Proposta de Metodologia para Avaliação de Riscos de Privacidade para Órgãos do Poder Judiciário no Brasil

Inovações, inteligência artificial e tecnologias de informação e comunicação em sistemas de justiça

Carlos Eduardo Miranda Zottmann (Tribunal Superior Eleitoral - TSE)
Marcus Aurélio Carvalho Georg (Superior Tribunal de Justiça - STJ)
Renato Solimar Alves (Conselho da Justiça Federal - CJF)
Marcelo Antonio da Silva (Supremo Tribunal Federal - STF)
Rafael Rabelo Nunes (Universidade de Brasília – UnB)

RESUMO

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, dispõe sobre o tratamento de dados pessoais, e deve ser observada por todos os órgãos públicos. A adequação do Poder Judiciário à LGPD é regida pela Resolução CNJ nº 363/2021, que, entretanto, carece de orientações práticas que facilitem sua implementação. Em paralelo, o Poder Executivo pelo Ministério da Economia publicou um Guia de Boas Práticas que, entre outras recomendações, lista 14 riscos de privacidade de dados pessoais. Ao mesmo tempo, o Conselho Nacional de Justiça (CNJ) prescreveu controles mínimos de segurança cibernética que devem ser implementados pelos órgãos do poder judiciário, por meio da Resolução 396/2021, sem detalhar como esses controles mitigam riscos de privacidade. Este trabalho teve como objetivo elaborar uma metodologia de avaliação de riscos de privacidade para órgãos do poder judiciário baseando-se nos 14 riscos elencados pelo Ministério da Economia com base na norma ISO 29.134, em combinação com os controles de segurança cibernética recomendados pelo CNJ. Para isso, foram realizadas consultas a grupos de especialistas em segurança cibernética a respeito de seu entendimento sobre os riscos de privacidade e dos respectivos controles de segurança aplicáveis. A partir dos dados levantados foi construída uma matriz que relaciona riscos e controles para subsidiar o processo de avaliação de riscos de privacidade, e por conseguinte, a produção de Relatórios de Impacto de Privacidade de Dados alinhados com os controles prescritos pelo CNJ. Esse trabalho pode contribuir unindo esforços de programas de privacidade e de programas de segurança cibernética.

Palavras-Chave: Riscos; Proteção de dados pessoais; Judiciário; Tomada de Decisão

1. Introdução

A internet e as tecnologias de informação vêm impulsionando inovações e melhorias nos serviços sociais. Muitos dos benefícios decorrentes são proporcionados por dados sobre indivíduos, tratados por diversos sistemas produtos e serviços, cuja quantidade e complexidade dificulta que esses indivíduos compreendam adequadamente os impactos sobre sua privacidade (NIST, 2020).

Conforme afirma Lima (2016), a facilidade de comunicação e interação por meio das redes sociais revela um aspecto preocupante: a violação da privacidade, direito fundamental que merece essencial proteção. Com efeito, frequentemente tomamos conhecimento de notícias a respeito do vazamento de dados pessoais, como o caso de 2021 envolvendo a rede social profissional "Linkedin" onde houve o vazamento de dados pessoais de 700 milhões de usuários, que, inclusive, passaram a ser comercializados na *Dark Web* (Marks, 2021). Em outro exemplo, em nível nacional, tivemos o vazamento de mais de 200 milhões de CPFs e dados pessoais a eles associados (Grupo Globo, 2021).

A criticidade desse cenário tem feito surgir uma série de novos instrumentos normativos que determinam as condições que o tratamento de dados pessoais deve observar, tais como a Lei Geral de Proteção de Dados Pessoais (LGPD), no caso brasileiro, na tentativa de garantir a segurança nesse tratamento e, em última instância, a privacidade dos titulares dos dados pessoais.

Entretanto, como se trata de um assunto que tem ganhado espaço e atenção apenas recentemente, muitas vezes os titulares de dados podem não entender os riscos envolvidos nesse tratamento e seus potenciais consequências. Infelizmente, em muitos casos nem mesmo as próprias organizações responsáveis pelo tratamento de dados pessoais possuem a correta compreensão sobre esses riscos (NIST, 2020).

A gestão de riscos, entretanto, é uma questão que já vem sendo estudada, e deve ser utilizada pelas organizações para auxiliar nessa compreensão. A norma ABNT NBR ISO 31.000, por exemplo, traz definições sobre os princípios, a estrutura e o processo de gestão de riscos, apresentando como principais etapas as atividades de identificação, análise e avaliação de riscos, sendo esta última a responsável por auxiliar na tomada de decisão sobre a necessidade de tratamento dos riscos identificados (ABNT, 2018).

Buscando auxiliar os órgãos públicos na execução dessa tarefa, o Ministério da Economia (2020) produziu um Guia de Avaliação de Riscos de Segurança e Privacidade, com intuito de servir como documento de orientação sobre identificação de riscos de privacidade em sistemas, contratos e processos de trabalho. O documento baseia-se em 14 riscos de privacidade descritos no Guia de Boas Práticas da Lei Geral de Proteção de Dados (LGPD), desenvolvido pelo Comitê Central de Governança de Dados (CCGD, 2020). Adicionalmente, sugere 113 controles de segurança aplicáveis ao contexto de privacidade, agrupados em três dimensões, a saber: Estrutura, Sistema e Privacidade. Importante mencionar que há alguma sobreposição desses controles com os prescritos pelo Conselho Nacional de Justiça (CNJ) para serem aplicados pelos órgãos do Poder Judiciário, por meio da Portaria nº 162/2021 (CNJ, 2021c), que compõe a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) instituída por meio da Resolução CNJ nº 396/2021 (CNJ, 2021b). A aplicação dos controles de segurança da informação do CNJ também contribui para a mitigação de riscos de privacidade.

Faz-se importante destacar que o CNJ tem como atribuição “o controle da atuação administrativa e financeira do Poder Judiciário”, conforme definido na Emenda Constitucional nº 45/2004 (não tendo competência, entretanto, sobre o Supremo Tribunal Federal). Dessa forma, suas resoluções devem ser observadas por esses órgãos.

Assim, embora o Guia de Avaliação de Riscos de Segurança e Privacidade tenha aplicabilidade para os órgãos públicos membros do Poder Executivo Federal, convém que seja adaptado para o Poder Judiciário a partir de suas resoluções e portarias, notadamente aquelas que tratem sobre privacidade de dados e segurança da informação.

