risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 10/10/2022
Aceitação/Acceptance: 22/12/2022

Judiciário sob ataque *hacker*: riscos de negócio para segurança cibernética em tribunais brasileiros

Renato Solimar Alves[1], Marcus Aurélio Carvalho Georg[1], Rafael Rabelo Nunes[1,2,3]

renatosolimar@gmail.com; georg@stj.jus.br; rafaelrabelo@unb.br

[1] Universidade de Brasília (UnB), Campus Darcy Ribeiro, Departamento de Engenharia Elétrica, CEP 70910-900 Brasília-DF Brasil

[2] Universidade de Brasília (UnB), Campus Darcy Ribeiro, Departamento de Administração, CEP 70910-900 Brasília-DF Brasil

[3] Centro Universitário Atenas, Rua Euridamas Avelino de Barros, nº 1400, Prado, CEP 38602-002 Paracatu-MG Brasil

Pages: 344-357

Resumo: Ataques cibernéticos recorrentes têm impactado a atividade finalística de diversos tribunais do Poder Judiciário, prejudicando a sua imagem e o alcance de seus objetivos estratégicos. Nesse sentido, este estudo tem como objetivo identificar os principais riscos de negócio de tribunais. Para tal, foi realizada pesquisa bibliográfica sobre o tema, foram entrevistados gestores públicos atuantes nas áreas jurídica, administrativa e de tecnologia e realizada uma oficina com grupo focal de especialistas. Como resultado foi obtida a relação dos 10 principais riscos de negócio de tribunais, aproximadamente 40 diferentes causas possíveis para os riscos e mais de 30 possíveis consequências. Os resultados obtidos permitem relacionar os riscos de negócio com diversos riscos operacionais, contribuindo para a gestão dos riscos, a gestão da segurança do processo judicial eletrônico, bem como a definição de controles que reduzam a probabilidade de ocorrência ou minimizem as consequências caso os riscos se concretizem.

Palavras-chave: avaliação de riscos; segurança da informação; análise preliminar de perigos; método *bow tie*.

Judiciary under hacker attack: business risks for information security in Brazilian courts

Abstract: Recurring cyber-attacks have impacted the final activity of various bodies of the Judiciary, harming their image and the achievement of strategic objectives. This study aims to understand the key activities and identify the main business risks of the Judiciary. To this end, bibliographic research was carried out on the subject, public managers working in the legal, administrative, and technology areas were interviewed, and a workshop was held with a focus group of specialists. As a result, a list of the ten main business risks of the Judiciary was obtained, with approximately 40 different possible causes for the risks and more than 30 possible consequences. The results obtained also allow the linking of business risks with

various operational risks, contributing to risk management and security of the electronic judicial process, as well as the definition of controls that reduce the probability of occurrence or minimize the consequences if the risks materialize.

***Keywords**:* risk assessment; information security; electronic process of law; preliminary hazard analysis; bow tie method.

1. Introdução

O Poder Judiciário promoveu a transformação do sistema judicial brasileiro por meio da ampla adoção da tecnologia no processo judicial. A transformação experimentada pela utilização do processo eletrônico aumentou a agilidade da distribuição e tramitação dos processos, bem como no aumento da produtividade em razão da maior produção de julgados, o que resultou na celeridade e na melhora da prestação do serviço jurisdicional (Hino & Cunha, 2020).

A pandemia acelerou ainda mais esse processo de transformação e a inovação tecnológica na Justiça, com destaque para o incremento da realização de videoconferências e audiências virtuais (Martins, 2021), além da possibilidade de citações por meios eletrônicos, o atendimento remoto por meio de "balcão virtual" e utilização de inteligência artificial na análise dos processos (Conselho Nacional de Justiça [CNJ], 2021a).

Neste cenário, a tecnologia, que já era um fator crítico, passa a ter um papel ainda mais relevante para o alcance dos objetivos estratégicos do Judiciário e para a efetiva prestação jurisdicional ao cidadão. Contudo, juntamente com os benefícios introduzidos pelo uso da tecnologia, são inseridos também novos fatores de risco (Moreira et al., 2021).

Em anos recentes, de 2019 a 2022, pôde-se observar ataques cibernéticos de grandes proporções, que impactaram negativamente ou paralisaram a atividade-fim de diversos órgãos do Poder Judiciário. Afetaram a órgãos tais como: STJ, TJ-RS, TRF da 1ª Região, TSE, STF, TRT-ES, TRF da 3ª Região, TRT-RS, Justiça Federal em Pernambuco e TJDFT (Reina, 2022).

Não só a indisponibilização de serviços se concretizou, como, também, a garantia da integridade dos dados foi atingida. Destaca-se o ocorrido no Tribunal Regional Federal da 3ª Região, onde foram levantadas evidências de que um *hacker* obteve acesso ao sistema processual eletrônico, possibilitando a mudança de pareceres do MPU, a conversão de sentenças de condenação em absolvição e a alteração das contas destinatárias para o recebimento de valores legítimos em outros processos (Moura & Borges, 2022) (Tribunal Regional Federal da 3ª Região, 2021).

