo aberto, o que beneficia ambas as linhas. A primeira linha fica apta a relacionar o risco cibernético dentro do gerenciamento dos riscos corporativos e torna-se mais bem preparada para as eventuais decisões de risco. Por outro lado, a segunda linha se adequa melhor com as capacidades e planos da primeira linha (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 através das outras linhas (BANTLEON, et al. 2020).

A Figura 4 ilustra de forma simplificada a disposição e atribuição das respectivas funções das três linhas, ilustrando também suas relações:

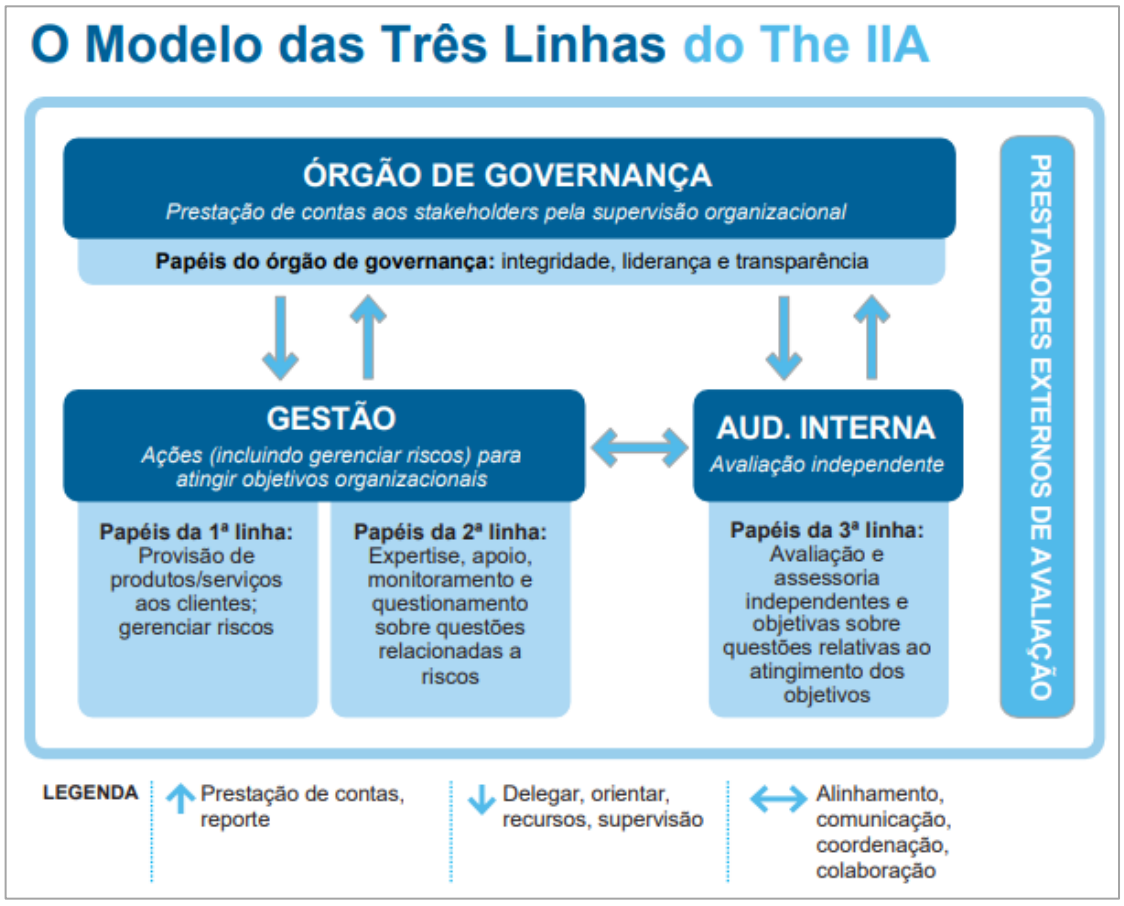


Figura 4 – O Modelo das Três Linhas do IIA. Fonte: Modelo das Três Linhas do IIA 2020, IIA, 2020.

> Organizações que possuem fortes três linhas de defesa geralmente são mais inteligentes em relação aos riscos. Elas são capazes de identificar e reagir rapidamente ao risco, elas 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 menos surpresas e perdas, menores custos de transferência de risco e maior probabilidade de que os objetivos da organização sejam alcançados (POTTER & TOBUREN, 2016, p. 16)

Entre as críticas ao modelo, percebe-se que muitas delas se concentram no setor financeiro/bancário, no qual foi implementado em diversos países. Davies & 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 em 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 e resultando em controles ineficazes em diversos níveis da organização.

> O Modelo das Três Linhas pode ser visto como um instrumento organizacional para facilitar a supervisão dentro das instituições financeiras na prática, com seu surgimento repentino como um sintoma do aumento do foco regulatório nos riscos dentro das empresas (DAVIES & ZHIVITSKAYA 2018, p. 38).

Chambers & Odar (2015) trazem que o Modelo das Três Linhas não foi totalmente eficaz e deu uma falsa sensação de segurança, ao analisarem 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".

2.6. Caracterizando a 2ª Linha de Defesa

O presente capítulo 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 o desenvolvimento e eficácia dessa pesquisa no âmbito de obter informações por meio da pesquisa estruturada.

Ainda que não seja completamente independente, é de suma importância a existência de funções de segunda 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 primeira linha de defesa (ANDERSON & EUBANKS, 2015). Considerando que deve haver uma interação regular entre a gestão e auditoria interna, de forma que o trabalho da terceira linha seja relevante e esteja alinhado às necessidades, torna-se necessária a colaboração entre os papéis da primeira, segunda e terceira linha de defesa (IIA, 2020).

Conforme o posicionamento do Instituto dos Auditores Internos (2013), a 2ª linha possui funções típicas, presentes na maioria das organizações. Cada uma dessas funções possui um certo nível de independência da 1ª linha, mas por natureza são funções gerenciais. O posicionamento esclarece:

> - 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. Nesse quesito, a função separada reporta diretamente à alta administração e, em alguns setores do negócio, diretamente ao órgão de governança. Múltiplas funções de conformidade existem frequentemente na mesma organização, com responsabilidade por tipos específicos de monitoramento da conformidade, como saúde e segurança, cadeia de fornecimento, ambiental e monitoramento da qualidade;
> - Uma função de controladoria que monitore os riscos financeiros e questões de reporte financeiro (IIA, 2013, p. 4)

Anderson & Eubanks (2015) trazem que a 2ª linha tem como principal função de supervisionar a gestão operacional e garantir que os riscos e controles são gerenciados corretamente no contexto de instituições financeiras. Davies & Zhivitskaya (2018), discorrem que, no setor bancário, existe a grande discussão relacionada à segunda linha de defesa sobre se a equipe operacional deve estar diretamente envolvida na gestão de risco de cada transação, ou se deve supervisionar os riscos de maneira mais distante, já que na prática, os gestores centrais de risco de grandes bancos realizam essa rotina nas principais transações.

Sob a ótica da segurança cibernética, a função de gestão de risco fica englobada na segunda linha, apoiando e monitorando as atividades de segurança cibernética, atrelada à primeira linha (BEVAN et al. 2018). Mabwe, Ring, & Webb (2017) realizaram um estudo baseado no Modelo das Três Linhas, em que muitos entrevistados comentaram sobre a indefinição inerente entre as duas primeiras linhas, além de identificar que o papel de supervisão da segunda linha sobre a primeira acaba removendo o conceito da independência da segunda linha, e crie 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 primeira linha de defesa, dependente da segunda linha, recebe as seguintes responsabilidades:

> 1. A primeira linha de defesa 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.
> 2. A primeira linha de defesa 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.
> 3. De forma a assegurar sua adequação e eficácia, os controles internos devem ser integrados ao processo de gestão, dimensionados e desenvolvidos na proporção requerida pelos riscos, de acordo com a natureza, a complexidade, a estrutura e a missão da organização (BRASIL, 2017a, p. 3).

Seguindo a função de supervisora apartada da primeira linha, são atribuídas à segunda linha de defesa as funções a seguir:

> 1. As instâncias de segunda linha de defesa estão situadas ao nível da gestão e objetivam assegurar que as atividades realizadas pela primeira linha sejam desenvolvidas e executadas de forma apropriada.
> 2. 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 primeira linha de defesa, que incluem gerenciamento de riscos, conformidade, verificação de qualidade, controle financeiro, orientação e treinamento.
> 3. Os Assessores e Assessorias Especiais de Controle Interno (AECI) nos Ministérios integram a segunda linha de defesa e podem ter sua atuação complementada por outras estruturas específicas definidas pelas próprias organizações (BRASIL, 2017a, p. 3).

A AECI é um órgão de assistência que responde diretamente ao Ministro do Planejamento, Desenvolvimento e Gestão e seu objetivo foca na atuação nas áreas de gestão de risco, controle, transparência e integridade da gestão (MINISTÉRIO DA ECONOMIA, 2021). As competências do AECI são:

> 1. Assessorar diretamente o Ministro de Estado da Justiça e Segurança Pública nas áreas de controle, risco, transparência e integridade da gestão;
> 2. Assistir o Ministro de Estado no pronunciamento estabelecido no art. 52 da Lei nº 8.443, de 16 de julho de 1992;
> 3. Prestar orientação técnica ao Secretário-Executivo, aos gestores do Ministério e aos representantes indicados pelo Ministro de Estado em conselhos e comitês, nas áreas de controle, risco, transparência e integridade da gestão;
> 4. Prestar orientação técnica e acompanhar os trabalhos das unidades do Ministério com vistas a subsidiar a elaboração da prestação de contas anual do Presidente da República e do relatório de gestão;
> 5. Prestar orientação técnica na elaboração e na revisão de normas internas e de manuais;
> 6. Apoiar a supervisão ministerial das entidades vinculadas, em articulação com as respectivas unidades de auditoria interna, inclusive quanto ao planejamento e aos resultados dos trabalhos;

> 7. Auxiliar na interlocução sobre assuntos relacionados com a ética, a ouvidoria e a correição entre as unidades responsáveis no Ministério e os órgãos de controle interno e externo e de defesa do Estado;
> 8. Acompanhar processos de interesse do Ministério junto aos órgãos de controle interno e externo e de defesa do Estado;
> 9. Acompanhar a implementação das recomendações da Controladoria-Geral da União e das deliberações do Tribunal de Contas da União, relacionadas ao Ministério da Justiça e Segurança Pública, e atender outras demandas provenientes dos órgãos de controle interno e externo e de defesa do Estado; e
> 10. Apoiar as ações de capacitação nas áreas de controle, risco, transparência e integridade da gestão BRASIL, 2021b, p. 1-2).

Percebe-se que a 2ª linha de defesa é responsável por funções gerenciais de modo a garantir a operação da 1ª linha e possui 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. O procedimento de coleta de dados ocorreu por meio da pesquisa documental, com os dados tratados via análise de conteúdo.

Pode ser classificada 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). Além disso, esse tipo de pesquisa é desenvolvido com o objetivo de proporcionar uma visão ampla sobre um fato e envolveu um levantamento bibliográfico e documental, 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, reduzir a distância entre indicador e indicado, entre teoria e dados, entre contexto e ação (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".

Como método de coleta de dados, foi realizada 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. Utilizou-se também dados obtidos através de pedidos de acesso à informação, via canais disponibilizados por ouvidorias e canais oficiais dos órgãos, respeitando a lei nº 12.527, de 18 de novembro de 2011, que institui a lei de acesso à informação. Cellard (2008) traz 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 quando ela for a única abordagem qualitativa, sendo usada como método autônomo.

Baseando-se no cenário atual de segurança cibernética do Poder Judiciário e no potencial impacto de um ataque cibernético bem-sucedido nos órgãos, esta pesquisa delimitou o escopo para os 6 tribunais sediados em Brasília-DF, buscando analisar suas estruturas de segurança cibernética. Os tribunais analisados foram: Supremo Tribunal Federal, Superior Tribunal de Justiça, Superior Tribunal Militar, Tribunal de Justiça do Distrito Federal e dos Territórios, Tribunal Regional Federal da 1ª Região e Tribunal Superior do Trabalho.

