DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Proposta de uma Linha de Base de Controles de Segurança da Informação para Mitigação dos Riscos de Negócio do Poder Judiciário Brasileiro

Renato Solimar Alves

Programa de Pós-Graduação Profissional em Engenharia Elétrica
DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Proposta de uma Linha de Base de Controles de Segurança da Informação para Mitigação dos Riscos de Negócio do Poder Judiciário Brasileiro

Renato Solimar Alves

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Prof. Rafael Rabelo Nunes, Dr., ADM/FACE/UnB _____
Orientador

Prof. Joao Souza Neto, Dr., FT/UnB _____
Examinador Interno

Profa. Trícia Navarro Xavier Cabral, Dra., UFES _____
Examinador Externo

Fábio Lúcio Lopes de Mendonça, Dr., FT/UnB _____
Examinador interno substituto

FICHA CATALOGRÁFICA

ALVES, RENATO SOLIMAR
Proposta de uma Linha de Base de Controles de Segurança da Informação para Mitigação dos Riscos de Negócio do Poder Judiciário Brasileiro [Distrito Federal] 2024.
xvi, 180 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2024).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Gestão de Riscos
2. Segurança Cibernética
3. Segurança da Informação
4. Poder Judiciário
I. ENE/FT/UnB
II. Título (série)

PUBLICAÇÃO: PPEE.MP.066

REFERÊNCIA BIBLIOGRÁFICA

ALVES, R. S. (2024). *Proposta de uma Linha de Base de Controles de Segurança da Informação para Mitigação dos Riscos de Negócio do Poder Judiciário Brasileiro*. Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 180 p.
PUBLICAÇÃO: PPEE.MP.066

CESSÃO DE DIREITOS

AUTOR: Renato Solimar Alves
TÍTULO: Proposta de uma Linha de Base de Controles de Segurança da Informação para Mitigação dos Riscos de Negócio do Poder Judiciário Brasileiro.
GRAU: Mestre em Engenharia Elétrica ANO: 2024

É concedida à Universidade de Brasília permissão para reproduzir cópias desta Dissertação de Mestrado e para emprestar ou vender tais cópias somente para propósitos acadêmicos e científicos. Do mesmo modo, a Universidade de Brasília tem permissão para divulgar este documento em biblioteca virtual, em formato que permita o acesso via redes de comunicação e a reprodução de cópias, desde que protegida a integridade do conteúdo dessas cópias e proibido o acesso a partes isoladas desse conteúdo. O autor reserva outros direitos de publicação e nenhuma parte deste documento pode ser reproduzida sem a autorização por escrito do autor.

Renato Solimar Alves
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Dedico este trabalho aos guardiões da defesa cibernética, os heróis anônimos que operam na linha de frente deste campo dinâmico e desafiador. Esses especialistas, armados com conhecimento técnico avançado e um compromisso inabalável, permanecem em constante estado de vigilância. Eles enfrentam um panorama de ameaças que evolui rapidamente, adaptando-se continuamente para defender contra ataques cibernéticos sofisticados e multifacetados. Apesar de suas contribuições serem cruciais na prevenção de inúmeras incursões digitais, sua atuação é frequentemente subestimada e reconhecida apenas em momentos de crise, quando um ataque *hacker* consegue penetrar suas barreiras. Esta dedicatória busca não apenas homenagear, mas também trazer luz à dedicação, ao sacrifício pessoal e ao conhecimento desses profissionais, que operam nos bastidores para garantir a integridade e a segurança do nosso mundo digital.

Além disso, dedico este trabalho especialmente aos meus pais, verdadeiros pilares de amor, apoio e inspiração em minha jornada. Meu pai, com sua habilidade única de plantar a semente da curiosidade e da análise de problemas práticos, me ensinou o valor da persistência. Minha mãe, com seu carinho e alegria inesgotáveis, nutriu essas sementes, fazendo-as crescer e florescer. Em cada obstáculo que enfrentei, foi na sabedoria de suas palavras e na força de seus exemplos que encontrei inspiração para seguir adiante. Esta conquista é tanto deles quanto minha, e uma verdadeira manifestação do sacrifício, do amor incondicional e da fé constante que depositaram em mim. A eles, minha eterna gratidão e amor, por serem a bússola que me guia, não apenas nesta jornada acadêmica, mas em todos os caminhos da vida.

AGRADECIMENTOS

Agradeço imensamente à minha esposa pelo apoio e pelos sacrifícios feitos durante este percurso. Sua força foi essencial não só para superar os desafios desta jornada acadêmica, mas também para enfrentar as adversidades da vida, permitindo a realização deste trabalho. Aos meus amados filhos, Júlia e Davi, expresso meu agradecimento pelo sacrifício do nosso convívio e das brincadeiras nos finais de semana. A alegria e o carinho de vocês foram a motivação para seguir em frente, mesmo nos momentos mais desafiadores.

Um agradecimento especial é direcionado aos participantes das entrevistas, cujas experiências e conhecimentos foram fundamentais para enriquecer este estudo. Sua confiança e disposição em compartilhar suas vivências trouxeram um valor imensurável a este trabalho.

Aos membros do grupo focal, meus estimados companheiros no campo da segurança da informação, segurança cibernética e gestão de riscos, estendo minha gratidão pela parceria e pelo apoio contínuo na construção desta pesquisa. A colaboração de cada um de vocês foi vital para o desenvolvimento e sucesso deste projeto.