Quando tais ataques chegam a afetar o funcionamento do sistema jurídico, se revelam fragilidades que abalam a confiança depositada na Justiça, sendo necessário que o nível de segurança seja o mais elevado possível (Hirata & Oliveira, 2022).

Considerando que os riscos são os efeitos das incertezas sobre os objetivos, torna-se essencial que sejam adequadamente identificados (Associação Brasileira de Normas Técnicas [ABNT], 2018), de forma que gestão de riscos seja capaz de reduzir a probabilidade ou os efeitos dos incidentes sobre a integridade, disponibilidade e/ou confidencialidade das atividades-críticas (Nunes, Perini, & Pinto, 2022) (Lima, et al., 2022).

No Poder Judiciário, destacam-se as atividades de recebimento e distribuição de processos, análise e relatoria de processos, produção de decisão, julgamento, processamento judicial e execução de atos cartorários e o cumprimento de despachos e decisões (Supremo Tribunal Federal, 2018a).

O framework MITRE ATT&CK documenta as táticas e técnicas utilizadas por hackers em situações reais, apresentando 14 táticas, 191 técnicas, 363 subtécnicas e milhares de procedimentos utilizados por *hackers* nos ataques cibernéticos (MITRE Corporation, 2021), o que evidencia o desafio de aplicar os controles de segurança na proteção de sistemas de informação.

Existem outros *frameworks* que listam os controles de segurança necessários para se proteger contra esses comportamentos maliciosos. A título de exemplo, o *Cybersecurity Framework* do NIST descreve 5 funções, 22 categorias, 98 subcategorias e aproximadamente 1200 possíveis controles de segurança necessários para identificar, proteger, detectar, responder ou se recuperar de ataques cibernéticos criminosos (NIST, 2022). Portanto, considerando a grande quantidade de possíveis controles de segurança cibernética, se faz necessário priorizar os controles que sejam relevantes para o tratamento dos riscos que afetem o negócio (Conselho Nacional de Justiça,2021b, pp. 15-16). Apesar disso, os riscos que podem afetar o judiciário brasileiro decorrentes à riscos cibernéticos não estão documentados em literatura.

Nesse sentido, este estudo tem como objetivo identificar os principais fatores de riscos de negócio relacionados às atividades principais do Poder Judiciário, contribuindo para o processo de avaliação de riscos e de definição dos controles de segurança cibernética prioritários para os órgãos do Poder Judiciário.

O presente trabalho segue a seguinte estrutura: na seção 2 são indicados os principais conceitos da bibliográfica sobre o tema; na seção 3 é evidenciada a metodologia utilizada para a identificação dos riscos de negócio; na seção 4 são apresentados os riscos de negócio do Poder Judiciário e são avaliados os resultados; na seção 5 são apontadas as limitações do trabalho, as propostas de trabalhos futuros e as conclusões.

2. Referencial Teórico

Nessa seção apresentam-se os conceitos necessários para que se compreenda esse trabalho. Primeiro, discorre-se sobre Risco, a Gestão de Riscos e o Processo de Avaliação de Riscos; na sequência, apresentam-se as atividades e processos de negócio principais de tribunais; e por fim, apresentam-se trabalhos correlatos a esse.

2.1. Risco, Gestão de Riscos e o Processo de Avaliação de Riscos

O risco faz parte de qualquer iniciativa humana. As atividades triviais cotidianas, tais como despertar, utilizar um transporte coletivo, ir à escola ou ao trabalho, ou até mesmo dormir, expõem as pessoas a diferentes níveis de risco. Enquanto alguns riscos são desprezíveis, outros exercem influência significativa no modo de vida de muitas pessoas (Damodaran, 2009, p. 21). Muitas das inovações e avanços civilizatórios somente foram experimentados porque alguém se dispôs a correr riscos e a mudar o estado presente de coisas. O desejo de eliminar riscos, tanto quanto a disposição de exposição ao

risco, geraram muitas das mais duradouras e valiosas invenções criadas pelo homem (Damodaran, 2009, pp. 21-26).

As organizações enfrentam influências e fatores que tornam incerto o alcance de seus objetivos. O efeito dessa incerteza é denominado "risco". Gerir riscos auxilia as organizações a estabelecer estratégias, a alcançar objetivos, a tomar decisões fundamentadas e a ter por propósito a criação e proteção de valor (ABNT, 2018, pp. Vi, 2). Os riscos precisam ser identificados, a exposição deve ser medida e estimada, os efeitos da exposição precisam ser analisados, os controles precisam ser avaliados quanto aos seus custos e benefícios, uma estratégia de mitigação deve ser estabelecida e o desempenho desse processo deve ser criticamente avaliado (Crouhy, Galai, & Mark, 2014).