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 se referem aos comitês de segurança da informação dos tribunais identificados através da análise documental. A primeira solicitação buscava confirmar a existência dos comitês, e, se porventura existem outros comitês sobre segurança da informação no respectivo órgão. A segunda solicitação buscava confirmar a situação desses comitês e se ainda continuam 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).

Baseando-se em Bardin (2016), a análise de conteúdo seguiu as seguintes etapas:

1. Pré-análise: consistiu na coleta de documentos de fontes oficiais, que descrevem a estrutura organizacional dos tribunais e o funcionamento dos órgãos que compõem essa estrutura, de forma a obter informações preparadas para a análise;
2. Exploração do material: consistiu na análise e agrupamento das informações dispostas nos documentos, de modo a caracterizar o material para comparação e construção de concepções capazes de caracterizar os componentes das estruturas no Modelo das Três Linhas dentro de segurança cibernética; e
3. Interpretação dos resultados: partindo da análise da segunda etapa, foi realizada a interpretação dos dados levantados, de forma a levantar conclusões acerca do objetivo desta pesquisa.

Conforme Gil (2008), fontes documentais podem muitas vezes proporcionar ao pesquisador dados suficientes e ricos, trazendo economia de tempo na pesquisa e em muitos casos a investigação social só é possível através 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. Baseado nessas afirmações, foi definida a metodologia desta pesquisa.

4. ANÁLISE E DISCUSSÃO

Neste capítulo são apresentados os resultados dos dados coletados de seis tribunais do poder Judiciário do DF, disponíveis em seus respectivos sites oficiais e através de ouvidorias abertas por meio da lei de acesso à informação. Através da 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

O Supremo Tribunal Federal (STF) dirige em conjunto do CNJ o Poder Judiciário, responsável pela solução de conflitos da sociedade e garantia de direitos dos cidadãos. (BRASIL, 2022b). O Presidente do STF é também o Presidente do CNJ. O STF julga a ação direta de inconstitucionalidade de lei ou ato normativo federal ou estadual e o descumprimento da Constituição Federal (BRASIL, 2019a).

A estrutura organizacional apresentada no organograma do STF, (Anexo A) nas Figuras 5 e 6, 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 no organograma.

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 Tecnologia da Informação, justificando sua classificação dentro do modelo.

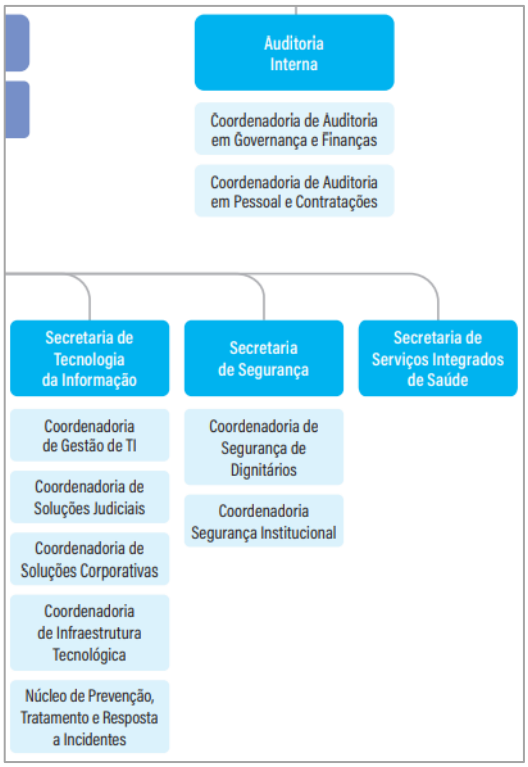


Figura 5 – Organograma do STF – STI e AI. Fonte: Organograma Supremo Tribunal: Ato Regulamentar n. 25, de 29/11/2021. Supremo Tribunal Federal. Brasília (DF), 2021. Disponível em: https://portal.stf.jus.br/textos/verTexto.asp?servico=sobreStfOrganograma. Acesso em: 02 mar. 2022.

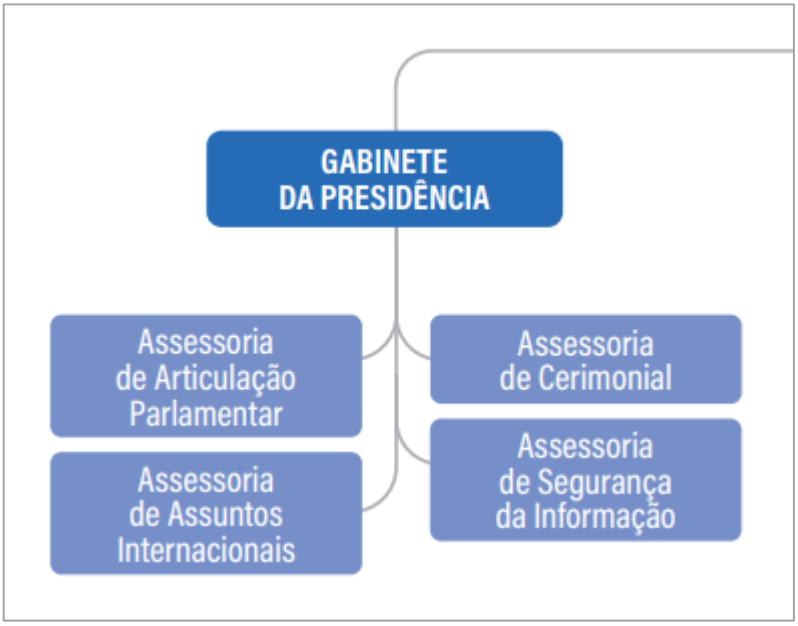


Figura 6 – Organograma do STF - ASI. Fonte: Fonte: Organograma Supremo Tribunal: Ato Regulamentar n. 25, de 29/11/2021. Supremo Tribunal Federal. Brasília (DF), 2021. Disponível em: https://portal.stf.jus.br/textos/verTexto.asp?servico=sobreStfOrganograma. Acesso em: 02 mar. 2022.

Representando a 2ª linha, considerou-se a ASI como detentor desse papel, pois trata-se de uma estrutura organizacional apartada da STI com funções de supervisão e assessoramento. Em conjunto da ASI, o STF conta com comitês de segurança da informação, em especial o Comitê Corporativo de Segurança da Informação (CCSI) instituído pela Resolução 612, de 23/04/2018, que define atribuições diretamente relacionadas à 2ª linha de defesa:

> I - Indicar as necessidades corporativas de segurança da informação;
>
> II - Propor a elaboração e a revisão de políticas, diretrizes, normas e procedimentos inerentes à segurança da informação, bem como analisar periodicamente sua efetividade;
>
> III - Manifestar-se sobre propostas de alteração, de revisão da PCSI/STF, minutas de normativos e iniciativas de natureza estratégica ou que necessitem de cooperação entre unidades, que versem sobre segurança da informação, além de outras matérias que lhe sejam submetidas;
>
> IV - Propor a implementação de ações corporativas de segurança da informação e o acompanhamento de seus resultados;
>
> V - Promover a definição, a implantação, o monitoramento e a revisão do Sistema de Gestão de Segurança da Informação do STF (SGSI/STF); e
>
> VI - Promover a divulgação de boas práticas de segurança da informação (BRASIL, 2018, p. 5).

Complementando as atividades da ASI e do CCSI, existe também o Comitê Executivo de Segurança da Informação (CESI), que possui 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 612, de 23/04/2018, 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 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

O Superior Tribunal de Justiça (STJ) é responsável por uniformizar a interpretação da lei federal, além de solucionar casos civis e criminais oriundas da Justiça Comum, sendo que o principal tipo de processo julgado pelo STJ é o recurso especial. (BRASIL, 2022b).

A partir da estrutura organizacional disposta no organograma do STJ (Anexo B) nas Figuras 7 e 8, disponibilizado publicamente em seu website oficial, realizou-se a interpretação relacionada à estrutura organizacional sob a ótica de segurança cibernética. No documento, é apresentada Secretaria de Tecnologia da Informação e Comunicação (STI), que possui 6 coordenadorias no total, destacando as coordenadorias de Tecnologia da Informação, a de apoio à Governança e Gestão de TIC (CGOT) e a de Segurança da Informação e Defesa Cibernética (CSID). O documento apresenta também a Secretaria de Auditoria Interna, funcionando como área independente das demais secretarias do tribunal.

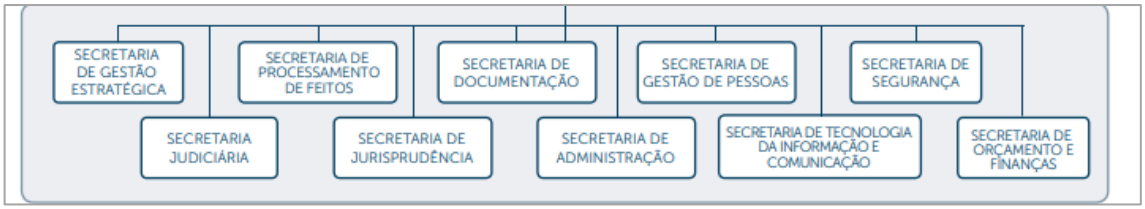


Figura 7 – Organograma do STJ - STI. Fonte: Organograma: Estrutura Básica. Superior Tribunal de Justiça. Brasília (DF), 2018. Disponível em: https://www.stj.jus.br/static_files/STJ/Midias/arquivos/2482_Org_Estrutura_Basica.pdf. Acesso em: 02 mar. 2022

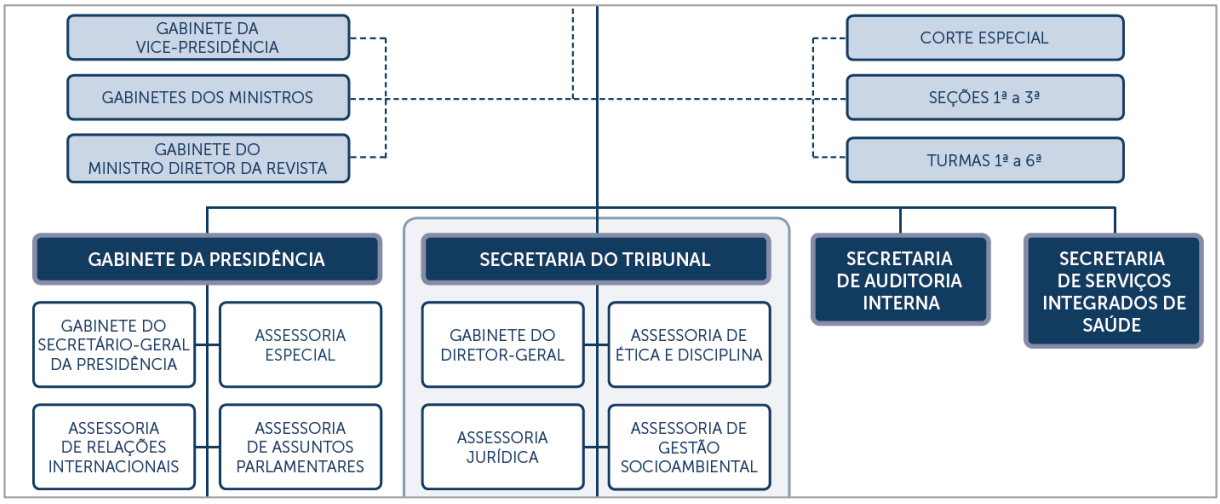


Figura 8 – Organograma do STJ - SAI. Fonte: Organograma: Estrutura Básica. Superior Tribunal de Justiça. Brasília (DF), 2018. Disponível em: https://www.stj.jus.br/static_files/STJ/Midias/arquivos/2482_Org_Estrutura_Basica.pdf. Acesso em: 02 mar. 2022.