Agradeço sinceramente aos meus amigos, colegas de trabalho, Divailton Teixeira, Tiago Peixoto, Lúcio Melre e Dra. Simone Lemos Fernandes, que em diferentes momentos desempenharam papéis de liderança profissional durante a realização deste trabalho. O incentivo e o apoio de vocês foram fundamentais para o início e a continuidade deste projeto, especialmente diante dos inúmeros desafios que enfrentamos em nosso ambiente de trabalho dinâmico.

Gostaria também de expressar minha gratidão ao Nélio Alves pelo apoio na análise comparativa de ferramentas de *business intelligence* e pela orientação e assistência na exploração das funcionalidades da solução escolhida.

Por fim, quero estender meu sincero agradecimento aos professores, colegas de estudo e pesquisa do Programa de Pós-Graduação em Engenharia Elétrica (PPEE). À professora Edna Canedo, devo minha entrada no programa e reconheço sua importância como minha primeira mentora nesta jornada. Agradeço especialmente ao professor e orientador Rafael Rabelo, cuja serenidade, generosidade e visão foram essenciais para o sucesso desta empreitada conjunta. Seu apoio e orientação foram como faróis que iluminaram cada etapa deste trabalho, guiando-me na busca por este importante marco.

RESUMO

O Poder Judiciário Brasileiro, responsável por funções vitais como o controle de constitucionalidade, condução do processo eleitoral, gestão de elevados valores em depósitos judiciais e precatórios, e manuseio de um grande volume de informações sensíveis de pessoas e organizações, enfrenta novos desafios com a digitalização intensiva de seus serviços. Riscos cibernéticos emergentes incluem interrupções nas prestação jurisdicional, emissões indevidas de sentenças, desvios de valores e a inserção de conteúdo inadequado de decisões. Este estudo visa propor um conjunto de medidas de controle de segurança da informação necessárias para mitigar os mais proeminentes riscos às funções essenciais da Justiça. A metodologia aplicada engloba revisão bibliográfica e entrevistas com profissionais das áreas jurídica, de tecnologia da informação, gestão de riscos e segurança cibernética. Foi adotado um *framework* de referência para a seleção de controles, complementado por medidas adicionais específicas ao contexto judiciário, e realizadas sessões de grupo focal para análise e revisão dos resultados. A Técnicas de classificação, análise de dados e *business intelligence* foram empregadas para auxiliar no diagnóstico de prioridades. Os resultados apontam para os 10 riscos de negócio mais relevantes, 40 causas potenciais, 22 consequências impactantes, além de 232 medidas de segurança para mitigação dos riscos, com ênfase no diagnóstico de ações e de prioridades de implementação. Este trabalho oferece uma contribuição para a gestão de riscos e o estabelecimento de estratégias de segurança da informação no Judiciário, aprimorando a comunicação entre as áreas técnicas e a alta administração e fornecendo uma visão detalhada para direcionar e otimizar os investimentos em segurança da informação, com recomendações práticas e adaptáveis a diferentes contextos institucionais.

ABSTRACT

The Brazilian Judiciary, responsible for vital functions such as constitutional control, electoral process management, handling of significant values in judicial deposits and court orders, and managing a large volume of sensitive information from individuals and organizations, faces new challenges with the intensive digitalization of its services. Emerging cyber risks include interruptions in judicial services, wrongful issuance of sentences, diversion of funds, and inappropriate insertion of content in decisions. This study aims to propose a set of information security control measures necessary to mitigate the most prominent risks to the essential functions of Justice. The applied methodology encompasses bibliographic review and interviews with professionals from the legal, information technology, risk management, and cybersecurity areas. A reference framework was adopted for the selection of controls, complemented by additional measures specific to the judicial context, and focus group sessions were conducted for analysis and validation of the results. Classification techniques, data analysis, and business intelligence were employed to assist in the diagnosis of priorities. The results point to the 10 most relevant business risks, 40 potential causes, and 22 impactful consequences, in addition to 232 security measures for risk mitigation, with an emphasis on diagnosing actions and implementation priorities. This work provides a contribution to risk management and

the establishment of information security strategies in the Judiciary, improving communication between technical areas and top management, and offering a detailed view to direct and optimize investments in information security, with practical recommendations adaptable to different institutional contexts.

SUMÁRIO

1 INTRODUÇÃO 1
1.1 MOTIVAÇÃO E JUSTIFICATIVA 2
1.2 PROBLEMA DE PESQUISA 4
1.3 OBJETIVOS 5
1.3.1 OBJETIVO GERAL 5
1.3.2 OBJETIVOS ESPECÍFICOS 5
1.4 RESULTADOS ESPERADOS 5
1.5 METODOLOGIA DE PESQUISA 6
1.6 PUBLICAÇÕES RESULTANTES DESSA PESQUISA 7
1.7 ESTRUTURA DA DISSERTAÇÃO 7

2 REFERENCIAL TEÓRICO 9
2.1 RISCO 9
2.2 CATEGORIAS DE RISCO 10
2.3 GESTÃO DE RISCOS 12
2.4 PROCESSO DE AVALIAÇÃO DE RISCOS 17
2.4.1 IDENTIFICAÇÃO DE RISCOS 20
2.4.2 ANÁLISE DE RISCOS 21
2.4.3 AVALIAÇÃO DE RISCOS 23
2.5 TRATAMENTO DE RISCOS 25
2.6 SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA 26
2.7 CONTROLES DE SEGURANÇA 31
2.8 FRAMEWORKS DE SEGURANÇA 32
2.8.1 ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA DO PODER JUDICIÁRIO - ENSEC-PJ 35
2.9 ATIVIDADES E PROCESSOS DE NEGÓCIO DOS TRIBUNAIS 35
2.10 TRABALHOS CORRELATOS 38