O processo de gestão de riscos busca responder as questões fundamentais (ABNT, 2012, p. xiii): o que pode acontecer e por qual motivo? Quais são as consequências? Qual é a probabilidade de ocorrência? Existem fatores que mitigam a consequência do risco ou a sua probabilidade de ocorrência? Qual é o nível tolerável de risco? Desse modo, são realizadas diversas atividades para responder à essas questões: o estabelecimento do escopo, o processo de avaliação de riscos (identificação, análise e avaliação), tratamento de riscos, monitoramento e análise crítica, registro e relato e a comunicação e consulta (ABNT, 2018, p. 9).

Essas atividades são fundamentais e tem por finalidade fornecer, aos tomadores de decisão e às partes interessadas, informações baseadas em evidências para a tomada de decisão sobre como tratar riscos específicos dentre as opções disponíveis (ABNT, 2012, pp. 1-2). A Norma ABNT NBR ISO/IEC 31010:2012 esclarece que:

> O processo de avaliação de riscos fornece aos tomadores de decisão e às partes responsáveis um entendimento aprimorado dos riscos que poderiam afetar o alcance dos objetivos, bem como a adequação e eficácia dos controles em uso. [...] A saída do processo de avaliação de riscos é uma entrada para os processos de tomada de decisão da organização (ABNT, 2012, p. 6).

A etapa *identificação de riscos* do processo de avaliação de riscos visa identificar as situações que poderiam afetar o alcance dos objetivos. Há diversos métodos para a identificação de riscos, por exemplo: listas de verificação, análise de dados históricos, *brainstorm*, HAZOP, Delphi, dentre várias outras (ABNT, 2012, p. 7).

A etapa *análise de riscos* considera as causas e fontes de risco e suas consequências, além de sua probabilidade de ocorrência, para poder definir qual é o nível do risco. Um evento pode ter múltiplas consequências e afetar vários objetivos, e essa análise pode ser qualitativa, semi-quantitativa e quantitativa (ABNT, 2012, pp. 8-9).

A etapa de *avaliação de riscos* compara os níveis de risco obtidos com critérios definidos no estabelecimento do contexto, a fim de: avaliar quais riscos precisam ser tratados, quais são as prioridades de tratamento, se alguma atividade de ser evitada e, dentre as alternativas, que caminho será tomado. A decisão para tratamento deve levar em conta os custos e benefícios de assumir o risco bem como o de implementar os controles (ABNT, 2012, pp. 11-12).

É comum classificar os riscos após a sua avaliação. Grouhy et al. (2014) dividem os riscos nessas categorias principais: risco de mercado, risco de crédito, risco de liquidez, risco operacional, risco legal e regulatório, risco de negócio, risco estratégico e risco de reputação (Crouhy, Galai, & Mark, 2014).

2.2. Atividades e Processos de Negócio dos Tribunais

Cadeia de Valor é uma ferramenta de gestão que representa graficamente o conjunto dos macroprocessos e os principais processos desenvolvidos por uma organização para o alcance de sua missão institucional. Este instrumento visualmente apresenta o conjunto de atividades desempenhadas para agregar valor aos produtos e serviços que presta, possibilitando uma visão global dos processos finalísticos e de apoio, suas correlações e dependências. Na Cadeia de Valor do Supremo Tribunal Federal, pode-se observar os macroprocessos principais que geram valor organizacional dentro de um Tribunal (Supremo Tribunal Federal, 2018a).

Dentre as atividades apresentadas na cadeia de valor do STF, destacam-se as que envolvem a elaboração de despachos e de decisões, onde os magistrados desempenham a atividade fim dos tribunais (Supremo Tribunal Federal, 2018a). Essa atividade nem sempre é realizada pelos próprios membros visto que há equipe de assessores, analistas e técnicos que auxiliam nessa tarefa. De forma a exemplificar, na Suprema Corte brasileira cada magistrado dispõe de 30 cargos para serem providos (Supremo Tribunal Federal, 2022).

O Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário – PGCRC-PJ, Portaria CNJ n. 162 de 10 de junho de 2021, estabelece que as atividades críticas, necessárias para a consecução dos produtos e serviços fundamentais dos órgãos, devem ter os seus riscos continuamente avaliados. A adequada gestão destes riscos críticos pode impactar diretamente na continuidade do negócio dos órgãos do Poder Judiciário (Conselho Nacional de Justiça, 2021b, pp. 15-16).

2.3. Trabalhos correlatos

No decorrer da pesquisa, identificou-se alguns trabalhos relacionados à identificação de riscos ou à segurança da informação no Poder Judiciário no Brasil. Rover (2015) realizou mapeamento quantitativo das publicações científicas envolvendo as áreas temáticas de gestão do judiciário, processo eletrônico e segurança da informação, identificando-se que a "temática do e-judiciário não é objeto de forte publicação em revistas de excelência" (Rover, 2015, p. 163). Wanderley (2020) propôs um modelo, elaborou artefatos para suportar o processo de gestão de riscos em segurança da informação no Tribunal de Justiça do Tocantins e aplicou estudo de caso em ambiente de *datacenter* para validação do modelo. Machado (2018), traçando paralelo com área bancária, propôs a definição de uma linguagem comum aos órgãos do Poder Judiciário para a identificação e categorização dos riscos operacionais. Costa (2021) aborda o compartilhamento de informações entre equipes virtuais na Justiça Federal e o risco de vazamento, se constatando o uso dominante de dispositivos celulares na comunicação e a necessidade de utilização exclusiva de instrumentos tecnológicos autorizados pelo respectivo Tribunal. Leite (2021) aborda o risco da exposição midiática e a necessidade de

o Poder Judiciário aprimorar sua capacidade de comunicação visando dar transparência e preservar sua imagem e credibilidade.

