Protegendo a Justiça: as estruturas institucionais de governança de segurança cibernética no Poder Judiciário de Pernambuco, Brasil ante as instituições nacionais e internacionais[1]

Protegendo la Justicia: las estructuras institucionales de gobernanza de seguridad cibernética en el Poder Judicial de Pernambuco, Brasil ante las instituciones nacionales y internacionales

João Vitor Sales Zaidan[2]
Orientação: Claire Craig

Setembro de 2024

[1] Esta pesquisa foi desenvolvida no âmbito do Programa Líderes 2024, do Registro de Endereçamento da Internet para a América Latina e o Caribe (LACNIC). As opiniões e pontos de vista expressos neste relatório são de total responsabilidade do autor e não refletem a posição do LACNIC.

[2] Graduando em Direito na Universidade Federal de Pernambuco, Brasil. Pesquisador em Direito Internacional dos Direitos Humanos, com bolsa da Fundação de Amparo à Ciência e Tecnologia de Pernambuco.

Resumo

De que maneiras os órgãos do Poder Judiciário estadual e federal de Pernambuco estruturam a segurança cibernética de seus sistemas ante diretrizes nacionais e internacionais? Em um contexto de crescente digitalização de atividades, em especial do serviço público e do Poder Judiciário, esta investigação busca desvelar arranjos institucionais e processos de formulação de instituições, enquanto regras, que guiam práticas em matéria de segurança cibernética do Tribunal de Justiça de Pernambuco e do Tribunal Federal da 5ª Região. Por meio da análise de conteúdo categorial de normativas internas dos tribunais, busca-se entender como os órgãos estruturam-se em relação ao tema e aplicam recomendações e políticas nacionais e internacionais, como as do Conselho Nacional de Justiça e a Estratégia Nacional de Segurança Cibernética. A pesquisa traz uma fundamentação sobre o debate conceitual e institucional no tema no Brasil e no mundo, sublinhando questões como a compartimentalização da regulação no Brasil, fragmentação entre atores e a dinâmica de ameaças e maturidade. Como resultados, foram categorizados 78 documentos, sendo que 34% correspondem a boas práticas e disseminação de informações, 21%, a estrutura organizacional, e 22% têm conteúdo geral. Destacam-se questões como a maior força institucional das resoluções do CNJ no TJPE, uma dupla compartimentação no TRF5, a reafirmação da fragmentação, com baixa previsão de cooperação com outros atores e problemas de transparência unidos a uma lógica de urgência no tratamento de incidentes e ameaças que vai de encontro à participação social e ao dever de publicidade. Com a multiplicação de ameaças no ciberespaço, a governança da segurança cibernética reafirma-se como um tema no topo da agenda, sendo esta pesquisa uma forma de contribuir para a compreensão de como o Judiciário local lida com a questão.

Palavras-chave: segurança cibernética; instituições; normativas internas; estruturação; tribunais de justiça.

Abstract

In which ways the bodies of the state and federal Judiciary Branch of Pernambuco structure the cybersecurity of their systems over national and international directives? In a context of mounting digitalization of activities, especially of public service and of the Judiciary Branch, this investigation aims to uncover institutional arrangements and institution-making processes that guide cybersecurity practices of the Pernambuco Court of Justice (TJPE) and the Federal Justice Court of the 5th Região (TRF5). Through categorial content analysis of the courts' internal normative, it is sought to understand how the bodies structure themselves when it comes to the matter and apply recommendations and national and international policies, such as the National Council of Justice and the National Cybersecurity Strategy. The research brings a theoretical basis of the conceptual and institutional debate in Brazil and in the world, underscoring issues such as the compartmentalization of the regulation in Brazil, fragmentation between actors and the threats and maturity dynamic. As results, 78 documents were categorized: 34% correspond to good practices and information dissemination, 21%, to organizational structure, and 22% have a general content. Some issues stand out, such as the bigger institution strength of CNJ resolutions in TJPE, a double compartmentalization in TRF5, the reassurance of fragmentation, with low prevision of cooperation with other actors and transparency problems united to a logic of urgency in incidents and threats treatment that goes against social participation and the publicity duty. With multiplying threats in cyberspace, cybersecurity governance reassures itself as a theme in the top of the agenda, with this research being a way of contributing to the understanding of the local Judiciary addresses the issue.

Keywords: cybersecurity; institutions; internal normative; structuring; justice courts.

SUMÁRIO

INTRODUÇÃO 4

1 O DEBATE SOBRE SEGURANÇA CIBERNÉTICA NO BRASIL E NO MUNDO5

2 SEGURANÇA CIBERNÉTICA: PANORAMA DAS INSTITUIÇÕES E DIRETRIZES NO BRASIL E NO MUNDO 11

2.1 EVOLUÇÃO HISTÓRICA 11

2.2 ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA E CONTEXTO ATUAL 17

2.3 PODER JUDICIÁRIO E SEGURANÇA CIBERNÉTICA 21

3 METODOLOGIA E DESENHO DE PESQUISA 26

4 O PODER JUDICIÁRIO EM PERNAMBUCO E A FORMULAÇÃO DE NORMAS EM SEGURANÇA CIBERNÉTICA 28

4.1 OBJETIVOS, METAS E INDICADORES 33

4.2 ESTRUTURA ORGANIZACIONAL E DE COMPETÊNCIAS 36

4.3 BOAS PRÁTICAS, CAPACITAÇÃO E DISSEMINAÇÃO DE INFORMAÇÕES 39

4.4 RESPOSTA A INCIDENTES E GESTÃO DE RISCOS 42

4.5 INFRAESTRUTURA E ORÇAMENTO 47

4.6 TRANSPARÊNCIA E FISCALIZAÇÃO 48

CONSIDERAÇÕES FINAIS 50

REFERÊNCIAS 52

INTRODUÇÃO

De que maneiras os órgãos do Poder Judiciário estadual e federal de Pernambuco estruturam a segurança cibernética de seus sistemas ante diretrizes nacionais e internacionais? Em um contexto de crescente digitalização de atividades, em especial do serviço público e do Poder Judiciário (Hino; Cunha, 2020), esta investigação busca desvelar os arranjos institucionais e os processos de formulação de instituições, enquanto regras, que guiam práticas em matéria de segurança cibernética dos âmbitos pesquisados. Com a multiplicação de ameaças no ciberespaço (Stolz; Axon, 2023) — que têm o potencial de comprometer sistemas de informação e comunicação e acessar informações sigilosas, por exemplo — a governança da segurança cibernética reafirma-se como um tema no topo da agenda, de especial importância para órgãos que prestam serviços essenciais à sociedade, sendo esta pesquisa uma forma de contribuir para a compreensão de como o Judiciário local lida com a questão e se relaciona com normas mais abrangentes.

Especificamente, pretende-se descrever de que maneiras o Tribunal de Justiça de Pernambuco (TJPE) e o Tribunal Federal da 5ª Região (TRF5), em âmbito local, aplicam na prática recomendações e políticas nacionais e internacionais de segurança cibernética, de modo a descrever como os sistemas digitais de tais organizações protegem-se de ameaças. A ideia é compreender como ocorre o delineamento dessa estratégia, ou mesmo se há alguma estratégia, comparando semelhanças e diferenças entre diferentes esferas (como estadual e federal), e analisando aspectos como estabelecimento e disseminação de boas práticas, destinação de recursos, formulação de regras internas, accountability e gestão de riscos.

Como apontado por Alves, Carvalho & Nunes (2023), em uma realidade de serviços e processos judiciais digitalizados, os riscos dessas atividades devem ser levados em conta. Eles incluem o comprometimento de dados e de decisões, assim como a proteção de infraestruturas relacionadas. Vale ressaltar, ainda, que o TRF5, em 2022, já sofreu um ataque cibernético, assim como outros tribunais (Alves; Carvalho; Nunes, 2023), como o Superior Tribunal de Justiça, corroborando a necessidade de se revisar e garantir um arranjo institucional efetivo em matéria de segurança cibernética. Nesse sentido, é clara a relevância desta investigação, de modo a compreender como os tribunais analisados figuram nesse sentido, inclusive quanto à necessidade de alinhamento de políticas, conforme ressaltado por Hurel (2021), em especial por se constatar, na literatura, uma escassez de pesquisas aplicadas ao estudo de estruturas institucionais nesse campo.

O presente trabalho organiza-se em quatro seções principais, além da introdução e das considerações finais. A primeira resgata os principais pontos do debate sobre segurança cibernética no Brasil e no mundo. A segunda elenca o arcabouço institucional no tema no Brasil e no mundo, incluindo diretrizes e resoluções de órgãos nacionais. A terceira detalha a

metodologia utilizada e o desenho de pesquisa, incluindo análise de conteúdo categorial e comparativa dos documentos internos dos tribunais. A quarta, por sua vez, traz os resultados da investigação, com a análise das normativas e documentos internos dos tribunais pesquisados, com destaque a algumas variáveis de análise.

1 O DEBATE SOBRE SEGURANÇA CIBERNÉTICA NO BRASIL E NO MUNDO

Esta seção tem o objetivo de apresentar os principais pontos do debate sobre cibernética, com foco no Brasil, de modo a compreender as questões mais relevantes nesse sentido, o histórico da discussão sobre o tema no país e os impulsionadores dos avanços nesse âmbito. Utilizou-se revisão bibliográfica, majoritariamente de autores brasileiros, considerando o propósito de levantar os pontos de relevo no contexto nacional, a ser relacionado ao panorama institucional nacional sobre segurança cibernético, tema da seção seguinte.

A conceituação de segurança cibernética surge em um contexto de preocupação com a proteção de sistemas informatizados contra ameaças virtuais (Assunção, 2023, p. 23). Tal visão é observada no marco de uma utilização maior e mais intensa do ciberespaço, isto é, do espaço virtual, constituído pelos serviços e atividades realizados na internet, a partir do termo criado cunhado pelo escritor William Gibson. Canongia & Mandarino Junior (2009), obra de quinze anos atrás, enfatiza a proporção e número crescente, já na época, de ataques de hackers em diversos países. Os debates sobre o tema datam, mais inicialmente, da década de 1980, sendo concentrados nos Estados Unidos, inclusive a partir do National Institute of Standards and Technology (NIST). Até a atualidade, como mostra a análise bibliométrica de Assunção (2023), trabalhos de pesquisadores do país norte-americano ainda são os mais citados no campo da segurança cibernética.

A União Internacional de Telecomunicações (UIT), em sua definição de segurança cibernética como coleção de práticas em torno da proteção do ambiente virtual e de ativos contra riscos, inclui também objetivos-atributos que devem estruturar a atuação na matéria (Alves Júnior, 2011, p. 20). Eles compreendem disponibilidade, integridade, autenticidade, não-repúdio e confidencialidade, de modo a garantir sistemas que são estáveis e com baixa vulnerabilidade a ataques e ameaças. (UIT, 2008) Tais princípios são basilares para a segurança cibernética, estando em normativas de outras organizações e do Brasil, como será explorado na seção seguinte. Mais do que apenas a segurança de computadores, trata-se de redes e de informação, além de outras áreas adjacentes, abrangendo diversas áreas econômicas, sociais e políticas (Viganò; Loi; Yaghmaei, 2020). Como aponta Hurel (2021), não apenas redes são abrangidas pela segurança cibernética, mas também o enfrentamento

de ameaças híbridas e estabilidade de serviços essenciais, eleições e preservação da democracia e da participação multissetorial na governança digital.

A definição do conceito, contudo, não é consensual, com algumas sendo mais centradas em sistemas e indivíduos e outras, no ciberespaço em si, com uma abordagem mais generalizante (Hurel, 2021). No Brasil, conforme destacado por Da Cruz (2013), é possível notar, ao menos nos primeiros momentos da institucionalização da temática, uma maior ênfase em sistemas entendidos como estratégicos (Barros; Gomes; Freitas, 2011). Esse enfoque pode ser compreendido como consequência de um processo de securitização do tema, como será abordado à frente. Mais recentemente, como expresso no Glossário de Segurança da Informação do Gabinete de Segurança Institucional (GSI) da Presidência da República, publicado pela Portaria nº 93/2021 do órgão, tem-se que a segurança cibernética são "ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético" (Brasil, 2021), trazendo também os objetivos-atributos da definição da UIT e uma preocupação com os dados processados, armazenados os transmitidos nos sistemas. Tem-se, então, um foco nestes, em detrimento do indivíduo.

Hurel & Lobato (2018) apontam que segurança cibernética insere-se dentro de uma esfera maior, que é a da segurança da informação, relacionada a riscos de sistemas de informação e controles de diferentes tipos. Antes de ganhar um tratamento mais dedicado, a primeira, no Brasil, deu e ainda dá guarida para iniciativas relacionadas à segunda. Há, ainda, a defesa cibernética, que é mais ligada à dimensão militar, de soberania nacional e de ameaças externas. Tais divisões ensejam competências no Brasil, com atores que se dedicam, especificamente, a cada um desses âmbitos. Apesar de os temas apresentarem convergências e, assim, demandar-se cooperação entre entidades envolvidas, ainda são observados obstáculos para tal. Belli *el al.* (2023), por sua vez, entendem que é o contrário: a segurança da informação é uma dimensão da segurança cibernética, sendo a visão contrária limitante no que tange à formulação de políticas.

A segurança cibernética abarca diferentes dimensões em matéria de implementação de normas e construção de capacidades. Há tanto questões de infraestrutura e domínio de produção de equipamentos e sistemas, como de resposta a incidentes e ataques e em especial de arranjo institucional que possibilite tais atividades, assim como a disseminação de boas práticas. Stolz & Axon (2023), por exemplo, ao construir um modelo de maturidade de capacidade de segurança cibernética, incluem política, estratégia, cultura e sociedade no âmbito da problemática, bem como a geração de conhecimento e capacidade, regulação e normas e padrões e tecnologias. Nota-se, dessa maneira, como a área é múltipla e inclui diferentes necessidades que se completam, ainda que exijam esforços específicos.

Belli *et al.* (2023) chamam a atenção para a importância de se tomar em conta quão dinâmicas são as ameaças, motivo que intensifica a necessidade de coordenação intersetorial e da superação da fragmentação. Os autores apontam para a multiplicidade de ataques que podem ocorrer tanto a partir da ação de atores quanto do descuido e da ausência de adoção de boas práticas, diminuindo o custo dos ataques e levando a impactos no fornecimento de serviços e nos esforços necessários para restabelecê-los. Entre os eventos possíveis, estão desinformação, uso de código e sistemas maliciosos para obter dados, estelionato de dados, em que se leva pessoas a compartilharem informações por meio de engenharia social, fraudes, roubo de identidades, ataques em que adentra o sistema da vítima e até exploração de vulnerabilidades não identificadas anteriormente. Assevera-se, pois, a necessidade de uma compreensão holística da segurança cibernética, para além dos objetivos-atributos da UIT, considerando também a dimensão da soberania digital e da autonomia em termos cibernéticos.

No Brasil, apesar de haver normativas e produções no âmbito da segurança cibernética desde o início do século, como será explorado na próxima seção, Aguiar (2023) e Hurel & Lobato (2018) destacam que o processo de institucionalização foi catalisado por algumas situações em específico. A primeira delas é o Marco Civil da Internet, que surgiu em um contexto de revelação de programas de espionagem dos Estados Unidos de comunicações de líderes incluindo a então presidenta da República, Dilma Rousseff. A preocupação gerada por esse evento lançou luz sobre questões como a privacidade e proteção de dados, bem como segurança da informação, em especial cibernética. Já a segunda deu-se no âmbito de megaeventos sediados no Brasil entre 2012 e 2016, como os Jogos Olímpicos.

A partir desses vetores, tanto novos órgãos foram criados, como o Comando e o Centro de Defesa Cibernética (ComDCiber), das Forças Armadas, quanto organizações já existentes foram mobilizadas para tratar do assunto. Observa-se, nesse sentido, alguns aspectos e consequências do processo acelerado de institucionalização da questão. Hurel & Lobato (2018) destacam que existe uma certa sobreposição de competências e de atuações entre distintos órgãos da Administração Pública. Além dos criados no contexto de maior ênfase do tema, há participação de atores como o Comitê Gestor da Internet no Brasil (CGI.br), criado em 1995, e o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, criado em 1996, além de outros que também têm outras funções, a exemplo da Polícia Federal, em especial no que tange aos crimes cibernéticos. O GSI e a Agência Brasileira de Inteligência (ABIN) têm, ainda, papel destacado nesse âmbito, como será demonstrado no panorama de instituições formais de segurança cibernética, na próxima seção.

Contudo, ainda que haja uma da multiplicidade de atores envolvidos, uma característica trazida por Hurel & Lobato (2018) é a excessiva participação do setor militar na arquitetura de proteção da segurança cibernética. Em especial a partir do contexto de megaeventos, em

que a questão ganhou um tom de maior urgência, devido às ameaças mais pronunciadas de ataques e com maior atenção e do seu reconhecimento como prioridades de segurança nacional. A ocorrência de ataques a sites governamentais, como o registrado em 2013, deu ainda mais força a esse processo de securitização, algo institucionalizado com a criação, por exemplo, do ComDCiber e a inclusão, na primeira Estratégia Nacional de Defesa do Brasil, publicada em 2008, do espaço cibernético como um dos setores estratégicos (junto aos nuclear e espacial) para a segurança e a defesa nacional, responsabilizando o Exército Brasileiro pela execução e coordenação de programas relativos à área, ainda que haja espaço para cooperação.

Esse processo de maior envolvimento de organizações militares no delineamento e execução de regras, bem como na repartição de competências, pode ser associado à teoria da securitização (Cepik; Canabarro; Borne, 2014). Como apontam Buzan, Wæver & Wilde (1998), o conceito consiste em um processo de retirada do tema da esfera política e inserção no âmbito militar, tornando-o preocupação deste. Trata-se de um contexto que em a segurança internacional passou a abarcar novos temas, vistos como relevantes a nível securitário. Em resumo, o processo compreende a identificação de uma ameaça e a proposta, por parte de um ator securitizador, agente com autoridade sobre um tema para apresentá-lo a um público relevante e fazê-lo aceitar e legitimar as medidas emergenciais, em um chamado movimento securitizador. A aceitação por parte do público é fator essencial para o sucesso de tal processo, na medida em que ele é baseado na argumentação de que a esfera política torna-se insuficiente para enfrentar a ameaça em questão, sendo necessário lançar mão de medidas que fogem do escopo político, em um contexto de emergência (Silva; Pereira, 2019, p. 4).

A argumentação emergencial surge não apenas com os megaeventos, como também com a ideia de ameaças constantes e a consequente necessidade de tomar medidas de forma urgente para combatê-los e manter sistemas, em especial as chamadas infraestruturas críticas, seguros. Consequências desse arranjo institucional incluem uma tensão entre o imperativo de defesa e segurança e a asseguração de direitos, como à privacidade (Aguiar, 2023, p. 42). O respeito ao princípio da legalidade — que deve basear os atos da Administração Pública, conforme Mello (2023) — coloca-se, pois, em colisão com a questão da segurança, em detrimento de uma abordagem que una as duas esferas, em um processo de formulação de políticas que as coloque lado a lado.