3 METODOLOGIA 42

4 ANÁLISE DE RESULTADOS 49
4.1 FASE 1 49
4.1.1 ATIVIDADES PRINCIPAIS 49
4.1.2 RISCOS DE NEGÓCIO 50
4.1.3 CAUSAS DOS RISCOS DE NEGÓCIO 52
4.1.4 CONSEQUÊNCIAS DOS RISCOS DE NEGÓCIO 56
4.2 FASE 2 61
4.2.1 SELEÇÃO DE *Framework* 61

4.2.2 Controles de Segurança da Informação 61
4.3 Fase 3 92
4.3.1 Funções de segurança 92
4.3.2 Categorização dos controles 92
4.3.3 Tipos de ativos 98
4.3.4 Prioridades de implantação 100
4.4 Avaliação e aplicação da proposta 104

5 Considerações finais 106

REFERÊNCIAS BIBLIOGRÁFICAS 110

Apêndices 119
I.1 Causas e consequências dos riscos de negócio 119
I.2 Classificações dos controles 130
.3 Painéis de Business Intelligence - BI 176

LISTA DE FIGURAS

2.1 Categorias de risco. 11
2.2 Tipos de risco 12
2.3 Visão COSO da gestão de riscos alinhada à estratégia e aos resultados. 13
2.4 Abordagem de gestão de risco em toda organização 14
2.5 Princípios, estrutura e processo de gestão de risco. 15
2.6 Processo de gestão de risco. 16
2.7 Fatores-chave de sucesso para a gestão de riscos. 16
2.8 Processo de avaliação de riscos. 17
2.9 Modelo de interligação dos estágios de informação dos riscos de decisão. 19
2.10 Exemplo de matriz de risco resultante da análise de riscos. 24
2.11 Relacionamento entre segurança de TI, segurança da informação e segurança cibernética. ... 28
2.12 Relacionamento entre segurança de TI, segurança da informação e segurança cibernética. ... 29
2.13 Cadeia de Valor do STF. 36
2.14 3º Nível da Cadeia de Valor do TJPR. 36
2.15 Cadeia de Valor do TJDFT. 37
2.16 Cadeia de Valor do STJ. 37

3.1 Primeira fase da pesquisa. 43
3.2 Primeira fase da pesquisa. 44
3.3 Segunda fase da pesquisa. 46
3.4 Terceira fase da pesquisa. 47

4.1 Causas e consequências de um risco de negócio. 55
4.2 Relacionamento entre controles de segurança da informação e consequências dos riscos de negócio. 56
4.3 Distribuição dos controles conforme a sua função. 93
4.4 Distribuição dos controles por categoria. 95
4.5 Distribuição das categorias dos controles CIS. 96
4.6 Distribuição das categorias dos controles adicionais. 97
4.7 Visão alternativa das categorias agrupando Estratégia, Gestão e Processos. 97
4.8 Tipos de ativo 100
4.9 Relação entre os tipos de ativos e as categorias dos controles 101
4.10 Distribuição dos controles por prioridade de implantação. 102
4.11 Relações entre controles do grupo 1, categorias e ativos 103
4.12 Relações entre controles do grupo 2, categorias e ativos 103
4.13 Relações entre controles do grupo 3, categorias e ativos 104

1 Visão geral 176
2 Relações das causas dos riscos de negócio 176
3 Total de consequências por risco de negócio 177

4 Painel geral para filtragem e seleção de controles por meio da associação entre categoria do controle, ativo envolvido, função de segurança e prioridade de implantação. 177
5 Relações entre categorias dos controles e tipos de ativos. 178
6 Relações entre funções de segurança e prioridades de implantação. 178
7 Painel geral de interações entre as classificações dos controles. 179
8 Quantidade de controles relacionados com cada consequência dos riscos de negócio. 179
9 Quantidade de controles por cada risco operacional. 180

LISTA DE TABELAS

2.1 Sumário de uso do termo *cybersecurity* 30

4.1 Atividades Principais do Poder Judiciário 49
4.1 Atividades Principais do Poder Judiciário 50
4.2 Riscos de Negócio do Poder Judiciário 51
4.3 Causas dos Riscos de Negócio 52
4.3 Causas dos Riscos de Negócio 53
4.3 Causas dos Riscos de Negócio 54
4.4 Consequências dos Riscos de Negócio 57
4.5 Controles de Segurança oriundos do CIS Controls 62
4.5 Controles de Segurança oriundos do CIS Controls 63
4.5 Controles de Segurança oriundos do CIS Controls 64
4.5 Controles de Segurança oriundos do CIS Controls 65
4.5 Controles de Segurança oriundos do CIS Controls 66
4.5 Controles de Segurança oriundos do CIS Controls 67
4.5 Controles de Segurança oriundos do CIS Controls 68
4.5 Controles de Segurança oriundos do CIS Controls 69
4.5 Controles de Segurança oriundos do CIS Controls 70
4.5 Controles de Segurança oriundos do CIS Controls 71
4.5 Controles de Segurança oriundos do CIS Controls 72
4.5 Controles de Segurança oriundos do CIS Controls 73
4.5 Controles de Segurança oriundos do CIS Controls 74
4.5 Controles de Segurança oriundos do CIS Controls 75
4.5 Controles de Segurança oriundos do CIS Controls 76
4.5 Controles de Segurança oriundos do CIS Controls 77
4.5 Controles de Segurança oriundos do CIS Controls 78
4.6 Controles de Segurança Adicionais 80
4.6 Controles de Segurança Adicionais 81
4.6 Controles de Segurança Adicionais 82
4.6 Controles de Segurança Adicionais 83
4.6 Controles de Segurança Adicionais 84
4.6 Controles de Segurança Adicionais 85
4.6 Controles de Segurança Adicionais 86
4.6 Controles de Segurança Adicionais 87
4.6 Controles de Segurança Adicionais 88
4.6 Controles de Segurança Adicionais 89
4.6 Controles de Segurança Adicionais 90