Convém apontar que as coordenadorias do STJ possuem suas respectivas seções subordinadas, conforme demonstrado no organograma da STI (Anexo C) na Figura 9, obtido através do Plano Diretor de Tecnologia da Informação e Comunicação 2021 – 2022 (SUPERIOR TRIBUNAL DE JUSTIÇA, 2021). A CSID possui 2 seções: a de Segurança da Informação e Proteção de Dados e de Operação de Segurança de TIC, que obtém destaque para esta pesquisa. Outra informação relevante é que a CSID possui um gestor responsável pela segurança da informação.

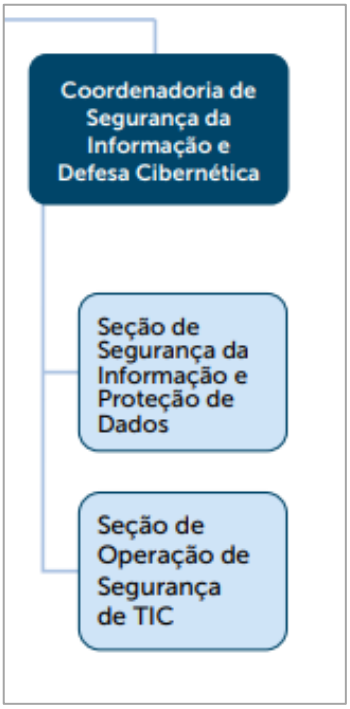


Figura 9 – Organograma da STI. Fonte: Plano Diretor de Tecnologia da Informação e Comunicação. Superior Tribunal de Justiça. Brasília (DF), 2021. Disponível em: https://www.stj.jus.br/publicacaoinstitucional/index.php/PDTIC/issue/archive. Acesso em: 03 mar. 2022.

Sobre uma das atribuições da STI, a Resolução STJ/GP n. 11 de 12 /11/2015 traz: "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 à 1ª linha de defesa a Secretaria de Tecnologia da Informação e Comunicação, por realizar operações de segurança de TIC. A CSID encontra-se apartada das demais coordenadorias do STI e possui um coordenador específico em segurança da informação

enquanto está subordinada ao secretário de tecnologia da informação em conjunto das outras coordenadorias.

Com o objetivo de apoiar o funcionamento da segurança cibernética e da informação do STJ, existem 3 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/GDC n. 178/2021, que institui o CGPD, declara que 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, cabe à 2ª linha de defesa do STJ o CGPD, CGeTIC e CGovTIC. De acordo com resposta obtida pela ouvidoria do Superior Tribunal de Justiça, por meio de pedido de acesso à informação, os 3 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 se encontra apartada das outras secretarias e responde diretamente ao Ministro Presidente do STJ. Complementando essa afirmação, de acordo com a Resolução STJ/GPN n. 11 de 12/11/2015, "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

O Superior Tribunal Militar (STM) compõe a Justiça Militar da União, que julga os crimes militares previstos no Código Penal Militar (BRASIL, 2022c). O STM "contribui para a proteção dos direitos humanos quando julga os crimes definidos em lei, respeitando o devido processo legal, [...] de acordo com o sistema acusatório democrático" (BRASIL, 2022d, p.1).

Através do organograma obtido por meio do website oficial do STM (Anexo D), Figuras 10 e 11, obteve-se conclusões referentes à segurança cibernética do órgão. O organograma dispõe a Diretoria de Tecnologia da Informação (DITIN), que possui 4 coordenadorias e 2

núcleos sob sua gestão. No contexto desta pesquisa, destaca-se a Coordenadoria de Tecnologia, que controla 3 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 como área independente das outras 2 secretarias do Superior Tribunal Militar (STM).

De acordo com a Resolução n. 222 de 03 de fevereiro de 2016, fica instituída a Política de Segurança da Informação da Justiça Militar da União, que define a Secretaria de Segurança Institucional (SESEG) como 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" (BRASIL, 2016, p. 8). A SESEG não é exibida no atual organograma do STM, portanto, interpreta-se que sua responsabilidade foi transferida à SAGRE.

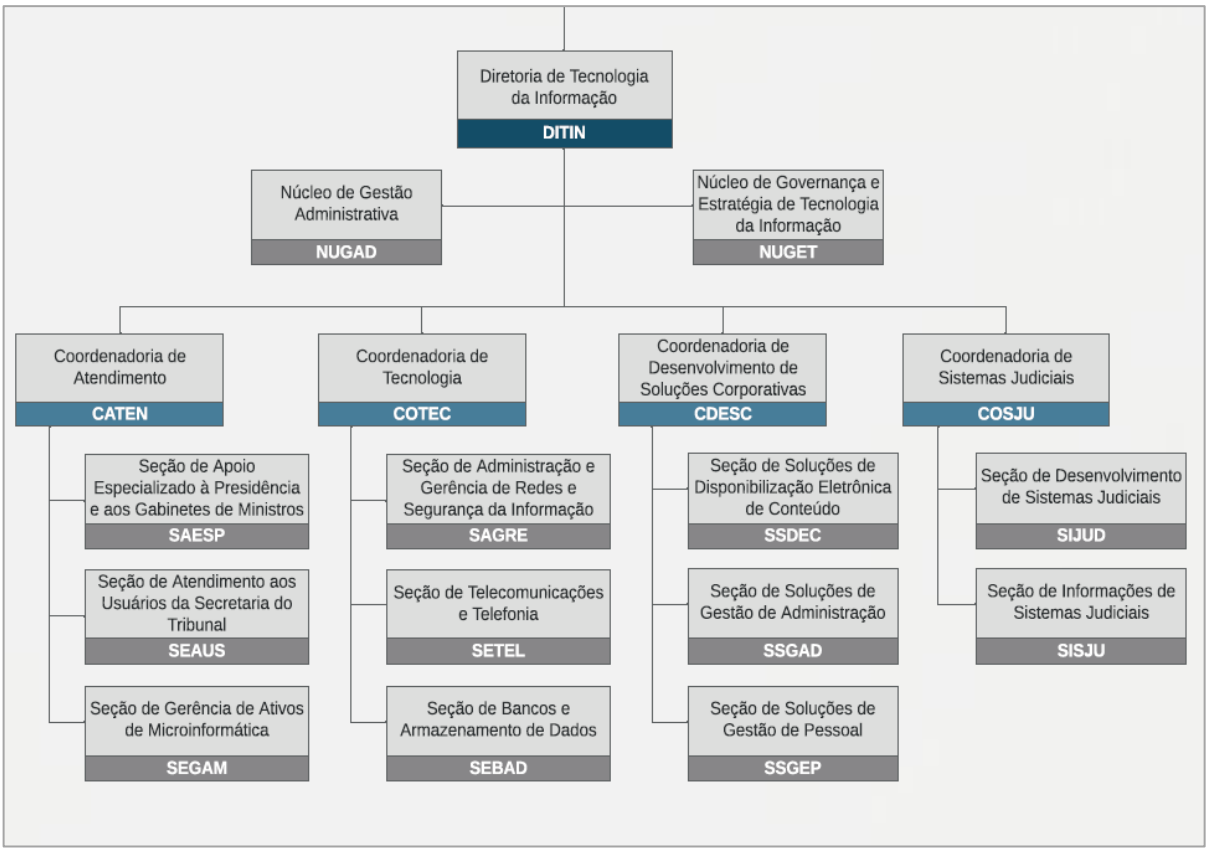


Figura 10 – Organograma do STM - DITIN. Fonte: Estrutura Organizacional: Resolução n. 306, de 16 de fevereiro de 2022. Superior Tribunal Militar. Brasília (DF), 2022. Disponível em: https://www.stm.jus.br/images/arquivos/institucional/Organograma_estrutura%20organizacional_v10.pdf. Acesso em: 09 mar. 2022

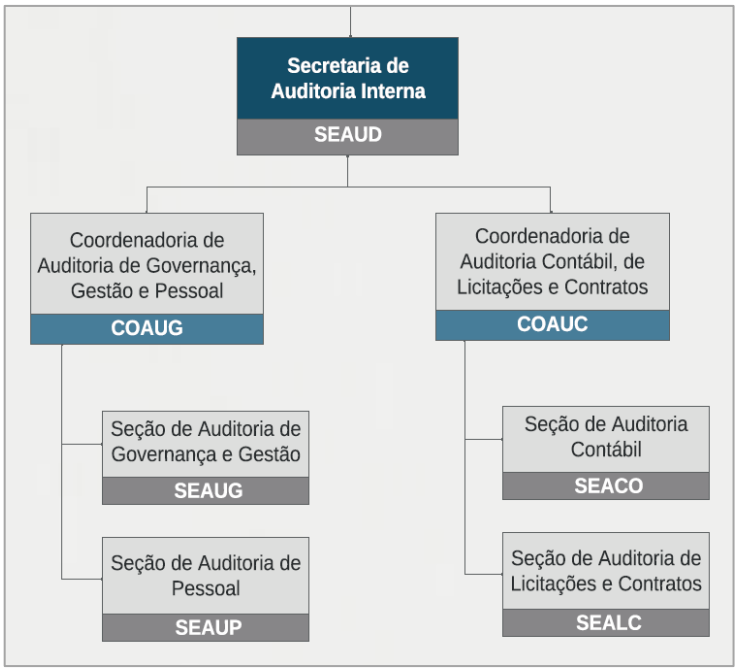


Figura 11 – Organograma do STM - SEAUD. Fonte: Estrutura Organizacional: Resolução n. 306, de 16 de fevereiro de 2022. Superior Tribunal Militar. Brasília (DF), 2022. Disponível em: https://www.stm.jus.br/images/arquivos/institucional/Organograma_estrutura%20organizacional_v10.pdf. Acesso em: 09 mar. 2022

A Resolução n. 298, de 04/08/2021, traz: “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, através das SAGRE e SEBAD, respectivamente.

Ainda no âmbito da 1ª linha de defesa, o Superior Tribunal Militar tem o Comitê de Crises e Incidentes Cibernéticos (CCIC), que deve reportar os 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 como a 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 08/09/2021 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 a 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 04/08/2021, "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, através da lei de acesso à informação, o CGovTIC não possui registro de reunião, porém a primeira reunião semestral está prevista para junho de 2022.

4.4. Tribunal de Justiça do Distrito Federal e dos Territórios

O Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT) analisa e julga ações apresentadas à Justiça do Distrito Federal em sua primeira instância, além de reexaminar as decisões proferidas pela primeira instância quando proferidas à apreciação da segunda instância (BRASIL, 2019b). O órgão também participa de iniciativas voluntárias e demais questões sociais, de modo a trazer benefícios à população com doações, cursos e informações (BRASIL, 2019b).

Por meio do organograma do TJDFT (Anexos E e F), Figuras 12 e 13, disponível em seu website oficial, foi realizada a intepretação da estrutura organizacional do órgão, sob o contexto de segurança cibernética. O documento apresenta a Secretaria Geral do Tribunal (SEG), que possui 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 em cima do campo de segurança cibernética. A Secretaria de Auditoria Interna (SEAI) encontra-se separada das demais secretarias e áreas funcionais, operando de forma independente.

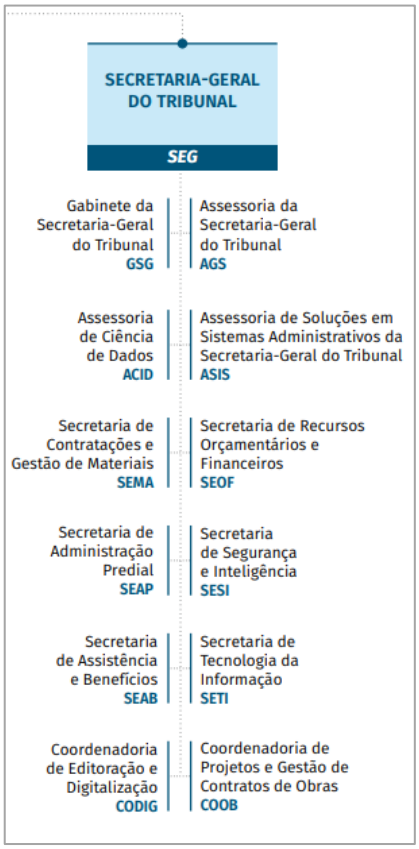


Figura 12 – Organograma do TJDFT - SEG. Fonte: Estrutura Organizacional. Tribunal de Justiça do Distrito Federal e dos Territórios. Brasília (DF), 2022. Disponível em: https://www.tjdft.jus.br/transparencia/estrutura-organizacional. Acesso em: 09 mar. 2022.