Atualmente no âmbito do Poder Judiciário da União não existe instrumento normativo ou documento técnico que traga recomendações sobre o processo de gestão de riscos de privacidade, tampouco sobre como avaliá-los, de forma que se alinhem com a Portaria nº 162/2021 do CNJ. O judiciário conta apenas com a Resolução nº 363/2021 do CNJ que estabelece medidas para o processo de adequação à LGPD a serem adotadas, mas o tema gestão de riscos de privacidade não é tratado no normativo (CNJ, 2021a). Entretanto, de acordo com a norma ISO 27.701, a organização deve aplicar o processo de avaliação de riscos de segurança da informação para identificar os riscos associados à perda de confidencialidade, integridade e disponibilidade, e os riscos de privacidade relativos ao tratamento de dados pessoais (ABNT, 2019).

Mediante essa realidade, se baseando no Guia de avaliação de riscos do Ministério da Economia e nos normativos do judiciário que compõem a ENSEC-PJ, o presente trabalho teve como objetivo elaborar uma metodologia de avaliação de riscos de privacidade para órgãos do poder judiciário se baseando nos 14 riscos de tratamento de dados pessoais elencados pelo guia de boas práticas da LGPD, juntamente com a identificação da implementação dos controles de segurança cibernética descritos na Portaria nº 162/2021 do CNJ.

Muito embora o trabalho tenha como objetivo específico propor uma metodologia aplicável aos órgãos do Poder Judiciário, seus resultados podem ser aplicados por qualquer instituição, na medida em que tanto o Guia de Avaliação de Riscos de Segurança e Privacidade publicado pelo Ministério da Economia quanto a Portaria CNJ 162/2021 são baseados em *frameworks* destinados a instituições de qualquer

ramo de atuação, aceitos como boas práticas pelo mercado, além de demonstrar as sobreposições que existem na gestão da segurança da informação e da gestão da privacidade de dados.

2. Referencial teórico

O direito à privacidade é definido pela Enciclopédia Jurídica da USP como "(...) uma forma de impedir que o avanço tecnológico, juntamente com o já conhecido crescimento populacional, com uma consequente ocupação territorial, pudesse violar o direito de cada um de estar com si próprio sem interferência alheia" (Hirata, 2017). Complementando o tema, a LGPD define que dados pessoais são aqueles que têm o condão de nos identificar perante terceiros, e dados pessoais sensíveis são aqueles que podem ensejar tratamentos discriminatórios.

Ainda de acordo com a LGPD, as instituições que tenham como parte da sua missão, ou que decidam realizar o tratamento de dados pessoais ou dados pessoais sensíveis, têm a importante responsabilidade de realizá-lo de forma a minimizar o risco de seu acesso indevido, por terceiros não autorizados. Tal obrigação está prevista em seu Art. 6º, inciso VII, que traz como um dos princípios a serem ser observados no tratamento de dados a segurança, definida como "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão" (Brasil, 2018).

Da obrigatoriedade da observação da segurança nas atividades de tratamento de dados pessoais deriva a importância da avaliação de riscos associados a esse tratamento. Com efeito, a ISO 27701 recomenda que os riscos de tratamento de dados pessoais sejam analisados por meio de uma avaliação de impacto de privacidade, o que inclui a determinação dos elementos que são necessários para a avaliação de impacto e privacidade completa (ABNT, 2020).

De forma a contribuir com essa tarefa e oferecer aos órgãos de governo um embasamento e um modelo inicial de boas práticas, o Ministério da Economia, por meio da Secretaria de Governo Digital, vem elaborando importantes documentos de referência, dentre os quais destacam-se, para os objetivos deste trabalho, o Guia de Boas Práticas da Lei Geral de Proteção de Dados (CCGD, 2020) e o Guia de Avaliação de Riscos de Segurança e Privacidade (Ministério da Economia, 2020).

O primeiro documento, de escopo mais amplo, tem como objetivo "fornecer orientações de boas práticas aos órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional para as operações de tratamento de dados pessoais, conforme previsto no art. 50 da LGPD", e traz, em seu item 2.5.2.6 – Identificar e avaliar os riscos, uma proposta inicial de 14 riscos referentes ao tratamento de dados pessoais (Ministério da Economia, 2020).

Já o segundo documento, de caráter mais específico, tem como objetivo "fornecer aos responsáveis pelo tratamento de dados pessoais no órgão ou entidade uma orientação para identificar lacunas de segurança da informação e de privacidade sobre os sistemas, contratos e processos da instituição" (Ministério da Economia, 2020).

Esses documentos, em conjunto, representam uma iniciativa bem consolidada no sentido de fornecer aos gestores públicos ferramentas para a identificação de riscos relacionados ao tratamento de dados pessoais.

Paralelamente, em outra dimensão, o serviço público vem também empreendendo esforços no sentido de fortalecer sua postura quanto à segurança cibernética, e nesse sentido, o Conselho Nacional de Justiça (CNJ) estabeleceu, para o Poder Judiciário, por meio da Resolução nº 396/2021, a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Em complementação à estratégia definida, o CNJ

publicou a Portaria nº 162/2021, contendo os Protocolos e Manuais criados pela resolução. Dentre eles, é de especial interesse para o objetivo deste trabalho o Protocolo de Proteção de Infraestruturas Críticas de TIC, que traz uma relação de Controles Críticos Recomendados, adaptados a partir do *framework* CIS-Controls versão 7.1, levando em consideração a realidade dos órgãos do Poder Judiciário e as capacidades de suas equipes de TI.

Além do método de gestão de riscos e controles de segurança para privacidade descritos, que congregam iniciativas já adotadas por órgãos públicos nacionais, é importante mencionar outros métodos que são relevantes para este trabalho.

2.1 NIST Privacy Framework

O NIST Privacy Framework, é uma "ferramenta para incrementar a Privacidade por meio da Gestão de Riscos Corporativa, de forma a viabilizar práticas que suportem os conceitos de "privacy by design" e auxiliar as organizações a protegerem a privacidade dos indivíduos" (NIST, 2020).

Ainda segundo o mesmo documento, o *framework* se subdivide em cinco funções principais: Identify-P, Govern-P, Control-P, Communicate-P e Protect-P (em tradução livre, Identificar, Governar, Controlar, Comunicar e Proteger, sendo que o sufixo "-P" se refere a privacidade).

A função "Protect-P" (Proteger a Privacidade) se destina à gestão de riscos associados a eventos de cibersegurança relacionados à privacidade. Um segundo *framework* também elaborado pelo NIST, o Cybersecurity Framework (NIST CSF), destinado especificamente à gestão de riscos de cibersegurança, e, por sua vez, apoiado na Publicação Especial NIST 800-53 (Controles de Segurança e Privacidade para Sistemas de Informação e Organizações) pode ser utilizado para a implementação dessa função.