1 Relação entre causas e consequências dos riscos de negócio 119

2 Categorias dos controles 130

LISTA DE ABREVIATURAS E SIGLAS

AAA	Autenticação, Autorização e Auditoria
ABNT	Associação Brasileira de Normas Técnicas
ADM	Departamento de Administração
AGU	Advocacia Geral da União
ALARP	*As Low As Reasonably Practicable* (tão baixo quanto razoavelmente praticável)
API	*Application Programming Interface* (interface de programação de aplicação)
ATT&CK	*Adversarial Tactics, Techniques, and Common Knowledge* (táticas, técnicas e conhecimentos comuns adversários)
CD	*Compact Disc*
CEPEJ	*Council of Europe European Commission for the efficiency of justice*
CIS	*Center for Internet Security*
CISO	*Chief Information Security Officer*
CJF	Conselho da Justiça Federal
CNJ	Conselho Nacional de Justiça
CNSSI	*Committee on National Security Systems Instruction*
COBIT	*Control Objectives for Information and Related Technologies*
COSCA	*Conference of State Court Administrators*
COSO	*Committee of Sponsoring Organizations of the Treadway Commission*
CPS	*Cyber-Physical Systems*
CSF	*Cybersecurity Framework*
CSP	Cloud Service Provides (provedor de serviço de nuvem)
CyBOK	*The Cyber Security Body of Knowledge*
DDoS	*Distributed Denial of Service*
DHCP	*Dynamic Host Configuration Protocol*
DKIM	*DomainKeys Identified Mail*
DLL	*Dynamic-link library*
DLP	*Data Loss Prevention* (Prevenção de Perda de Dados)
DMARC	*Domain-based Message Authentication, Reporting and Conformance*
DNS	*Domain Name System* (sistema de nomes de domínio)
EDR	*Endpoint Detection and Response*
ENAJUS	Encontro Nacional de Administração de Justiça
ENE	Departamento de Engenharia Elétrica
ENISA	*European Union Agency for Cybersecurity*
ENSEC-PJ	Estratégia Nacional de Segurança Cibernética do Poder Judiciário

EUA	Estados Unidos da América
ERM	*Enterprise Risk Management* (gestão de risco empresarial)
FACE	Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas
FBI	*Federal Bureau of Investigation*
HAZOP	*Hazard and Operability Study* (análise de perigos e operabilidade)
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
IA	Inteligência Artificial
ICS	*Industrial Communication System* (sistema de controle industrial)
IEC	*International Electrotechnical Commission*
IG	*Implementation Group* (grupo de implementação)
ISAC	*Information Sharing and Analysis Center (centro de compartilhamento e análise de informações*)
ISACA	*Information Systems Audit and Control Association*
IoT	*Internet of Things* (internet das coisas)
IP	*Internet Protocol* (protocolo de internet)
ISO	*International Organization for Standardization*
ITU-T	*International Telecommunication Union Telecommunication Standardization Sector*
JTC1	*Joint Technical Committee on Information technology of ISO and IEC*
JTC	*Joint Technology Committee*
MFA	*MultiFactor Authentication* (autenticação multifator)
MITRE	*MITRE Corporation*
MPF	Ministério Público Federal
MDM	*Mobile Device Management* (gestão de dispositivos móveis)
MPU	Ministério Público da União
NaaS	*Network-as-a-Service*
NACM	*National Association for Court Management*
NBR	Norma Técnica Brasileira
NCSC	e *National Center for State Courts*
NIDS	Network Intrusion Detection System (sistema de detecção de intrusão de rede)
NIPS	Network Intrusion Prevention System (sistema de prevenção de intrução de rede)
NIST	*National Institute of Standards and Technology*
OCX	*OLE Control Extension*
OpenSSH	*Open Secure Shell*
OTAN	Organização do Tratado do Atlântico Norte
OWASP	*Open Worldwide Application Security Project*
PF	Polícia Federal
PGCRC-PJ	Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário
PMI	*Project Management Institute*