Figura 13 – 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: 09 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 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 possui 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 de segurança da informação do tribunal e promoção da cultura de segurança da informação (BRASIL, 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” (BRASIL, 2020a, p. 3).

A responsabilidade 3ª linha de defesa fica à 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 possível revogação do comitê. Desta forma, não é possível confirmar a ocorrência de reuniões regulares do comitê.

4.5. Tribunal Regional Federal da 1ª Região

O Tribunal Regional Federal da 1ª Região é composto por 15 seções judiciais, uma delas estando no Distrito Federal e julga as causas em que a União, autarquias e empresas públicas federais sejam interessadas, além de julgar crimes praticados em detrimento de bens, serviços ou interesses da União ou empresas públicas (BRASIL, 2012)

A partir da estrutura disposta no organograma do TRF1 (Anexo G) nas Figuras 14 e 15, 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). A Nutec é composta pela Seção de Sistemas, Suporte Técnico e Infraestrutura (Sesis), que por sua vez é dividida em 3 setores. É apresentado Núcleo de Auditoria Interna (Nuaud), separado das demais secretarias e núcleos.

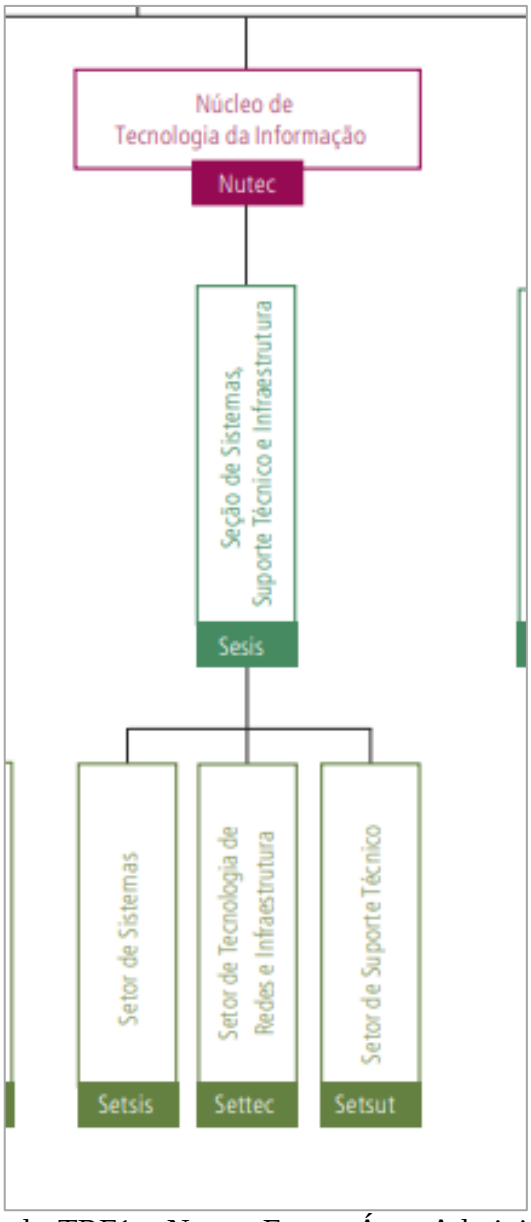


Figura 14 – Organograma do TRF1 - Nutec. Fonte: Área Administrativa: De acordo com a Portaria Diref 636/2021, de 3 de novembro de 2021. Seção Judiciária do Distrito Federal. Brasília (DF), 2021. Disponível em: https://portal.trf1.jus.br/portaltrf1/institucional/organizacao/organograma/organograma.htm. Acesso em: 09 mar. 2022.

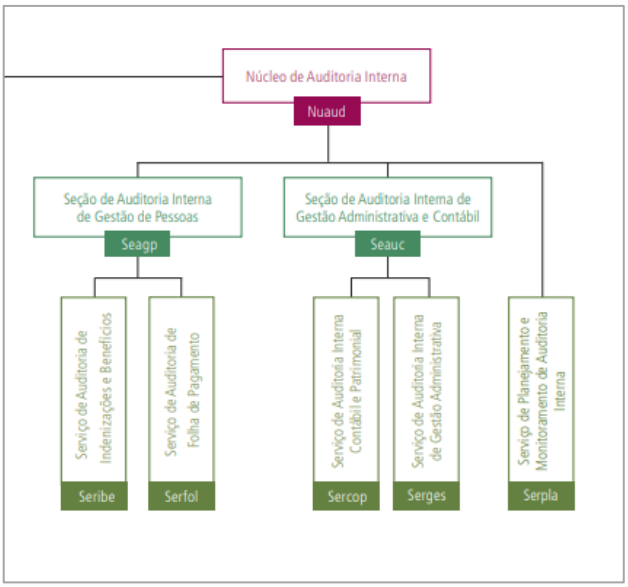


Figura 15 – Organograma do TRF1 - Nuaud. Fonte: Área Administrativa: De acordo com a Portaria Diref 636/2021, de 3 de novembro de 2021. Seção Judiciária do Distrito Federal. Brasília (DF), 2021. Disponível em: https://portal.trf1.jus.br/portaltrf1/institucional/organizacao/organograma/organograma.htm. Acesso em: 09 mar. 2022.

No que tange o Modelo das Três Linhas e segurança cibernética, interpreta-se como a 1ª linha de defesa do TRF1 a Nutec, considerando 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 a 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 abordam planos referentes à segurança da informação, como o Plano de Contratações de Soluções de Tecnologia da Informação (PCSTI) de 2022, que teve enfoque a segurança dos dados do tribunal (TRF1, 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 se encontra apartada da Nutec e demais corpos funcionais do TRF1 e responde diretamente à alta administração. Complementando essa interpretação, a Portaria Diref n. 11858602 traz 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 Tribunal Superior do Trabalho (TST), tem jurisdição em todo o Brasil e possui a função de uniformizar a jurisprudência trabalhista brasileira (BRASIL, 2022g). É responsável por conciliar e julgar ações judiciais entre trabalhadores e empregadores, além de julgar outras questões que envolvem a relação de trabalho (BRASIL, 2022g)

O organograma do TST (Anexo H), Figuras 16 e 17, 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 2 coordenadorias, em destaque a Coordenadoria de Auditoria de Gestão Administrativa (CAUGE), que possui a Seção de Auditoria de Tecnologia da Informação e Comunicação (SAUTIC).

A SETIN, possui 4 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 4 seções, uma delas sendo a Seção de Segurança da Informação e Proteção de Dados (SIPD) enquanto a CITEC possui 6 seções, em destaque a Seção de Gerenciamento de Redes (SGRE).

Caracterizando a estrutura organizacional do TST no Modelo das 3 Linhas e trazendo ao contexto de segurança cibernética, cabe à SETIN o papel de 1ª linha de defesa, executado pela CITEC e CGOV. A CITEC implementa busca 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.

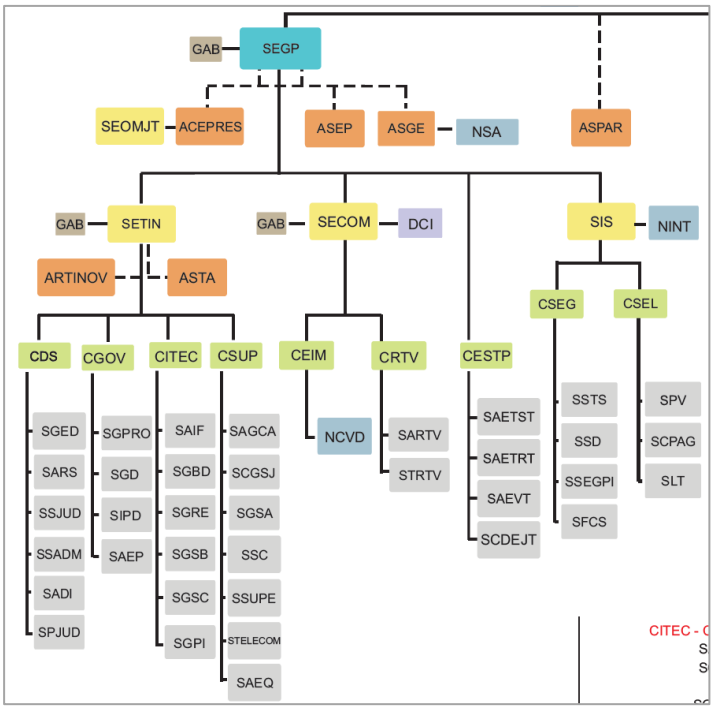


Figura 16 – Organograma do TST - SETIN. Fonte: Estrutura Organizacional. Tribunal de Justiça do Distrito Federal e dos Territórios. Brasília (DF), 2022. Disponível em: https://www.tjdft.jus.br/transparencia/estrutura-organizacional. Acesso em: 09 mar. 2022.

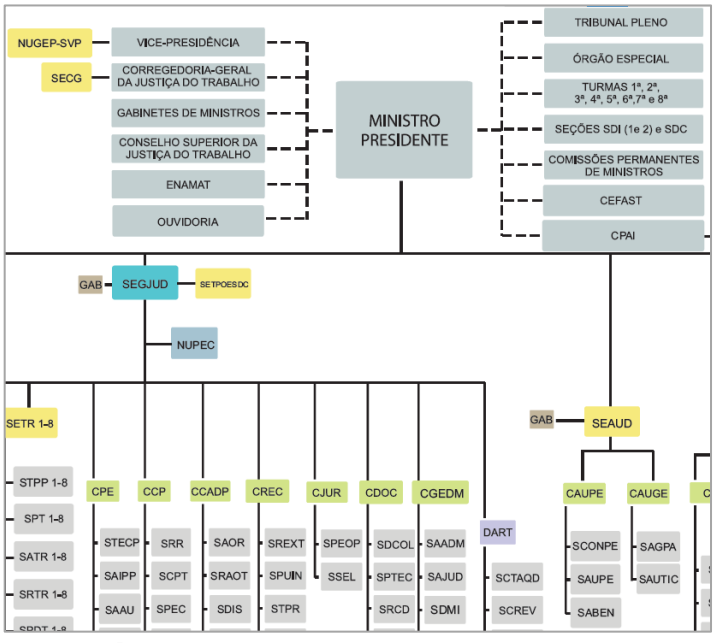


Figura 17 – Organograma do TST - SEAUD. Fonte: Estrutura Organizacional. Tribunal de Justiça do Distrito Federal e dos Territórios. Brasília (DF), 2022. Disponível em: https://www.tjdft.jus.br/transparencia/estrutura-organizacional. Acesso em: 09 mar. 2022.

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

No âmbito da 2ª linha de defesa, pode-se interpretar que a CGOV possui funções de planejamento e supervisão em relação à segurança da informação do TST, entretanto, a CGOV não estaria apartada da 1ª linha, pois compõe a SETIN. Existe o Comitê de Governança de Tecnologia da Informação e Comunicação (CGTI) que possui atribuições que podem justificariam sua classificação como 2ª linha, além de não integrar diretamente à SETIN. De acordo com o Ato n. 65/TST.GP, de 06/04/2021, 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, se encaixa no papel de 3ª linha de defesa do tribunal. A partir do organograma, cabe 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 07/10/2021, porém, não foi recepcionada despacho da ouvidoria confirmando se esta foi a reunião mais recente. Considerando o ato que institui o CGTI, as reuniões ocorrem trimestralmente, portanto, interpreta-se que o comitê continua se reunindo.

4.7. Tabela Resumo e Discussão

A Tabela Resumo mostra a síntese dos resultados obtidos através da análise documental sobre os tribunais do poder Judiciário do Distrito Federal 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.