Em âmbito internacional verifica-se que Comitê Conjunto de Tecnologia (JTC, na sigla em inglês) da Conferência de Administradores de Tribunais de Justiça Estaduais (COSCA, na sigla em inglês), da Associação Nacional de Gestão De Tribunais (NACM, na sigla em inglês) e do Centro Nacional de Tribunais Estaduais (NCSC, na sigla em inglês), desenvolveram um guia com recomendações para preparação e prevenção necessários para se responder de forma eficaz aos de incidentes de segurança cibernética. Dentre as diversas boas práticas, destaca-se a necessidade de antecipar o impacto potencial da perda ou mudanças não autorizadas em ativos essenciais de dados, incluindo ordens de juízes, identidade e testemunho de testemunhas, identidades de jurados, gravações judiciais, informações de transações financeiras, evidências digitais e informações pessoais (Joint Technology Committee, 2019, p. 8).

Gordon & Garrie (2020) também demonstram importância de segurança cibernética para a proteção do processo judicial e indicam uma ampla relação de melhores práticas, incluindo: desenvolver e praticar uma forte "higiene cibernética", identificar e proteger as "joias da coroa", possuir planos de comunicação e de resposta a incidentes, identificar as ameaças com base na gestão de riscos específicas para o sistema judicial, utilizar criptografia, dentre outras.

Não se identificou estudos que objetivassem identificar de forma objetiva quais seriam os riscos de negócio ou operacionais das atividades principais do Poder Judiciário Brasileiro.

3. Metodologia

Este estudo se trata de uma pesquisa de natureza aplicada, pois visa a aplicação prática e a solução de problemas específicos. Se adotou abordagem qualitativa para se interpretar e significar um fenômeno do mundo real sujeito a subjetividade e que nem sempre pode ser representado em números (Silva & Menezes, 2005, p. 20).

A pesquisa possui objetivo exploratório pois pretende proporcionar melhor entendimento do problema, visando esclarecer conceitos, aprimorar ideias, construir hipóteses ou a descoberta de novas intuições (Gil, 2018, p. 24), sendo a que possui menor rigidez de planejamento, geralmente envolvendo o levantamento bibliográfico e documental, entrevistas não estruturadas e estudos de caso. Sendo utilizada especialmente quando o tema é pouco explorado e se torna desafiador formular hipóteses exatas. A Figura 1 demonstra as etapas decorridas nesse trabalho.

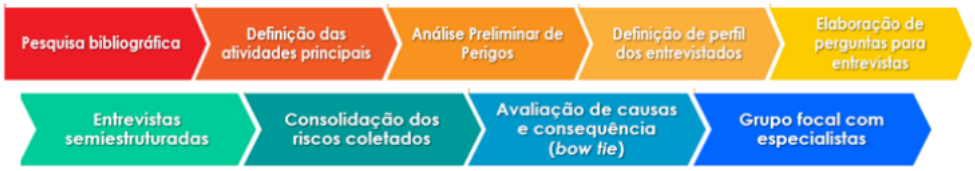

Figura 1 – Etapas da pesquisa

Neste estudo, os riscos legais e regulatórios, estratégicos e de reputação foram agrupados em uma mesma categoria de riscos, denominada riscos de negócio. Para a identificação de riscos adotou-se duas técnicas fortemente aplicáveis para a identificação de riscos: análise preliminar de perigos e entrevistas semiestruturadas (ABNT, 2012, p. 18).

A análise preliminar de perigos (APP) consiste na análise indutiva com o objetivo de identificar situações e eventos perigosos que podem causas danos em determinada atividade, sistema ou instalação. Geralmente é realizada em fase inicial de projeto, quando há pouca informação disponível (ABNT, 2012, pp. 29-30). A APP é versátil e amplamente utilizada em variados campos, indo da análise de riscos em terminais de inflamáveis, do uso de drogas injetáveis ou o projeto de produtos robóticos (Yana & Xu, 2019, pp. 1-2). A análise preliminar de perigos foi realizada com base em histórico de eventos ocorridos em órgãos Poder Judiciário e em situações hipotéticas de risco.

Nas entrevistas semiestruturadas, cada um dos entrevistados respondeu individualmente a um conjunto de questões pré-elaboradas que constam de roteiro que buscava incentivar os participantes apresentar situações de risco vivenciadas em sua experiência profissional, a avaliar algumas situações sob deferentes perspectivas e a indicar os riscos potenciais ou reais (ABNT, 2012, pp. 25-27).