PPEE	Programa de Pós-Graduação Profissional em Engenharia
RISTI	Revista Ibérica de Sistemas e Tecnologias de Informação
RMF	*Risk Management Framework*
SASE	*Secure Access Service Edge*
SCAP	*Security Content Automation Protocol*
SGSI	Sistema de Gestão de Segurança da Informação
SIEM	*Security Information and Event Management* (Sistema de Gestão de Eventos e Informações de Segurança)
SO	*Shared objects*
SP	*Special Publication*
SPF	*Sender Policy Framework*
SRA	*Society for Risk Analysis*
SSH	*Secure Shell*
SSO	*Single Sign-On* (login único)
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
STM	Superior Tribunal Militar
SWOT	*Strengths, Weaknesses, Opportunities, Threats* (forças, fraquezas, oportunidades, ameaças)
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
TLS	*Transport Layer Security*
TRF1	Tribunal Regional Federal da 1ª Região
TSE	Tribunal Superior Eleitoral
TST	Tribunal Superior do Trabalho
UnB	Universidade de Brasília
VPN	*Virtual Private Network*
URL	*Uniform Resource Locator*
WPA2	*Wi-Fi Protected Access 2*

1 INTRODUÇÃO

O Poder Judiciário Brasileiro, em seus diversos ramos, desempenha funções cruciais para o Estado, sendo essencial para a estabilidade e harmonia social. Suas responsabilidades incluem o controle de constitucionalidade e legalidade, gerenciamento do processo eleitoral, e a administração de depósitos judiciais e precatórios significativos [1]. Além disso, as entidades judiciárias lidam rotineiramente com vasta informação confidencial de indivíduos e organizações [2].

Esses processos e atividades críticas dependem substancialmente de sistemas de informação, utilizados por magistrados, servidores e colaboradores. A adoção de meios eletrônicos de processamento da informação trouxe avanços indiscutíveis, essenciais para o aumento da produtividade e celeridade do Judiciário [3]. Assim, os sistemas eletrônicos tornaram-se ativos valiosos e estratégicos, essenciais para enfrentar os desafios presentes e atender às expectativas impostas ao Poder Judiciário, visando a razoável duração do processo e garantia do direito constitucional da privacidade dos cidadãos [4] [5].

O Poder Judiciário do Brasil experimentou uma relevante transformação do seu sistema judicial, impulsionada pela adoção extensiva de tecnologias digitais nos processos judiciais. Essa mudança, caracterizada principalmente pela implementação do processo eletrônico, contribuiu substancialmente para a agilização da distribuição e tramitação de processos judiciais. Além disso, observou-se um aumento na produtividade, refletido no maior volume de decisões judiciais emitidas. Este avanço tecnológico resultou em uma maior celeridade processual e na melhoria da eficiência na prestação dos serviços jurisdicionais [4] [6] [7].

A pandemia de COVID-19 funcionou como um catalisador para a já em curso transformação tecnológica no sistema de Justiça, intensificando a adoção de inovações tecnológicas. Um aspecto notável deste avanço foi o aumento substancial no uso de videoconferências e audiências virtuais [8], facilitando a continuidade dos processos judiciais em um contexto de restrições físicas. Além disso, a implementação de citações por meios eletrônicos, o atendimento ao público através de 'balcões virtuais', e a aplicação de inteligência artificial na análise processual [9] representam marcos significativos na direção de um sistema judiciário mais ágil e adaptado às demandas contemporâneas

Nesse contexto, a tecnologia, anteriormente reconhecida como um elemento crítico, ascende a um papel de protagonismo indiscutível na concretização dos objetivos estratégicos do Judiciário e na entrega eficiente de serviços jurisdicionais ao cidadão [10]. Esta evolução, embora represente um avanço relevante, traz consigo uma gama de novos desafios e riscos. Os benefícios da tecnologia são inegáveis, mas sua implementação também introduz complexidades adicionais e potenciais vulnerabilidades que precisam ser cuidadosamente geridas [11].

As instituições que compõem o sistema de Justiça estão expostas a uma extensa variedade de riscos, cada qual com suas causas específicas e com a possibilidade de desencadear consequências severas para as próprias instituições, seus servidores, e para a sociedade em geral. Diante deste cenário, torna-se imperativo que tais órgãos adotem uma abordagem proativa e estratégica na mitigação de riscos por meio da adoção de medidas rigorosas de proteção de informações e dados [10] [2].

O acentuado crescimento no número e na severidade dos ataques cibernéticos nos últimos anos des-

taca a urgência de uma gestão eficaz da segurança cibernética [12]. Relatórios recentes, como o de crimes cibernéticos do FBI (IC3) [13], revelam que a pandemia global intensificou a dependência de recursos tecnológicos, oferecendo aos criminosos uma oportunidade para ampliar seus ataques pela internet. De acordo com esse relatório, os prejuízos causados por crimes cibernéticos em 2020 ultrapassaram 4 bilhões de dólares, representando um aumento alarmante de cerca de 70% em relação ao ano anterior. Notavelmente, o Brasil é apontado como um dos países mais afetados por crimes cibernéticos globalmente.

Além disso, a Agência para Segurança Cibernética da União Europeia (ENISA) em seu relatório do cenário de ameaças de 2022 [14], ressalta uma escalada contínua nos ataques cibernéticos, tanto em frequência quanto em gravidade, especialmente durante o segundo semestre de 2021 e o primeiro semestre de 2022. O relatório aponta que a crise entre Rússia e Ucrânia inaugurou uma nova fase na guerra cibernética e no *hacktivismo*, com expectativas de um aumento nos ataques patrocinados por Estados, trazendo consequências de grande magnitude.

No Brasil, a tendência é igualmente preocupante. A Check Point, em seu relatório sobre tendências de segurança do terceiro trimestre de 2022, observa que o Brasil enfrenta um volume de ataques semanais superior à média global, com um incremento de 37% em relação ao mesmo período do ano anterior. A Fortinet, por sua vez, reportou um aumento impressionante de 94% nas tentativas de ataques cibernéticos no Brasil no primeiro semestre de 2022, totalizando 31,5 bilhões de tentativas, em comparação com o primeiro semestre de 2021.