De acordo com Hurel & Lobato (2018), esses elementos relacionam-se com a falta de participação de atores não-estatais no processo de formulação de políticas de segurança cibernética. O regime de Governança da Internet no Brasil, ao contrário, apresenta uma arquitetura multissetorial, com uma composição relativamente equânime da sociedade civil, do setor técnico-científico e do governamental. Em matéria de segurança cibernética,

contudo, órgãos estatais dedicados ao tema são notavelmente fechados à participação social e multissetorial e com obstáculos para a cooperação entre órgãos e grupos. Esse arranjo institucional leva a questões como a tensão entre direitos e criminalização de condutas e uma maior preferência por política de bloqueio e remoção de conteúdo. Além disso, considerando

Com a análise da literatura sobre o tema do Brasil, em especial de publicações com mais de seis anos de veiculação, foi possível notar uma maior ênfase à estrutura organizacional e de competências em matéria de segurança cibernética, em detrimento de discussões sobre a delimitação conceitual do tema. Tal observação reflete o que Cepik, Canabarro & Borne (2014) observam quanto a uma falta de definição clara sobre tipos de incidentes e outros temas correlatos, levando a uma confusão semântica sobre a problemática. Também relacionado à questão está a fragmentação entre setores apontada por Hurel (2021), de modo que há lacunas em matéria de coordenação e cooperação, algo essencial em se tratando do ciberespaço e para efetivar instituições e regras propostas (Da Cruz Junior, 2013).

Belli et al. (2023) chamam essa falta de coordenação e de força institucional de documentos nacionais de compartimentalização: em detrimento de uma estratégia e princípios, objetivos e diretrizes convergentes, há resoluções e regras de segurança cibernética setoriais em diferentes esferas, notadamente infraestruturas críticas. Nesse sentido, agências reguladoras e áreas como mercado financeiro têm normas próprias sobre o tema, o que é sintoma da fragmentação, levando a uma compartimentação de cada setor dentro do seu próprio arcabouço de normas, algo que mina a capacidade institucional do país como um todo e de estratégias abrangentes na agenda ora estudada. Esse cenário, para os autores, é estimulado pela legislação e pela organização de planos nacionais, criando vulnerabilidades sistêmicas.

Outra consequência desse cenário de desconexão entre atores é a dificuldade de adaptar políticas do campo estratégico para o operacional, com a implementação de estratégias mais abrangentes em contextos locais (Cepik; Canabarro; Borne, 2014). Esse ponto está diretamente ligado ao objeto desta pesquisa, na medida em que se busca analisar um recorte da realidade nacional em matéria de segurança cibernética, a partir da realidade local e em um campo específico. Investigar as estruturas internas do Poder Judiciário e de outras esferas do setor público permite, desse modo, permite compreender até que ponto essa disseminação de estratégias abrangentes, pensadas por autoridades centralizadas, materializa-se em organizações de âmbito mais limitado.

Especificamente no campo do Judiciário, objeto desta investigação, é possível singularizar algumas questões da segurança cibernética de órgãos dessa esfera do Estado. Para Alves, Carvalho & Nunes (2023), existe um distanciamento entre riscos da esfera cibernética e os riscos considerados na gestão de tribunais. Os autores, contudo,

demonstram que há uma cadeia de vinculação entre os dois, na medida em que vulnerabilidades cibernéticas podem levar a problemas nos trabalhos e objetivos dos referidos órgãos. Entre muitos riscos apontados pela pesquisa, pode-se destacar os de divulgação antecipada de decisões, vazamento de informações sigilosas, alteração de determinações, manipulação da distribuição de processos, perda de dados, parcialidade no processo de tomada de decisão judiciais, bem como de inserção de assuntos indesejados ou adulterados em decisões e espionagem.

Ou seja, em um contexto em que diferentes etapas de processos judiciais estão sendo digitalizadas, como a apresentação de documentos e provas e o registro de decisões judiciais e outras manifestações em um processo, o armazenamento e a disponibilidade desses dados relacionam-se diretamente à governança da segurança cibernética. Assim, a nível operacional, podem ser observados no Judiciário riscos como cópias de processos em meios de armazenamento pessoais, vazamento intencional de informações sensíveis por pessoas que tenham acesso a elas e código-fonte de sistemas utilizados, relacionados, por sua vez, a causas diversas, como perda de informações, limitações do sistema, assédio de hackers e grupos de interesses, bem como falhas no processo de desenvolvimento, más práticas e falta de padronização do código (Alves; Carvalho; Nunes, 2023, pp. 352-353).

Nesse sentido, autores como Costa (2021) destacam a importância das boas práticas por parte de servidores e atores envolvidos nos processos de tribunais para que instituições de segurança cibernética tenham efetividade e a exposição a riscos seja menor. O autor trabalha a questão do compartilhamento de informações entre equipes virtuais e o risco de vazamento, em especial ao utilizar aparelhos pessoais de maneira preponderante, em detrimento de instrumentos autorizados pelo tribunal e que passaram por protocolos de segurança no desenvolvimento. Machado (2018), por sua vez, chama atenção para a relevância de uma linguagem comum no âmbito do Judiciário para a identificação e categorização de riscos, dialogando com o que Hurel (2021) trata a respeito da fragmentação da governança do campo no Brasil e a necessidade de maior cooperação entre setores.

Exploradas as principais questões do debate sobre a segurança cibernética no Brasil e no mundo, cumpre delinear também o panorama institucional no tema, destacando o processo de produção de normas e os principais atores envolvidos, assim como a sua evolução no tempo. Com isso, será possível construir uma base de análise das normativas internas dos tribunais, possibilitando compreender condutas esperadas e objetivos e estratégicas nesse campo, de modo a situar a atuação interna dos tribunais e o que os órgãos devem implementar.

2 SEGURANÇA CIBERNÉTICA: PANORAMA DAS INSTITUIÇÕES E DIRETRIZES NO BRASIL E NO MUNDO

Esta seção tem o objetivo de reunir as principais instituições formais no Brasil relacionadas à segurança cibernética e da informação. A metodologia para a construção desta parte do trabalho consistiu, majoritariamente, de análise de legislação, normas administrativas e outras diretivas de órgãos de abrangência nacional. A seção foi dividida em três partes: a primeira traz um histórico não exaustivo da evolução da produção de normas do país em relação tema, a segunda, debruça-se sobre sobre o contexto normativo e de capacidades atual, com foco na Estratégia Nacional de Segurança Cibernética (ENSC), enquanto a terceira tem como escopo o Poder Judiciário e resoluções e portarias do Conselho Nacional de Justiça (CNJ). Essa contextualização é importante para melhor fundamentar a análise das normas internas dos tribunais, de modo a se observar convergências e semelhanças.

Como apontam North (1991) e Nóbrega & Teixeira (2023), no sentido colocado pela corrente teórica neoinstitucionalista, uma instituição traduz-se em uma regra, seja ela informal — observada e veiculada no âmbito da própria sociedade — ou formal — estatal. Não se pode confundir o conceito, pois, com o de organização, que é um conjunto de atores que se relacionam com as instituições. Nesse sentido, a presente pesquisa busca identificar o histórico e atualidade das regras formais em matéria de segurança cibernética, concentradas no âmbito da Administração Pública Federal e, no caso do Poder Judiciário, do CNJ. A partir do que elas preconizam, será realizada a análise das normativas internas dos tribunais objetos desta investigação.

Conforme destacado por Hurel (2021), na atualidade, a governança da segurança cibernética no Brasil inclui diferentes setores, desde organizações governamentais, à sociedade civil, à academia e o setor privado. Apesar das questões de falta de coordenação apontadas na seção anterior, a noção de governança, como colocado por autores como Rosenau & Czempiel (1992), traz também arranjos institucionais que transcendem o Estado, incluindo mecanismos informais e a participação de diferentes atores. Esta seção, contudo, concentrar-se-á nas instituições formais — isto é, veiculadas por órgãos oficiais —, devido ao escopo da pesquisa de compreender a sua implementação.

2.1 EVOLUÇÃO HISTÓRICA

Até chegar ao arcabouço institucional atual em matéria de segurança cibernética, houve um desenvolvimento ao longo dos anos, desde meados do início deste século. As iniciativas, no Brasil, concentram-se no contexto da Administração Pública Federal (APF), notadamente em setores que se dedicam à segurança. Tais instituições demonstram a

evolução dos protocolos e padrões do país no assunto, servindo de base não apenas para órgãos federais da Administração direta quanto da indireta e até de outras esferas de governo. Essa caixa de ferramentas anteriormente utilizada também é base do que existe na atualidade, tendo contribuído para a conformação do que existe.

Como aponta Aguiar (2023), o marco inicial do tratamento normativo dessa temática foi o Decreto nº 3.505, de 13 de junho de 2000, que institui a primeira Política de Segurança da Informação da Administração Pública Federal. Neste momento, a APF é incluída no âmbito de incidência da norma, de certa maneira limitando-a a esse âmbito. A norma insere fundamentos até hoje observados em instituições de segurança cibernética, como objetivos de garantia de direitos, criação de consciência e capacitação, assim como de garantir a segurança de sistemas, eliminação de dependência externa e desenvolvimento nacional de tecnologias, promoção de cooperação entre organizações, criação de arcabouço normativo e interoperabilidade. Também chama a atenção a harmonização com a conceituação da UIT, incluindo os objetivos-atributos de confidencialidade, integridade, autenticidade, não-repúdio e disponibilidade de informações. Há, ainda, em 2000, a criação do Comitê Gestor de Segurança da Informação, então associado ao Conselho de Defesa Nacional, que tinha a incumbência de acompanhar a implementação da PSI, estabelecer normas e padrões e coordenar atividades no tema. A Agência Brasileira de Inteligência foi outro órgão incluído entre os competentes para apoiar o CDN nesse âmbito, em atividades científicas e tecnológicas.

Ainda que apenas tenha sido ratificada e promulgada no Brasil em 2022, a Convenção de Budapeste sobre Crimes Cibernéticos também exerceu papel sensível como fonte de normas em matéria de segurança cibernética, especificamente sobre crimes cibernéticos, como aponta Alves Junior (2011). Ainda, o CGI.BR e o Núcleo de Coordenação da Informação do Ponto BR, ligado ao primeiro, desempenham atividades relevantes para a questão, ao disciplinar diversos pontos de Governança da Internet no Brasil, o que inclui a segurança de redes e da informação. Também nesse contexto está o Centro de Estudos, Resposta e Tratamento dos Incidentes de Segurança no Brasil (CERT.br), o qual monitora ocorridos em matéria de segurança de redes, emite recomendações sobre o tema e atua como organização civil que lida com incidentes a nível nacional, além das Forças Armadas, com o ComDCiber, entre outros órgãos. Conforme o Decreto nº 4.801/2003, a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo, criada pela norma, também tem, entre as suas atribuições, a formulação de ações relativas à segurança cibernética e da informação.

A nível internacional, além da UIT, é possível elencar contribuição da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE), à qual o Brasil está em processo de adesão, para a segurança cibernética. Em 2002, um documento na área foi

publicado pela organização (Canongia; Mandarino Junior, 2009). As Diretrizes para a Segurança de Sistemas e Redes de Informação (Recomendação da Sessão 1037) destacam questões como sensibilização de atores e da população, resposta a incidentes, avaliação de risco, ética, proteção da democracia, bem como reavaliação institucional periódica, de modo a criar uma cultura de segurança (OCDE, 2002). Há ainda a Recomendação do Conselho sobre a Proteção de Infraestrutura de Informação, de 2009, que inclui pontos como adoção de políticas claras em alto nível de governo, identificar competências, cooperação entre setores e partes interessadas, transparência, revisão sistemática de políticas, e estabelecimento de níveis de segurança para sistemas e redes (Mandarino Junior; Canongia, 2009).

Nacionalmente, o Gabinete de Segurança Institucional da Presidência da República — em especial do seu Departamento de Segurança da informação e Comunicações (DSIC), criado em 2006 — teve e tem papel destacado no processo de formulação e veiculação de normas em matéria de segurança cibernética e, de modo geral, da informação. Pode-se entender que o processo de securitização das temáticas de segurança cibernética no Brasil contribui para a relevância do GSI no processo de produção de normas nessa matéria. Conforme destacado por Da Cruz Junior (2013), o Acórdão do Tribunal de Contas da União nº 1.233/2012 estabeleceu que, caso as diretrizes determinadas pelo órgão sejam descumpridas, os órgãos em questão estariam em desconformidade com o ordenamento jurídico, podendo ser objeto de sanções. Tais processos, desse modo, criam claros incentivos para uma maior força institucional dessas instituições, inclusive estimulando que órgãos de outras esferas, como estados e municípios, sigam as normativas do GSI. Ao gabinete, está subordinado o Centro de Prevenção, Tratamento e Resposta a Incidentes de Rede de Governo (CTIR.gov, precedido pela Coordenação-Geral de Tratamento de Incidentes em Rede, criada dentro do DSIC pelo Decreto nº 5.772/2006, e criado em 2009 como Centro de Tratamento e Resposta a Incidentes de Rede de Governo), que também emite recomendações de práticas a serem seguidas, em especial pela APF.

Do GSI, partiram instituições como a Instrução Normativa nº 1, de 2008, que disciplina a gestão da segurança da informação e comunicações na APF, repartindo competências de órgão como o Comitê Gestor de Segurança da e fixando conceitos, bem como Normas Complementares a partir de tal IN dedicadas a temas específicos, como elaboração de políticas de segurança por órgãos da APF (NC nº 3/IN01) gestão de risco (NC nº 4/IN01) e criação de equipes de tratamento de incidentes em cada órgão federal (NC nº 5/IN01). Além disso, em meio à criação de subgrupos e órgãos nesse arcabouço, o Gabinete fixou conceitos que, mesmo sendo reformulados futuramente, ajudaram a fundamentar o processo de formulação de políticas.

A Portaria nº 45, de 8 de setembro de 2009, por exemplo, que traz a seguinte conceituação de segurança cibernética como "a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus Ativos de Informação e suas Infraestruturas Críticas" (Brasil, 2009b). A mesma normativa estabelece que ativos de informação são "meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso" e que infraestruturas críticas são "instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade" (Brasil, 2009b).

O conceito de infraestruturas críticas, vale notar, surge nas instituições brasileiras relativas à infraestrutura cibernética formuladas pelo GSI nesse contexto. Como aponta Alves Junior (2011), ele também aparece na Portaria nº 34 do GSI, de 5 de agosto de 2009, que instituiu um Grupo de Trabalho de Segurança das Infraestruturas Criticas da Informação no âmbito do CGSI. Para tal normativa, infraestruturas críticas são "subconjunto de ativos da informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade" (Brasil, 2009b). A definição vai ao encontro da UIT, que compreende tais infraestruturas como sistemas, serviços e funções chave cuja interrupção tenha um impacto debilitante em áreas como saúde pública, segurança, comércio e segurança nacional, incluindo tanto elementos físicos quanto virtuais e podendo incluir outros campos a depender do local, como comunicações, energia e transporte (UIT, 2010).

Também é valido citar a primeira Estratégia Nacional de Defesa, publicada pelo Ministério da Defesa em 2008, que reconhece o setor cibernético como estratégico para a defesa e segurança, como mencionado anteriormente. Tal inclusão legitimou e abriu espaço para uma participação maior das Forças Armadas, em especial do Exército Brasileiro. Ainda, o GSI publicou, em 2010, o Livro Verde de Segurança Cibernética no Brasil, que trouxe propostas de diretrizes sobre diferentes questões relacionadas ao tema, incluindo objetivos, marcos recentes e pontos a serem contempladas em uma futura Política Nacional de Segurança Cibernética, com expectativa de amplo debate social, incluindo diferentes setores e com visões de curto, médio e longo prazos. A literatura (Hurel; Lobato, 2018; Aguiar, 2023), contudo, como discutido, aponta que, na prática tal participação social não ocorre de forma satisfatória no processo de produção de normas na matéria. O documento cita, ainda, uma "prerrogativa do Gabinete de coordenar a atividade de Segurança da Informação, mantendo o compromisso com o Estado" (Brasil, 2010, p. 5).

Como consequência dos chamados megaeventos, discutidos na seção anterior, e da subsequente Comissão Parlamentar de Inquérito sobre espionagem, houve, em 2015, a publicação da Estratégia de Segurança da informação e Comunicações e de Segurança

Cibernética da Administração Pública Federal 2015-2018 (Hurel; Lobato, 2018, p. 12). O documento foi formulado pelo GSI após recomendação do TCU no Acórdão 3.051/2014-TCU-Plenário. Ele inclui um mapa estratégico, assim como objetivos e metas de orçamento, aprendizagem, crescimento e inovação, governo e resultados para a sociedade, bem como 10 objetivos e 38 metas estratégicas para diferentes prazos, incluindo implementação de recomendações, ações colaborativas, maturidade, conscientização, institucionalização e adoção do modelo de governança sistêmica.

Por fim, em 2018, foi publicada a Política Nacional de Segurança da Informação (Decreto nº 9.637/2018), atualizando a do ano 2000. Ela não mais restringiu-se à APF e passou a ter o adjetivo "nacional" em seu nome, assim como tal abrangência. O documento reafirma os princípios de disponibilidade, integridade, confidencialidade e autenticidade da informação, existentes desde ao menos as recomendações da UIT de 2008, além de elencar princípios, que incluem questões como soberania, responsabilidade, cooperação, dever de proteção do sigilo de informações imprescindíveis à segurança e consentimento para tratamento de informação sigilosa, fornecendo maior previsibilidade e um horizonte estratégico para o tema (Hurel, 2021).

Há, ainda, objetivos, instrumentos e atribuição de competências, incluindo segurança do indivíduo, proteção de informações de pessoas físicas, além de infraestruturas críticas e de entidades públicas, e a previsão de estabelecimento de cinco estratégias sobre segurança da cibernética, defesa cibernética, das estrutura, da informação sigilosa bem como proteção contra vazamento de dados, refletindo intenções já expressas no Livro Verde, por exemplo. Também foi criado, com o decreto, um novo Comitê Gestor de Segurança da Informação, com função de assessoramento do GSI, com participação de órgãos governamentais. Além de normas que são diretamente relacionadas à segurança cibernética, autoras como Aguiar (2023) e Hurel (2021) lembram do papel do Marco Civil da Internet e da Lei Geral de Proteção de dados, ao incluir a segurança do armazenamento de dados entre as suas previsões normativas.

Para Belli *et al.* (2023, p. 71), a PNSI adota uma abordagem "conceitualmente questionável", por enquadrar a segurança cibernética como parte da segurança da informação, e não o contrário, o que pode ser limitante. Ainda, além de favorecer a compartimentação da regulação segurança cibernética, a Política seria insuficiente para abordar as dimensões atuais da questão, limitando-se aos objetivos-atributos de disponibilidade, integridade, confidencialidade e integridade. Não se consideram, porém, outras dimensões da segurança cibernética importantes para uma resposta sólida à questão, notadamente em relação à democracia e a ameaças mais complexas.

O Quadro 1 sintetiza as principais instituições ora discutidas, com a sua data de publicação, a normativa em questão, o órgão de origem e um resumo do seu conteúdo.