Para a adequada identificação de riscos é necessário reunir diferentes áreas de conhecimento (ABNT, 2012, pp. 3). Desta forma, foram entrevistados oito gestores públicos com ampla experiência em sua área de atuação e com lotação em Tribunais Superiores e Regionais de relevância do Poder Judiciário. Sendo que destes: quatro possuem formação jurídica e atuavam no assessoramento de Ministros de Tribunais Superiores; três atuam em variadas funções relacionadas à tecnologia da informação, incluindo o desenvolvimento de sistema judicial eletrônico e segurança cibernética, e; um entrevistado atua na gestão de riscos corporativos de seu órgão. O tempo médio de atuação dos entrevistados no Poder Judiciário é de 19,6 anos. Com o objetivo de favorecer a livre manifestação de situações reais de risco, foi assumido compromisso de não divulgação direta ou indireta dos participantes. Salienta-se que as respostas apresentadas nas entrevistas se tornaram repetitivas, o que motivou a limitar as entrevistas a 8 participantes.

As perguntas foram enviadas previamente e, durante a entrevista, todos foram instados a citar situações de risco enfrentadas em sua área de atuação e que poderiam afetar o alcance dos objetivos primários do Judiciário. Foi apresentada, ainda, a lista preliminar de perigos com o objetivo de instigar a identificação de outros possíveis cenários que talvez ainda não tivessem sido imaginados.

Após a realização das entrevistas, sua análise e estruturação dos riscos, foi necessário comparar as respostas e analisar quais respostas eram de fatos riscos e quais seriam causas ou consequências dos riscos. Foi utilizado o método *bow tie* de avaliação de riscos (ABNT, 2012, pp. 68-70) para a análise dos riscos identificados na etapa de entrevistas. Embora tenha sido utilizado o método *bow tie*, inicialmente não foram indicadas as barreiras preventivas e mitigatórias para as causas e consequências dos riscos identificados.

Para análise e validação da técnica da consolidação dos resultados, foi formado grupo focal com seis especialistas em gestão de riscos ou segurança da informação que atuam no

CJF, Funpresp-Jud, STF, STJ e TSE. Em oficina foi apresentada proposta de separação de causas, riscos e consequências, que foram analisadas criticamente por todos.

Os autores declaram que este trabalho é original e inédito, que os entrevistados permitem a sua publicação com a manutenção de seu anonimato e que todos os autores contribuíram significativamente na elaboração deste.

4. Resultados e Discussões

Este estudo buscava identificar os principais riscos de negócio do Poder Judiciário, visando contribuir para a avaliação dos riscos e a definição dos controles de segurança cibernética prioritários para o Judiciário. Foram obtidos os seguintes resultados.

4.1. Atividades principais e a Análise Preliminar de Perigos

Identificou-se que, conforme demonstrou a Cadeia de Valor do STF, se destacam os agrupamentos de processos organizacionais relativos ao recebimento e distribuição de processos, análise e relatoria de processos, elaboração de decisão, julgamento, processamento judicial e execução de atos cartorários e o cumprimento de despachos e decisões pós julgamento. Para o foco do estudo, se concentrou na atividade de produção de elaboração de decisão.

A análise preliminar de perigos foi realizada com base em histórico de eventos e casos hipotéticos de risco e indicou os seguintes riscos: modificação de informações necessárias para o processo decisório na cadeia de fornecimento; emissão de determinação ou decisão fraudulenta; descumprimento do princípio do juiz natural, permitindo a identificação do magistrado que conduzirá e, potencialmente, julgará o caso; vazamento de informações de processos sigilosos; interrupção da prestação jurisdicional; acesso antecipado a determinações e decisões, ainda que sem modificação de informação; inclusão de assuntos indesejados ou inadequados em determinações ou decisões.

4.2. Entrevistas e a Análise das Causas e Consequências

Os entrevistados indicaram cerca de 110 possíveis riscos de negócio. Contudo, verificou-se que seria necessária uma avaliação mais aprofundada para a correta identificação do que seriam de fato os riscos, das suas possíveis causas ou consequências. Após a uso da técnica *bow tie* de análise de riscos, foi possível separar os riscos propriamente ditos de suas causas ou consequências. Os resultados foram tabulados e foram avaliados por especialistas utilizando a técnica de grupo focal.

Ao final de todas as etapas, foram identificados os 10 principais riscos de negócio do Poder Judiciário, aproximadamente 40 diferentes causas possíveis para esses riscos e mais de 30 possíveis consequências. Os resultados completos estão disponíveis em https://cutt.ly/KCFVmcn. Os riscos de negócio identificados foram transcritos na Tabela 1.