1.1 MOTIVAÇÃO E JUSTIFICATIVA

No Brasil, uma tendência preocupante tem sido a frequente ocorrência de ataques cibernéticos bem-sucedidos contra órgãos do Poder Judiciário. Esses ataques, ocorrendo com alarmante regularidade, têm se estabelecido como uma ameaça significativa à realização dos objetivos estratégicos do Judiciário e ao desempenho eficiente de suas funções essenciais. A repetição desses ataques hackers em diversos órgãos judiciários não apenas causou prejuízos tangíveis aos cidadãos e ao sistema judicial, mas também infligiu danos substanciais à reputação das instituições de justiça. Além disso, tais incidentes têm abalado a confiança do público no Judiciário, um pilar fundamental para a manutenção da ordem e da justiça. Diante dessa realidade, torna-se evidente que para o sistema de Justiça é fundamental garantir o mais alto nível de segurança cibernética como uma medida essencial para proteger não apenas as informações, mas também a integridade e a confiança na Justiça [15] [16] [17].

De acordo com a análise realizada por Reina [18], o período entre novembro de 2020 e abril de 2022 foi marcado por uma série de ataques cibernéticos significativos ao Poder Judiciário brasileiro. Neste período, pelo menos 13 tribunais de diferentes esferas e regiões sofreram ataques de grandes proporções que, em muitos casos, paralisaram completamente as atividades essenciais desses órgãos judiciários. Este padrão preocupante sugere que, em média, ocorreu um ataque cibernético de grande escala a cada 41 dias, afetando instituições judiciais importantes como o STJ, o TSE, o TRE do Espírito Santo, o TRT do Rio Grande do Sul, o TRF da 1ª Região, TJDFT, entre outros [19].

Além dos ataques que causam a interrupção dos serviços judiciais pela indisponibilidade de tecnologias

da informação ou pelo sequestro de dados, existem ameaças igualmente sérias e potencialmente mais prejudiciais. Estas incluem ataques que visam a alteração de informações críticas, explorando vulnerabilidades nos sistemas de informação judiciais essenciais para o funcionamento do Poder Judiciário. Tais ataques comprometem gravemente os atributos de *integridade* e *confidencialidade* das informações, resultando em consequências alarmantes. Alguns casos emblemáticos demonstram essas ameaças.

Um exemplo relevante ocorreu no Tribunal Regional Federal da 3ª Região, onde um hacker conseguiu acesso não autorizado ao sistema processual eletrônico. Este indivíduo alterou pareceres do Ministério Público, converteu sentenças de condenação em absolvições e redirecionou contas destinatárias para a transferência de valores em diferentes processos [15] [20].

Outro caso grave foi no Tribunal Regional do Trabalho da 1ª Região. Aqui, o fraudador manipulou mecanismos de acesso e processos internos para efetivamente desviar mais de 4 milhões de reais através de alvarás de levantamento de valores falsos [21] [22].

O Conselho Nacional de Justiça (CNJ) também sofreu uma invasão notória, onde documentos falsos foram inseridos no sistema, resultando na emissão de onze alvarás de soltura fraudulentos. Este incidente incluiu até a emissão de um falso mandado de prisão em desfavor do ministro Alexandre de Moraes do Supremo Tribunal Federal (STF), que supostamente teria sido emitido por ele mesmo [23].

A preocupação com os riscos de segurança da informação e seus impactos no Judiciário transcende fronteiras nacionais. Em um painel realizado no Congresso dos Estados Unidos, juízes federais enfatizaram que os ataques cibernéticos não só representam um risco para o sistema judicial americano, mas também constituem um ataque direto aos pilares da democracia [24]. Foi ressaltado que os sistemas de informática desatualizados do Judiciário são particularmente vulneráveis a tais ataques, aumentando o risco de exposição de materiais confidenciais, incluindo minutas de decisões judiciais. Um dos juízes destacou que, apesar de não ser o único setor que necessita de modernização, o Judiciário guarda algumas das informações mais sensíveis relacionadas à aplicação da lei e à segurança nacional nos EUA.

Esta discussão no Congresso Americano foi motivada em parte pelo vazamento de uma minuta de decisão da Suprema Corte dos EUA, um documento de extrema importância que mudava o entendimento de aproximadamente 50 anos sobre o aborto, um tema de grande relevância social. O rascunho da decisão vazado, com 98 páginas e 118 notas de rodapé, continha comentários preliminares não compatíveis com o teor de uma decisão final [25]. Este incidente foi descrito como sem precedentes e a pior violação de segurança no história do tribunal. Especulou-se que o vazamento poderia estar ligado a motivações políticas que buscava aumentar a pressão pública sobre os magistrados e assim levar a uma suavização da decisão final [26]. Embora as decisões finais sejam públicas, o vazamento de informações pré-decisórias é extremamente delicado e ressalta a urgência de proteger os sistemas de informação [24].

Dessa forma, torna-se fundamental realizar uma investigação aprofundada sobre quais são os riscos mais relevantes que estejam relacionados às atividades principais do Poder Judiciário Brasileiro. É essencial compreender as causas e os possíveis impactos desses riscos, bem como avaliar e implementar medidas de segurança apropriadas. Estas ações visam não apenas reduzir a probabilidade de ocorrência desses riscos, mas também minimizar seu impacto nas atividades essenciais do Judiciário, garantindo assim a integridade e a confiabilidade da Justiça.