Quadro 1 — Linha do tempo de instituições em segurança cibernética.

Data de publicação	Normativa	Órgão de origem	Resumo
13 de junho de 2000.	Decreto nº 3.505/2000.	Presidência da República (Brasil).	Institui a Política de Segurança da Informação para a Administração Pública Federal.
6 de agosto de 2002.	OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security	Organização para a Cooperação e o Desenvolvimento Econômico.	Diretrizes iniciais da OCDE para segurança de sistemas e redes de informação, incluindo tratamento de incidentes, avaliação de risco e reavaliação de regras.
6 de agosto de 2003.	Decreto nº 4.801/2003.	Presidência da República (Brasil).	Cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo, com competência sobre segurança da informação e segurança cibernética (esta incluída pelo Decreto nº 7.009).
8 de maio de 2006.	Decreto nº 5.772/2006.	Presidência da República (Brasil).	Criação do Centro de Tratamento de Incidentes de Rede de Governo (hoje Centro de Prevenção, Tratamento e Resposta).
13 de junho de 2008.	Instrução Normativa GSI/PR nº 1/2008.	Gabinete de Segurança Institucional/Presidência da República.	Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.
18 de dezembro de 2008.	Decreto nº 6.703/2008 (Estratégia Nacional de Defesa de 2008).	Presidência da República (Brasil)/Ministério da Defesa.	Inclui o setor cibernético entre os três considerados estratégicos e essenciais para a defesa nacional.
5 de agosto de 2009.	Portaria GSI/PR nº 34.	Gabinete de Segurança Institucional/Presidência da República.	Institui Grupo de Trabalho de Segurança das Infraestruturas Criticas da Informação, no âmbito do Comitê Gestor de Segurança da Informação - CGSI.
8 de setembro de 2009.	Portaria GSI/PR nº 45	Gabinete de Segurança Institucional/Presidência da República.	Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e da outras providências.

Data de publicação	Normativa	Órgão de origem	Resumo
30 de abril de 2008.	Recommendation of the Council on the Protection of Critical Information Infrastructure.	Organização para a Cooperação e o Desenvolvimento Econômico.	Recomendação sobre proteção de infraestruturas críticas, incluindo questões como delineamento de políticas e repartição de competências.
11 de maio de 2015.	Estratégia de segurança da informação e comunicações e de segurança cibernética da Administração Pública Federal 2015-2018.	Gabinete de Segurança Institucional/Presidência da República.	Complementa a IN GSI/PR nº 01/2008 e traz conjunto de objetivos estratégicos e metas para os próximos quatro anos, contemplando diferentes aspectos.
26 de dezembro de 2018	Decreto nº 9.637/2018.	Presidência da República (Brasil).	Institui a Política Nacional de Segurança da Informação.

Fonte: elaboração própria, a partir de Alves Júnior (2011), Hurel & Lobato (2018), Assunção (2023) e Aguiar (2023).

2.2 ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA E CONTEXTO ATUAL

No contexto atual, a Estratégia Nacional de Segurança Cibernética (E-Ciber) exerce papel de destaque entre as instituições nacionais do Brasil do tema. Previsto na PNSI, o chamado Módulo E-Ciber da Estratégia Nacional de Segurança da Informação foi o primeiro a ser desenvolvido, na medida em que o recorte foi considerado de maior destaque em relação aos outros no campo da segurança da informação, tendo sido publicado com o Decreto nº 10.222, de 5 de fevereiro de 2020, com validade prevista para até 2023, prorrogada por mais um ano. Como aponta Hurel (2021), a E-Ciber foi resultado de meses de trabalho de discussão em diferentes etapas, três grupos temáticos, reuniões fechadas e consultas públicas. Em relação a estas, a literatura aponta que, apesar de ter sido um avanço por parte do GSI, ainda há desafios a serem enfrentados, como o prazo curto para envio de contribuições, falta de transparência quanto a como elas fora incorporadas no texto final e integração em mecanismos de operacionalização e revisão.

A Estratégia conta com três objetivos estratégicos e é organizada em eixos temáticos, contando ainda com dez ações estratégicas, além de recomendações. Os objetivos são: "tornar o Brasil mais próspero e confiável no ambiente digital", "aumentar a resiliência brasileira às ameaças cibernéticas" e "fortalecer a atuação brasileira em segurança cibernética no cenário internacional" (Brasil, 2020, p. 7-8). Trata-se de metas com alto grau de abstração e que formam um cenário ideal a ser construído no futuro, a longo prazo, com o

trabalho nas ações estratégicas. Os dois eixos Proteção e Segurança e os Transformadores, os quais incluem também os eixos de "Governança da Segurança Cibernética Nacional", "proteção e mitigação de ameaças cibernéticas" e "proteção estratégica", no caso do primeiro, e "dimensão normativa", "pesquisa, desenvolvimento e inovação", "internacional" e "educação", em relação aos segundos (Brasil, 2020, p. 7-8).

As dez ações estratégicas situam os objetivos e, de certa forma, também funcionam como metas de curto, médio e longo prazos, ainda que sem o estabelecimento de um prazo esperado. Elas incluem fortalecimento de ações, consolidação de modelo centralizado de governança — com recomendações de coordenar setores e com mecanismos informais de participação, incluindo também a criação de um conselho nacional de segurança cibernética e o estabelecimento de rotina de conformidade nos setores público e privado — além da promoção de ambiente participativo, colaborativo, seguro e confiável entre os diferentes setores. São também ações estratégicas o aumento do nível de proteção do governo e das Infraestruturas Nacionais Críticas, o aprimoramento do arcabouço legal, incentivo à concepção de soluções inovadoras, ampliação da cooperação internacional, ampliação da parceria entre diferentes setores e elevação do nível de maturidade em segurança cibernética (Brasil, 2020).

Entre as recomendações que compõem as ações estratégicas, reafirma-se o papel do GSI em coordenar o tema no Brasil, inclusive em matéria de recebimento de denúncias, apuração de incidentes e desenvolvimento de programas e projetos. Hurel (2021), por exemplo, questiona a capacidade do órgão de concentrar tantas competências, assim como a sua relação frágil com a sociedade civil. Há, ainda, previsões de realização de debates e de convergência de esforços, tanto em matéria de governança, quanto de incidentes e de vulnerabilidades, assim como exercícios com presença de diversos setores. Tais recomendações, porém, precisam se materializar em uma efetiva participação sistemática no processo de formulação de instituições, algo que depende da abertura do GSI e de um conselho nacional de segurança cibernética, que seria criado no futuro.

Há também a previsão de estímulo a boas práticas, incluindo criptografia e compartilhamento de informações sobre incidentes, embora faltem protocolos para tal, assim como necessidade de inclusão de requisitos de segurança cibernética em contratações na administração pública e no uso de computadores. A questão da cooperação é tratada também ao se prever interação entre reguladores de infraestruturas críticas e estímulo de notificações de incidentes ao CTIR.gov; também é falado em fortalecimento deste órgão e dos Centros de Tratamento e Resposta a Incidentes existentes em todo o país. Em matéria de arcabouço legal, além de recomendações mais abrangentes, como a de identificar lacunas, há a de elaboração de um anteprojeto de lei sobre segurança cibernética, com "diretrizes que

irão proporcionar alinhamento macroestratégico ao setor e contribuir de forma decisiva para elevar a segurança das organizações e dos cidadãos" (Brasil, 2020, p. 11).

Outras inclusões na E-Ciber são as de incentivar pesquisas e empresas na área, assim como reconhecimento da importância de se desenvolver tecnologias com privacidade e segurança desde a concepção. A Estratégia sublinha, ainda, a adoção de padrões globais de tecnologia e a interoperabilidade, assim como a importância da cooperação internacional e da participação do Brasil em fóruns internacionais relacionados à segurança cibernética e em fóruns de estruturação normativa e criação de padrões. A ampliação de parcerias entre setor privado, diferentes esferas do setor público, a academia e a sociedade é estruturada em diferentes recomendações e, de mesmo modo, a elevação da maturidade, com foco em ações relacionadas à cultura de segurança e conscientização.

De modo geral, a Estratégia é uma grande carta de intenções e de diagnóstico da segurança cibernética nacional, sem, por exemplo, um plano orçamentário ou indicadores para acompanhar o progresso e necessitando de outros instrumentos e atores para dar andamento aos objetivos e ações previstos. Hurel (2021) destaca cinco dimensões da E-Ciber: cooperação, capacitação, coordenação, integração de conhecimentos e sustentabilidade de esforços. Para a autora, cooperação e sustentabilidade de esforços são transversais no documento, o que se verifica ao observar a ênfase em mecanismos de participação, compartilhamento de informações e solidificação de processos. Enquanto isso, a coordenação tem propostas mais concretas e reforça o papel do GSI, ainda que com alguma participação de outros atores e com o possível anteprojeto de lei, enquanto capacitação e integração de conhecimentos abarcam recomendações mais abstratas e gerais, incluindo espaços e modelos para facilitar a integração multissetorial.

Belli *et al.* (2023) e Aguiar (2023) citam lacunas da E-Ciber, sugerindo a adoção de políticas públicas de incentivo multissetorial, assim como Hurel (2021). Belli et al. (2023) também propõe o estabelecimento de uma Agência Nacional de Segurança Cibernética, de modo a desconcentrar as competências do GSI, com comitês e redes multissetoriais, que incluam, de modo equânime, diferentes setores. Em dezembro de 2023, foi editado o Decreto nº 11.856, que institui a Política Nacional de Cibersegurança (PNCiber), proposta pelo GSI. Além de reafirmar objetivos como o de promoção da segurança, combate a crimes cibernéticos, gestão de riscos, mitigação de vulnerabilidades, atuação diligente, aumento da resiliência, fomento à pesquisa, coordenação, desenvolvimento de mecanismos de fiscalização e fortalecimento da atuação do país, a instituição criou o Comitê Nacional de Cibersegurança (CNCiber), cuja Secretaria Executiva é exercida pelo GSI. O órgão, porém, tem composição multissetorial, abarcando representantes do governo, da sociedade civil, de instituições científicas e do setor empresarial. O comitê tem como competências a proposição de atualizações para a E-Ciber, PNCiber e para o Plano Nacional de

Cibersegurança, além da sugestão de estratégias, inclusive para a cooperação técnica internacional no tema.

O CTIR.gov, criado no início do século, conforme mencionado, também vem emitindo recomendações, o que pode ser entendido como uma fonte de diretrizes para o setor público e até mesmo para particulares. Desde 2018, foram publicadas 97 recomendações, abarcando sobretudo boas práticas e notificações sobre ameaças e vulnerabilidades. O CERT.br também emite recomendações a partir do monitoramento de ameaças, incluindo também apontamentos para melhorar a notificação de incidentes e para melhorar a proteção de sistemas, requisitos mínimos e iniciativas de disseminação de conhecimento e criação de consciência.

Em 2023, o Ministério da Gestão e Inovação em Serviços Públicos publicou a portaria nº 852, que estabelece o Programa de Privacidade e Segurança da Informação, marcando um relativo alargamento no rol de atores envolvidos no processo de formulação de instituições do tema. Já no campo da defesa cibernética, como detalhado por Hurel (2021), o CDCiber, formalmente ativado em 2015, segue atuando, assim como o ComDCiber, oficialmente implantado em 2016, com foco em ameaças concernentes à soberania nacional. O tema foi objeto do Programa Estratégico do Exército Defesa Cibernética, instituído em 2017, assim como do Sistema Militar de Defesa Cibernética, criado em 2020. A questão também segue sendo incluída nas Estratégias e Políticas Nacionais de Defesa como setor estratégico, além de motivar a realização de exercícios, como o Guardião Cibernético.

O MGI também vem conduzindo atividades no campo da segurança cibernética, a partir da área de governo digital, o que pode representar uma oportunidade de dessecuritizar o tema, ao consolidá-lo no campo das políticas públicas, desconcentrá-lo do GSI e retirar a preponderância do tratamento militar/de inteligência. No âmbito do PPSI, foram criados os Centros de Excelência em Privacidade e Segurança da Informação do Governo Digital e Integrado de Segurança Cibernética. Um conceito importante nesse sentido é o de ETIR as a service, isto é, de tratamento, prevenção e resposta a incidentes como um serviço, com apoio para a sua implantação, plataforma de compartilhamento de informações sobre softwares maliciosos, testes e análise ativa de vulnerabilidade. Os Centros, vale notar, conectam-se com o CTIR.gov e com o CERT.br, mostrando a importância dessa interconexão para a força institucional de normas de segurança cibernética.

Na esfera internacional, a OCDE atualizou as suas políticas e recomendações sobre segurança cibernética, inclusive as direcionadas a infraestruturas de informações críticas. O Digital Economy Paper nº 275, que faz um balanço do tema dez anos após as diretrizes anteriores, destacando a necessidade de um foco em serviços essenciais, em vez de infraestruturas críticas para alinhamento com outras instituições, bem como discussões sobre terminologia, dependências e interdependências, abordagem que envolva todo o

governo e a sociedade, parcerias e cooperação e flexibilidade na implementação das recomendações em diferentes culturas. Ainda, como destacado por Belli et al. (2023), a Organização Internacional para a Padronização, o NIST, dos EUA, e a União Europeia, com a sua Agência da UE para a Segurança Cibernética, também contam com padrões reconhecidos como referências, os quais abarcam gestão de riscos, implementação e gestão de controles, avaliação, proteção da privacidade e liberdade, cooperação entre autoridades, uniformização de medidas, boas práticas, como *backups*, formação, controle de acessos, autenticação multifator, segurança nas comunicações e aquisição de sistemas, entre outros.

A UIT, por sua vez, mantém um Índice de Segurança Cibernética Global, que considera indicadores de cooperação, desenvolvimento de capacidades, organizacional técnico e legal, abarcando legislação sobre segurança cibernética, regulações de proteção de dados, regulações de infraestruturas críticas, existência de centros de resposta e prevenção de incidentes, estratégias e agências focadas no tema, desenvolvimento de projetos e iniciativas e engajamento regional e internacional. Na última edição do índice, de 2020, Brasil ficou em terceiro lugar nas Américas e em 18º no mundo, com um índice de 96,6 (UIT, 2020). Além disso, o Centro Global de Capacidade de Cibersegurança da Universidade de Oxford já realizou duas revisões da capacidade de maturidade de segurança cibernética, a mais recente em 2023 (Stolz; Axon, 2023). A análise é baseada no modelo de maturidade de capacidade no campo, que inclui as dimensões de política, estratégica, cultura, sociedade, criação de conhecimento e capacidades, marcos legais e regulatórios e padrões e tecnologias, com fatores, aspectos e indicadores. Para o diagnóstico, ainda são desafios a resposta a incidentes, mecanismos de relatos de incidentes, proteção de infraestruturas críticas, controles técnicos e criptográficos, assim como confiança e segurança na internet, mídias sociais, conscientização, mercado de segurança cibernética e divulgação responsável. Já marcos jurídicos e de educação, mentalidade, defesa e estratégia são alguns dos fatores em que houve avanço do país.

Tem-se, desse modo, um panorama institucional atual em matéria de segurança cibernética no Brasil e no mundo, com a centralidade. A nível nacional, da E-Ciber, a qual ainda depende da atuação cooperativa de outros órgãos para que tenha a sua força institucional assegurada. Nesse sentido, é importante discutir a formulação de regras e o que existe em termos de instituições no âmbito da tema em tela no contexto específico do Judiciário no Brasil, ao que a próxima subseção dedicar-se-á.

2.3 PODER JUDICIÁRIO E SEGURANÇA CIBERNÉTICA

Como aponta Hurel (2021), a partir de uma demanda de cooperação e alinhamento de políticas da segurança cibernética, políticas setoriais no campo vêm sendo desenvolvidas em diversas áreas, como a financeira e a energética, incluindo as chamadas infraestruturas

críticas. No âmbito do Poder Judiciário no Brasil, o Conselho Nacional de Justiça (CNJ) exerce papel central na definição de diretrizes a serem seguidas pelos órgãos que compõem essa esfera do Estado, emitindo normativas que visam a harmonizar as práticas de tribunais e órgãos jurisdicionais, como também feito pelo CNJ em outros temas.

No que tange à segurança cibernética, o CNJ produziu, no ano de 2021, as suas principais portarias, resoluções, protocolos e outros documentos sobre o tema, que foi citado na Resolução nº 325/2020 do órgão, a qual estabelece a Estratégia Nacional do Poder Judiciário 2021-2026. Uma das primeiras normativas envolvendo o tema de maneira mais direta — após a Portaria nº 292/2020, que aprovou um Protocolo de Prevenção a Incidentes Cibernéticos — foi a Resolução nº 370, de 28 de janeiro de 2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD). Ela tem um objetivo geral de "constituir o principal instrumento de promoção da governança ágil e da transformação digital do Poder Judiciário por meio de serviços e soluções digitais inovadoras que impulsionem a evolução tecnológica do Poder Judiciário" (Brasil, 2021a, p. 2) e outros estratégicos, distribuídos em três perspectivas. O sétimo deles (no âmbito de processos internos) é de aprimorar a Segurança da Informação e a Gestão de Dados e com a meta de no mínimo 75% dos órgãos do Poder Judiciário atingirem, até dezembro de 2026, nível satisfatório no Índice de Governança de Tecnologia da Informação e Comunicação (iGovTIC-JUD), criado pela norma para medir a maturidade em TIC dos órgãos submetidos ao controle do CNJ. A Estratégia é dividida em dois domínios: Governança e Gestão de TIC e Serviços de TIC, estando a segurança inserida no segundo.

A Estratégia prevê a necessidade de elaboração de um Plano Diretor de TIC por parte cada órgão do Poder Judiciário, além de estabelecer que despesas de TIC terão preferência sobre as demais e que propostas orçamentárias de TIC devem ser harmonizadas com os Planos. Também é colocado o dever de constituir um Comitê de Governança de Tecnologia da Informação e Comunicação, com representantes de todas as áreas estratégicas do órgão e do campo de TIC, com diversas competências sobre o tema, incluindo gestão de riscos, estratégias, promoção de ações, definição de responsabilidades e monitoramento de boas práticas. Há diretrizes para áreas como estrutura organizacional, transformação digital e atendimento ao usuário, além de medidas específicas em termos de sistemas e segurança. A norma indica a criação futura, ainda, de um repositório nacional disponível a todos os órgãos do Judiciário com editais de licitação, lista de fornecedores por produto, contratos de bens e serviços de TIC, bem como compartilhamento de boas práticas e avanços no campo.

O art. 29 da Resolução estipula a adoção do padrão nacional definido pelo CNJ para credenciais de login, na seção sobre sistemas de informação. A contratação de serviços envolvendo sistemas, por sua vez, deve respeitar os requisitos da instituição, assim como a adoção de arquitetura e serviços em nuvem deve atender as diretrizes propostas pelo

Conselho e a requisitos de segurança da informação e proteção de dados. Também se estabelece a necessidade de incluir, em contratações de desenvolvimento de sistemas da iniciativa privada, cláusula de depósito de documentação e informações relacionadas à tecnologia e o código-fonte junto à autoridade competente para garantia de continuidade, com um manual de referência a ser disponibilizado pelo CNJ. Os sistemas de informação contratados devem, ainda, atender a padrões de interoperabilidade, bem como aos requisitos de: portabilidade, disponibilidade para dispositivos móveis, responsividade, ter documentação atualizada, oferecer suporte para assinatura com certificado na forma da Infraestrutura de Chaves Públicas Brasileira (ICP Brasil) e ao Modelo de Acessibilidade em Governo Eletrônico, além de ser recomendada a utilização de sistemas já disseminados e o uso do Repositório Nacional anteriormente mencionado.