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

Tabela Resumo: Agrupamento dos resultados obtidos

Percebe-se que o STF se destaca entre os demais tribunais por ser o único a possuir dentro do Gabinete da Presidência, um setor de Assessoria de Segurança da Informação apartado do setor de TI, a STI. Além de apresentar essa estrutura interna, ele também conta com um comitê focado de 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 dos riscos e controles serem gerenciados com eficiência (ANDERSON & EUBANKS, 2015). Com base no cenário observado, e no que dizem Potter & Toburen (2016), o STF reage de forma mais eficiente às ameaças e o órgão como um todo tem a tendência de ser mais inteligente perante os riscos.

Constatou-se que o STJ, TST e 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 Instituto dos Auditores Internos (2020), A combinação dos papéis da 1ª e 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 nos tribunais TJDFT e TRF1, que por consequência possuem apenas comitês de segurança da informação desenvolvendo políticas e ações relacionadas ao tema. Jamison, Morris, & Wilkinson (2018), discorrem sobre a possível desordem causada pela

baralhada dos papéis da 1ª e 2ª linha em organizações que não possuem um setor específico de segurança da informação. No cenário analisado, apenas o STF possui um setor de segurança da informação efetivamente apartado do setor de TIC, então pode-se interpretar que o STJ, STM e TST não estão em condições ideais para segurança cibernética no Modelo das Três Linhas.

No que tange as semelhanças entre os tribunais, a principal delas 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. No escopo da 2ª linha de defesa, o IIA (2013) admite esta 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 possuem 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), complementa esta afirmação ao dizer que as os recursos de cada linha não são independentes através delas mesmas, podendo causar na 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 auditoria interna. Portanto, o STM e o TDJFT podem não atender essa orientação do IIA, pois não foi confirmada a existência das reuniões regulares de seus respectivos comitês.

5. CONCLUSÕES E CONSIDERAÇÕES FINAIS

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 traz: "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" (BRASIL, 2021a). A partir da documentação analisada, não foram encontradas evidências de que os tribunais subordinados à ENSEC-PJ atendem essa exigência.

Considerando o cenário atual 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 perda ou vazamento de dados de cidadãos e entidades brasileiras. A adequação do 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.

A presente 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 TST, além da eventual indisponibilidade de documentos atualizados nas páginas web oficiais dos tribunais.

Como sugestão para trabalhos futuros, pode-se analisar os órgãos do poder Judiciário fora do Distrito Federal pela perspectiva de outros modelos e *frameworks* de gestão de riscos dentro de segurança cibernética. Pode-se pesquisar também caso existam planos futuros de adequação de estrutura organizacional dos tribunais analisados, de modo a atender integralmente a ENSEC-PJ.

6. REFERÊNCIAS

ABU-MUSA, A. A. **The Perceived Threats to the Security Computerized of Computadorized Accounting Information Systems**. Journal of American Academy of Business. Cambridge, v. 3, 2003.

AMERICANAS. Americanas: site volta a funcionar parcialmente após suposto ataque hacker. **InfoMoney**, 23 fev. 2022. Disponível em: https://www.infomoney.com.br/minhas-financas/americanas-site-volta-a-funcionar-parcialmente-apos-suposto-ataque-hacker/. Acesso em: 11 abr. 2022.

AMORIM, F. Barroso vê 'motivação política' e pede apuração da PF a ataques contra TSE. **UOL**, 16 nov. 2020. Disponível em: https://noticias.uol.com.br/eleicoes/2020/11/16/barroso-pede-investigacao-da-policia-federal-a-ataque-contra-sistema-do-tse.htm. Acesso em: 11 abr. 2022.

ANDERSON, D. J., & EUBANKS, G. The Commitee of Sponsoring Organizations of the Treadway Commission. **Leveraging COSO Across The Three Lines of Defense**. Carolina do Norte - EUA, 2015.

ANDERSON, K; TERP, A. **Risk Management, Andersen T.J. (ed.), Perspectives on Strategic Risk Management**. Denmark: Copenhagen Business School Press, 2016.

APLICATIVO. Aplicativo do ConecteSUS deixa de apresentar vacinas; site está fora do ar. **G1**, 10 dez. 2021. Disponível em: https://g1.globo.com/saude/noticia/2021/12/10/site-do-ministerio-da-saude-sofre-ataque-de-hackers-e-sai-do-ar.ghtml. Acesso em: 11 abr. 2022.

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

ARAÚJO, M. A gestão de riscos no âmbito da transformação digital. **TI INSIDE**, 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.

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

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NORMA BRASILEIRA ABNT NBR ISO/IEC 27005: Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação**. Rio de Janeiro, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NORMA BRASILEIRA ABNT NBR ISO/IEC 27001: Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos**. Rio de Janeiro, 2013.

BANTLEON, U. *et al.* Coordination challenges in implementing the three lines of defense model. **Wiley**, 2020, p. 59-74. 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. *et al.* **Cybersecurity and the risk function**. McKinsey&Company, 2018.

BONISCH, P. Excuse Me, How Many Lines of Defence? The New Financial Maginot Lines. **Thinking about strategy & uncertainty**, 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: 05 abr. 2022.

BRASIL. Memória. **Superior Tribunal Militar**, 2022d. Disponível em: https://www.stm.jus.br/o-stm-stm/memoria. Acesso em 09 mar. 2022.

BRASIL. **Ato nº 65/TST.GP, de 6 de abril de 2021**. Brasília, DF: Tribunal Superior do Trabalho, 2021f.

BRASIL. Atribuições. **Superior Tribunal de Justiça**, 2022b. Disponível em: https://www.stj.jus.br/sites/portalp/Institucional/Atribuicoes. Acesso em 09 mar. 2022.

BRASIL. Competência. **Justiça Federal: Seção Judiciária da Bahia**, 25 out. 2012. Disponível em: https://portal.trf1.jus.br/sjba/institucional/competencia/competencia.htm. Acesso em: 09 mar. 2022.

BRASIL. Governo Federal lança Plano Tático de Combate a Crimes Cibernéticos. **Governo do Brasil**, 23 mar. 2022a. Disponível em: https://www.gov.br/pt-br/noticias/justica-e-seguranca/2022/03/governo-federal-lanca-plano-tatico-de-combate-a-crimes-ciberneticos. Acesso em 06 abr. 2022.

BRASIL. Institucional. **Superior Tribunal Militar**, 2022c. Disponível em: https://www.stm.jus.br/o-stm-stm/institucional. Acesso em 09 mar. 2022.

BRASIL. Institucional. **Supremo Tribunal Federal**, 25 jan. 2019a. Disponível em: https://portal.stf.jus.br/textos/verTexto.asp?servico=sobreStfConhecaStfInstitucional. Acesso em 09 mar. 2022.

BRASIL. **Instrução normativa nº 3, de 9 de junho de 2017**. Brasília, DF: Diário Oficial da União, 2017a.

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

BRASIL. **Portaria GPR 1204 de 02 de julho de 2020**. Brasília, DF: Tribunal de Justiça do Distrito Federal e dos Territórios, 2020a.

BRASIL. **Portaria Nº 76, de 4 de março de 2021**. Brasília, DF: Diário Oficial da União, 2021b.

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

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

BRASIL. **Resolução nº 222, de 3 de fevereiro de 2016**. Brasília, DF: Superior Tribunal Militar, 2016.

BRASIL. **Resolução nº 298, de 4 de agosto de 2021**. Brasília, DF: Superior Tribunal Militar, 2021d.

BRASIL. **Resolução nº 301, de 8 de setembro de 2021**. Brasília, DF: Superior Tribunal Militar, 2021e.

BRASIL. **Resolução nº 396, de 7 de junho de 2021**. Brasília, DF: Conselho Nacional de Justiça, 2021a.

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

BRASIL. Sobre a Justiça do Trabalho. **Tribunal Superior do Trabalho**, 2022g. Disponível em: https://www.tst.jus.br/web/acesso-a-informacao/justica-do-trabalho. Acesso em 09 mar. 2022.

BRASIL. Sobre o TJDFT, **Tribunal de Justiça do Distrito Federal e dos Territórios**, 06 ago. 2019b. Disponível em: https://www.tjdft.jus.br/carta-de-servicos/conhecendo-o-tjdft Acesso em 09 mar. 2022.

BRASIL. Sobre o Tribunal Superior do Trabalho. **Tribunal Superior do Trabalho**, 2022f. Disponível em: https://www.tst.jus.br/web/acesso-a-informacao/conheca-o-tst. Acesso em 09 mar. 2022.

BRASIL. **TJDFT: Plano Diretor de Tecnologia da Informação e de Comunicação**. Brasília, 2022e. Disponível em: https://www.tjdft.jus.br/transparencia/governanca-de-tic/planejamento-de-tic/pdtic/pdtic-2022.pdf. Acesso em: 03 mar. 2022.

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

CHAMBERS, A. D., & ODAR, M. **A new vision for internal audit**. Managerial Auditing Journal, 34-55, 2015.

COMO. Como a tecnologia pode melhorar a gestão de riscos? **Redação upLexis**, 27 jun. 2017. Disponível em: https://uplexis.com.br/blog/artigos/tecnologia-e-gestao-de-riscos/. Acesso em: 26 abr. 2022.

COSTA, F. J. **Mensuração e desenvolvimento de escalas: aplicações em administração**. Rio de Janeiro, Ciência Moderna, 2011.

COUTO, J. C. Auditoria de Cibersegurança: um caso de estudo. 2018.

CRAIGEN, D., DIAKUN-THIBAULT, N., & PURSE, R. Defining Cybersecurity. **Technology Innovation Management Review**, 13-21, 2014.

DAMODARAN, A. **Gestão estratégica do risco**. Bookman, 2009.

DAVIES, H., & ZHIVITSKAYA, M. Three Lines of Defence: A Robust Organising Framework, or Just Lines in the Sand? **Global Policy**, v. 9, 2018, p. 34-42. Disponível em: https://onlinelibrary.wiley.com/doi/10.1111/1758-5899.12568. Acesso em: 10 ago. 2021.

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

FONTE, E. C. Gerenciamento de Riscos: Uma Comparação entre o Guia PMBOK 6ª Edição e a ISO 31000:2018. **Revista Boletim do Gerenciamento**, 2019, p. 22-32. Disponível em: https://nppg.org.br/revistas/boletimdogerenciamento/article/view/63. Acesso em: 04 fev. 2022.

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.

GREGORIO, D. **Re-thinking country risk: insights from entrepreneurship theory**. 2005.

GUERRA, E. A Era dos Dados e a preocupação com cibersegurança. Fonte: **TI Inside**, 07 abr. 2022. Disponível em: https://tiinside.com.br/07/04/2022/a-era-dos-dados-e-a-preocupacao-com-ciberseguranca/. Acesso em: 11 abr. 2022.

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 ago. 2021.

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

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **Risk Management ISO 31000**. Suíça, 2018. Disponível em: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100426.pdf. Acesso em: 23 mar. 2022.

INTERNATIONAL TELECOMMUNICATION UNION. **Understanding cybercrime: a guide for developing countries**. Technical Report, 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**. Internal Audit Foundation, 2018.

JUSTIÇA. Justiça Federal em Pernambuco sofre ataque cibernético e sistemas ficam fora do ar. **G1**, 06 abr. 2022. Disponível em: https://g1.globo.com/pe/pernambuco/noticia/2022/04/06/justica-federal-em-pernambuco-ataque-sistema-fora-do-ar.ghtml. Acesso em: 11 abr. 2022.

KUMAR, S. **Overlap between Second and Third Line of Defense for Risk Management**. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3938315. Acesso em: 09 fev. 2022.

LAGINESTRA, A. **Cibersegurança no Território Brasileiro: Impacto da LGPD e normas de Segurança da Informação na Defesa Nacional**. Abian Laginestra, 2021.

LAUDON, K. C., & LAUDON, J. P. **Sistemas de informação gerenciais**. México, Pearson Education, 2014.

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**, 2015, p. 243-250. 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.