1.2 PROBLEMA DE PESQUISA

A gestão de riscos é crucial na mitigação dos efeitos das incertezas sobre os objetivos de uma organização [27]. Neste contexto, a identificação adequada de riscos é fundamental. O processo de avaliação de riscos serve como um instrumento vital para identificar eventos de risco potenciais, avaliar suas probabilidades e impactos, e auxiliar na priorização dos riscos mais críticos [28] [29].

Posteriormente, o processo de resposta ou tratamento de riscos é essencial para definir as ações mais apropriadas em resposta aos riscos identificados, analisados e priorizados [30]. Este tratamento envolve o desenvolvimento de estratégias de controle concretas para manter os riscos em níveis aceitáveis. Os controles são fundamentais, pois é através deles que se estabelece a proteção necessária, utilizando uma combinação de procedimentos, estruturas organizacionais, práticas administrativas, e abordagens técnicas ou legais [31].

À medida que os sistemas e dispositivos de informação evoluem, tornando-se redes cada vez mais complexas e interconectadas, as questões de segurança e privacidade se tornam cada vez mais importantes. O aumento na complexidade no funcionamento dos ativos - incluindo questões de *hardware*, *software*, *firmware* e sistemas - expande a superfície de ataque, criando novas oportunidades para que atacantes explorem vulnerabilidades. Este cenário aumenta o risco de comprometimento da integridade dos sistemas e de acesso não autorizado a ativos críticos [32].

Para garantir a segurança adequada dos ativos de informação, a implementação de *frameworks* de segurança que delineiam práticas específicas é essencial. Por exemplo, o framework MITRE ATT&CK detalha as táticas, técnicas e procedimentos empregados por hackers em situações reais, abrangendo 14 táticas, 191 técnicas, 363 subtécnicas e uma vasta gama de procedimentos utilizados em ataques cibernéticos [33].

Existem outros *frameworks* que listam os controles de segurança necessários para se proteger contra as ameaças cibernéticas. 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 [32].

Diante da vasta quantidade de controles possíveis, torna-se crucial para o Poder Judiciário identificar aqueles mais relevantes para o tratamento de riscos específicos ao seu negócio. Uma linha de base de controles mínimos de segurança, alinhada com os riscos particulares do Judiciário, pode evitar a seleção aleatória de controles pelos gestores de segurança e a aplicação de *frameworks* genéricos desalinhados com as especificidades deste setor [34].

Assim, a identificação de controles de segurança da informação pertinentes para mitigar riscos específicos enfrentados pelo Poder Judiciário é fundamental [35]. Este processo facilitará a criação de uma base de referência de controles de segurança estrategicamente alinhados com os riscos inerentes ao negócio judicial, evitando a adoção de abordagens genéricas. A implementação de uma estratégia de segurança cibernética customizada e contextualizada é essencial para assegurar a eficácia e a relevância dos controles no ambiente único do Poder Judiciário.

Portanto, foi estabelecido o seguinte problema de pesquisa:

Problema: *Quais são os controles de segurança da informação que devem ser implementados para*

prevenir a ocorrência de eventos de risco que afetem as atividades principais do Poder Judiciário?

Com base neste problema, estabeleceu-se a seguinte hipótese:

Hipótese: *A definição de controles tecnológicos não é suficiente para a mitigação dos riscos de segurança da informação associados às atividades principais do Poder Judiciário.*

1.3 OBJETIVOS

1.3.1 Objetivo geral

O objetivo principal desta pesquisa é construir uma lista de controles de segurança da informação que sirva de referência para a aplicação de medidas que tenham o potencial de reduzir as probabilidades de eventos de risco que possam impactar negativamente nas atividades essenciais do judiciário brasileiro. Esta proposta poderá ser utilizada como um guia para a implementação de medidas de segurança no contexto específico do Judiciário.

1.3.2 Objetivos específicos

- Identificar as atividades principais do Poder Judiciário e que necessitam de maior proteção;
- Compreender os principais riscos de negócio associados a estas atividades;
- Entender a relação entre ações operacionais de segurança da informação e os riscos de negócio;
- Apontar, a partir de um *framework* internacional de referência, os controles de segurança que possuem o potencial de mitigar os riscos de negócio identificados;
- Auxiliar os órgãos judiciais na identificação de papéis, responsabilidades e ações prioritárias.

1.4 RESULTADOS ESPERADOS

Espera-se que os resultados deste estudo contribuam para a gestão de riscos e o aprimoramento das estratégias de segurança da informação no Poder Judiciário. Pretende-se também oferecer subsídios para aprimorar a comunicação entre as áreas técnicas e a alta administração, estabelecendo um diálogo mais eficiente, pautado na compreensão mútua dos desafios e requisitos em segurança da informação. Adicionalmente, o estudo proporcionará *insights* sobre a melhor maneira de direcionar e otimizar os investimentos em segurança da informação.