Itens de infraestrutura tecnológica adotados por tribunais e demais órgãos do Judiciário precisam, ainda, atender especificações, temporalidade de uso e obsolescência definidos em outros instrumentos não especificados, devendo-se observar necessidades estratégicas. Em matéria de serviços de nuvem, há a recomendação de utilização dos que simplificam a estrutura, possibilitam a integração, requisitos aceitáveis de segurança, proteção de dados, disponibilidade e padronização. Já em se tratando de riscos, cada órgão, segundo a resolução, deve elaborar Planos de Gestão de Continuidade de Negócios ou de Serviços e de Gestão de Riscos de TIC, incluindo estratégias e planos de ação que assegurem a continuidade dos serviços em caso de falhas, bem como a manutenção e a mitigação de ameaças, de modo a atuar de forma preditiva e preventiva.

Há também a necessidade de elaborar práticas e processos de segurança da informação e proteção de dados, inclusive uma Política de Segurança da Informação (PSI) de acordo com os objetivos institucionais de cada órgão. Devem ainda ser criados, pelos tribunais, um Comitê Gestor de Segurança da Informação, multidisciplinar e responsável pela revisão da PSI e acompanhamento de processos relacionados, e de outro comitê gestor relacionado à Lei Geral de Proteção de Dados — a qual, junto às normativas do CNJ, devem balizar as ações de cada órgão —, com responsabilidade de avaliar mecanismos de proteção de dados, propor ações e formular requisitos na área de TIC.

A ENTIC-JUD determinou, nesse sentido, o alinhamento dos Planos Diretores de TIC de tribunais e demais órgãos à Estratégia, a outras diretrizes, metas e ações associadas, bem como que indicadores e metas de medição serão divulgados e que o cumprimento da ENTIC-JUD será verificado. Ainda, cada órgão do Judiciário deve estabelecer um Plano de Trabalho para atendimento às instituições estabelecidas pela Resolução, havendo prazos definidos para cumprimento intermediário de cada área, sendo o de segurança da informação e proteção de dados de um ano, a partir de 2021. Há, ainda, a fixação de mecanismos de acompanhamento dos situações dos tribunais, inclusive por meio do iGovTIC-JUD. Em

comparação com a E-Ciber, a ENTIC-JUD tem uma linguagem mais operacional e que visa a uma maior força institucional, considerando os diversos elementos que visam a garantir o seu cumprimento por parte dos tribunais e as medidas mais específicas, ainda que seja uma política setorial.

Como complemento à Estratégia, o CNJ publicou, também em 2021, o Guia da ENTIC-JUD 2021-2026, o qual está sujeito à revisão anual, de acordo com a Resolução nº 370 do CNJ. Ele detalha a composição e metodologia de composição e cálculo do iGovTIC-JUD, que envolve a realização de questionários com órgãos do Judiciário, os quais incluem perguntas nos oito domínios estabelecidos pela Estratégia e outras de Diagnostico Complementar. Cada pergunta é pontuada e, a partir de um cálculo ponderado por graus de importância, chega-se ao nível de maturidade em TIC do órgão, que pode ser baixo, satisfatório, aprimorado e excelência. Há, ainda, um modelo do Plano de Trabalho mencionado na Resolução, diretrizes para o Plano de Transformação Digital dos órgãos, além de critérios de categorização de serviços, incluindo matriz de risco, e uma definição sobre o Repositório Nacional, o Connect-Jus.

Especificamente no campo da segurança cibernética, a Resolução nº 396, de 7 de junho de 2021, estabeleceu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Apesar de não citar diretamente a E-Ciber, ela também adota os objetivos-atributos presentes no conceito da UIT e nos documentos do GSI (disponibilidade, integridade, confidencialidade e autenticidade), abarcando segurança da informação, física, proteção de dados e ativos, funcionamento dos processos de trabalho, continuidade operacional, além de ações de planejamento, conscientização e formação. Outro ponto de convergência com a E-Ciber é a noção de maturidade, expressa no objetivo da ENESC-PJ: "aprimorar o nível de maturidade em segurança cibernética nos órgãos do Poder Judiciário, abrangendo os aspectos fundamentais da segurança da informação para o aperfeiçoamento necessário à consecução desse propósito" (Brasil, 2021c, p. 3). Outros objetivos incluem tornar o Judiciário mais seguro e inclusivo, aumento da resiliência a ameaças, estabelecimento de governança e fortalecimento de gestão e coordenação integradas, bem como manutenção dos serviços.

Também pode ser destacada, como aproximação com a E-Ciber, a adoção do modelo centralizado, neste caso coordenado pelo CNJ, com o Comitê Gestor de Segurança da Informação do Poder Judiciário (CGSI-PJ), criado pela Resolução. O engajamento de todos os órgãos do Judiciário, à exceção do Supremo Tribunal Federal, e a sua implementação da ENESC-PJ é, porém, reconhecido como essencial para que a Estratégia obtenha sucesso, em especial no que tange à proteção do serviço. São, então, elencadas ações da medida, que abarcam o conceito de infraestruturas críticas, no sentido de elevar o seu nível de segurança, além de fortalecer ações e estabelecer rede de cooperação do Judiciário. Há a previsão de

estabelecimento de um Sistema de Gestão em Segurança da Informação em cada órgão, são elencadas práticas necessárias para a proteção de infraestruturas críticas, como manter uma equipe de tratamento e resposta a incidentes e é detalhada a Rede de Cooperação do Judiciário na área de segurança cibernética. Estabelece-se que a competência sobre a governança da segurança da informação é da alta administração dos órgãos do Judiciário, bem como que cada um deve estabelecer um Comitê Gestor de Segurança da Informação, com função de assessoramento e análise, e uma estrutura no campo, que tem a função de gerir o Sistema antes previsto, implementar controles, procedimentos de resposta e tratamento de incidentes e programas.

A Resolução traz ainda a Política de Segurança Cibernética do Poder Judiciário (PSEC-PJ), a qual também traz princípios convergentes com a E-Ciber, como a garantia do sigilo de informações "imprescindíveis à segurança da sociedade e do Estado" (Brasil, 2021c, p. 10), além de segurança jurídica, respeito e promoção dos direitos humanos, visão abrangente e sistêmica de segurança cibernética, cooperação, educação e orientação à gestão de riscos. Já entre os objetivos, há o de contribuir com a segurança do indivíduo, da sociedade e do Estado, além de aprimorar o nível de maturidade do campo no Judiciário, fomento à pesquisa e à formação e capacitação e a orientação de ações que envolvem a segurança da informação e cibernética.

A ENESC-PJ é elencada como instrumento da Política, assim como os Protocolos aprovados pela Portaria nº 162 do CNJ, que tratam de prevenção de incidentes cibernéticos, gerenciamento de crises cibernéticas e investigação para ilícitos cibernéticos — com procedimentos de coleta de evidências e comunicação de ocorridos a órgãos competentes — no âmbito do Judiciário, além de Manuais de Referência sobre proteção de infraestruturas críticas, prevenção e mitigação de ameaças, gestão de identidades e educação e cultura em segurança cibernética. Nesses documentos, há o estabelecimento de requisitos mínimos, conceitos e diretrizes para cada área, podendo ser observada harmonização explícita com critérios da Organização Internacional para a Padronização e da Associação Brasileira de Normas Técnicas, bem como uma diferenciação conceitual entre incidente — mais pontual — e crise cibernética, que é um evento que não pode ser mitigado rapidamente, com diretrizes de ação em diferentes estágios, como antes e durante de crises. Além disso, é estabelecido que as atividades críticas, que são necessárias para o funcionamento adequado dos produtos e serviços fundamentais dos órgãos, devem ter os seus riscos continuamente avaliados, algo que também é previsto nas diretrizes da OCDE.

A Resolução nº 396 estabelece que todos os órgãos do Judiciário devem adotar e seguir os Protocolos e Manuais de Referência, bem como ações que os órgãos devem incluir nas suas Políticas de Segurança da Informação, abrangendo gestão de ativos, política de

controle de acesso, tratamento de informações com restrição de acesso, treinamento e certificação internacional, requisitos mínimos de segurança em contratações e acordos, uso de criptografia e articulação de medidas. Em matéria de gestão de usuários de sistemas, há a previsão de ato do CNJ a definir um padrão (o Manual de Referência parte da Portaria nº 162), incluindo gerenciamento de identidades, acessos e privilégios, com objetivo de uniformização da experiência. Também se determina a criação de uma rubrica orçamentária específica para execução das ações estratégicas, de modo a facilitar a avaliação.

Já a Portaria nº 172/2022, por fim, cria o Centro de Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), a partir do disposto na ENESC-PJ; o órgão é dirigido pelo CGSI-PJ e composto pela Rede de Cooperação do Judiciário, a qual, por sua vez, é integrada pelas ETIRs de cada órgão do Judiciário. Tais arranjos contam com canal seguro de comunicação por meio do qual há troca de informações, disseminação de boas práticas e avisos sobre incidentes ameaças e ações de defesa, além de auxiliar órgãos que estejam sofrendo ataques. O Centro reúne-se semestralmente para avaliar sugestões da Rede e promover a melhoria da gestão da segurança da informação ou cibernética, podendo ser convocado de forma extraordinária para tratar de incidentes graves ou crise (Brasil, 2021d).

Com a caracterização do arranjo institucional em matéria de segurança cibernética específico do CNJ realizada, a próxima seção exporá a metodologia e desenho da pesquisa, enquanto a seguinte dedicar-se-á à análise das normativas internas dos tribunais à luz das instituições mais abrangentes. Com a discussão dos parâmetros que devem balizar a ação de agentes e organizações públicas a nível nacional e internacional, será possível realizar uma análise das instituições produzidas dentro dos dois tribunais analisados, de modo a compreender os processos de formação das suas estruturas internas dedicadas à temática, bem como o cumprimento e possíveis lacunas das normativas do CNJ e possíveis diálogos com a E-Ciber.

3 METODOLOGIA E DESENHO DE PESQUISA

Esta investigação adota método dedutivo, partindo de acepções e diretrizes gerais, como a Estratégia Nacional de Segurança Cibernética, para os casos específicos analisados. A metodologia é qualitativa, com abordagem comparativa, de modo a verificar a compatibilidade e o nível de convergência entre diretrizes internas dos órgãos locais com as regras e recomendações mais abrangentes. Desse modo, foram utilizados como unidades de análise resoluções, portarias e outras normas administrativas disponíveis nos sítios eletrônicos do TJPE e do TRF5 e demais dados sobre as estruturas de funcionários dos tribunais do estado e os recursos destinados para a área de informática, notadamente para a segurança, com dados públicos sobre orçamento e contratações.

Foram compiladas informações advindas dos tribunais supracitados sobre o tema analisado e disponíveis nos respectivos sítios eletrônicos, de modo a entender o que se julga importante de se publicizar e seu conteúdo. Também foram feitos dois pedidos de acesso à informação, com base na Lei de Acesso à Informação (Lei nº 12.527/2011), aos dois tribunais, focados em entender o cumprimento de normativas do CNJ relativas a aquisições e sistemas. Escolheu-se o período desde 2010 como universo temporal das diretrizes, de modo a incluir a série histórica das normas internas relativas ao tema em questão, buscando atingir o objetivo de entender como o Poder Judiciário em Pernambuco internaliza práticas em segurança cibernética e, pois, protege dados e infraestruturas relativos a um serviço público essencial. Ao incluir um período de quase quinze anos, é possível observar a evolução do processo de formulação de normas e organização da segurança cibernética nos tribunais, a partir do surgimento de novos desafios e regulações a nível nacional.

As normas internas dos tribunais foram submetidas à análise de conteúdo categorial. Conforme Sampaio & Lycarião (2021), trata-se de uma técnica de pesquisa qualitativa que, a partir de procedimentos sistemáticos e validados, permite criar inferências sobre conteúdos verbais, visuais ou escritos, de modo a descrever, de diferentes formas, fenômenos em termos de significados e contextos com base no corpus textual analisado. O método foi, de acordo com Krippendorff (2004), inicialmente utilizado com notícias jornalísticas como unidades de análise, embora, na atualidade, seja empregado em diversas áreas, com mais sucesso ao ser usado para estudar campos como atribuições feitas em discursos e textos, realidades sociais, comportamentos públicos e relações institucionais.

Nesse sentido, as normativas internas e outros documentos compilados, como pareceres, cartilhas e políticas, constituindo as unidades de análise, foram categorizados a partir do seu objeto em duas categorias: de tema predominante e de ano de publicação. A primeira dela tem cinco códigos: geral; estrutura organizacional e de competências; boas práticas, capacitação e disseminação de informações; resposta a incidentes e gestão de riscos; infraestrutura e orçamento. Tais pontos foram definidos a partir da revisão de literatura realizada, em especial de produções como o modelo de maturidade de capacidade de Stolz & Axon (2023), que elencam áreas como as escolhidas para as categorias para analisar a maturidade em matéria de segurança cibernética de um país. A categoria viabiliza uma descrição dos temas mais mobilizados pelos tribunais no âmbito da segurança cibernética, levando a uma compreensão mais profunda sobre processos de formulação de normas. Já o ano de publicação permite observar a série histórica dos documentos e os momentos em que houve maior edição e/ou atualização de novas normas, tendo como códigos todos os anos de 2010 a 2024.

As instituições internas dos tribunais também foram analisadas de maneira comparativa às nacionais, de modo a verificar compatibilidades e convergências entre ambas.

Ou seja, buscou-se, ainda, verificar o cumprimento e a proximidade das normativas criadas pelos dois órgãos analisados com os planejamentos estratégicos e objetivos mais abrangentes, que foram tratados nas revisões das seções anteriores. Com isso, pode-se entender mais detalhes sobre os processos de formulação de regras internos, assim como as normas que têm uma maior força institucional no contexto local e que são mobilizadas, implícita ou explicitamente, por parte dos tribunais.

O TJPE e o TRF5 foram eleitos como estudos de caso para a análise conteúdo de normativas internas em matéria de segurança cibernética. Embora estejam ambos em âmbito local, a comparação entre ambos permitirá perceber possíveis diferenças e semelhanças no que tange à formulação de normas, organização de competências e demais variáveis que compõem o desenho de pesquisa, assim como matizes na convergência com políticas nacionais. O objeto é, pois, focado na realidade local, com grau limitado de generalização, ainda que favoreça e facilite comparações com outros contextos, assim como represente um caminho metodológico para investigações seguintes.

Além disso, o desenho de pesquisa incluiu, majoritariamente, informações públicas e normas de tribunais, com uma análise comparativa em relação às diretrizes nacionais e internacionais. Processos de formulação de normas mais ocultos podem, desse modo, fugir às lentes da pesquisa, sendo esta uma possível limitação que deve ser destacada. Ainda assim, a descrição a partir dos documentos que são publicizados, inclusive a evolução das políticas internas dos tribunais permite realizar um diagnóstico em matéria institucional, de modo a pensar de forma mais precisa como diretivas abrangentes materializam-se e internalizam-se em escalas menores.

4 O PODER JUDICIÁRIO EM PERNAMBUCO E A FORMULAÇÃO DE NORMAS EM SEGURANÇA CIBERNÉTICA

Esta seção traz os resultados da análise de normativas internas sobre segurança cibernética dos dois tribunais analisados. São expostos os dados, de forma geral, com observações mais abrangentes e números advindos da análise. Então, há seis subseções, cinco delas correspondentes a cinco dos códigos estabelecidas para a análise de conteúdo categorial, e uma sexta sobre objetivos, metas e indicadores. A divisão visa a destacar os pontos sensíveis dentro de cada questão, assim como — em especial no caso dos objetivos — servir de unidades de comparação entre as normativas internas dos tribunais e normativas do CNJ, a E-Ciber e outras instituições anteriormente discutidas e/ou relevantes.

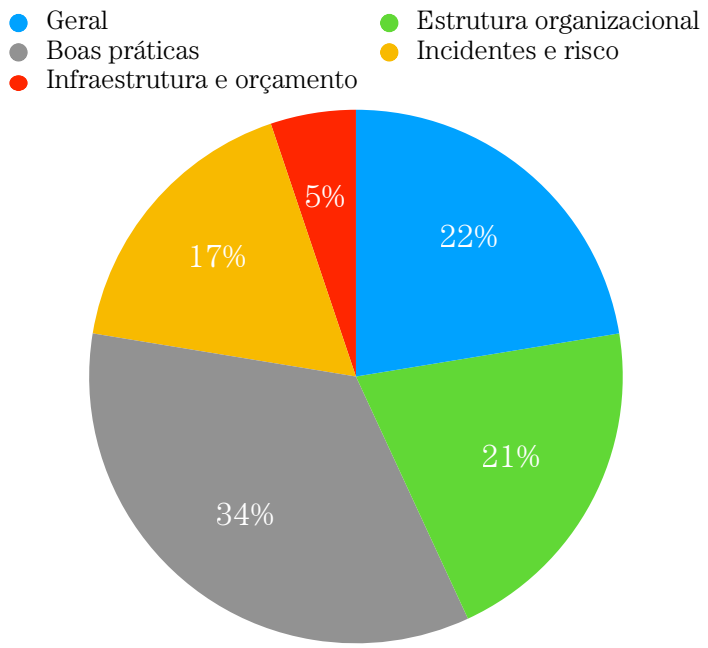
As unidades de análise desta investigação, como mencionado na seção de metodologia e desenho de pesquisa, compreenderam documentos e informações públicas nos sítios eletrônicos do TJPE e do TRF5. Foram compilados, ao total, 76, sendo 58 referentes ao TJPE

(1 plano diretor de tecnologia da informação, 3 resoluções, 5 atos, 1 manual operacional, 3 instruções normativas, 5 instruções de serviço, 3 portarias, 9 cartazes, 17 pareceres, 2 cartilhas e 1 termo de responsabilidade, 1 glossário, 4 planos, 1 planejamento orçamentário e 3 protocolos) e 18, ao TRF5 (4 versões de plano diretor de TI, 3 políticas, 1 estratégia, 1 cartilha, 3 resoluções, 3 portarias, 1 inventário de iniciativas, 1 base de dados de estrutura organizacional e 1 documento de indicadores).

Com a categorização a partir dois seis códigos estabelecidos, o resultado foi o seguinte: 13 documentos foram classificados como gerais, por terem o status de diretiva abrangente, com objetivos, metas e disposições referentes a áreas diversas; a 12 foi atribuído o código de estrutura organizacional, a maioria criando comitês, comissões e órgãos internos, assim como fixando competências relativas à segurança da informação e cibernética; já 20 foram classificados como pertencentes ao código de boas práticas, capacitação e disseminação de informações, com destaque a normativas e documentos que objetivam estabelecer padrões de conduta gerais; 10 documentos foram associados a incidentes e risco; 3 ficaram sob o código de infraestrutura e orçamento, com ênfase para planejamento de alocações orçamentárias em matéria de TIC e de segurança cibernética. A Ilustração 1 mostra a distribuição de códigos da categoria.