MAANEN, 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.

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: 09 fev. 2022.

MACIEL, C.Tribunal Federal em São Paulo sofre ataque hacker e suspende serviços. **Agência Brasil**, 30 mar. 2022. Disponível em: https://agenciabrasil.ebc.com.br/justica/noticia/2022-03/tribunal-federal-em-sao-paulo-sofre-ataque-hacker-e-suspende-servicos. Acesso em: 08 abr. 2022.

MAGALHÃES, I. L., & PINHEIRO, W. B. **Gerenciamento de TI na prática: uma abordagem com base na ITIL**. São Paulo, Novatec, 2007.

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

MINISTÉRIO DA ECONOMIA. Assessoria Especial de Controle Interno (AECI**)**. **Ministério da Economia**, 12 out. 2021. Disponível em: https://www.gov.br/economia/pt-br/acesso-a-informacao/institucional/planejamento/unidades/aeci. Acesso em: 06 fev. 2022.

MOURA, R. M.. A impunidade dos hackers que colocaram o Judiciário de joelhos. **VEJA**, 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. V. **A definição de uma estratégia nacional de cibersegurança: cibersegurança**. Lisboa, 2012.

PAXSON, D., & WOOD, D. **The Blackwell Encyclopedic Dictionary of Finance**. Massachusetts, Blackwell Publishers Ltd., 1998.

PONTES, F. STJ é alvo de ataque de hacker e Polícia Federal investiga o sistema. **Agência Brasil**, 04 nov. 2022. Disponível em: https://agenciabrasil.ebc.com.br/justica/noticia/2020-11/stj-e-alvo-de-ataque-de-hacker-e-policia-federal-investiga-o-sistema. Acesso em 11 abr. 2022.

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-Good-Risk-Management-. Acesso em: 05 ago. 2021.

PRADO, F. Brasil foi 5º país com mais ataques cibernéticos no ano: relembre os principais. **ISTOÉ Dinheiro**, 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 08 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**, 25 mar. 2013. Disponível em: http://dgpdn.blogspot.com/2013/03/artigo-de-opiniao-ciberseguranca-e.html. Acesso em: 10 out. 2021.

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.

THE HARRIS POLL. **2022 Cyber Safety Insights Report**. 2022. Disponível em: https://www.nortonlifelock.com/us/en/newsroom/press-kits/2022-norton-cyber-safety-insights-report-special-release-online-creeping/. Acesso em: 24 fev. 2022.

TRANCHARD, S. (2018). The new ISO 31000 keeps risk management simple. **ISO**, 15 fev. 2018. Disponível em: https://www.iso.org/news/ref2263.html. Acesso em: 06 abr. 2022.

TRIBUNAL REGIONAL FEDERAL DA 1ª REGIÃO. INSTITUCIONAL: 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 fev. 2022.

TRIBUNAL SUPERIOR DO TRABALHO. (s.d.). Justiça do Trabalho. **Justiça do Trabalho**, s.d. Disponível em: https://www.tst.jus.br/web/gestaoestrategica/processos-conceitos. Acesso em: 09 mar. 2022.

TRIBUNAL SUPERIOR DO TRABALHO. **Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC)**. Brasília, 2020.

TRIBUNAL. Tribunal Regional do Trabalho do ES sofre ataque cibernético. **G1**, 21 fev. 2022. Disponível em: https://g1.globo.com/es/espirito-santo/noticia/2022/02/21/tribunal-regional-do-trabalho-do-es-sofre-ataque-cibernetico.ghtml. Acesso em: 11 abr. 2022.

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

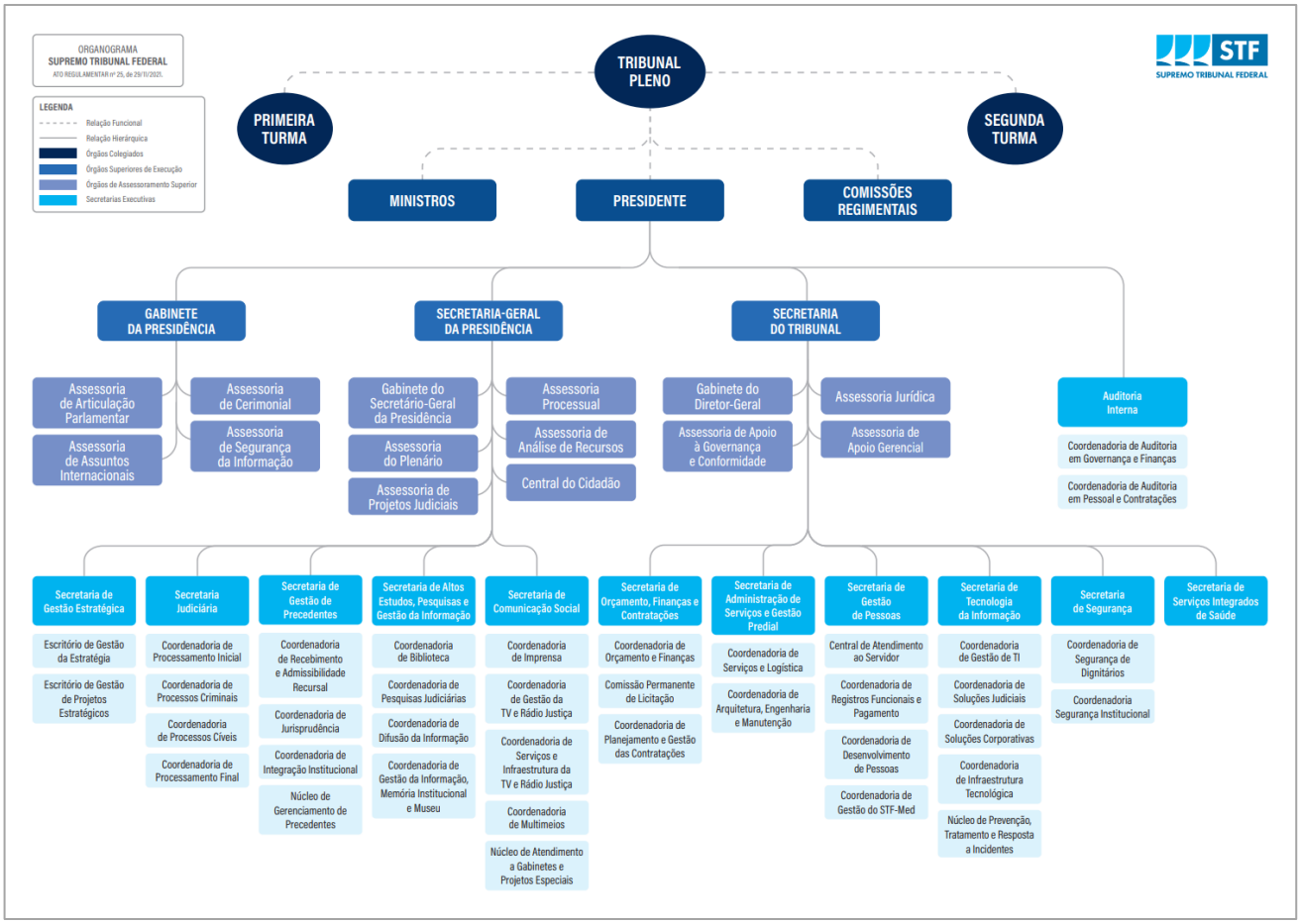
VALENTE, J. Brasil é o país com maior número de vítimas de phishing na internet. **InfoMoney**, 04 mar. 2021. Disponível em: https://www.infomoney.com.br/consumo/brasil-e-o-pais-com-maior-numero-de-vitimas-de-phishing-na-internet/. Acesso em: 11 abr. 2022.

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, 2021, p. 95-110.

WHITMAN, M. E., & MATTORD, H. J. (2018). **Principles of Information Security**. Geórgia-EUA, Cengage Learning, 2018.