Número	Risco de Negócio
[1]	Divulgação antecipada de votos, determinações ou decisões
[2]	Vazamento de informações sigilosas, protegidas por segredo de Justiça ou dados pessoais

Número	Risco de Negócio
[3]	Emissão ou alteração não autorizada de determinações ou decisões
[4]	Interrupção da prestação jurisdicional
[5]	Previsibilidade ou manipulação da distribuição dos processos
[6]	Perda de informações
[7]	Parcialidade ou favorecimentos pessoais
[8]	Assuntos indesejados ou inadequados em determinações e decisões
[9]	Julgamentos legítimos, porém, com base em elementos adulterados
[10]	Espionagem de outras nações e/ou grupos de interesse

Tabela 1 – Riscos de negócio das atividades principais do Poder Judiciário

4.3. Discussão dos resultados

Ao analisar os resultados observa-se que não se identifica relação imediata entre os riscos de negócio com os riscos ou os controles de segurança cibernética. Esta dificuldade de relacionamento é conhecida, e Eling et al. (2021) relacionam várias dessas dificuldades apontadas em outros estudos.

O risco cibernético dificilmente se integra nas estruturas de gerenciamento de risco corporativo (ERM, na sigla em inglês) e que comumente se estabelece num silo funcional. Esse isolamento entre o gerenciamento do risco cibernético e o gerenciamento do risco corporativo resulta na falha da governança do risco (Eling, McShane, & Nguyen, 2021).

Embora os riscos de segurança cibernética estejam sendo promovidos como riscos a serem considerados pelos níveis mais altos de administração, muitos conselhos ainda não estão prontos para essa tomada de decisão e as decisões relacionadas ao risco corporativo acabam sendo tratadas em níveis mais baixos. São recomendadas pesquisas sobre a inclusão do risco cibernético nas decisões da alta administração e na governança geral (Eling, McShane, & Nguyen, 2021).

Buscou-se, com este estudo, contribuir para diminuir o distanciamento entre o negócio e as áreas técnicas. Os resultados demonstram, pela análise das causas, que é possível criar uma cadeia de vinculação entre os riscos de negócio e os riscos operacionais. A Tabela 2 demonstra exemplos em que as causas dos riscos de negócio são, por sua vez, os próprios riscos operacionais.

Causas e Fontes do Risco Operacional	Risco Operacional	Risco de Negócio
Perda de informações durante a elaboração de análises e minutas de decisões Sistema não permitir salvamento automático ou alerta da necessidade salvamento do documento em elaboração Sistema não possibilizar o versionamento de documentos em fase de elaboração, impossibilitando a recuperação de informações modificadas durante a elaboração da minuta	**Cópia de processos e minutas em computadores ou meios de armazenamento pessoais**	[1] [2]

Causas e Fontes do Risco Operacional	Risco Operacional	Risco de Negócio
Assédio por partes ou interessados em causas Assédio de grupos hacker Assédio de governos estrangeiros Atuação de organizações criminosas Histórico criminoso Insatisfação e desmotivação Problemas emocionais Doenças psicológicas	**Vazamento intencional por pessoas que tenham acesso a documentos ou informações sensíveis**	[1] [2] [10]
Desconhecimento dos desenvolvedores em boas práticas de desenvolvimento seguro Falha no processo de revisão e avaliação da qualidade do código Aproveitamento de código de fontes inseguras Não utilização de ferramentas de análise estática de código - SAST Falta de padronização dos sistemas judiciais eletrônicos, dificultando o controle do código-fonte Comprometimento do repositório de código-fonte	**Código-fonte com vulnerabilidades de segurança**	[1] [2] [3] [4] [5] [8] [9] [10]

Tabela 2 – Exemplos de riscos operacionais identificados a partir dos riscos de negócio

Cada risco operacional, igualmente ao risco de negócio, possui as suas próprias causas. E cada causa evidencia uma possibilidade de controle de segurança. Apesar da pesquisa, neste momento, não objetivar a identificação dos riscos operacionais ou os controles de segurança, verificou-se ser possível a compreensão dessas relações de causa e efeito.

Desta forma, restando razoável propor que os resultados obtidos permitem não apenas identificação dos riscos de negócio das atividades principais do Poder Judiciário, mas também os principais riscos operacionais associados a estes riscos de negócio. Que por sua vez, ao se analisar as causas destes riscos operacionais, é possível identificar os riscos de segurança cibernética e definir os controles de segurança necessários para mitigar os riscos.

Acredita-se, portanto, que essa metodologia de análise permite conectar toda a cadeia de riscos, deste o negócio ao controle de segurança cibernética. Potencialmente atendendo ao proposto por Eling et al. quanto a necessidade de integrar o risco cibernético à estrutura de gestão de riscos corporativos – ERM. Porém, para que seja efetivo se faz necessário que esses riscos sejam adequadamente quantificados (Eling, McShane, & Nguyen, 2021).

Sendo necessário seguir para as próximas etapas do processo de avaliação de riscos, analisando e atribuindo valor para a probabilidade de ocorrência dos riscos e os potenciais impactos nos objetivos, e, conforme o apetite para o risco, estabelecer controles preventivos e mitigatórios para os tratamentos dos riscos prioritários.