2.2. CIS Privacy Companion Guide (Guia Complementar de Privacidade)

O Center for Internet Security (CIS) publicou o CIS Privacy Companion Guide, já traduzido para o português (CIS, 2022), que destaca os controles do CIS Controls se aplicam ao tema, inclusive com a motivação associada a cada um.

Como formas de acompanhamento da aplicação do CIS Controls podemos citar o CIS RAM (Risk Assessment Method) e as planilhas desenvolvidas pela Enclave Security (essas últimas sugeridas pela Secretaria de Governo Digital como ferramenta a ser utilizada pelos órgãos do poder executivo).

A utilização conjunta dessas publicações e ferramentas pode também guiar uma instituição na tarefa de identificação e aplicação de controles de segurança aplicáveis à privacidade.

2.3. ISO 27.701

A norma NBR ISO/IEC 27.701 é uma norma internacional publicada pela International Organization for Standardization (ISO), traduzida para o português pela Associação Brasileira de Normas Técnicas (ABNT) cujo objetivo é definir requisitos e diretrizes para a gestão de privacidade da informação. É uma extensão das normas que tratam especificamente sobre segurança da informação (ISO 27.001 e 27.002).

A ISO 27.701 basicamente revisita cada um dos requisitos de segurança especificados na ISO 27.001, bem como as diretrizes para a implementação de controles contidos na ISO 27.002, e os complementa com os requisitos e diretrizes para a implementação referentes à questão da privacidade, apresentando como anexos referências específicas de controles e objetivos de controle para Controladores de Dados Pessoais e Operadores de Dados Pessoais,

respectivamente. Outro anexo relevante da norma é o que traz um mapeamento entre sua estrutura e os artigos da LGPD.

Faz-se importante destacar que o conjunto de controles recomendados pela ISO 27.701 difere do conjunto de controles propostos pelo Guia de Avaliação de Riscos de Segurança e Privacidade publicado pelo Ministério da Economia, muito embora ambos façam referência a normativos da família ISO 27.000. Enquanto a ISO 27.701 contemple um mapeamento entre os controles que recomenda e a norma ISO 29.100 (que fornece uma estrutura de privacidade, especificando os atores e seus papéis no tratamento de dados pessoais, e descreve considerações e salvaguarda de privacidade), o Guia foi estruturado a partir dos riscos de privacidade definidos na norma ISO 29.134 (que define diretrizes para a avaliação de impacto de privacidade).

Resumidamente, o mapeamento apresentado na ISO 27.701 entre sua estrutura e os controles preconizados pela ISO 29.100 apresenta quatro controles (e subcontroles) voltados a Controladores de Dados Pessoais, e mais quatro controles (e subcontroles) voltados a Operadores de Dados Pessoais, enquanto o Guia é estruturado com base em 12 riscos de privacidade obtidos da ISO 29.134 complementados por mais 2 riscos identificados como importantes pelo Ministério.

Dessa diferença de embasamento decorre o fato de que nem todos os controles recomendados pela ISO 27.701 estão presentes, ao menos explicitamente, no Guia publicado pelo Ministério da Economia, a exemplo daqueles relacionados a transferências internacionais, descarte de dados pessoais, dentre outros.

2.4. Trabalhos relacionados

Além dos métodos já descritos até aqui, há ainda trabalhos acadêmicos publicados, relacionados a metodologias que envolvem uma perspectiva de análise da privacidade. Tais trabalhos são elencados e resumidos a seguir.

Em 2016 foi descrita uma metodologia de análise de riscos de privacidade chamada PRIAM (Privacy Risk Analysis Methodology), que possui uma fase de coleta de informações, na qual é realizado o levantamento de todos os fatores que têm impacto nos riscos de privacidade, além de uma fase da efetiva avaliação dos riscos. A metodologia é aplicável a sistemas de informação, que devem ser descritos em relação a sua especificação funcional (e.g. interfaces, fluxos de dados, ativos, atores, etc). Também devem ser definidos os dados pessoais existentes no sistema, as fontes de riscos envolvidos, as fraquezas que tangem a privacidade, entre outros. Posteriormente é elaborada uma árvore de dados composta por esses itens, e avaliado o risco associado a cada item a partir de uma métrica com parâmetros pré-definidos (Joyee De & Le Métayer, 2016).

Já o ciclo de vida do desenvolvimento de software também deve ser objeto de análise dos riscos de privacidade. Nesse contexto o LINDDUN é um *framework* que propõe uma abordagem sistemática para modelar ameaças de privacidade, realizando o levantamento dos requisitos de privacidade para o software que será desenvolvido, devendo ser embutido dentro da metodologia de desenvolvimento da organização. O *framework* define que o software deve ser modelado via Diagramas de Fluxo de Dados (DFD's), a partir dos quais serão identificadas as ameaças de privacidade, que serão gerenciadas durante o processo de desenvolvimento. O acrônimo LINDDUN se refere a 7 tipos de ameaças de privacidade comumente encontradas em sistemas, dentre elas a capacidade de ligação (i.e. Linkability), descrita como a possibilidade de relacionamento de ações, identidades ou partes de informação que não deveria ser viável por questões de privacidade. Uma versão simplificada do *framework*, denominada LINDDUN GO, foi publicada em 2020 (Wuyts et. Al, 2020).

Muito embora o tema privacidade esteja ganhando maior atenção recentemente, a questão de avaliação de riscos associada a ambientes de tecnologia da informação vem sendo estudada e implementada há bastante tempo. Com efeito, Peotta de Melo

(2008), propunha a implementação de funções de gestão de risco referentes a vulnerabilidades associadas a ativos de tecnologia da informação, apresentando um score de risco para cada ativo, possibilitando assim a priorização de ações de correção com base na criticidade do ativo.

Já Lohmann et. al (2020), realizaram uma revisão sistemática da literatura com o intuito de contribuir para as discussões a respeito das melhores práticas na elaboração de Relatórios de Impacto sobre Proteção de Dados (RIPD), a partir das experiências relacionadas à elaboração dos relatórios de Privacy Impact Assessment (PIA) e Data Protection Impact Assessment (DPIA), no contexto da GDPR, concluindo que dentre os principais benefícios da elaboração desse tipo de relatório são a "construção da confiança, da cultura de privacidade e da conformidade com as legislações de privacidade".

O RIPD é definido no Art. 5º da LGPD, tem como intuito garantir que os direitos dos titulares dos dados processados pela organização estejam sendo realmente cumpridos (Lohman et. al, 2020), e pode ser solicitado a qualquer momento pela Agência Nacional de Proteção de Dados (ANPD) para a avaliação das atividades de tratamento de dados pessoais (ANPD, 2023). Deve contemplar a descrição dos processos de tratamento de dados pessoais para os quais há riscos de privacidade associados e descrever os mecanismos de mitigação de risco adotados (Lei 13.719, 2018).