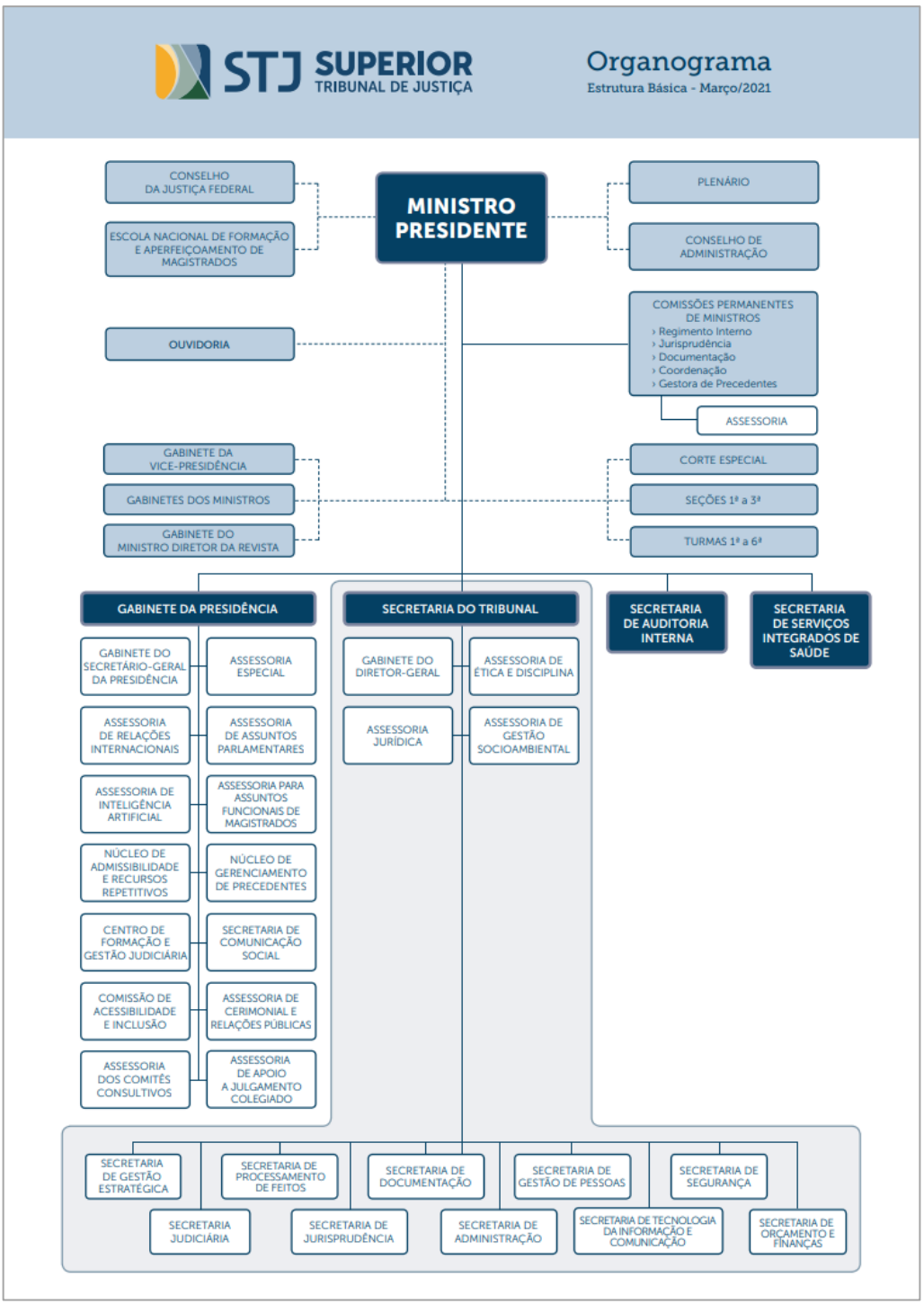
7. ANEXOS

ANEXO A – ORGANOGRAMA STF



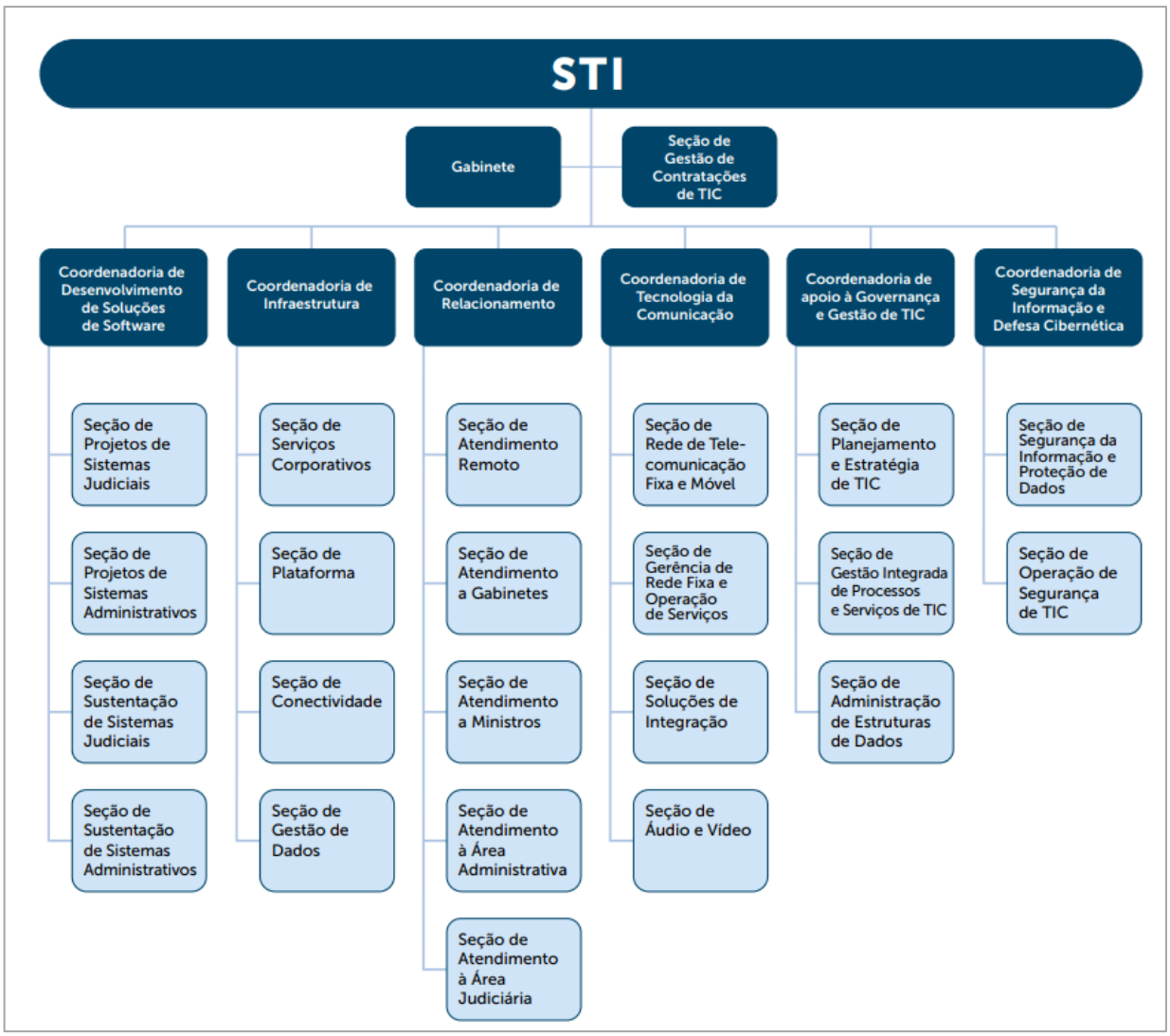
Fonte: Organograma Supremo Tribunal: Ato Regulamentar n. 25, de 29/11/2021. Supremo Tribunal Federal. Brasília (DF), 2021. Disponível em: https://portal.stf.jus.br/textos/verTexto.asp?servico=sobreStfOrganograma. Acesso em: 02 mar. 2022.

ANEXO B – ORGANOGRAMA STJ



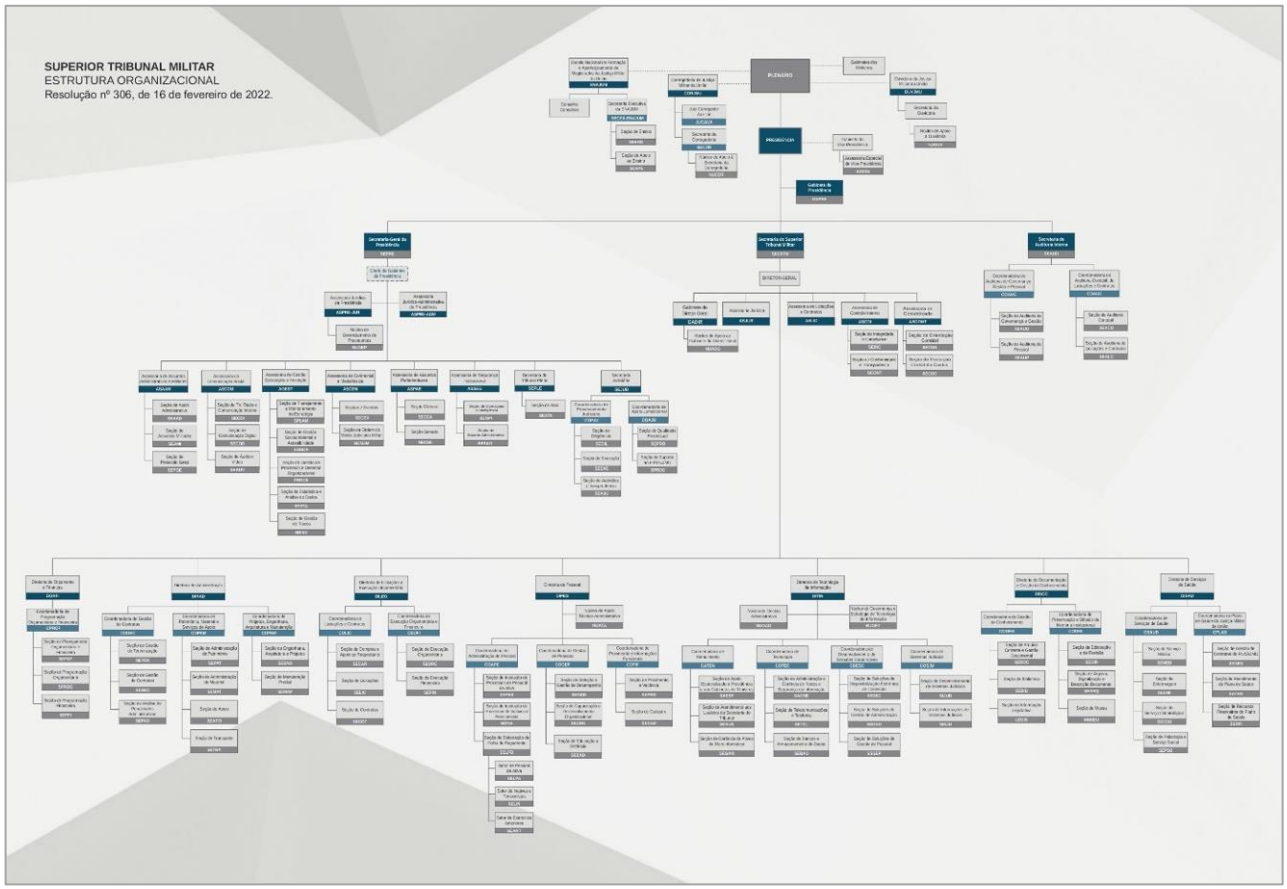
Fonte: Organograma: Estrutura Básica. Superior Tribunal de Justiça. Brasília (DF), 2018. Disponível em: https://www.stj.jus.br/static_files/STJ/Midias/arquivos/2482_Org_Estrutura_Basica.pdf. Acesso em: 02 mar. 2022.

ANEXO C – ORGANOGRAMA DA STI/STJ



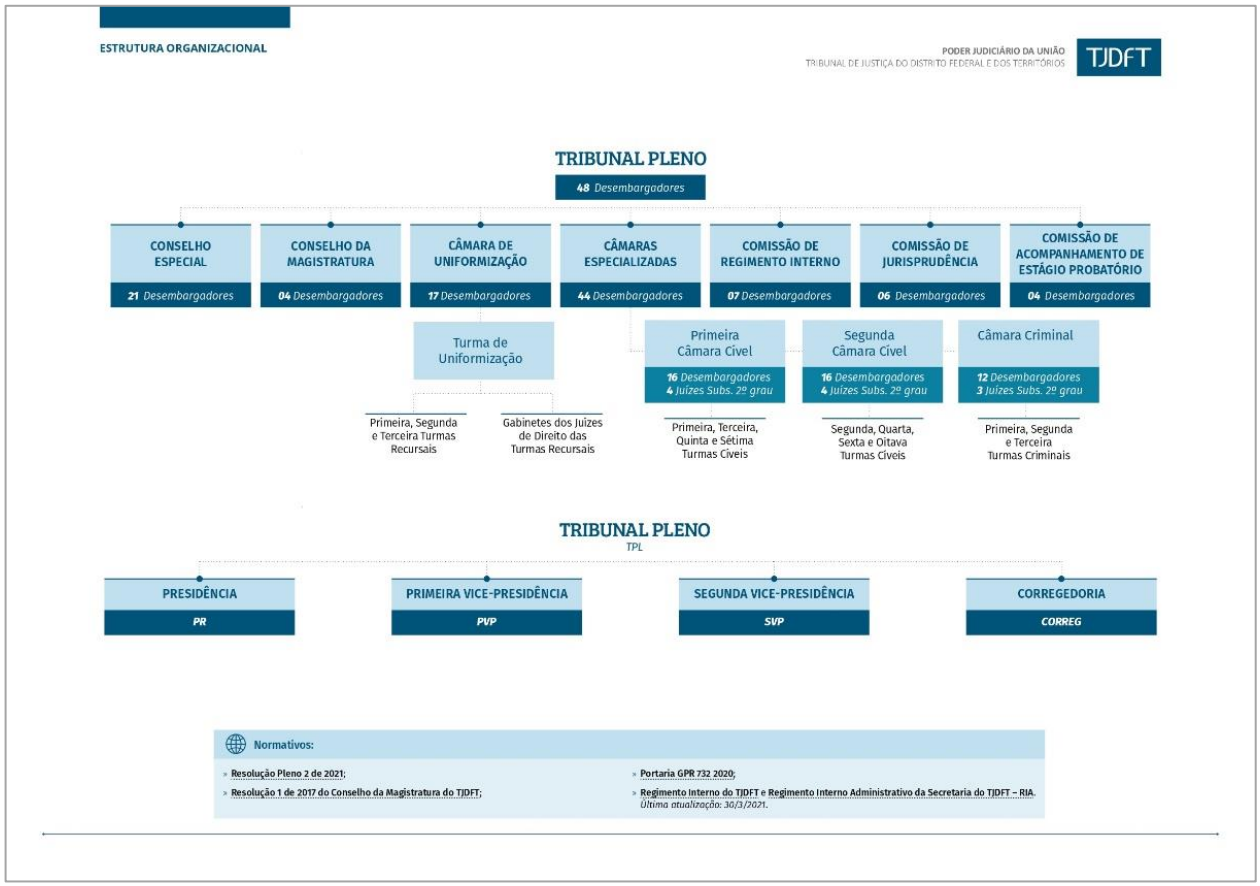
Fonte: Plano Diretor de Tecnologia da Informação e Comunicação. Superior Tribunal de Justiça. Brasília (DF), 2021. Disponível em: https://www.stj.jus.br/publicacaoinstitucional/index.php/PDTIC/issue/archive. Acesso em: 03 mar. 2022.