Os resultados demonstram, ainda, que muitos riscos possuem causas comuns, antevendo que o tratamento de alguns riscos operacionais poderão evitar a probabilidade de ocorrência de diversos riscos de negócio.

Observa-se também que a maioria das consequências dos riscos de negócio do Poder Judiciário, diferentemente de organizações privadas, não estão relacionados a perdas financeiras, mas à riscos de reputação (Crouhy, Galai, & Mark, 2014).

A confiança no Poder Judiciário é fundamental para a pacificação social e se vislumbra que a gestão de riscos possa se tornar o principal instrumento de comunicação clara e direta deste pilar do Estado Nacional com a sua principal parte interessada: o cidadão.

5. Conclusões

Considerando os ataques cibernéticos recorrentes ocorridos no Poder Judiciário, este estudo buscava identificar os riscos de negócio das atividades principais com o objetivo de verificar as possíveis relações com a necessidade de implementação de controles de segurança cibernética.

Constata-se que o objetivo foi atendido pois o trabalho conseguiu identificar as atividades principais do Poder Judiciário, os principais riscos de negócio, estabelecer vinculação com os riscos operacionais relacionados ao negócio e propor metodologia para interrelacionar os riscos de segurança cibernética ao risco de negócio.

Neste estudo realizou-se a revisão bibliográfica sobre gestão de riscos, foram entrevistados gestores públicos atuantes tribunais, utilizou-se o método *bow tie* para análise dos dados coletados e a realização de grupo focal com especialista para validação dos resultados.

Diante da metodologia proposta, observa-se que poderiam ter sido entrevistados gestores atuantes no 1º grau de jurisdição para ampliar a identificação dos riscos inerentes a esta esfera de atuação. Verifica-se ainda que, não obstante, a função principal do Judiciário ser a jurisdição, há ramos especializados da Justiça que possuem atividades finalísticas próprias, a exemplo da Justiça Eleitoral. Sendo necessário adaptar as atividades principais ao contexto de atuação específico. Possivelmente resultando na ampliação das atividades principais e muito provavelmente na ampliação da relação dos riscos de negócio e suas correlações de causa e consequência.

Como trabalhos futuros, sugere-se ampliar o escopo de profissionais e órgãos participantes das entrevistas para aprofundar a identificação dos riscos de negócio do Poder Judiciário. Propõe-se ainda que os riscos identificados sejam avaliados para fins de análise de criticidade, a continuidade da análise dos riscos operacionais relacionados ao de negócio e a priorização dos controles de segurança cibernética necessários para tratamento dos riscos de negócio mais relevantes.

Referências

Associação Brasileira de Normas Técnicas [ABNT]. (2012). Norma NBR ISO/IEC 31010. *Gestão de riscos — Técnicas para o processo de avaliação de riscos*. Rio de Janeiro, RJ, Brasil: ABNT.

Associação Brasileira de Normas Técnicas [ABNT]. (2018). Norma NBR ISO 31000. *Gestão de riscos — Diretrizes, 2ª*. Rio de Janeiro, RJ, Brasil: ABNT.

Conselho Nacional de Justiça [CNJ]. (2021a). *Justiça 4.0*. Acesso em 21 de maio de 2022, disponível em https://www.cnj.jus.br/tecnologia-da-informacao-e-comunicacao/justica-4-0/

Conselho Nacional de Justiça. (2021b). Estratégia Nacional de Segurança Cibernética do Poder Judiciário. Portaria CNJ n. 162/2021. Fonte: https://atos.cnj.jus.br/files/compilado140230202106146 0c7617672ec5.pdf

Costa, R. L. (18 de dezembro de 2021). 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, 7*(2), 76-96.

Crouhy, M., Galai, D., & Mark, R. (2014). *The Essentials of Risk Management* (2nd ed.). McGraw-Hill Education.

Damodaran, A. (2009). *Gestão Estratégica do Risco: uma referência para a tomada de riscos empresariais*. (F. Nonnenmacher, Trad.) São Paulo, SP, Brasil: Bookman Companhia Editora.

Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review, 10*(1), 93-125. doi:10.1111/rmir.12169

Gil, A. C. (2018). *Como Elaborar Projetos de Pesquisa* (6ª ed.). São Paulo: Atlas.

Gordon, L. M., & Garrie, D. B. (2020). *Cybersecurity & the Courthouse: safeguarding the judicial process*. New York: Wolters Kluwer.