Ainda em relação ao RIPD, Miranda (2021) realiza um comparativo entre a previsão legal do relatório de impacto na Lei Geral de Proteção de Dados (LGPD) e no Regulamento Geral de Proteção de Dados (GDPR), indicando que o tema é tratado com maiores detalhes na GDPR, que se incumbe inclusive de determinar os melhores momentos em um projeto de tratamento de dados pessoais para elaborá-lo e de definir as operações de tratamento que indicam alto risco.

Vale de Castro (2021), por sua vez, propõe um *framework* baseado na metodologia BEST (Business Engaged Security Transformation) para apoiar o desafio da adequação de empresas aos requisitos exigidos pela LGPD. O *framework* é composto por quatro programas (1 - Sistema de Gestão de Cibersegurança e Segurança da Informação - SGCSI, 2 - Proteção da Informação, 3 - Aprimoramento da privacidade e Atitudes Seguras). Os programas 2 e 3 chegam a mencionar ações de segurança que podem ser aplicadas para garantir a privacidade de dados, entretanto não alcançam o nível de detalhamento existente na metodologia proposta pelo presente trabalho, uma vez que não se debruçam sobre controles específicos que devam ser implementados.

Por fim, Santos (2022), traz uma contribuição para o tema por meio da definição de um conjunto de recomendações que apoie a implementação do conceito "*Privacy by design*" no processo de desenvolvimento de software, com o objetivo de garantir que sistemas e aplicações a serem desenvolvido por uma dada organização seja aderente às exigências contidas na LGPD.

3. Metodologia utilizada para a realização do trabalho

Segundo Gil (2019), pesquisa aplicada é aquela que "decorre do desejo de conhecer com vistas a fazer algo de maneira mais eficiente ou eficaz". Assim, o trabalho tem a natureza de pesquisa aplicada, uma vez que tem como objetivo propor uma metodologia que possa ser diretamente aplicada pelos órgãos do Poder Judiciário para a definição de controles de segurança aplicáveis a projetos de sistemas e aplicações que façam o tratamento de dados pessoais.

Ainda segundo o mesmo autor, pesquisas podem ter objetivos exploratórios, descritivos ou explicativos. Uma pesquisa descritiva "tem por objetivo primordial a descrição das características de determinada população ou fenômeno ou, então, o estabelecimento de relações entre variáveis". O trabalho, portanto, tem natureza

descritiva, uma vez que pretende propor um método de seleção de controles de segurança a partir da combinação de dois outros métodos já definidos, e realiza a análise dos dados de forma qualitativa, uma vez que há uma certa dose de subjetividade no tocante à atribuição quanto à natureza e peso dos controles.

A elaboração da metodologia passou, primeiramente, por uma pesquisa documental de forma a selecionar os *frameworks* que poderiam ser utilizados para suportar as decisões; em seguida, passou-se para a elaboração da metodologia propriamente dita que observou as etapas necessárias para se realizar uma avaliação de riscos, prescritos na norma ABNT ISO 31.000:2018, com destaque para as etapas de identificação, análise e avaliação de riscos. A seção seguinte detalha cada uma dessas etapas.

4. Elaboração da metodologia para avaliação de riscos de privacidade, e seus Resultados:

Neste tópico descreveremos as etapas realizadas para a elaboração da metodologia, apresentando exemplos de sua aplicação.

4.1. Seleção dos *frameworks* a serem utilizados para embasar a elaboração da metodologia

A partir do objetivo definido para o trabalho, selecionou-se as boas práticas relacionadas ao tema de Privacidade e Proteção de Dados Pessoais. Dentre o rol de normativos nacionais publicados pela Associação Brasileira de Normas Técnicas (ABNT), identificou-se a norma ABNT NBR ISO 29134:2017, que traz diretrizes para a avaliação de impacto de privacidade, bem como uma relação de riscos de privacidade que devem ser tratados.

Estendendo o olhar para eventuais recomendações relativas a privacidade e proteção de dados pessoais publicadas por órgãos dos demais poderes do estado brasileiro,

identificamos o Guia de Boas Práticas sobre a LGPD (Comitê Central de Governança de Dados, 2020) e o Guia de Avaliação de Riscos de Segurança e Privacidade (Ministério da Economia, 2020), destinados aos órgãos do Poder Executivo, com intuito de servir como orientação sobre avaliação de riscos de privacidade em sistemas, contratos e processos de trabalho.

O primeiro Guia tem como objetivo fornecer orientações de boas práticas para as operações de tratamento de dados pessoais, trazendo a recomendação de identificação, análise e avaliação de riscos de privacidade, e a consequente identificação de medidas para o tratamento dos riscos identificados.

Em complementação a esse primeiro documento, o Guia de Avaliação de Riscos de Segurança e Privacidade adota a norma ABNT NBR ISO 29134:2017 como fonte de identificação de riscos de privacidade, construindo, a partir dos 14 riscos por ela relacionados, uma relação adaptada para subsidiar as tarefas de gestão de riscos aqui citadas.

Adicionalmente, a partir da experiência de análise de segurança de sistemas críticos, efetuada no âmbito da Secretaria de Governo Digital, traz uma extensa relação de controles destinados a elevar a segurança da informação no desenvolvimento de sistemas diante dos pilares de confidencialidade, integridade, disponibilidade e autenticidade, já adaptados às exigências relativas aos critérios de privacidade.

Uma análise detida do Guia evidencia que tais controles são oriundos das recomendações de segurança emanadas pelo Gabinete de Segurança Institucional da Presidência da República, em especial por suas Normas Complementares, a partir das principais normas ABNT relacionadas ao tema, tais como a 27002:2013, 27701:2019, 27005:2019, 29151:2017, 29134:2017, e ainda a partir de referências técnicas publicadas pela OWASP.

Por fim, o Guia completa o método com procedimentos para associação dos controles de segurança aos riscos de privacidade, para a definição da probabilidade e impacto da ocorrência desses riscos, e, por fim, para a definição do nível de risco associado ao objeto sob avaliação.

Entretanto, observando-se os conjuntos de boas práticas que embasaram a elaboração do Guia de Avaliação de Riscos de Segurança e Privacidade, verifica-se que não são coincidentes com os conjuntos de boas práticas que subsidiaram a elaboração da Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), em especial no tocante aos controles de segurança contidos na Portaria CNJ 162/2021. Em especial, o manual de controles de segurança para infraestruturas críticas baseia-se no *framework* CIS Controls versão 7.1.