Vale notar que, por exemplo, documentos no código “Geral” tratam também de temas como boas práticas e estrutura organizacional, conforme será detalhado. Na classificação, contudo, optou-se por atribuir o código predominante ao conteúdo do documento, considerando o apontado por Sampaio & Lycarião (2021). Já as demais categorias abarcaram normativas mais específicas, que regulamentam algum aspecto específico do respectivo tema, tendo sido encaixadas nos códigos específicos desta categoria. Dos 18 documentos referentes ao TRF5, 6 foram categorizados no código “Geral”.

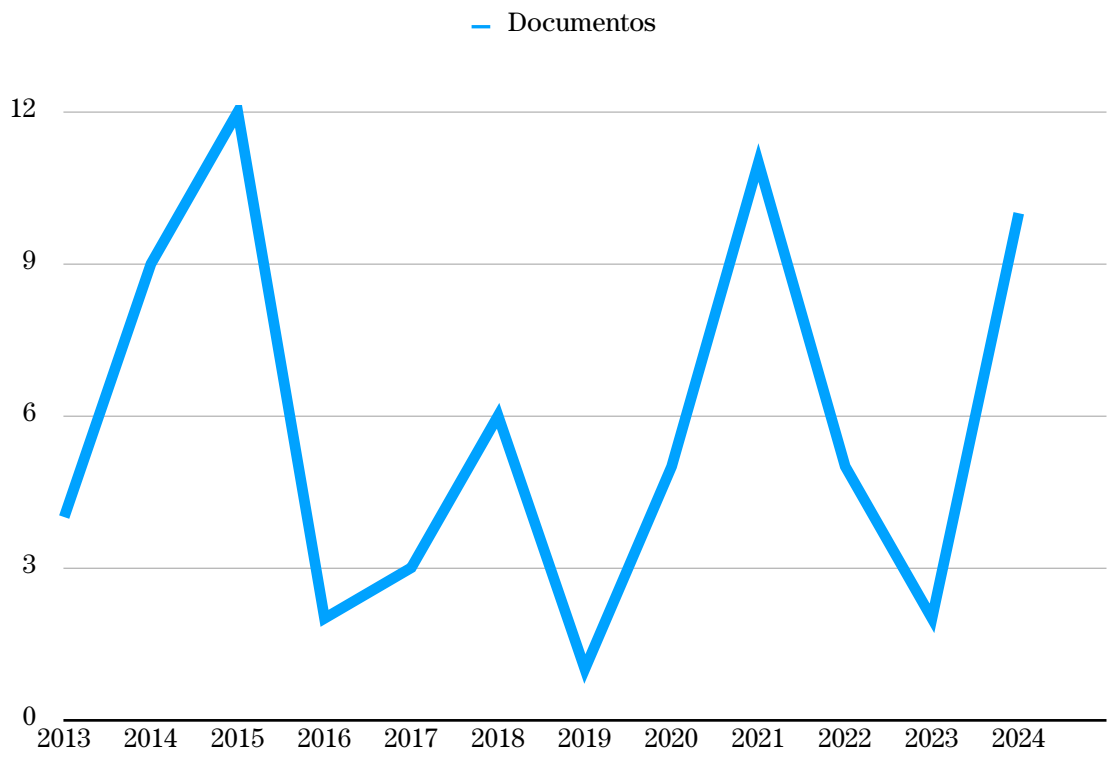
Ilustração 1 — Gráfico de setores com proporção de códigos da primeira categoria e corpus analisado.



Fonte: Elaboração própria, a partir de análise de conteúdo dos documentos do TJPE e do TRF5.

Já em matéria de ano de publicação, nota-se que a maioria dos documentos analisados são mais recentes. Em 2013 (primeiro ano dos documentos que compuseram o corpus), foram 4 documentos publicados, em 2014, 9; em 2015, 12; em 2016, 2; em 2017, 3; em 2018, 6; em 2019,1; em 2020, 5; em 2021, 11; em 2022, 5; em 2023, 2; em 2024, 10. Desde o primeiro ano com documentos compondo a amostra, dessa forma, não há necessariamente uma tendência constante de aumento ou de queda de documentos internos relativos à segurança cibernética. Observam-se, nessa categoria, variações ao longo dos anos, com quedas e aumentos no número de documentos anualmente, como mostra a Ilustração 2.

Ilustração 2 — Gráfico com quantidade de documentos analisados por ano.



Fonte: elaboração própria, a partir de análise de conteúdo dos documentos do TJPE e do TRF5.

Pareceres do TJPE compõem a maior parte dos documentos publicados em 2014, no ano imediatamente posterior ao da publicação da Política de Segurança da Informação do tribunal. Alguns são solicitados por órgãos internos específicos; todos, em geral, visam a esclarecer dúvidas dos servidores sobre temas em específico, detalhando permissões e deveres a partir de normas internas, como a PSI. Já em 2015, a maior parte dos documentos foi de cartilhas e cartazes, que são importantes para garantir a efetividade de normas

internas e abrangentes e disseminar o conhecimento sobre segurança cibernética, algo inclusive previsto na E-Ciber. Em 2024, há mais documentos especificamente relativos à segurança da informação e cibernética, inclusive a partir das normativas do CNJ. Documentos de anos anteriores são predominantemente sobre tecnologia da informação em geral: apesar de se relacionarem à segurança, como ao fixar boas práticas ou estrutura organizacional e competências, nota-se que o tema, no processo de formulação de instituições internas do TJPE, vem ganhando mais espaço de forma autônoma mais recentemente.

Os documentos classificados como gerais são compostos, em sua maioria, por políticas abrangentes de segurança da informação, como a Resolução nº 687/2020 do Conselho da Justiça Federal e a Resolução nº 346/2013 do TJPE, e/ou normativas de caráter estratégico e estruturante. Também estão nesta categoria os Planos Diretores de TI (PDTIs) dos tribunais, tendo sido incluídos todas as versões disponíveis, mesmo as que não mais vigoram, de modo a observar a sua evolução e transformações. O TRF5, por exemplo, conta com PDTIs trienais, sendo o primeiro de 2015 e o mais recente de 2024, com vigência até 2026. A continuidade da reavaliação de tais planos, ainda que não sejam apenas sobre segurança cibernética, é indicativo de preocupação quanto à atualização desses planejamentos.

Os PDTIs apresentam diretrizes gerais, planos de iniciativas a serem realizadas, além de estruturas organizacionais, missão, visão e referenciais estratégicos. No caso do TRF5, há, nas diretrizes, referências inclusão do desenvolvimento de software com compatibilidade com a política de segurança da informação da Justiça Federal, bem como dos princípios de disponibilidade, confiabilidade, integridade, autenticidade e sigilo (também presentes no preâmbulo do PDTIC 2024-2026 do TJPE). O CNJ é citado no que se refere a contratações de infraestrutura, devendo ser respeitadas as suas normativas. Nos objetivos estratégicos, o de número quatro menciona a promoção da segurança da informação digital, bem como a instituição de normas e práticas com vistas à proteção de dados. Cria-se, inclusive, um índice de institucionalização de normas da PSI da JF, além de se fixarem reuniões de acompanhamento, avaliação e revisão do PDTI, com os seus respectivos responsáveis. No plano de iniciativas, pode-se destacar a implantação de processos de e políticas de segurança da informação, conscientização de usuários, manutenção e evoluções de soluções, implantação de um Centro de Operações de Segurança, estruturação de dados, desativação de sistemas levados, serviços de nuvem privada e pública e de videoconferência — que podem ser termos sensíveis em termos de segurança e de soberania digital, como apontado por Belli *et al*. (2023).

No PDTIC 2024-2026 do TJPE, que tem caráter estratégico, há uma ênfase bastante maior às resoluções do CNJ, notadamente a ENTIC-JUD, utilizada como base para diversas fases da elaboração do Plano do tribunal, desde preparação a diagnóstico e planejamento,

sendo a Estratégia do Conselho um dos documentos de referência e os seus objetivos, explicitamente incluídos. O alinhamento estratégico com o documento também é distinguido como uma das premissas do PDTIC, com a explícita intenção de que a Resolução mais abrangente seja, por meio do plano interno, implementado, ainda que haja limitações. Entre as iniciativas em alinhamento estratégico, estão algumas relacionadas ao objetivo de aprimorar a segurança da informação e a gestão de dados, como implantação de sistemática para desenvolvimento, sustentação de sistemas, novas plataformas e atendimento a demandas por dados, produtividade e estatística. Tais citações constantes às resoluções do CNJ revelam uma intenção, ao menos formal, de mostrar implementação de diretrizes mais abrangentes.

No caso do TRF5, a PSI utilizada e disponível no sítio eletrônico é a formulada pelo Conselho da Justiça Federal (Res. Nº 687/2020), que é o órgão de controle de toda a JF. O CJF tem um Conselho de Segurança da Informação, responsável pela formulação da norma, que traz a previsão explícita de revisão periódica, algo importante para a discussão de novos desafios e presente em diretrizes da OCDE, por exemplo. A PSI, de 2020, cita a primeira política de segurança da informação da Administração Pública, de 2000, mas não a PNSI de 2018, além de ter como referência a NC nº 3 da IN 1 do GSI, sobre elaboração de PSI, e a ENTIC-JUD, de 2015, do CNJ, citando resoluções do CNJ e do CJF de forma geral nos objetivos. São estabelecidos Comitês Locais de Segurança da Informação, assim como há a menção aos princípios de disponibilidade, autenticidade, integridade e confidencialidade. A PSI define, ainda, as estruturas de governança e gestão da segurança, incidentes e ativos de informação, com diretrizes para serem aplicadas nos órgãos da JF, órgãos a serem criados e medidas a serem tomadas, outras normas internas a serem formuladas, monitoramento e auditoria. Vale notar a previsão de intercâmbio com outras organizações, incluindo o CERT.br e o CTIR.gov, na parte de gestão de incidentes, algo muito importante para superar a fragmentação entre setores apontada por Hurel (2021), embora seja necessário ver a aplicação de tal norma na prática.

Já a PSI do TJPE é mais antiga (Res. Nº 349/2013), trazendo tanto repartições de competências quanto ao tema, envolvendo diferentes setores do tribunal, quanto diretrizes de classificação da informação e boas práticas em geral, além de prever uma Estrutura Normativa de Segurança da Informação. As normas são direcionadas, em parte, a áreas específicas, como a Secretaria de Tecnologia da Informação e Comunicação, mas também para os servidores em geral, na medida em que também há regras de utilização de recursos de tecnologia bastante específicas, incluindo a utilização de antivírus, limitações para troca de mensagens e a necessidade de firmar Termos de Confidencialidade para tratamento de informações. Há também disposições sobre aquisição e desenvolvimento de sistemas, auditorias, resposta a incidentes, gerenciamento de riscos e sanções. Outro documento

relacionado é um glossário da PSI, com definições de termos utilizados, o que contribui ainda para a disseminação de informações e de boas práticas — há, na própria PSI do CJF, tópico com o mesmo fim.

No contexto do TJPE, pode-se notar uma maior consolidação do CNJ como veículo de instituições em segurança cibernética a nível setorial, no contexto do Poder Judiciário, notadamente após 2020. Especificamente na justiça estadual de Pernambuco, resoluções do órgão nacional têm uma maior força institucional do que no contexto do TRF5, em que as regras formuladas pelo CJF são aplicadas. Diferentes razões podem ser suscitadas para explicar tais diferenças, mas pode-se afirmar que o modelo centralizado proposto nas resoluções do CNJ tem certo sucesso em se colocar como fonte de regras para órgãos do Judiciário, em especial no contexto do TJPE.

Pode-se relacionar essa observação ao que Belli *et al.* (2023) chamam de compartimentação. Apesar de haver algumas pontes de diálogo com a E-Ciber ou a PNCiber, elas — quando ocorrem — são implícitas. No caso do TRF5, apesar de haver uma compartimentação mais específica, na medida em que diretrizes do CJF são utilizadas pelo tribunal, há a citação de normas abrangentes — em que pese estarem desatualizadas — e o reconhecimento da necessidade de cooperar em termos de incidentes. Prevalecem, dessa maneira, regulações e diretrizes setoriais do Poder Judiciário, assim como observado pela literatura em outros setores. Essa realidade revela ainda desafios em termos de coordenação nacional de esforços em segurança, bem como a persistência da fragmentação entre atores e setores, ainda que o TJPE cite, na Portaria nº 16/2022, a necessidade de harmonizar normas de segurança cibernética com as da Administração Pública Federal. De todo modo, ao transformar preocupações em um arcabouço institucional prático, pode-se afirmar que há a operacionalização de tais questões, transformando-as em práticas claras a serem adotadas.

Havendo realizado essas observações iniciais, serão destacados pontos relacionados aos códigos da primeira categoria da análise de conteúdo, que são as temáticas predominantes nas normativas e documentos.

4.1 OBJETIVOS, METAS E INDICADORES

Como visto nas seções anteriores, documentos como a E-Ciber, resoluções do CNJ e organizações como a UIT apresentam objetivos e estratégias ao tratar de segurança cibernética. De mesmo modo, as políticas internas dos tribunais analisados trazem objetivos, princípios, metas e indicadores próprios. Dessa forma, é importante observar como eles se comparam em termos de segurança cibernética, na medida em que são estruturantes em relação ao restante do arcabouço institucional

Em matéria de objetivos relativos à segurança cibernética, ao comparar a E-Ciber, a PNCiber, a ENESC-PJ e as PSIs e normativas correlatas dos tribunais, nota-se relativa convergência entre os formulados pelos tribunais objetos desta análise e os presentes em

normativas mais abrangentes. Pode-se afirmar que os objetivos mais amplos estão contemplados nas realidades específicas, especialmente no que tange à resiliência de organizações, combate a ações maliciosas, gestão de riscos e mitigação de ameaças. O Quadro 2 exibe uma comparação dos objetivos das diferentes normativas ora tratadas.

Quadro 2 — Comparação de objetivos de diferentes normativas relativos à segurança cibernética.

PNCiber	"I - promover o desenvolvimento de produtos, serviços e tecnologias de caráter nacional destinados à segurança cibernética; II - garantir a confidencialidade, a integridade, a autenticidade e a disponibilidade das soluções e dos dados utilizados para o processamento, o armazenamento e a transmissão eletrônica ou digital de informações; III - fortalecer a atuação diligente no ciberespaço, especialmente das crianças, dos adolescentes e dos idosos; IV - contribuir para o combate aos crimes cibernéticos e às demais ações maliciosas no ciberespaço; V - estimular a adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, evitar, mitigar, diminuir e neutralizar vulnerabilidades, incidentes e ataques cibernéticos, e seus impactos; VI - incrementar a resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos; VII - desenvolver a educação e a capacitação técnico-profissional em segurança cibernética na sociedade; VIII - fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança cibernética; IX - incrementar a atuação coordenada e o intercâmbio de informações de segurança cibernética entre: a) a União, os Estados, o Distrito Federal e os Municípios; b) os Poderes Executivo, Legislativo e Judiciário c) o setor privado; d) a sociedade em geral; X - desenvolver mecanismos de regulação, fiscalização e controle destinados a aprimorar a segurança e a resiliência cibernéticas nacionais; e XI - implementar estratégias de colaboração para desenvolver a cooperação internacional em segurança cibernética.”
E-Ciber	"1. Tornar o Brasil mais próspero e confiável no ambiente digital; 2. Aumentar a resiliência brasileira às ameaças cibernéticas; 3. Fortalecer a atuação brasileira em segurança cibernética no cenário internacional” (Brasil, 2020, p. 7)
ENESC-PJ	"aprimorar o nível de maturidade em segurança cibernética nos órgãos do Poder Judiciário, abrangendo os aspectos fundamentais da segurança da informação para o aperfeiçoamento necessário à consecução desse propósito”.

PDTIC TJPE	"aprimorar o nível de maturidade em segurança cibernética nos órgãos do Poder Judiciário, abrangendo os aspectos fundamentais da segurança da informação para o aperfeiçoamento necessário à consecução desse propósito". (Adota os mesmos da ENESC-PJ).
PSI CJF e PDTIC TRF5	"estabelecer as diretrizes e os princípios da Segurança da Informação com o objetivo de nortear a implementação de medidas de proteção que deverão ser aplicadas às informações que têm valor, independentemente de seu suporte material ou tecnológico (ativo de informação), com vistas ao resguardo da missão, da visão, dos objetivos estratégicos e da imagem dos órgãos." "Alinhar os objetivos e estratégias de segurança da informação com os objetivos e estratégias de negócio, observando a conformidade com as leis, normativos aplicáveis (resoluções do CNJ e CJF), determinações e recomendações dos órgãos de controle; Agregar valor para a Justiça Federal e para a sociedade em geral; Garantir que os riscos da informação estejam sendo adequadamente endereçados por meio de uma abordagem de gestão de riscos, apoiada por sistemas de controles internos." (PSI-CJF, p. 4) "Instituir e aperfeiçoar normas e práticas adotadas pelo órgão relacionadas à Segurança da Informação Digital visando à proteção dos dados pessoais e organizacionais" (PDTIC 2024-26, p. 26).

Fonte: elaboração própria, a partir de Brasil (2020; 2021c).

É especialmente válido destacar que o PDTIC 2024-26 do TJPE utiliza de forma explícita os mesmos objetivos da ENTIC-PJ, do CNJ. Pode-se interpretar essa escolha por prever metas iguais como um sinal claro de demonstrar a busca da implementação e da convergência de esforços com o CNJ. Trata-se de mais um indício de força institucional das resoluções do órgão, inclusive considerando a ausência de citações à E-Ciber ou à PNCiber. Esse aspecto também é revelador das diferentes nuances em termos de produção de normas entre TJPE e TRF5, na medida em que o PDTI 2024-26 do segundo também cita a resolução do CNJ, mas formula os próprios objetivos.

Em relação ao objetivo do PDTI relacionado à segurança cibernética, o TRF5 fixa a meta de atingir, até 2026, a regulamentação de 13 normativos nacionais, além de um índice de institucionalização das normas da PSI da JF como indicador. Ou seja, formalmente a meta do órgão é implementar as instituições veiculadas pelo seu órgão superior específico — ainda mais compartimentadas que as do CNJ, que tem competência sobre todo o Poder Judiciário. Outro objetivo do plano do TRF5 menciona, ainda, a atuação sistêmica e a uniformização de procedimentos, assim como a interoperabilidade e compartilhamento do conhecimento, embora também fixe o CJF como referência.