Hino, M. C., & Cunha, M. A. (2020). Adoção de tecnologias na perspectiva de profissionais de direito. *Revista Direito GV, v. 16*(n. 1), e1952. doi:10.1590/2317-6172201952

Hirata, A., & Oliveira, C. G. (2022). *39 dias após o ataque cibernético ao STJ: reflexões e desafios*. Acesso em 22 de Maio de 2022, disponível em Migalhas: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/337701/39-dias-apos-o-ataque-cibernetico-ao-stj--reflexoes-e-desafios

Joint Technology Committee. (2019). Cybersecurity Basics for Courts. Conference of State Court Administrators (COSCA), National Association for Court Management (NACM) and the National Center for State Courts (NCSC). Fonte: https://www.ncsc.org/__data/assets/pdf_file/0037/68887/JTC-2021-05-Cybersecurity-QR_Final-Clean.pdf

Leite, R. V. (2021). Poder Judiciário e meio de comunicação: do dever de transparência aos riscos de exposição midiática. *ReJuB - Revista Judicial Brasileira, 1*(1), 205-226. doi:10.54795/rejub.n.1.83

Lima, E. d., Moreira, F. R., de Deus, F. E., Nze, G. D., De Sousa, R. T., & Nunes, R. R. (2022). Avaliação da Rotina Operacional do Operador Nacional do Sistema Elétrico Brasileiro (ONS) em Relação às Ações de Gerenciamento de Riscos Associados à Segurança Cibernética. *RISTI (PORTO), E49*, 301-312.

Machado, M. B. (2018). Taxonomia de eventos de risco operacional do Poder Judiciário. Brasília, Distrito Federal, Brasil. Fonte: http://repositorio.enap.gov.br/handle/1/3399

Martins, T. d. (2021). Acesso à Justiça e pandemia. *Revista Jus Navegandi, 6412*. Acesso em 21 de maio de 2022, disponível em https://jus.com.br/artigos/88048/acesso-a-justica-e-pandemia

MITRE Corporation. (2021). *MITRE ATT&CK*. Acesso em 25 de maio de 2022, disponível em MITRE: https://attack.mitre.org/matrices/enterprise/

Moreira, F. R., Da Silva Filho, D. A., Nze, G. D., De Sousa Junior, R. T., & Nunes, R. R. (2021). Evaluating the Performance of NIST's Framework Cybersecurity Controls Through a Constructivist Multicriteria Methodology. *IEEE Access, 9*, 129605-129618. doi: 10.1109/access.2021.3113178

Moura, R. M., & Borges, L. (2022). *A impunidade dos hackers que colocaram o Judiciário de joelhos*. Acesso em 19 de maio de 2022, disponível em: https://veja.abril.com.br/politica/a-impunidade-dos-hackers-que-colocaram-o-judiciario-de-joelhos/

NIST. (2022). *NIST Cybersecurity Framework*. (National Institute of Standards and Technology) Acesso em 25 de maio de 2022, disponível em NIST: https://www.nist.gov/cyberframework/framework

Nunes, R. R., Perini, M. T., & Pinto, I. E. (2022). A gestão de riscos como instrumento para a aplicação efetiva do Princípio Constitucional da Eficiência. *Revista Brasileira de Políticas Públicas, 11*, 259-281. doi:10.5102/rbpp.v11i3.7903

Reina, E. (2022). *Ameaça Virtual - Em 18 meses, hackers violaram sistemas de tribunais no Brasil a cada 41 dias*. (Revsita Consultor Jurídico) Acesso em 22 de maio de 2022, disponível em Conjur: https://www.conjur.com.br/2022-abr-15/onda-invasoes-hackers-estruturas-tecnologicas-tribunais

Rover, A. J. (2015). O E-Judiciário no Brasil: Uma Bibliometria Temática. *Conpedi Law Review, 1*, p. 155. doi:10.26668/2448-3931_conpedilawreview/2015.v1i9.3376

Silva, E. L., & Menezes, E. M. (2005). *Metodologia da Pesquisa e Elaboração de Dissertação*. Florianópolis, Santa Catarina, Brasil: Universidade Federal de Santa Catarina.

Supremo Tribunal Federal. (2018a). Acesso em 8 de setembro de 2022, disponível em portal.stf.jus.br: https://portal.stf.jus.br/textos/verTexto.asp?servico=centralDoCidadaoAcessoInformacaoGestaoEstrategica

Supremo Tribunal Federal. (2018b). *Cadeia de Valor*. Acesso em 1 de junho de 2022, disponível em http://www.stf.jus.br/arquivo/cms/intranetAGE/anexo/MapProcessos/CadeiaValor/CadeiadevalorSTF2018.pdf

Supremo Tribunal Federal. (2022). *Resolução nº 781/2022*.

Tribunal Regional Federal da 3ª Região. (2021). *Justiça Federal condena hackers por falsificação de documento público em sistema processual*. (Assessoria de Comunicação Social do TRF3) Acesso em 19 de maio de 2022, disponível em TRF3: https://web.trf3.jus.br/noticias-sjms/Noticiar/ExibirNoticia/48-justica-federal-condena-hackers-por-falsificacao-de

Wanderley, D. L. (2020). Um framework para o gerencimaento de riscos em segurança da informação no Poder Judiciário do Tocantins. Palmas, Tocantins, Brasil: Universidade Federal do Tocantins. Fonte: http://hdl.handle.net/11612/2388

Yana, F., & Xu, K. (2019). Methodology and case study of quantitative preliminary hazard analysis based on cloud model. *Journal of Loss Prevention in the Process Industries, 60*, pp. 116-124. doi:10.1016/j.jlp.2019.04.013