4.2. Elaboração da metodologia para Avaliação de Riscos de Privacidade

A metodologia elaborada tem como propósito avaliar e permitir a priorização de ações para mitigar os riscos relacionados à privacidade das informações coletadas e tratadas pelos tribunais, garantindo assim a conformidade com as leis e regulamentações aplicáveis, além de promover a transparência e a confiança dos cidadãos em relação ao tratamento dos seus dados pessoais, mesclando as recomendações constantes do Guia de Avaliação de Riscos de Segurança e Privacidade publicado pelo Poder Executivo com as diretrizes dos controles de segurança cibernética descritos na Portaria nº 162/2021 do CNJ.

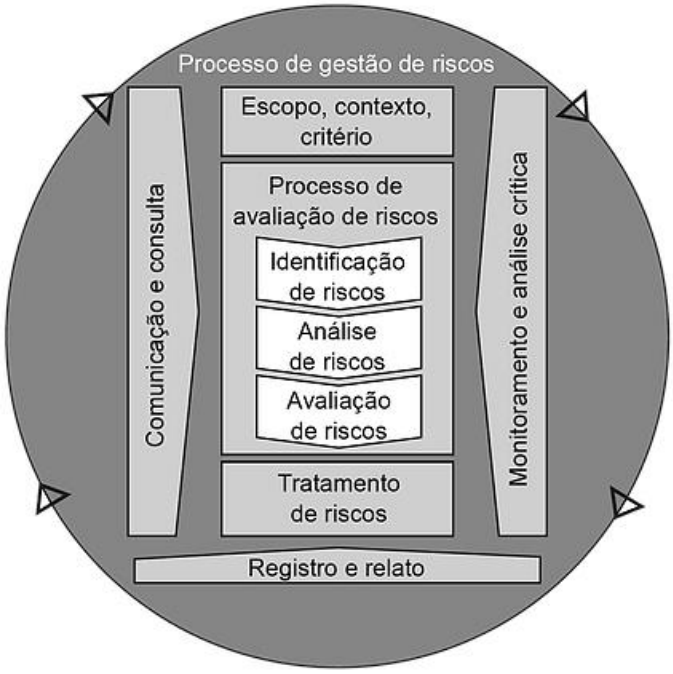
Assim, contribui para que os tribunais possam avaliar os riscos de privacidade em consonância com os riscos de segurança da informação, adotando uma linguagem compatível com o método mais comumente adotado para a gestão de riscos corporativos, baseado na norma ISO 31.000 (ABNT, 2019), o que facilita o processo de avaliação e tomada de decisão, de forma a auxiliar as atividades para o cumprimento desse direito fundamental dos cidadãos.

4.2.1. O processo de Gestão de Riscos de Privacidade

Tomando-se como base a norma ISO 31.000, tem-se que o processo de Gestão de Riscos é composto das atividades de "comunicação e consulta, estabelecimento do contexto e avaliação, tratamento, monitoramento, análise crítica, registro e relato de riscos", Figura 1.

Figura 1

Processo de Gestão de Riscos



Fonte: (ABNT, 2018)

A presente metodologia cobre o processo de avaliação de riscos, incluindo as etapas de identificação, análise e avaliação dos riscos.

a) Identificação de Riscos

A primeira etapa da Avaliação de Riscos preconizada pela ISO 31.000 é a Identificação de Riscos, que consiste em identificar possíveis ameaças e

vulnerabilidades que possam comprometer a privacidade dos dados pessoais tratados pela organização. Como o escopo de avaliação de riscos já é definido, tem-se que a relação dos riscos pertinentes é a definida pelo Guia de Avaliação de Riscos de Segurança e Privacidade, prescritos pelo Ministério da Economia, por sua vez baseado nos riscos elencados pela ISO/IEC 29.134:2017, Tabela 1 (Brasil, 2020).

Tabela 1
Riscos à privacidade de dados

Risco		**Descrição**
1	Acesso não autorizado	Acesso indevido (permissões indevidas) a um ambiente físico ou lógico.
2	Coleção excessiva	Coleta de dados pessoais em quantidade superior ao mínimo necessário à finalidade do tratamento ou atividade que fará uso do dado pessoal.
3	Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais	Instituição não atende sua finalidade legal e compartilha os dados sem consentimento do titular dos dados pessoais (LGPD, art. 27).
4	Falha em considerar os direitos do titular dos dados pessoais	Garantia de atendimento dos direitos do titular, conforme descrito nos artigos 17 a 23 da LGPD.
5	Falha ou erro de processamento	Dados de entrada que não são corretamente validados, operações de tratamento automatizadas de sistema que alteram de maneira indevida a composição do dado armazenado
6	Informação insuficiente sobre a finalidade do tratamento	O tratamento de dados pessoais realizado de forma eletrônica ou documento em papel deve atender a uma finalidade e ser exposto de forma transparente e clara ao detentor dos dados pessoais.
7	Modificação não autorizada	Usuário sem permissões de alteração para um determinado dado pessoal ou registro realiza a modificação não autorizada. Um processamento indevido pode gerar uma modificação não autorizada.
8	Perda	Perdas provocadas por ações intencionais de usuários oriundas de uma exclusão indevida ou devida e não comunicada, e provenientes de ações não intencionais como falhas em sistemas,

		sobrescrita de dados, falhas em hardware, entre outras.
9	Reidentificação de dados pseudonimizados	Dados pessoais podem ser reidentificados por cruzamento simples de dados pessoais (LGPD, art. 12 e 13).
10	Remoção não autorizada	Usuário não tem a permissão para retirar ou copiar dados pessoais para outro local.
11	Retenção prolongada de dados pessoais sem necessidade	O término da prestação de um serviço ou do prazo da retenção dos dados pessoais para fins legais deve culminar com a exclusão e/ou descarte seguro(a) dos dados pessoais.
12	Roubo	Dados roubados nas dependências interna do controlador/operador19, falhas nos controles de segurança dos sistemas (a exemplo da ausência ou fraca criptografia, falha de sistema que permita escalação de privilégio ou tratamentos indevidos), entre outras.
13	Tratamento sem consentimento do titular dos dados pessoais (caso o tratamento não esteja previsto em legislação ou regulação pertinente)	Controlador de dados pessoais não obtém consentimento do titular para realizar um tratamento de dados pessoais sem embasamento legal.
14	Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular	A realização de operação de processamento de dados pessoais deve estar em conformidade com a LGPD. Qualquer operação de processamento que não atenda esse requisito pode produzir informações com vinculações ou associações indevidas.

b) Análise de Riscos

Para avaliar o nível de cada um dos riscos elencados deve-se avaliar o objeto (sistema, processo de trabalho, atividade) sob três dimensões: Estrutura, Sistema e Privacidade. A dimensão “Estrutura” trata aspectos estruturais do sistema: processos e infraestrutura que o sustentam. A dimensão “Sistema” tem alicerce no conceito “*Security-by-Design*”, que visa garantir a segurança da informação durante todo o ciclo de vida do sistema, propiciando a redução da superfície de ataque. Inclui temas como

desenvolvimento seguro, controles de acesso lógico, segurança web e outros. E por fim, a dimensão “Privacidade”, que está relacionada ao alcance da conformidade legal com a privacidade de tratamento de dados pessoais.