Ambos os documentos trazem ainda planos de iniciativas, que são ações específicas a serem feitas para cumprir os objetivos elencados, inclusive com o status de implementação no caso do TRF5. No caso do TJPE, cinco das 40 Iniciativas em Alinhamento Estratégico

dizem respeito ao objetivo estratégico que inclui a segurança da informação, incluindo sistemática para desenvolvimento de sistemas, novas plataformas, Ferramenta de Gerenciamento de Acesso Privilegiado — demanda da Res. Nº 396/2021 do CNJ, conforme citado no próprio plano — e contratação de serviços para gerenciamento da questão, também a partir de exigência do CNJ. Destaca-se também uma ação que prevê o investimento no desenvolvimento de soluções de inteligência artificial generativa, inclusive ChatGPT, Gemini e Copilot. Tal previsão prejudica esforços de desenvolvimento e fortalecimento de soluções nacionais, além de criar vulnerabilidades em termos de soberania digital (Belli *et al.*, 2023). Já no caso do TRF5, há iniciativas como gestão de riscos, governança de dados, conscientização, Red Instant Alert e atualização do parque tecnológico.

Os dois tribunais também implementaram o indicador de desempenho iGovTIC, conforme diretriz do CNJ, expresso nos Planos Diretores e em outros documentos. No caso do TJPE, o nível de maturidade no IGovTIC é eleito como indicador, referindo-se ao objetivo estratégico de fortalecer a estratégia nacional de TIC e a proteção de dados, tendo como descrição atingir o nível de excelência, embora não haja mais informações sobre cálculo e acompanhamento. Já no que tange ao TRF5, foi formulada a meta de atingir, em 2024, o índice de 0,75 e, em 2026, de 0,8.

4.2 ESTRUTURA ORGANIZACIONAL E DE COMPETÊNCIAS

Mesmo dentro dos tribunais, é possível notar a existência de diferentes atores responsáveis não apenas pela parte de Tecnologia da Informação, mas também, especificamente, por diferentes dimensões da segurança da informação e cibernética. Vale notar a incidência das Resoluções do CNJ, que estabelecem de forma explícita a estrutura mínima que os órgãos do Poder Judiciário, como detalhado na seção anterior. Não apenas as normativas classificadas com esse código, como as gerais também trazem provisões relativas a competências, a exemplo das PSIs dos tribunais.

Na PSI do TJPE, que é de 2013, há a repartição de competências entre diferentes agentes e órgãos do tribunal, inclusive em termos de produção de instituições, algo que vai ao encontro das recomendações da OCDE. Enquanto complete ao Tribunal Pleno formular, aprovar e revisar a própria PSI, com instruções mais gerais, as normas — as quais contam com controles, restrições e responsabilidades para atendimento à PSI são de responsabilidade do Comitê Gestor de Tecnologia da Informação e Comunicação (CGTIC). Já os procedimentos, definidos como operações de atendimento à PSI e outras normas correlatas, que devem ser aprovados pelo Núcleo de Segurança da Informação, da Secretaria de TIC. Cria-se, dessa forma, uma estrutura hierarquizada e interdependente de produção de

normas internas, cada qual com uma função mais específica. Vale notar também a previsão explícita de revisões de normativas, desde o documento publicado em 2013.

Inclui-se também um rol de boas práticas a serem obrigatoriamente seguidas pelos agentes e por chefias, a serem tratadas em mais detalhes na subseção seguinte, mas cuja presença é notável, na medida em que mobiliza todos a participarem do processo de garantir a segurança da informação. O Comitê Gestor de Tecnologia da Informação e Comunicação (então CGTIC, hoje CGESTIC), por sua vez, tem como competências a proposição de alterações à PSI e termos acessórios, elaboração de normas, análise de casos de violação, incidentes e tentativas de burla da PSI, proposição de medidas e planejamento e alocação de recursos, controle de responsáveis por informações, locais de rede, sítio e dispositivos e recursos de TIC. Trata-se, pois, de um órgão fonte de diretrizes estruturantes para o restante do tribunal.

Então, a Secretaria de Tecnologia da Informação e Comunicação (SETIC) é a responsável por ações mais operacionais, tais como gerenciar permissões e credenciais de acesso, sendo expressamente previsto o princípio do conjunto mínimo de permissões que precisam ser atribuídas, manutenção de registros de atividade de usuários, orientar outros órgãos em políticas adequadas, apoiar campanhas de conscientização e publicar e atualizar o Glossário da PSI, anteriormente mencionado. Já o Núcleo de Segurança da Informação da SETIC tem atribuições mais próximas aos destinatários das normas (servidores do tribunal), incluindo promoção de campanhas, fomento de ações para implementação de diretrizes, relato de violações ou tentativas à SETIC, criação de normas, solicitação de revogação de credenciais de acesso, coordenação do plano de continuidade do negócio e prevenção a desastres, resposta a consultas sobre normas relativas à PSI, aprovação de softwares e equipamentos para utilização por agentes, além de aplicação de medidas de segurança para preservação de infraestrutura.

Dois outros órgãos que cuidam primariamente de outras questões internas e/ou têm competências amplas também têm competências atribuídas a eles pela PSI. No caso da Secretaria de Gestão de Pessoas e da Secretaria Judiciária, há a atribuição de manter atualizados dados sobre modificações no quadro funcional do TJPE, que tem repercussões sobre permissões de acesso, além de indicar as credenciais que precisam ser atualizadas, apoiar campanhas e manter a guarda de Termos de Confidencialidade, mantendo-o como documento obrigatório para exercício dos magistrados. Nota-se, desse modo, relativa interdependência entre áreas administrativas ligadas à questão da segurança cibernética e outras que não cuidam diretamente do tema.

Com o tempo, foram sendo criadas outras instâncias internas dedicadas à segurança da informação e cibernética, notadamente nos últimos anos, após a publicação das resoluções do CNJ sobre o tema — as quais, como discutido, incluem requisitos de estrutura

organizacional. Antes das normativas mais recentes do CNJ, houve, em 2013, delegação (Ato nº3742013-SEJU) para o Diretor Geral autorizar outras classes de agentes judiciários e o público externo a usar recursos de TIC, o que pode ter repercussões em termos de segurança, riscos e incidentes. Já em 2018, a Resolução nº 414 reformulou competências de diversos órgãos, trazendo a Assessoria de Governança de TIC, além de incluir, entre as atribuições do Núcleo de Gestão de Segurança da Informação, a criação do sistema de gestão, buscar seguir padrões de referência, apoiar a gestão de contratos e de projetos e formular requisitos para aquisições. Em 2020, o Ato nº 478 do TJPE criou um Grupo de Trabalho para estudos sobre adequação à Lei Geral de Proteção de Dados, havendo também um Comitê Gestor de Proteção de Dados.

Em 2022, com a Portaria nº 16, o TJPE instituiu o Comitê de Governança de Segurança da Informação, que é responsável por elaboração e direcionamento da respectiva política. Sua composição é de desembargador, juiz, chefe da SETIC, Assessoria Especial da Presidência, chefe da Consultoria Jurídica, coordenador do CGPD e encarregado de proteção de dados. Suas atribuições são amplas, envolvendo formulação de planos e normas, implementação de normas do CNJ, incluindo a ENESC-PJ (explicitamente citada), articulação entre setores, troca de informações, análise de incidentes, acompanhamento da gestão orçamentária e aprovação de acesso à rede. Há ainda uma previsão de que podem ser convidados representantes de outros órgãos e especialistas técnicos para ações específicas, favorecendo a cooperação e a integração. Também existe o Comitê de Governança em TI, responsável por apoiar e orientar iniciativas na área, enquanto o CGESTIC tem funções de planejamento mais operacional e tático, acompanhamento de execuções e desenho de indicadores.

No TRF5, por sua vez, em 2021, foi criado o Comitê Gestor de Proteção de Dados (Ato da Presidência nº 70). Com a Resolução nº 24/2023, o órgão transformou-se em Comitê Gestor de Proteção de Dados Pessoais, sendo composto por um desembargador, juízes, diretores (incluindo o da Diretoria de Tecnologia da Informação) e pelo chefe da Assessoria Jurídica. Há também, assim como no TJPE, um Comitê de Governança de TIC, criado pela Resolução do Conselho de Administração nº 14/2016, com competência de estabelecimento de políticas de gestão, estratégicas, indicadores, metas e planos de ação, e um Comitê Gestor de TIC (Portaria nº 360/2017), que tem entre as suas atribuições a proposição e aplicação de ações com objetivo de melhorar a gestão serviços na área, zelar pela boa aplicação dos recursos, tratar da adequação da estrutura organizacional, segurança da informação, infraestrutura, elaborar planos táticos e operacionais, acompanhar execuções de planos e estabelecer indicadores.

A PSI da JF, vale notar, estabelece que os TRFs devem ter uma unidade de gestão da segurança da informação vinculada à Alta Administração, não podendo ser subordinada a

áreas operacionais. Nesse sentido, especificamente nesse campo, com a Portaria nº 134/2021, o TRF5 criou a Comissão Local de Segurança da Informação. Vale ressaltar que o próprio nome do órgão mostra como a estrutura do tribunal tem como referente a nacional, sendo essa uma “sucursal" local, criada formalmente em razão da PSI, e não das Resoluções do CNJ. Entre os seus objetivos, estão a gestão da segurança da informação, elaboração dos Documentos Acessórios Locais, apoio à presidência em temas relacionados, intercâmbio com outras CLSIs, ações preventivas e educativas, definição de metodologia de análise avaliação de riscos e de tolerância e categorias de risco, promoção da aplicação de normas, disciplinamento de temas, monitoramento de desempenho e de resultados, intercâmbio com a unidade responsável pelo acesso à informação e coordenação de atividades da Comissão Local de Resposta a Incidentes. A CLSI é composta por juízes, diretores de departamentos e representantes das seções judiciárias, com reuniões semestrais.

Há, ainda, o Comitê de Crises Cibernéticas e a CLRI, como comentado, dos quais tratar-se-á na subseção dedicada ao tema. A nível nacional, existe o Comitê de Segurança da Informação da Justiça Federal – CSI-Jus, responsável pela produção de normas e tratamento do tema para toda a JF, bem como pela revisão da PSI e de documentos elaborados pelos tribunais, recomendação de medidas, acompanhamento da evolução de conhecimento, monitoramento do desempenho e promoção da Avaliação de Maturidade da Segurança da Informação. Ele é composto por membros de todos os TRFs e por representantes técnicos das áreas nacionais. Nota-se, pois, mais uma afirmação da compartimentação dupla no contexto do Poder Judiciário federal, haja vista que já existe um órgão de controle do Judiciário como um todo (o CNJ), que também emite regulações setoriais no tema.

4.3 BOAS PRÁTICAS, CAPACITAÇÃO E DISSEMINAÇÃO DE INFORMAÇÕES

O código ao qual mais foram atribuídos documentos foi este, com 19 no total. Eles incluem tanto normativas que ordenam condutas em termos de uso de recursos eletrônicos quanto cartazes e outros materiais que têm o objetivo de disseminar informações, capacitar e garantir a efetividade da organização dos tribunais em termos de segurança cibernética. Tanto normas foram incluídas nesse âmbito quanto outros materiais encontrados na pesquisa, como pareceres e cartazes, que também contribuem para a conformação do arranjo institucional e da definição e fortalecimento de padrões a serem seguidos e condutas a serem evitadas.

A PSI do TJPE, já em 2013, trouxe um rol de boas práticas a serem adotadas pelos agentes do órgão. Há diretrizes de classificação da informação, restrição a acesso e uso de recursos de TIC para pessoas credenciadas, dever de cumprir com níveis de segurança

exigidos por informações classificadas, proteção de identidade digital, além de seguimento dos princípios de conjunto mínimo de permissões que precisam ser atribuídas, de modo que o acesso a ambientes e recursos deve ser controlado e restrito a pessoas autorizadas, também no sentidos de necessidade e mais restrita permissão cabível. Busca-se, desse modo, diminuir riscos e variáveis no contexto da utilização de recursos eletrônicos e dos sistemas do tribunal.

Em termos de aquisição, utilização e controle de recursos, diversas disposições são fixadas. Há direito exclusivo de uso do TJPE sobre informações criadas e acessadas por agentes, enquanto recursos de TIC podem ser usados apenas por magistrados e servidores; outras classes e o público externo devem ter autorização para fazê-lo. Reitera-se que o uso de recursos da infraestrutura de tecnologia deve ser restrito às atividades desempenhadas pelos agentes, no sentido da concessão de permissões apenas indispensáveis para atividades, algo importante em termos de disciplinamento da relação agentes-tecnologia-segurança. Todos os equipamentos, pois, estão sujeitos à PSI, e devem ter diferentes tipos de software de proteção instalados.

São, então, fixados como direitos do TJPE registro, bloqueio, permissão e suspensão de dispositivos, inclusive a prerrogativa de registrar, isolar e apreender dispositivos de terceiros no seu perímetro lógico ou físico. Proíbe-se a captura de imagens e outros registros do ambiente no perímetro físico sem autorização, assim como o acesso a conteúdos ilegais, que não condigam com as atividades ou que possam causar prejuízo à infraestrutura do órgão, incluindo a instalação de softwares maliciosos, não homologados pelo NSI ou pirateados. Também se informa o monitoramento de todas as atividades realizadas em ambientes de TIC institucionais, com o objetivo de proteger ativos, reputação e conhecimento, com previsão de Processo Administrativo e sanções em caso de descumprimento das regras.

Outras disposições da PSI incluem a sugestão de evitar publicar em redes sociais a rotina de trabalho, criação de processo de gerenciamento de mudanças para mitigar problemas de disponibilidade de recursos de TIC após alterações, permissão de trocas de mensagens apenas para fins profissionais e usando sistemas homologados ou fornecidos pela SETIC, que igualmente o faz com o acesso remoto. O art. 34 da PSI do TJPE traz uma diretriz importante, no sentido de que agentes devem portar informações, quando necessário, pelo menor tempo possível e com controle de restrição, inclusive por criptografia, devendo excluir a informação após o trânsito ou uso e/ou aplicar procedimento para impedir futuro uso.

Permite-se o uso de dispositivos de TIC pessoais no ambiente de trabalho, embora tal permissão seja tratada como benefício, que pode ser perdido caso a utilização vá de encontro à PSI, a outras normas ou ao exercício do trabalho, além de os agentes serem responsáveis

pelo conteúdo armazenados nos aparelhos. Relacionamentos com compartilhamento de informações e a concessão de acesso a ambientes devem ser precedidos por Termos de Confidencialidade que tratem de segurança da informação, enquanto o descarte de informações deve ser feito de forma segura e os agentes devem cuidar para não expor documentos com informações restritas ou deixar computadores desbloqueados sem supervisão ou uso, por exemplo. São, ainda, previstas análises de conformidade e auditorias, além de se prever que o desenvolvimento e aquisição de recursos.

Além da PSI, outra fonte de boas práticas encontrada foram pareceres formulados pela SETIC. Como mencionado anteriormente, trata-se de uma suporte de veiculação de instituições com aplicabilidade direta ao comportamento de agentes do órgão. Apesar de não serem exatamente normas, os 17 pareceres encontrados descrevem a compatibilidade de práticas e usos com a estrutura normativa. Os textos tratam de questões como emissão de certificados digitais, videoconferência, uso de aplicativos como Dropbox, WhatsApp, Netflix e Skype. É feita uma avaliação abrangente sobre os riscos decorrentes da utilização das plataformas, a partir de seus termos de uso, opções e formas de utilização, assim como implicações em termos de vulnerabilidade, impacto para infraestrutura e diretrizes a serem seguidas pelos servidores.

Outras normas, como Instruções de Serviço e Instrução Normativa, disciplinam outras práticas, como utilização de verificação em duas etapa, regulação de uso de recursos de rede, uso de certificados digitais e operação de *tokens*. É válido destacar, ainda, a produção de cartazes, com o objetivo de disseminar informações e boas práticas de forma mais acessível. Eles abrangem temas como uso de pen drives, bloqueio de computadores ao não usar, monitoramento, criação e uso de senhas e de e-mail institucional para comunicações de trabalho e certificados digitais. Cartilhas também tratam de alguns desses temas, de modo a disseminar a questão. Nota-se que os temas de tais materiais têm como foco pontos sensíveis do uso das redes e das normativas internas, os quais podem gerar vulnerabilidades e incidentes em caso de violação das normas e emprego de práticas que abram margem para a ação de ameaças cibernéticas. O PDTIC do TJPE também prevê ações de capacitação, atividade que é, ainda, competência de alguns órgãos, e há um Plano de Capacitação que contém ações incluindo temas como incidentes de segurança.

No que tange ao TRF5, duas normativas destacam-se: as Políticas de Controle de Acesso Lógico e de Segurança de Acesso Físico, que são definidas a partir da PSI da JF. A primeira traz disposições sobre assuntos como definições, identificação de usuários, credenciais, senhas, processos de desligamento ou movimentação de usuário, acesso local à rede e remoto, com ênfase para a obrigação da criptografia no caso do segundo, em linha com as diretrizes do CNJ, além de autenticação em dois fatores e uso de antivírus, como no TJPE. Há, ainda, tratamento de transferência de arquivos, a utilização de sistemas de

mensagens, com previsão de desenvolvimento de sistema próprio, acesso à rede sem fio, incluindo proibição de uso de dispositivos pessoais, com a possibilidade de exceções, bem como a previsão comum ao TJPE do privilégio mínimo.

Já a Política de Segurança de Acesso Físico inclui diretrizes que regulam o contato de agentes e outras pessoas com instalações físicas, notadamente relacionadas a sistemas e infraestrutura de tecnologia e processamento/armazenamento de dados do tribunal. São colocados limites a tal acesso, compreendendo autenticação em dois fatores, controle e registro de acesso e discrição de instalações, localização em área segura de equipamentos críticos e proibições de aparelhos eletrônicos em centros de processamento. De acordo com a resposta ao pedido de acesso à informação nº 4519147 — realizado pelo autor ao tribunal com base na Lei nº 12.527/2011 —, houve implementação parcial do sistema indicado pelo CNJ de crachás, credenciais e liberação de acesso.

Nota-se, pois, considerável compatibilidade de boas práticas estabelecidas entre ambos os tribunais, assim como com relação aos princípios do CNJ sobre cultura de segurança cibernética. A disseminação de tais práticas é importante para garantir a efetividade dos objetivos maiores, das PSIs e demais regramentos, e a segurança como um todo. Trata-se, pois, de envolver todos os agentes envolvidos a nível interno — considerando o alto nível de digitalização de processos no contexto do Judiciário já discutido —, no sentido do que Fallleti (2020) chama de legitimidade enquanto fonte social da força institucional. Ou seja, à medida que instituições (regras, como escreve North (1991) são mobilizadas pelos atores aos quais elas são aplicadas, elas passam de direitos aspiracionais para instituições de fato aplicadas e que moldam comportamentos. Essa é, dessa forma, a importância do rol de boas práticas para a estrutura institucional de segurança cibernética como um todo.