ANEXO D – ORGANOGRAMA DO STM



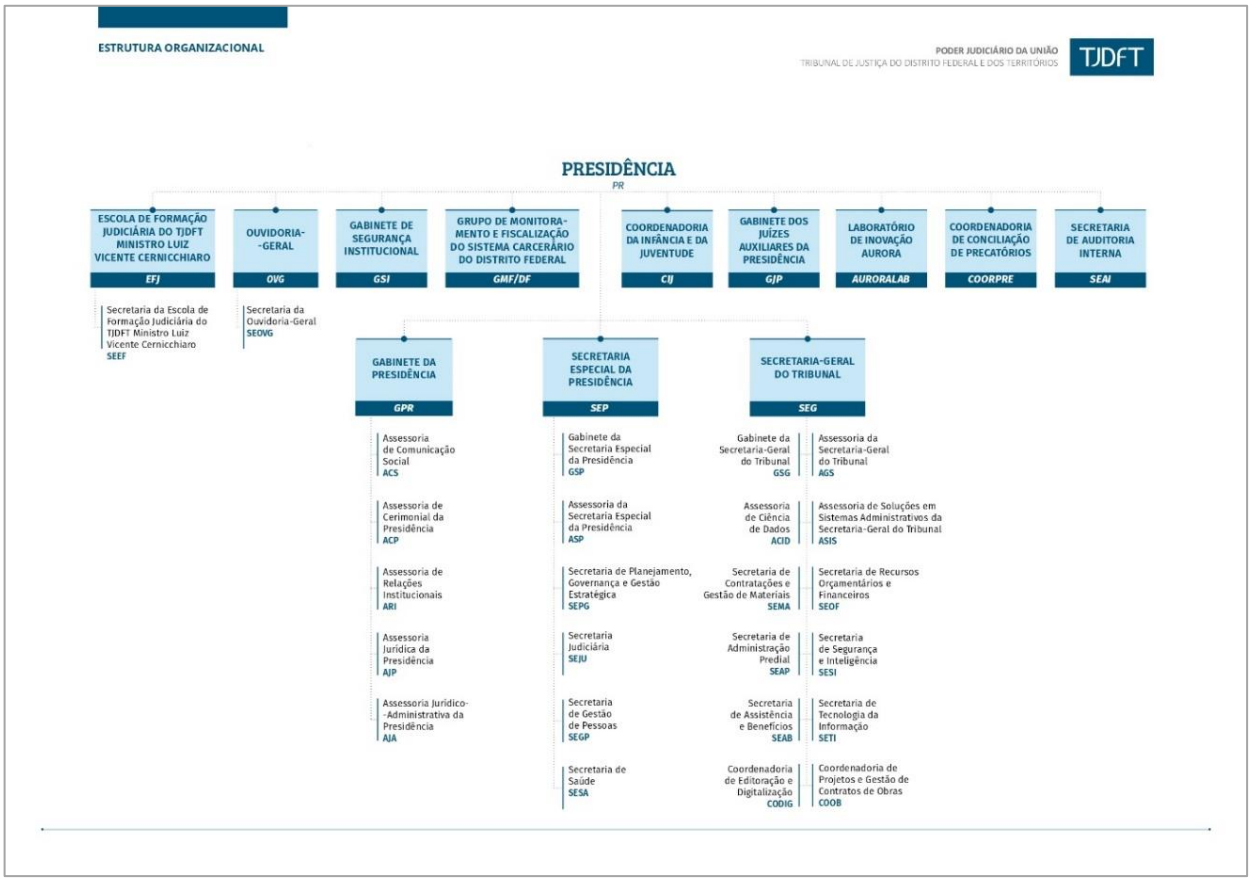
Fonte: Estrutura Organizacional: Resolução n. 306, de 16 de fevereiro de 2022. Superior Tribunal Militar. Brasília (DF), 2022. Disponível em: https://www.stm.jus.br/images/arquivos/institucional/Organograma_estrutura%20organizacional_v10.pdf. Acesso em: 09 mar. 2022.

ANEXO E – ORGANOGRAMA DO TJDFT



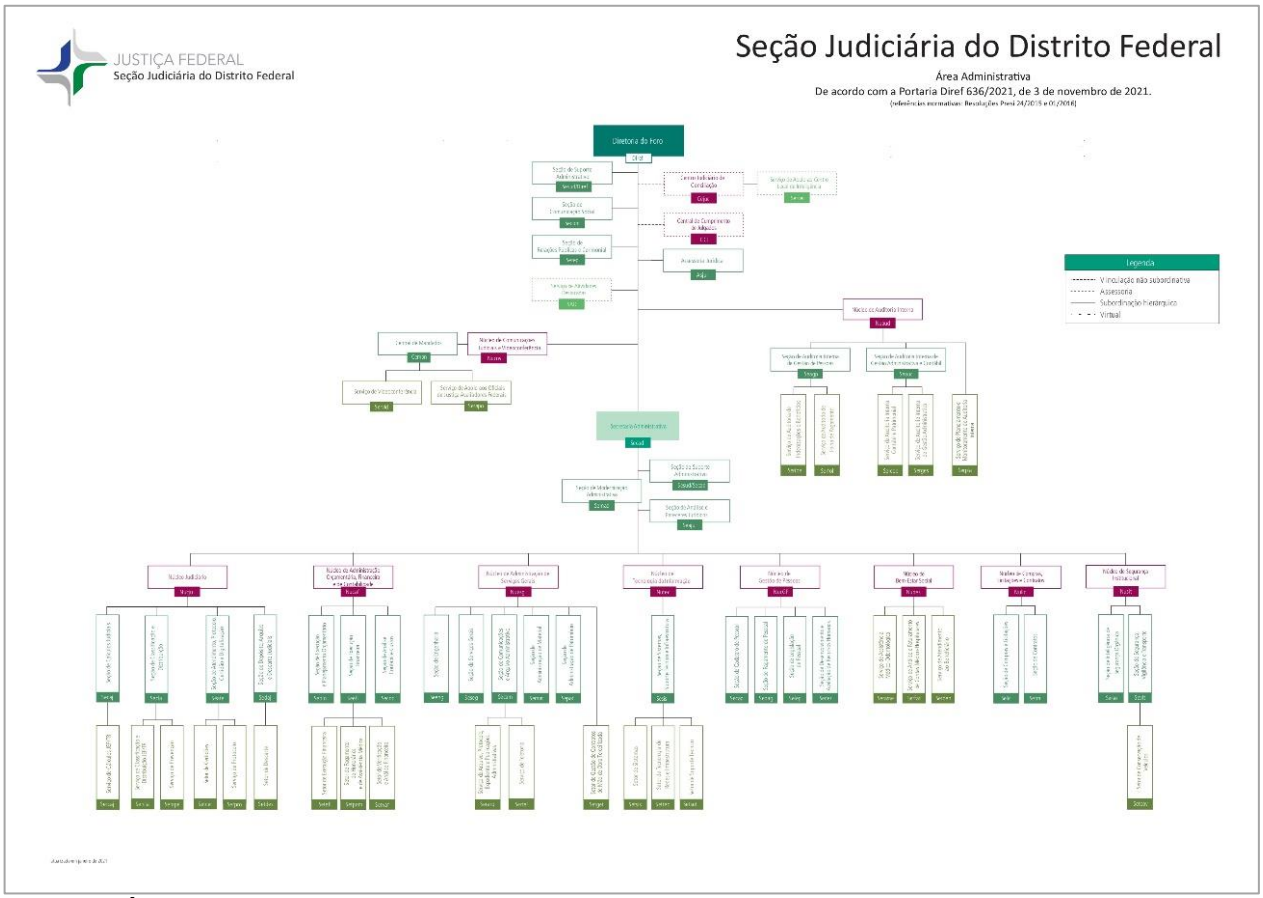
Fonte: Estrutura Organizacional. Tribunal de Justiça do Distrito Federal e dos Territórios. Brasília (DF), 2022. Disponível em: https://www.tjdft.jus.br/transparencia/estrutura-organizacional. Acesso em: 09 mar. 2022.

ANEXO F – ORGANOGRAMA DO TJDFT



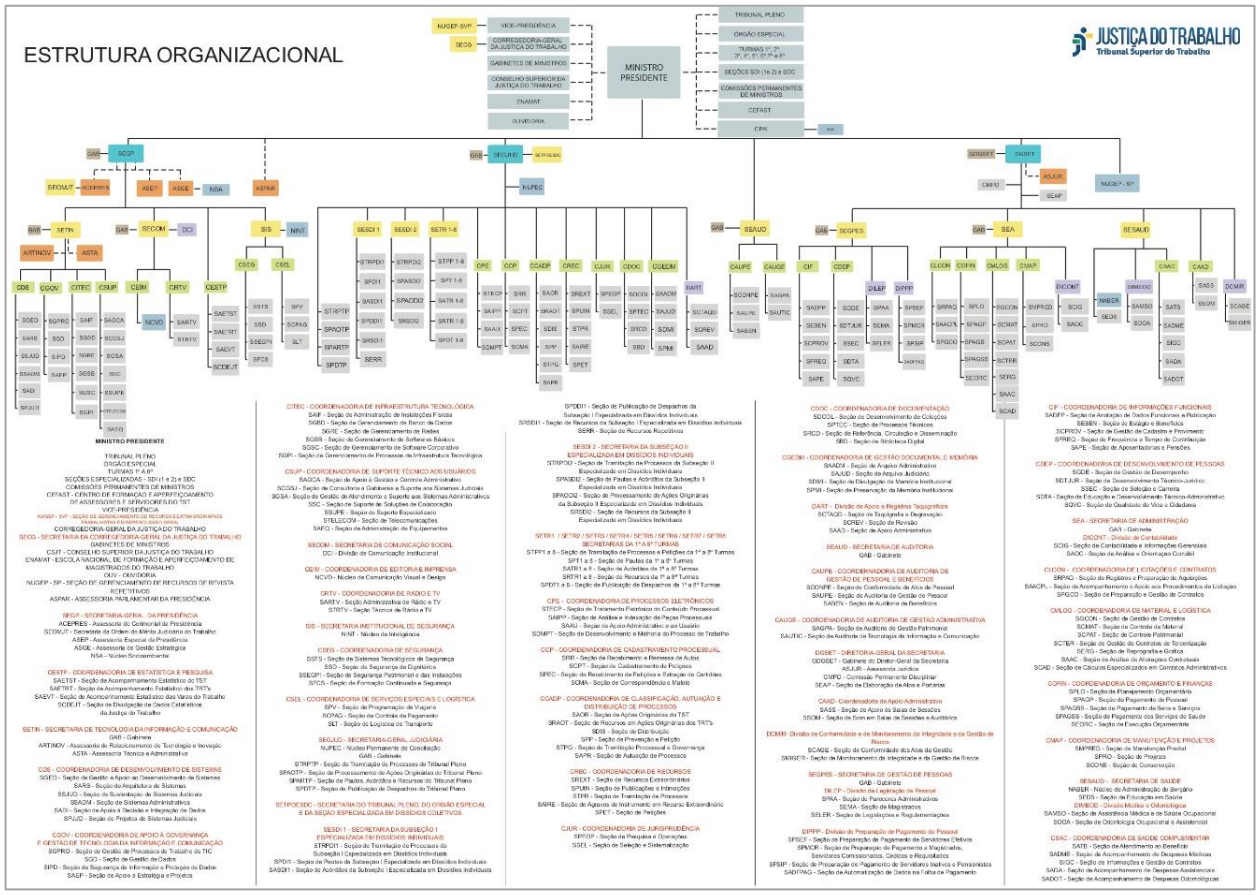
Fonte: Estrutura Organizacional. Tribunal de Justiça do Distrito Federal e dos Territórios. Brasília (DF), 2022. Disponível em: https://www.tjdft.jus.br/transparencia/estrutura-organizacional. Acesso em: 09 mar. 2022.

ANEXO G – ORGANOGRAMA DO TRF1



Fonte: Área Administrativa: De acordo com a Portaria Diref 636/2021, 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: 09 mar. 2022.

ANEXO H – ORGANOGRAMA DO TST



Fonte: Estrutura Organizacional. Tribunal Superior do Trabalho. Brasília (DF), Disponível em: https://www.tst.jus.br/web/acesso-a-informacao/organograma. Acesso em: 09 mar. 2022.