Para cada uma dessas dimensões estão associados controles de segurança pertinentes, sendo 113 controles, sendo 36 sob a dimensão “Estrutura”, 39 sob a dimensão “Sistema”; e 38 sob a dimensão “Privacidade” (Brasil, 2020). Exemplos desses controles são listados nas Tabelas 2, 3 e 4 (Brasil, 2020).

Tabela 2
Dimensão Estrutura

ID	Controle
15	As mudanças são comunicadas para todas as partes interessadas?
16	Existe um prazo formalmente definido para o tratamento de vulnerabilidades técnicas relevantes identificadas?
18	Há um processo de análise e monitoramento de vulnerabilidades?

Tabela 3
Dimensão Sistema

ID	Controle
48	O sistema em análise segue uma política de senha com definição de tamanho mínimo e formato?
55	O sistema implementa restrições/limitadores para sucessivas tentativas de acesso mal sucedidas?
66	É realizada análise estática e/ou análise dinâmica dos requisitos de segurança cibernética do sistema?

Tabela 4
Dimensão Privacidade

ID	Controle
76	As permissões de acesso (incluir, consultar, alterar, excluir) dos usuários que executam a operação de processamento de dados pessoais se limitam ao mínimo necessário para realizar o processamento?
81	A instituição utiliza técnicas ou métodos apropriados para garantir exclusão ou destruição segura de dados pessoais (incluindo originais, cópias e registros arquivados), de modo a impedir sua recuperação?

105	No processamento de dados, é utilizado o mínimo necessário de dados pessoais para atingir a finalidade pretendida?

É importante mencionar que vários desses controles são os mesmos prescritos pela Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). De forma mais específica, dos 113 controles previstos pelo Guia da SGD, identificou-se 27 controles em que há sobreposição com os controles recomendados pelo CNJ.

Considerando que os tribunais já dispõem dos controles recomendados pela ENSEC-PJ para a realização de suas mensurações de maturidade de segurança cibernética, e a necessidade de integração entre as ações de segurança da informação e de privacidade de dados, optou-se por utilizar, para esses controles sobrepostos, a mesma análise já utilizada na Segurança da Informação relativa aos 27 controles sobrepostos.

Essa análise tipicamente é realizada por meio da técnica de Autoavaliação dos Controles (ou Control Self Assessment – CSA), processo em que a própria organização realiza a avaliação de seus controles e riscos. A autoavaliação dos controles recomendados pelo CNJ pode ser realizada com base em métodos publicamente disponíveis. Considerando-se que ainda são baseados no CIS Controls v7, pode ser utilizado o método “CIS Critical Security Controls v7.1 Assessment Tool” (Enclave Security, 2023). Porém, caso o tribunal decida-se por se basear na versão atualizada dos controles, pode utilizar o próprio método de avaliação de riscos proposto pelo CIS, o CIS RAM (CIS, n.d.), ou o método atualizado pela Enclave Security (Enclave Security, 2023b).

No caso já utilizado na prática em um tribunal superior, a autoavaliação é realizada por meio do método “CIS Critical Security Controls v7.1 Assessment Tool”, em que as notas de avaliação de cada controle encontram-se em uma escala de 0 a 5. Para sua utilização neste método de avaliação de riscos de privacidade, essa nota é convertida para uma escala de 0 a 10, segundo a seguinte fórmula:

$$Nota_P = ((Nota_{SC} - 1)/4) * 10$$

Onde:

- $Nota_P$ é a nota de privacidade a ser utilizada nesta metodologia
- $Nota_{SC}$ é a nota obtida pelo controle na avaliação de segurança cibernética

Assim, a metodologia prevê a resposta “Sim” ou “Não” para a implementação dos controles onde não há sobreposição entre aqueles previstos pelo Guia da SGD e aqueles previstos pelas recomendações do CNJ, e a utilização da $Nota_P$ quando há sobreposição, considerando-se que, nesses casos, o tribunal já venha acompanhando com mais atenção o status de sua implementação.

A Tabela 5 exemplifica alguns dos controles em que foi identificada a sobreposição.

Tabela 5
Controles de privacidade também prescritos pela ENSEC-PJ

Dimensão Sistema	
ID	**Controle**
16	Existe um prazo formalmente definido para o tratamento de vulnerabilidades técnicas relevantes identificadas? (Grupo de controles 3 - Resolução 396 CNJ)
23	Há um sistema para monitoramento de aplicações, alertas e vulnerabilidades utilizado para auxiliar na detecção e tratamento de incidentes de segurança cibernética (IPS, IDS, etc.)? (Controle 6.6 - Resolução 396 CNJ)
28	Está estabelecida a abrangência dos procedimentos de backup para cada tipo de informação (por exemplo, completa ou diferencial)? (Grupo de controles 9 - Resolução 396 CNJ)

Dessa forma a metodologia aqui apresentada se torna adaptável, sendo capaz de acolher a eventual expansão da avaliação de controles de segurança por um determinado tribunal além dos controles mínimos atualmente recomendados pelo CNJ.

c) Avaliação dos Riscos

A ISO 31000 define que, ao final do processo de avaliação de riscos, cada risco deva ser classificado em um nível de criticidade de forma a subsidiar a forma como será tratado (aceitar, mitigar, transferir ou evitar), o que subsidiará a definição de que ações serão empreendidas para atuar no risco, e trazê-lo níveis aceitáveis.

Uma das formas de se calcular o nível do risco, de acordo com a referida norma, é a utilização de uma matriz de probabilidade e consequência em que o cruzamento desses dois eixos definirá o nível do risco sob análise, conforme exemplificado pela Tabela 6.