4.4 RESPOSTA A INCIDENTES E GESTÃO DE RISCOS

Conforme estabelecido pela E-Ciber, a gestão de riscos consiste nos conjuntos de princípios, estruturas e processos que possibilitam o conhecimento de vulnerabilidades, de modo a mitigar a sua exploração, bem como estabelecer um tratamento à ocorrência de incidentes. Tal parte do arcabouço de segurança cibernética, que também é tratado pela defesa cibernética, como discutido, motiva processos de securitização e de uma visão de maior urgência na abordagem. Como trazido nas seções anteriores, a cooperação na comunicação de incidentes e compartilhamento de experiências é importante para que se alcance um nível alto de maturidade de segurança cibernética como um todo, e não apenas setorial (Stolz; Axon, 2023; Belli *et al.*, 2023).

Nesse sentido, a questão de resposta a incidentes é também vista nas estruturas internas de segurança cibernética dos tribunais, inclusive a partir das resoluções e

protocolos do CNJ que criaram diretrizes nesse sentido. Tanto a PSI do TJPE quanto a da JF tratam da gestão de riscos e tratamento de riscos, sendo a segunda mais específica, já definindo objetivos — desenvolvimento de capacidades de gerenciar eventos e incidentes que afetem a segurança — competências de forma clara, com a criação do Comitê de Resposta a Incidentes da Justiça Federal (CRI-Jus) e com a indicação da criação das Comissões Locais, ambas tendo a função de Equipe de Tratamento e Resposta a Incidentes, nos moldes de órgãos como CTIR.gov e CERT.br. Enquanto o órgão nacional formula diretrizes e processos a serem seguidos, além de manter intercâmbio com outros, incluindo o CTIR.gov e CERT.br (nominalmente citados), e solicitar a assistência de especialistas externos sob a condição de confidencialidade, as CLRIs têm a atribuição de gestão local da questão, intercâmbio com outras CLRIs, tratamento de incidentes e notificação ao CSI-Jus quando estes ocorrerem.

No TJPE, a PSI de 2013 prevê a implementação futura, por parte da SETIC, de uma equipe de resposta a incidentes, com a comunicação de fragilidades e eventos de segurança associados aos ativos de informação ao CGTIC, com vistas à tomada de decisão para preservar e restabelecer serviços, além de guardar provas produzidas nesse contexto. São também previstas auditorias de modo a detectar vulnerabilidades e verificar o cumprimento da política. Apenas em 2021 foi criada a Equipe de Tratamento e Resposta a Incidentes (ETIR), com a Instrução Normativa nº 5, que foi posteriormente revogada pela IN nº 19/2022, que recriou a ETIR. A sua missão inclui a resposta a incidentes de segurança cibernética, de forma reativa e proativa, tendo como público-alvo todos os usuários do tribunal, podendo solicitar e prestar apoio a outras áreas, assim como receber comunicações de incidentes por um endereço de e-mail.

Entre as atribuições da ETIR, estão a recepção, triagem e tratamento de informações relacionadas a incidentes, de forma preferencialmente preventiva e evitando recorrência, coordenação e operação de ferramentas de registros de acesso, registro de detecções, triagens e tratamento de incidentes, de modo a manter histórico de fatos, comunicação de incidentes com potencial de impacto à SETIC, encaminhamento de necessidades de capacitação, além de haver uma diretriz específica para cumprimento de determinações do CNJ. A Equipe segue modelo de autonomia compartilhada, compartilhando o processo de tomada de decisão com outros setores do órgão, como a presidência, o CGSI e a SETIC, sendo composta por um Agente Responsável e cinco membros, bem como vinculada à Diretoria de Operações de TIC da SETIC.

Suas ações, segundo a IN, devem ser pautadas por tratamento sigiloso de informações, princípio da necessidade conhecimento, cuidado nas ações para restabelecer serviços e preservar evidências e consideração de requisitos legais. Chama a atenção a ausência de mecanismos ou disposições cooperativas com órgãos nacionais, do Judiciário ou

ainda mais abrangentes. Como colocado por Hurel (2021), a fragmentação no tratamento de ameaças cibernéticas prejudica a efetividade de iniciativas na área, na medida em que a coesão no enfrentamento é necessária. A ideia de sigilo irrestrito também vai de encontro ao dever de transparência de toda a administração pública, bem como a um desenho institucional mais favorável aos próprios objetivos de tratamento, catalogação e prevenção de incidentes.

Já no caso do TRF5, a CLRI foi criada pela Portaria nº 133/2021, junto à CLSI, tendo como atribuição a identificação e tratamento de incidentes de segurança cibernética no contexto da Justiça Federal da 5ª Região, bem como o desenvolvimento de ações preventivas e educativas, atuar como ETIR, dar tratamento e registrar incidentes de segurança da informação, escalar incidentes que atinjam outros órgãos, notificar o CRI-Jus sobre incidentes, solicitação de assistência, intercâmbio com outras CLRIs e propor melhorias aos processos. Sua composição é dos diretores da Divisão de Infraestrutura de Tecnologia da Informação e dos Núcleos de Gestão de Segurança e Serviços e de Gestão de Dados, bem como de representantes das seções judiciárias. Novamente, há a inserção do órgão em uma cadeia nacional, liderada por outras equipes ligadas ao CJF.

Também em 2021, foi criado, com a Portaria nº 132, o Comitê de Crises Cibernéticas, com objetivo de observar o Protocolo de Prevenção a Incidentes Cibernéticos do Poder Judiciário, do CNJ, avaliar riscos, monitoramento dos de maior criticidade, realizar simulações e testes de validação de planos, reunir sala de situação no caso de ocorrência de crise cibernética, garantir a comunicação entre unidades, documentação sobre lições e aprovação de relatórios finais sobre crises. Tem-se, pois, um órgão criado apenas para situações de especial exceção em termos de segurança cibernética, em que a CLRI não seria suficiente para lidar com a questão. Também chama a atenção a menção ao documento do CNJ, algo não tão frequente no TRF5 quanto no TJPE.

No âmbito do TJPE, outros documentos fizeram parte da análise de conteúdo e foram classificados nessa categoria. Enquanto os demais também, de certa forma, confundem-se com disposições de estrutura organizacional — ainda que voltadas para a gestão de incidentes e risco —, há outras instituições que têm maior foco procedimental/conceitual considerando a já existência de órgãos para lidar com a temática. A Justiça estadual, em 2017, publicou uma Instrução de Serviço (nº 1) para a gestão de riscos no âmbito da SETIC, estabelecendo conceitos como risco, análise, avaliação e gestão de riscos, controle e ativo, bem como obrigações e responsabilidades e diretrizes para o processo de análise e avaliação de cada ativo de informação, incluindo a elaboração futura de um plano de tratamento de riscos e de um relatório de monitoramento trimestral feito pelo NSI da SETIC para o CGTIC.

Em 2023, o TJPE também publicou o Plano de Gestão de Riscos de Tecnologia da Informação e Comunicação, atualizado em 2024. Ele tem o objetivo de implementação da IN nº 1/2017 sobre gestão de riscos, com diretrizes concretas e atribuição de responsabilidades, visando ao combate e prevenção de ameaças, conformidade e eficiência. O processo inclui as etapas de identificação (escopo de aplicação e cenários), análise (antecipação de situações que podem representar ameaças), avaliação, tratamento e aceitação (inclusive responsabilidade). Entre os documentos que baseiam o plano, estão diretrizes da ABNT e da Organização Internacional para a Padronização (ISO) sobre riscos o que indica uma maior incidência das instituições veiculadas por tal órgão em detrimento, a nível internacional, por exemplo, da UIT ou do NIST. É definida uma metodologia para a gestão de riscos, bem como são atribuídas responsabilidades a órgãos internos como CGTIC, CGDI, CGPD, CGESTIC, bem como para os agentes judiciários. Os principais riscos identificados são os estratégicos, de segurança da informação e comunicação, aos titulares de dados pessoais, para contratações, processos e projetos, enquanto um plano de ação inclui revisões de políticas e listas e a realização do processo de gestão de riscos para as áreas identificadas. São, ainda, previstas reuniões semestrais de acompanhamento.

Em julho de 2024, o TJPE publicou três protocolos, à semelhança dos do CNJ, nas Instruções Normativas nº 30, 31 e 32: os Protocolos de Gerenciamento de Crises Cibernéticas, Investigação de Ilícitos Cibernéticos e Prevenção de Incidentes Cibernéticos. Eles representam a implementação de maneira mais direta das diretrizes do CNJ, na medida em que adotam tanto a mesma estrutura normativa quanto arranjo institucional e conceitual, incluindo a diferenciação entre crise e incidente e o tratamento de processos. Cria-se o Comitê de Crises Cibernéticas, assim como no TRF5, com representantes da presidência, da SETIC, da ETIR, consultoria jurídica, comunicação, proteção de dados e segurança, bem como atribuições de levantamento de informações sobre o incidente que gerou a crise, plano para retorno à normalidade, identificação de boatos, avaliação de soluções, evitar vazamento de informações, inclusive as classificando, orientar envolvidos quanto a estratégias de resolução e delimitar informações que podem ser compartilhadas e como fazê-lo com entidades que podem também estar passando pela crise.

O presidente do Comitê, enquanto isso, tem atribuições de tomada de decisões e de aprovação de comunicação e de direcionamento. Há a previsão de uma sala de situação a ser estabelecida no decorrer de uma crise cibernética, física ou virtual, com ênfase no sigilo da comunicação e no controle das informações. São, ainda, identificadas atividades críticas, como ingresso e consulta a processos e audiências, que devem ter riscos monitorados e avaliados, assim como o tratamento deve considerar a prestação dos serviços no contexto de indisponibilidade de serviços. Os critérios de definição de crises cibernética são fixados, incluindo impacto, dano e persistência das ações de resposta por longo período, como

colocado pelo CNJ. Também são definidas ações para durante a após a crise, compreendendo notificação da ETIR para que o Comitê decida sobre a caracterização de um incidente como crise, seguimento de planos e diretrizes do órgão, análise de ações tomadas e construção de relatório final, incluindo identificação da causa do problema, medidas adotadas, impacto, mecanismos e processos de detecção, investigação e preservação de evidências, coordenação e processos de tomada de decisão, de modo que haja um registro que subsidie situações futuras. Conforme a ENESC-PJ, um relatório de comunicação do incidente deve ser divulgado com outros órgãos por meio da rede colaborativa do CNJ, algo previsto no protocolo do TJPE.

Já o protocolo relacionado à investigação de ilícitos cibernéticos estabelece padrões a serem seguidos em caso de incidentes, incluindo até o registro de entradas de acesso em sistemas, hora, detalhes sobre o processo de coleta e de preservação de evidências, incluindo priorização de não comprometimento de provas e estabelecimento de competências em termos de tomada de decisões nesse contexto, como armazenamento de cópias pela ETIR. Também são elencados os requisitos do Relatório de Comunicação de Incidente de Segurança, como nome do responsável pela preservação dos dados e pela ETIR, relato, descrição de atividades de resposta, resumo criptográfico de arquivos coletados e justificativa em caso de inviabilidade de coleta. São definidos também os procedimentos de envio e de recebimento de tais relatórios, passo importante na construção de uma segurança cibernética sólida, embora não haja previsão explícita de cooperação com órgãos de fora do Judiciário.

Por fim, o protocolo relativo à prevenção de incidentes tem como princípios críticos base de conhecimento e defesa, priorização, instrumentos de medição e métricas, inclusive quanto à propensão de agentes de serem atraídos por ameaças quanto a correções e a ferramentas, diagnóstico contínuo, formação, capacitação e conscientização, automação e resiliência, devendo ser aplicados de forma proporcional e balizada por avaliações de risco. Há, então, a definição de funções básicas e de seus respectivos responsáveis, incluindo identificação e mapeamento de riscos e ameaças, assim como de mitigação e aceitação de riscos, proteção (compreendendo ações de educação e de disseminação), detecção, resposta e recuperação. A ETIR, por sua vez, será adequada às exigências do CNJ, de acordo com as disposições do protocolo.

A análise dessas normativas classificadas na categoria de incidentes e risco mostra especialmente a inter-relação entre as diversas dimensões da segurança cibernética. Apesar de ter esse foco, as instituições também lançam mão de instrumentos relacionados a questões de estrutura organizacional e de competências, que são determinantes para que as regras sejam de fato aplicadas e o objetivo final de garantir a segurança seja atingido. Nota-se também uma dinâmica de urgência e de restrição das informações relativas a incidentes e

crises, justificada pela situação de exceção, mas que pode ser prejudicial à consolidação de uma arquitetura securitária nacional, como discutido pela literatura (Hurel, 2021).

4.5 INFRAESTRUTURA E ORÇAMENTO

Apesar de poucos documentos terem tido este código a eles atribuído (apenas três, como foi visto), a aquisição e composição de infraestrutura cibernética de tribunais, assim como a destinação orçamentária para a área, têm implicações sensíveis para a segurança cibernética. As aquisições de equipamentos não apenas são determinantes para a efetividade das instituições veiculadas, na medida em que as informações são neles processadas, como também para a dimensão de soberania digital colocada por Belli *et al.* (2023), prezando pelo controle e autonomia de soluções digitais como parte da dimensão de segurança. As resoluções do CNJ, vale notar, contam com requisitos e diretrizes para aquisições e contratações de produtos e serviços da área de tecnologia.

No caso do TJPE, há um plano de contratações e um plano orçamentário da SETIC de 2024, com planejamentos sobre alocação de recursos e contratações a serem realizadas no ano. Destacam-se, em matéria de segurança cibernética/da informação, o investimento em soluções tecnológicas para fins de educação em segurança da informação, assim como ferramenta de *phishing*. Entre as aquisições planejadas, estão um Security Operation Center, ferramenta de acesso privilegiado — possivelmente para implementar e armazenamento e de *backup*, embora não haja detalhes sobre os objetivos e estudos que baseiam as aquisições, na medida em que muitos termos estão sob sigilo. A despesa total do tribunal, em 2023, foi de R$2,37 bilhões, dos quais R$33,4 milhões foram destinados para aquisições de TIC e R$25,3 milhões, para custeio (TJPE, 2023).

Já em se tratando do TRF5, o Plano de Artefatos de Contratação de 2024, disponível no sítio eletrônico do tribunal destinado a informações sobre a governança de tecnologia, lista algumas contratações a serem realizadas. Entre elas, há serviços de suporte de infraestrutura de rede e bancos de dados, sistema de monitoramento de rede, manutenção, computadores, solução para gestão de chamados e de suporte. De acordo com o Demonstrativo da Execução Orçamentária do TRF5 de 2023, foram destinados, no ano, R$1,7 milhão para a segurança da informação, de um total de R$343 milhões, representando menos de 0,5% de todos os recursos (TRF5, 2024).

Um fator a ser destacado é a prevalência de empresas estrangeiras entre as fabricantes de dispositivos e serviços adquiridos pelos tribunais, como Huawei, IBM, Microsoft e Oracle. Em um contexto em que uma noção mais ampliada de segurança cibernética inclui a soberania digital, a dependência em relação a soluções estrangeiras pode representar uma vulnerabilidade em termos de disponibilidade continuada do serviço,

inclusive considerando as disposições do CNJ e da E-Ciber em termos de preferência por soluções nacionais. Como os documentos relativos a tais aquisições, no caso do TJPE, são colocados sob sigilo, prejudica-se a análise sobre a motivação e o processo que levou à contratação de tais serviços, em detrimento de outros. Vale mencionar, contudo, um acordo firmado entre o TJPE e o Instituto de Ciência e Tecnologia do Porto Digital, mencionado na descrição da despesa orçamentária de custeio de TIC, voltado ao desenvolvimento de soluções, importante no que tange à valorização da produção local e nacional.

Observando Estudos Técnicos Preliminares de licitações recentes relativos a aquisições de recursos tecnológicos, também é possível apontar a ausência de apontamentos e análises com relação aos riscos que produtos/vulnerabilidades que produtos adquiridos podem apresentar, com foco em riscos relativos à prestação do serviço por parte da contratada. Mostra-se, ainda, errática a aplicação dos requisitos da ENESC-PJ no contexto de processos licitatórios. Alguns estudos do TRF5 mencionam questões como interoperabilidade e segurança, como o relativo a serviços de suporte técnico, ainda que de forma superficial, enquanto outros não abordam o tema de forma alguma.

O tratamento da segurança cibernética no contexto de aquisições de equipamentos é importante, na medida em que representa a força institucional de normativas do CNJ e até dos próprios tribunais em termos de segurança cibernética. Mesmo o TJPE, pois, que demonstra buscar a implementação das diretrizes do órgão nacional no tema apresenta lacunas na efetividade na prática. Nos pedidos de acesso à informação feitos aos tribunais, foram solicitados dados sobre o atendimento aos requisitos, ao que foi respondido que tal informação estaria disponível nos portais de contratações e orçamento, algo que não se observa exatamente, posto que tais requisitos não aparecem em muitos documentos relativos a licitações relacionadas à área de tecnologia.

4.6 TRANSPARÊNCIA E FISCALIZAÇÃO

Inicialmente, quanto à transparência, é importante destacar que o próprio âmbito de análise desta pesquisa dependeu da transparência dos tribunais quanto às normativas internas e práticas em matéria de segurança cibernética. Assim, além de previsões normativas quanto à publicidade de questões relativas ao tema, a própria divulgação no sítio eletrônico e a facilidade de acesso são determinantes para que se possa ponderar a transparência dos órgãos objeto desta análise e, como comentado na seção de metodologia e desenho de pesquisa, são potenciais limitações, na medida em que depende de quão públicas são as instituições internas e o seu processo de formulação.

O site do TJPE, por exemplo, apresenta os documentos coletados em páginas diferentes, embora haja uma seção do site dedicada à segurança cibernética e da informação,

bem como à tecnologia da informação de forma geral. O TRF5 também tem uma seção correlata, mas foi notado que não todos os documentos relacionados ao tema, como portarias e normativas internas, estão nessa página. Essa disposição espalhada dos documentos prejudica o controle social e a compreensão do arcabouço institucional interno em matéria de segurança cibernética dos tribunais, tendo sido necessário ler os documentos para compreender as mudanças e a situação atual. Os documentos, contudo, apresentam histórico de versões e de atualizações, quando é o caso, o que é importante para compreender mudanças e transformações.

As normativas mais gerais, como os Planos Diretores, trazem a sua metodologia de formação, que revelam a restrição dos tribunais à participação e a qualquer arranjo multissetorial em seus órgãos. A composição de comitês e comissões é consistentemente de servidores e agentes judiciários, com abertura para colaboradores técnicos em alguns casos. Esse arranjo revela uma visão, por parte dos tribunais, que a garantia da segurança cibernética e a própria gestão de serviços tecnológicos diz respeito apenas aos próprios tribunais, e não que se insere em um contexto maior que depende de coesão e convergência de esforços para que se obtenha fortalecimento institucional a nível nacional, a partir de diversas contribuições coordenadas — e não compartimentalizadas, como apontam Belli *et al.* (2023).

Outra lacuna relevante em termos de coordenação é a pouca menção e estabelecimento institucional de compartilhamento de informações sobre incidentes, que, quando prevista, restringe-se ao Poder Judiciário. O TRF5, por exemplo, cita colaboração com universidades e com centros de tratamento de incidentes, embora não seja algo muito enfatizado e fique bastante ausente no caso do TJPE. Trata-se de um potencial inexplorado em matéria de colaborar para a arquitetura de segurança cibernética nacional, na medida em que dados sobre o ameaças e incidentes no contexto do Judiciário podem contribuir com os trabalhos de órgãos nacionais que tratam do tema, para além do CNJ ou do CJF. A ausência de divulgação de dados ou de estabelecimento de prazo para tal, considerando a sensibilidade, também vai de encontro ao princípio geral da publicidade.