Tabela 6

Exemplo de abordagem qualitativa aos critérios de risco

Probabilidade	**Consequência**				
	Catastrófico	**Crítico**	**Sério**	**Significativo**	**Menor**
Quase certo	Muito alto	Muito alto	Alto	Alto	Médio
Muito provavelmente	Muito alto	Alto	Alto	Médio	Baixo
Provável	Alto	Alto	Médio	Baixo	Baixo
Bastante improvável	Médio	Médio	Baixo	Baixo	Muito baixo
Improvável	Baixo	Baixo	Baixo	Muito baixo	Muito baixo

Fonte: Adaptado de ABNT NBR ISO 27005:2022

A metodologia prevê que, para a obtenção dos níveis de cada um dos 14 riscos de privacidade, seja feita a avaliação dos níveis de probabilidade e consequência resultantes da aplicação de cada um dos 113 controles sobre esses riscos.

Os controles podem assumir três pesos: 0, caso não se aplique ao risco, 0,5 caso se aplicar ao risco, e 1 caso se aplicar e for prioritário, e foram classificados como atuantes na prevenção do risco, na mitigação do risco, ou em ambos os casos.

A Tabela 7 exemplifica controles que atuam para prevenir a ocorrência dos riscos. A título de exemplo, evidencia que o controle 3 não tem qualquer efeito na prevenção dos riscos.

Já a Tabela 8 mostra como os controles atuam para mitigar seus efeitos, e evidencia que esse mesmo controle é efetivo, mas não prioritário, para mitigar os efeitos de materialização do Risco 5, e efetivo e prioritário para mitigar os efeitos da materialização do Risco 8.

Tabela 7
Pesos e aplicabilidade na prevenção de cada um dos 14 riscos

Controle	Risco 1	Risco 2	Risco 3	Risco 4	Risco 5	Risco 6	Risco 7	Risco 8	Risco 9	Risco 10	Risco 11	Risco 12	Risco 13	Risco 14
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	1	0,5	1	0,5	0,5	0,5
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
112	0	0	0	1	0	0	0	0	0	0	0	0	0	0
113	0	0	0	1	0	0	0	0	0	0	0	0	0	0
Somatório dos pesos	**64,5**	**20,5**	**18,5**	**34,5**	**16,5**	**13**	**67,5**	**51**	**17,5**	**71**	**19**	**71,5**	**26**	**33,5**

Tabela 8
Pesos e aplicabilidade na mitigação dos efeitos da materialização de cada um dos 14 riscos

Controle	Risco 1	Risco 2	Risco 3	Risco 4	Risco 5	Risco 6	Risco 7	Risco 8	Risco 9	Risco 10	Risco 11	Risco 12	Risco 13	Risco 14
1	1	1	1	1	1	0	1	1	1	1	1	1	0	1
2	0	0	0	0	0,5	0	0	1	0	0	0	0	0	0
3	0	0	0	0	0,5	0	0	1	0	0	0	0	0	0
4	0,5	0	0	1	0	0	1	1	0	1	0	1	0	0
5	0,5	0,5	0,5	0,5	0,5	0	0,5	0,5	1	0,5	1	0,5	0	0,5
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
112	0	0	0	1	0	0	0	0	0	0	0	0	0	0
113	0	0	0	1	0	0	0	0	0	0	0	0	0	0
Somatório dos pesos	**23**	**6**	**2,5**	**13**	**7,5**	**2,5**	**31,5**	**50**	**4**	**35**	**5**	**53**	**6,5**	**10**

Após a análise de implementação dos controles, com a indicação de “Sim” ou “Não” para cada um dos 86 controles não sobrepostos pela ENSEC-PJ, e a definição da nota da maturidade dos outros 27 controles já mensurados pela ENSEC, é possível calcular o percentual de implementação dos controles que atuam na prevenção de um $Risco_n$, e o percentual de implementação dos controles que atuam na mitigação desse mesmo $Risco_n$.

$$\text{IPP } Risco_n = \frac{\text{A} + \text{B}}{TPP}$$

$$\text{IPM } Risco_n = \frac{\text{C} + \text{B}}{TPM}$$

Onde:

- IPP $Risco_n$ é o percentual de implementação de controles para prevenção do $Risco_n$.
  - A é a soma dos pesos dos controles que atuam na prevenção do $Risco_n$, em que houve resposta “Sim”;

- B é a soma da multiplicação do peso pela nota de maturidade dos controles que atuam na prevenção do $Risco_n$, que esteja no grupo dos 27 controles sobrepostos pela ENSEC-PJ.
- TPP é o somatório dos pesos que atuam na prevenção do $Risco_n$;

- IPM $Risco_n$ é o percentual de implementação de controles para mitigação do $Risco_n$
  - C é a soma dos pesos dos controles que atuam na mitigação, em que houve resposta “Sim”
  - D é a soma da multipicação do peso pela nota de maturidade dos controles que atuam na mitigação do $Risco_n$ que esteja no grupo dos 27 controles sobrepostos pela ENSEC-PJ.
  - TPM é o somatório dos pesos que atuam na mitigação dos efeitos do $Risco_n$;

Após a obtenção dos valores do IPP e IPM para um determinado Risco, é possível a determinação dos níveis de probabilidade e consequência de acordo com a Tabela 9.

Tabela 9
Probabilidade e consequência associados ao $Risco_n$

	Probabilidade (IPP)	**Consequência (IPM)**
0 até 0,37	Quase certo	Catastrófico
0,38 até 0,59	Muito provavelmente	Crítico
0,60 até 0,75	Provável	Sério
0,76 até 0,84	Bastante improvável	Significativo
0,84 até 1	Improvável	Menor

Os valores de probabilidade e consequência devem então ser transportados para a Matriz de Probabilidade e Consequência citada anteriormente.

Em seguida, deve-se realizar a consolidação do nível de risco à privacidade de dados do objeto sob análise. A Tabela 10 exemplifica o resultado dessa etapa.

Tabela 10
Riscos à privacidade de dados

Risco		Nível do Risco
1	Acesso não autorizado	Risco médio
2	Coleção excessiva	Risco alto
3	Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais	Risco muito alto
4	Falha em considerar os direitos do titular dos dados pessoais	Risco alto
5	Falha ou erro de processamento	Risco médio
6	Informação insuficiente sobre a finalidade do tratamento	Risco baixo
7	Modificação não autorizada	Risco médio
8	Perda	Risco baixo
9	Reidentificação de dados pseudonimizados	Risco muito alto
10	Remoção não autorizada	Risco muito alto
11	Retenção prolongada de dados pessoais sem necessidade	Risco alto
12	Roubo	Risco médio
13	Tratamento sem consentimento do titular dos dados pessoais (caso o tratamento não esteja previsto em legislação ou regulação pertinente)	Risco médio
14	Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular	Risco muito baixo

5. Resultados e discussão

Com relação aos controles selecionados para a mitigação dos riscos, faz-se pertinente destacar que o Guia de Avaliação de Riscos de Segurança e Privacidade traz sua própria sugestão de 113 controles, que, a partir de uma experiência de pouco mais de dois anos de análise de sistemas críticos pela Secretaria de Governo Digital do Ministério da Economia, foram identificados como contributivos para o incremento da segurança da informação diante dos pilares de confidencialidade, integridade, disponibilidade e autenticidade, e sua associação aos riscos. O modelo então foi aprimorado para também atender aos critérios de privacidade.

Já o método aqui proposto considera também os controles de segurança recomendados pelo Protocolo de Proteção de Infraestruturas Críticas de TIC definido

pela Portaria CNJ 162/2021, que, por sua vez, é baseado no *framework* CIS Controls versão 7.1. A portaria esclarece que trata-se de recomendações iniciais mínimas, tendo sido considerados, para este primeiro momento, os controles de agrupamento "*Basic"* do CIS Controls 7.1, acrescidos dos controles referentes a E-mail e Proteções de Navegador web, Defesas contra *malware*, Capacidade de Recuperação de Dados e Proteção de Dados. Por ser baseado em um *framework* internacionalmente reconhecido, seus controles são considerados eficazes para o incremento da segurança cibernética, embora deva-se destacar o recorte realizado pelo CNJ para a definição do conjunto inicial mínimo de controles de segurança recomendados.

Faz-se importante frisar que tanto o Guia de Avaliação de Riscos de Segurança e Privacidade quanto o Protocolo de Proteção de Infraestruturas Críticas de TIC informam que os controles recomendados não são taxativos, devendo ser avaliados à luz da realidade de cada instituição, podendo ser excluídos ou acrescentados novos controles.

Observa-se ainda que nenhum dos dois métodos leva em consideração a norma ISO 27.701, que tem sua própria recomendação de controles de segurança e privacidade.

Importante registrar também que o *framework* CIS Controls já sofreu atualização, passando da versão 7.1 utilizada pelo CNJ para a versão 8, que, por sua vez, foi incrementada com a publicação do Guia Complementar de Privacidade, que aguarda a publicação de seu Anexo LGPD.

Assim, ainda que haja interseção entre os conjuntos de controles recomendados por cada uma das fontes, é importante uma futura avaliação dessas diversas fontes de forma coordenada, uma vez que tal análise pode resultar em um conjunto de controles que cubra de forma mais abrangente as necessidades de segurança e privacidade.

6. Conclusão

O modelo aqui proposto é capaz de prover os órgãos do poder judiciário de um método de seleção dos controles de segurança mínimos recomendados pela Portaria 162/2021 do CNJ, de forma a contribuir para o nível adequado de segurança e privacidade, podendo ser utilizado também por outras instituições que entendam que esse conjunto de controles mínimos é suficiente para sua realidade. É importante, entretanto, destacar que os controles recomendados pelo CNJ representam um conjunto inicial mínimo, que deve ser ampliado, à luz do próprio CIS Controls, para que seja alcançado um nível de segurança e privacidade adequado.

Ademais, a metodologia descrita no trabalho pode ser utilizada pelos órgãos do judiciário para gerar insumos para a elaboração do RIPD exigido pela LGPD. A ANPD disponibiliza uma página de perguntas e respostas sobre o RIPD (ANPD, 2023), que prevê a descrição de cada risco de privacidade associado aos dados tratados, acompanhado dos níveis de probabilidade e impacto de suas ocorrências, bem como do respectivo nível de risco.

Como sugestão de trabalhos futuros, visualiza-se a atualização do modelo para que seja baseado na versão 8 do CIS Controls, já contando com a indicação de seu Guia Complementar de Privacidade com relação aos controles que são aplicáveis à privacidade (com a respectiva motivação), e com as recomendações que estarão registradas em seu Anexo LGPD, ainda a ser publicado.

Adicionalmente, uma complementação do modelo à luz da norma ISO 27.701 também se mostra interessante, uma vez que ela recomenda controles adicionais que àqueles que compõem o CIS Controls, o que trará a possibilidade de obtenção de um modelo mais completo, combinando controles de segurança cibernética, controles de privacidade e controles organizacionais, validados pela comunidade internacional.

Referências

Associação Brasileira de Normas Técnicas. (2018). *Gestão de riscos - Diretrizes* ABNT NBR ISO/IEC 31000:2018:

Associação Brasileira de Normas Técnicas. (2020). *Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes*. ABNT NBR ISO/IEC 27701:2019.

Autoridade Nacional de Proteção de Dados (2023). Relatório de Impacto à Proteção de Dados Pessoais (RIPD). https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#p10

Center for Internet Security. n.d. CIS RAM (Risk Assessment Method). https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method

Conselho Nacional de Justiça. (2021a). *Portaria nº 162, de 10 de junho de 2021. Aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).* https://atos.cnj.jus.br/atos/detalhar/3982

Conselho Nacional de Justiça. (2021b). *Resolução nº 363, de 12 de janeiro de 2021. Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais*. https://atos.cnj.jus.br/atos.detalhar/3668

Conselho Nacional de Justiça. (2021c). *Resolução nº 396, de 07 de junho de 2021. Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).* https://atos.cnj.jus.br/atos/detalhar/3975

Comitê Central de Governança de Dados. (2020). *Guia de Boas Práticas - LGPD*. https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf/view

Enclave Security. (2023). Critical Security Controls. - CIS Critical Security Control v7.1 Assessment Tool. https://www.auditscripts.com/download/4229/?tmstv=1694884128

Enclave Security. (2023). Critical Security Controls. – CIS Critical Security Control v8.0 Assessment Tool. https://www.auditscripts.com/download/4588/?tmstv=1694884128

Gil, A.C. (2019). *Como elaborar projetos de pesquisa*. Editora Atlas S.A.

Lima, L. de A. (2016). *O Direito à Privacidade nas Redes Sociais na Internet*. [Dissertação de Mestrado]. Universidade Regional do Noroeste do Estado do Rio Grande do Sul – UNIJUI. Programa de Pós-Graduação em Direito - Direitos Humanos. https://bibliodigital.unijui.edu.br:8443/xmlui/handle/123456789/4204

Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais.* Presidência da República. http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

Ministério da Economia. (2020). *Guia de Avaliação de Riscos de Segurança e Privacidade - LGPD*. https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_avaliacao_riscos.pdf/view

Ministério da Economia. (2021). *Relatório de Impacto à Proteção de Dados Pessoais*. https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_template_ripd.docx/view

National Institute of Standards and Technology. (2020), NIST Privacy Framework: A Tool for improving Privacy through Enterprise Risk Management, version 1.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020pt.pdf

Tribunal de Contas da União. s.d. Fiscalização de tecnologia da informação. https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/autoavaliacao-de-controles/#_Toc40367506