Também é preocupante uma tendência de transformar o sigilo como regra em questões relativas a incidentes, especialmente crises cibernéticas, algo notado em ambos os tribunais. No TJPE, os protocolos têm várias disposições no sentido de restringir a divulgação de informações sobre incidentes e as colocar sob sigilo de forma indefinida, sem análise caso a caso ou definição de tempo, além de vários termos de aquisição de equipamentos estarem sob cláusula de confidencialidade, o que vai de encontro ao entendimento do sigilo como exceção, e não como regra, conforme a Lei de Acesso à Informação (Gruman, 2012). Já no TRF5, na resposta do pedido de acesso à informação realizado, foi mencionado que, por exemplo, o manual de gestão de identidade e controle de acesso é restrito acesso por ser um

tema sensível à política de segurança da informação, o que não é necessariamente uma justificativa para restringir acesso a documentos que são, a princípio, públicos.

Vale notar que o TRF5 já enfrentou um incidente de segurança cibernética, o que pode ter relação com essa conduta de restrição maior de acesso a informações sobre a estrutura institucional sobre o tema. A abordagem, todavia, não contribui para o fortalecimento da segurança, que não apenas depende da cooperação com outros atores para construção de uma arquitetura mais fortalecida, como não pode ir de encontro ao direito ao controle social e ao dever de transparência da administração pública. Um dos objetivos da CLSI do tribunal, ressalta-se, é realizar intercâmbios com a gestão do acesso à informação de modo a preservar informações sigilosas, o que pode gerar problemas em termos de transparência.

Apesar de as políticas dos tribunais conseguirem operacionalizar conceitos de segurança cibernética, ainda que com problemas em termos de harmonização com outros setores — desafio que a E-Ciber e a PNCiber devem enfrentar —, observa-se uma dinâmica semelhante aos processos de securitização. Mesmo não havendo participação de militares, nota-se que as normativas dão aos incidentes e crises uma lógica de emergência que justifica a relativização do dever de transparência e a adoção do sigilo como regra para tais questões. Além de prejudicar a própria efetividade da mitigação de riscos, do combate a ameaças e da construção de maturidade, esse arranjo institucional dificulta o *accountability* de gestores perante a sociedade e os outros poderes, assim como reforça a compartimentalização (Belli *et al.*, 2023; O'Donnel, 1998).

Somam-se a esses problemas de transparência a falta de clareza sobre a quantidade de incidentes aos quais se respondeu, bem como mais informações sobre os casos. Além de ocasionar as questões já apontadas, esse arranjo institucional denota uma visão, parte dos tribunais, de que a segurança cibernética é assunto meramente interno, devendo no máximo responder a organizações como o CNJ e o CJF. Se o direito à ação e a ter lesão a direito apreciada pelo Judiciário devem ser garantidos, o controle social sobre a segurança cibernética dos sistemas que sustentam a operacionalização contemporânea dessas garantias igualmente deve ser assegurado. De mesmo modo, arranjos cooperativos são importantes para garantir a força institucional de regras de segurança cibernética, pensando em um contexto nacional, e não apenas setorial.

CONSIDERAÇÕES FINAIS

O desenho desta pesquisa permitiu, por meio de uma lógica de dedução, compreender como a segurança cibernética pode ser pensada em escalas. O fortalecimento nacional depende também da atuação de setores e de comunidades específicas, embora a fragmentação de tais esforços, apontada pela literatura, prejudique resultados que poderiam ser obtidos com um cenário de maior coesão. Nesse sentido, a análise desde estratégias de

abrangência nacional, passando por regras operacionais setoriais e chegando à realidade órgãos locais viabiliza uma compreensão holística dos fenômenos apontados no debate sobre o tema no Brasil, nomeadamente os obstáculos para se construir uma realidade mais cooperativa e menos fragmentada e baseada em fechamentos operacionais.

A análise de conteúdo mostrou que os tribunais analisados têm estruturas formais de proteção da segurança cibernética e da informação como um todo, com órgãos internos dedicados ao assunto, ainda que sejam recentes e que apresentem diferenças entre si. A força institucional de normativas do CNJ, a repartição de competências ou a disposição maior ou menor à cooperação com outros atores foram algumas das diferenças notadas, ainda que haja também convergências. Foi, ainda, possível perceber as questões que mais mobilizam as organizações analisadas no contexto da temática, assim como os seus arranjos internos para tal e a evolução ao longo do tempo, notadamente nos últimos anos.

A investigação demonstrou, em especial, a relação entre segurança cibernética, acesso à informação/transparência, soberania digital e a necessidade cooperação e efetivação de uma rede nacional. A publicidade é importante no que tange ao direito de se informar e de entender as práticas da administração pública diante de hipóteses normativas e dos objetivos estabelecidos. Estes, por sua vez, quando são formulados em um contexto de cooperação e de harmonização de práticas a nível nacional, contribuem para um fortalecimento mais abrangente. Quando isso não acontece, em contrapartida, há o cenário de compartimentação apontado pela literatura e visualizado na prática, tanto com a maior força institucional do CNJ quanto do CJF, no caso do TRF5, bem como pela ausência de menções à E-Ciber. A soberania, por sua vez, representa também uma noção mais abrangente de segurança, ao mobilizar a autonomia e a dependência, bem como a produção nacional e o controle sobre equipamentos e a o desenvolvimento de equipamentos e sistemas.

O desenho institucional dos tribunais mostrou, ainda, uma preocupação com questões como boas práticas, tratamento de riscos e incidentes, além de repartição de competências, embora com uma visão bastante setorial, carecendo de um entendimento próprio de inserção na situação nacional. Trata-se, pois, de um desafio para a efetividade da E-Ciber e da PNCiber, bem como para a construção de esforços coesos com vistas ao fortalecimento da segurança cibernética a nível nacional. A percepção pode motivar novas iniciativas não apenas dos tribunais, como também de organismos nacionais, no sentido de trabalhar pela maior efetividades de estratégias, objetivos nacionais e de um envolvimento maior de todos os setores em um contexto mais abrangente.

A replicação desse desenho de pesquisa em outros tribunais, órgãos do Judiciário ou mesmo de outros setores permite compreender de uma maneira ainda mais aprofundada as diferentes tendências ora observadas, assim como alargar a comparação quanto aos assuntos

mais mobilizados. Limitações incluem uma determinação mais precisa, por exemplo, do grau de disseminação das boas práticas instituídas em normas, bem como da emergência de instituições informais. Ou seja, da força institucional de regras formais internas e de como os servidores de áreas, Varas e Seções diversas dos tribunais interagem com as normas e em que medida as aplicam em suas atividades.

Nesse sentido, alcança-se uma dimensão mais aprofundada e ampla dos significados da segurança cibernética, envolvendo diferentes atores, desde desenhos institucionais mais abrangentes até a sua implementação em contextos locais. Ao colocar tais questões sob a lupa da pesquisa, pode-se compreender o que motiva os atores por trás de processos de formulação de instituições e de organização em termos de segurança cibernética, bem como lacunas nesses campos, conforme se observou nos casos estudados. Com isso, consegue-se inclusive contribuir para a superação da fragmentação e a formação de redes colaborativas em matéria de segurança cibernética, algo essencial para se alcançar a harmonização conceitual e o fortalecimento necessário para o alcance de uma maturidade nesse âmbito, protegendo infraestruturas críticas e serviços essenciais, como o prestado pelo Judiciário.

REFERÊNCIAS

AGUIAR, T. **Políticas de segurança cibernética no Brasil**: de onde viemos e para onde vamos?. Montevidéu: Programa Líderes; Registro de Endereçamento da Internet para a América Latina e o Caribe, 2023. Disponível em: https://www.lacnic.net/6974/3/lacnic/#. Acesso em: 27 jun. 2024.

ALVES, R.; CARVALHO, M.; NUNES, R. **Judiciário sob ataque hacker**: riscos de negócio para segurança cibernética em tribunais brasileiros. RISTI - Revista Iberica de Sistemas e Tecnologias de Informação, n. 56, p. 344–357, 13 jun. 2023. DOI: 10.5281/zenodo.8032915.

ALVES JÚNIOR, S. A. G. **Políticas Nacionais de Segurança Cibernética:** O Regulador das Telecomunicações — Brasil, Estados Unidos, União Internacional das Telecomunicações (UIT). Dissertação (Mestrado em Regulação e Gestão de Negócios)—Brasília: Universidade de Brasília, 2011.

ASSUNÇÃO, N. M. S. **Segurança cibernética**: um estudo bibliométrico comparativo entre o Brasil e o mundo. Dissertação (Mestrado em Ciência da Computação)—Brasília: Universidade Católica de Brasília, 12 jul. 2023.

BARROS, O. S. R.; GOMES, U. M. G.; FREITAS. W., L (orgs.). **Desafios estratégicos para segurança e defesa cibernética**. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. Disponível em: https://livroaberto.ibict.br/handle/1/612/. Acesso em: 10 jul. 2024.

BELLI, L.; FRANQUEIRA, B.; BAKONYI, E.; CHEN, L.; COUTO, N.; CHANG, S.; HORA, N.; GASPAR, W. B. **Cibersegurança**: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil digitalmente soberano. Rio de Janeiro: FGV Direito Rio. 2023.

Disponível em: https://direitorio.fgv.br/conhecimento/cibersegurança-uma-visao-sistemica-rumo-uma-proposta-de-marco-regulatorio-para-um. Acesso em: 1º jul. 2024.

BRASIL. Conselho Nacional de Justiça. **Resolução nº 370**, de 28 de janeiro de 2021. Estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD). Brasília: CNJ, 2021a.

BRASIL**.** Conselho Nacional de Justiça. **Guia da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário.** Brasília: CNJ, 2021b.

BRASIL. Conselho Nacional de Justiça**. Resolução nº 396**, de 7 de junho de 2021. Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Brasília: CNJ, 2021c.

BRASIL. Conselho Nacional de Justiça. **Portaria nº 172**, de 25 de maio de 2022. Institui o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ). Brasília: CNJ, 2021d.

BRASIL. **Decreto nº 3.505**, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Brasília: Presidência da República, 2000. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm. Acesso em: 25 de junho de 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional da Presidência da República. **Portaria nº 34**, de 5 de agosto de 2009**.** Institui Grupo de Trabalho de Segurança das Infraestruturas Criticas da Informação, no âmbito do Comitê Gestor de Segurança da Informação - CGSI. Brasília: GSI/PR, 2009a.

BRASIL. Presidência da República. Gabinete de Segurança Institucional da Presidência da República. **Portaria nº 45**, de 8 de setembro de 2009**.** Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e da outras providências. Brasília: GSI/PR, 2009b.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Livro verde**: segurança cibernética no Brasil. Organização: Cláudia Canongia e Raphael Mandarino Junior. Brasília: GSIPR/SE/DSIC, 2010. Disponível em: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2015/10/Livro_Verde_SEG_CIBER.pdf. Acesso em: 1º jul. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018**. Disponível em: https://www.gov.br/gsi/pt-br/arquivos/4_estrategia_de_sic.pdf. Acesso em: 20 jul. 2024.

BRASIL. **Decreto nº 9.637**, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm. Acesso em: 19 jul. 2024.

BRASIL. **Estratégia Nacional de Segurança Cibernética**. Brasília: GSI/PR, 2020. Disponível em: https://www.gov.br/gsi/pt-br/ssic/estrategia-nacional-de-seguranca-cibernetica-e-ciber/e-ciber.pdf. Acesso em: 11 jul. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional da Presidência da República. **Portaria nº 93**, de 18 de outubro de 2021. Brasília: GSI/PR, 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370. Acesso em: 15 jul. 2024.

BUZAN, B.; WÆVER; WILDE, J. **Security**: A new framework for analysis. Boulder: Lynne Reinner, 1998.

CANONGIA, C.; MANDARINO JUNIOR, R. Segurança cibernética: o desafio da nova Sociedade da Informação. **Parcerias Estratégicas**, v. 14, n. 29, pp. 21–46, 2009.

CEPIK, M.; CANABARRO, D. R.; BORNE, T. A securitização do ciberespaço e o terrorismo: uma abordagem crítica. In: SOUZA, A. M.; NASSER, R.M.; MORAES, R. F. (eds.). **Do 11 de setembro de 2001 à guerra ao terror**: reflexões sobre o terrorismo no século XXI. Brasília: Instituto de Pesquisa Econômica Aplicada, 2014, pp. 161-186. Disponível em: https://repositorio.ipea.gov.br/handle/11058/3007. Acesso em: 25 jul. 2024.

COSTA, R. L. A Gestão da Informação em Equipes Virtuais no Poder Judiciário: desafios para uma comunicação eficiente e segura. **Revista de Política Judiciária, Gestão e Administração da Justiça**, v. 7, n. 2, p. 76–96, 2021.

DA CRUZ JÚNIOR, S. C. Texto para Discussão 1850 — A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual. Brasília: Instituto de Pesquisa Econômica Aplicada, 2013. Disponível em: https://hdl.handle.net/10419/91261. Acesso em: 28 jun. 2024.

FALLETI, T. Social Origins of Institutional Strength: Prior Consultation over Extraction of Hydrocarbons in Bolivia. In: BRINKS, D. M.; LEVITSKY, S.; MURILLO, M. V. **The Politics of Institutional Weakness in Latin America**. Cambridge; Nova Iorque: Cambridge University Press, 2020, pp. 253–276.

GRUMAN, M. Lei de Acesso à Informação: notas e um breve exemplo. **Revista Debates**, v. 6, n. 3, p. 97, 4 dez. 2012.

HINO, M. C.; CUNHA, M. A. Adoção de tecnologias na perspectiva de profissionais de direito. Revista Direito GV, v. 16, n. 1, e1952, 2020. DOI: 10.1590/2317-6172201952.

HUREL, L. M.; LOBATO, L. C. **Uma Estratégia para a Governança da Segurança Cibernética no Brasil**: Nota Estratégica. Rio de Janeiro: Instituto Igarapé, 2018. Disponível em: https://igarape.org.br/wp-content/uploads/2018/09/Uma-estrate%CC%81gia-para-a-governanc%CC%A7a-da-seguranc%CC%A7a-ciberne%CC%81tica-no-Brasil.pdf. Acesso em: 13 jul. 2024.

HUREL, L. M. **Cibersegurança no Brasil: uma análise da estratégia nacional**: Artigos Estratégicos, 54. Rio de Janeiro: Instituto Igarapé, 2021. Disponível em: https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf. Acesso em: 2 ago. 2024.

KRIPPENDORFF, K. **Content analysis**: an introduction to its methodology. Londres: Sage, 2004.

MACHADO, M. B. **Taxonomia de eventos de risco operacional do poder judiciário**. Trabalho de Conclusão de Curso (Especialização em Gestão Pública —Brasília: Escola Nacional de Administração Pública, mar. 2018. Disponível em: https://repositorio.enap.gov.br/handle/1/3399. Acesso em: 1º ago. 2024.

MELLO. C. A. B. **Curso de Direito Administrativo**. 35 ed. São Paulo: Malheiros; Juspodivm, 2021.

NÓBREGA, F. F. B.; TEIXEIRA, A. C. S. Compreendendo a Fragilidade Institucional: o poder e o desenho institucional nas instituições latino-americanas. **REI - Revista Estudos Institucionais**, v. 9, n. 1, pp. 95–109, 23 maio 2023.

NORTH, D. C. Institutions. **The Journal of Economic Perspectives**, v. 5, n. 1, p. 97–112, 1991.

O'DONNELL, G. Accountability horizontal e novas poliarquias. **Lua Nova**: Revista de Cultura e Política, n. 44, p. 27–54, 1998.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. Guidelines for the Security of Information Systems and Networks: Towards a culture of security. Paris: OCDE, 2002. DOI: **10.1787/9789264059177-en-fr**.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Policies for the protection of critical information infrastructure: Ten years later.** OECD Digital Economy Papers, n. 275. Paris: OCDE, 2019. DOI: 10.1787/efb55c54-en.

ROSENEAU, J. N.; CZEMPIEL, E.-O. Governance without Government: Order and Change in World Politics. Cambridge: Cambridge University Press. 1992

SAMPAIO, R. C.; LYCARIÃO, D. **Análise de Conteúdo Categorial: Manual de Aplicação**. Brasília: Escola Nacional de Administração Pública, 2021.

SILVA, C. C. V. E.; PEREIRA, A. E. A Teoria de Securitização e a sua aplicação em artigos publicados em periódicos científicos. **Revista de Sociologia e Política**, v. 27, n. 69, p. e007, 2019.

STOLZ, M.; AXON, L. **Revisão das capacidades de segurança cibernética do Brasil**. Oxford: Centro Global de Capacidade de Segurança Cibernética, 2023. Disponível em: <https://www.gov.br/gsi/pt-br/ssic/estrategia-nacional-de-seguranca-cibernetica-e-ciber/cmm-report-brazil-2023_final_pt.pdf>. Acesso em: 16 jun. 2024.

TRIBUNAL DE JUSTIÇA DE PERNAMBUCO. **Despesas e Dados Orçamentários - Res CNJ 76/2009**. Disponível em: https://portal.tjpe.jus.br/web/transparencia/despesas-e-dados-orcamentarios-resolucao-76/2009. Acesso em: 3 set. 2024.

TRIBUNAL REGIONAL FEDERAL DA 5ª REGIÃO. **Demonstrativo de Execução Orçamentária da Justiça Federal - 2023**. Recife: TRF5, 2024. Disponível em: https://www.trf5.jus.br/index.php/gestao-orcamentaria/resultado-pdf#conteudo. Acesso em: 2 set. 2024.

UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES. Recomendação X.1205. Series X: Data Networks, Open System Communications and Security — Telecommunication Security — Overview of cybersecurity. Genebra: UIT, 2008. Disponível em: http://www.itu.int/rec/T-REC-X.1205-200804-I. Acesso em: 1º jul. 2024.

UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES. ITU-D. **Question 22/1**: Securing information and communication networks: best practices for a developing country. Genebra: UIT, 2010. Disponível em: http://www.itu.int/publ/D-STG-SG01.22-2010/en. Acesso em: 22 jul. 2024.

UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES. **ITU-T approved security definitions**. Genebra: UIT, [s.d.] Disponível em: http://www.itu.int/dms_pub/itut/oth/0A/0D/T0A0D00000A0003ZIPE.zip. Acesso em: 1º jul. 2024.

UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES. **Global Cybersecurity Index 2020**. Genebra: UIT, 2020. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf. Acesso em: 10 jul. 2024.

VIGANÒ, E.; LOI, M.; YAGHMAEI, E. Cybersecurity of critical infrastructure. In: CHRISTEN, M.; GORDIJN, B.; LOI, M. **The Ethics of Cybersecurity**. Dublin: Springer, 2020. p. 157-177, 2020. DOI: 10.1007/978-3-030-29053-5.