Acredita-se firmemente que as sugestões práticas e adaptáveis propostas possam ser implementadas em uma variedade de contextos institucionais. Ao adotar essas práticas, o Poder Judiciário poderá não só mitigar os riscos existentes de maneira mais eficaz, mas também antecipar e prevenir potenciais ameaças

futuras. Tal abordagem resultará não apenas na proteção efetiva dos dados e na continuidade das operações judiciais, mas também na consolidação de uma imagem mais robusta e confiável do Poder Judiciário perante a sociedade. Este estudo, portanto, tem o potencial de transformar como a segurança da informação é percebida e gerenciada no âmbito judiciário, conduzindo a uma nova era de segurança institucional.

1.5 METODOLOGIA DE PESQUISA

Este estudo se trata de uma pesquisa de natureza aplicada, com abordagem qualitativa e objetivo descritivo e exploratório. Sendo realizadas as seguintes etapas metodológicas em três fases distintas:

- **Fase 1** - pesquisa bibliográfica, definição das atividades principais, criar uma lista inicial de riscos com base em eventos históricos, seleção de perguntas e de entrevistados, realização de entrevistas semiestruturadas com gestores da área jurídica, de tecnologia da informação, de gestão de riscos e de segurança cibernética para identificação dos riscos de negócio, avaliação de causas e consequências de acordo com o método *bow tie* e validar os resultados por meio de sessão de grupo focal. **Resultado esperado para a fase**: identificar os principais riscos de negócio das atividades primordiais do Poder Judiciário, fatores geradores dos riscos e que consequências poderiam ser enfrentadas em caso de ocorrência do risco.
- **Fase 2** - revisão da bibliografia, seleção de *framework* de referência, revisão das entrevistas e compilação de controles eventualmente indicados, seleção de controles do *framework* aplicáveis, crítica e revisão dos controles propostos em sessões de grupo focal com especialistas de segurança da informação e gestão de riscos, verificação da necessidade de inclusão de controles adicionais e validação de resultados em sessão de grupo focal. **Resultado esperado para a fase**: realizar o levantamento das medidas de segurança que, se aplicadas, poderiam tratar os riscos.
- **Fase 3** - analise e normalização dos dados obtidos, categorização dos controles, classificação dos ativos e funções de segurança, avaliação de prioridades de implementação, utilizar técnicas de *business intelligence* e análise de dados. **Resultado esperado para a fase**: analisar os dados obtidos e buscar formas de apresentar os resultados de forma que auxilie os órgãos a definir responsáveis, ações prioritárias e melhorias que poderão ser perseguidas.

A metodologia será melhor detalhada no capítulo 3. Metodologia. Contudo, se antecipa que a sistemática adotada teve como objetivo propor medidas para a mitigação de riscos aplicáveis a todos os órgãos do Poder Judiciário. No entanto, buscou-se não revelar fragilidades ou riscos específicos das instituições envolvidas nas diversas etapas da pesquisa.

1.6 PUBLICAÇÕES RESULTANTES DESSA PESQUISA

1. Alves, Renato Solimar; Georg, Marcus Aurélio Carvalho; Nunes, Rafael Rabelo. **Judiciário sob ataque hacker: riscos de negócio para segurança cibernética em tribunais brasileiros**. Revista Ibérica de Sistemas e Tecnologias de Informação - RISTI, 2023. (Qualis A4)
2. Alves, Renato Solimar; Georg, Marcus Aurélio Carvalho; Nunes, Rafael Rabelo. **Judiciário sob ataque hacker: fatores de risco para a segurança do processo decisório em sistemas judiciais eletrônicos**. Encontro Nacional de Administração da Justiça - ENAJUS, 2022. *Eleito entre os melhores trabalhos da edição*.
3. Alves, Renato Solimar; Zottmann, Carlos Eduardo Miranda; Georg, Marcus Aurélio Carvalho; Nunes, Rafael Rabelo; Arruda, Luiz Guilherme Schiefler de. **Enfrentando os Ataques Hackers: Controles de Segurança da Informação Prioritários para o Tratamento dos Riscos de Negócio do Poder Judiciário**. Encontro Nacional de Administração da Justiça - ENAJUS, 2023.
4. Queiroz, Carlos Eduardo Mancini; Alves, Renato Solimar; Junior, Aldery Silveira; Cunha, José Humberto da Cruz; Nunes, Rafael Rabelo. **Os Tribunais do Distrito Federal Possuem Estruturas para Gerenciar Riscos de Segurança da Informação? Um Estudo à Luz das Três Linhas de Defesa**. Encontro Nacional de Administração da Justiça - ENAJUS, 2022.
5. Zottmann, Carlos Eduardo Miranda; Nunes, Rafael Rabelo; Georg, Marcus Aurélio Carvalho; Alves, Renato Solimar; Silva, Marcelo Antônio da. **Proposta de Metodologia para Avaliação de Riscos de Privacidade para Órgãos do Poder Judiciário no Brasil**. Encontro Nacional de Administração da Justiça - ENAJUS, 2023.

Artigo aceito para publicação:

- Alves, Renato Solimar; Queiroz, Carlos Eduardo Mancini; Nunes, Rafael Rabelo. **Os Tribunais possuem Estruturas para Gerenciar Riscos de Segurança da Informação? Um Estudo à Luz das Três Linhas**. Revista CEJ. (Qualis A2)

1.7 ESTRUTURA DA DISSERTAÇÃO

O presente trabalho segue a seguinte estrutura:

- Capítulo 1 - Introdução.
- Capítulo 2 - Referencial teórico: visa indicar os principais conceitos e trabalhos bibliográficos sobre:
  - Definição de risco e suas categorias;
  - Gestão de risco;

  - Processos de avaliação e de tratamento de riscos;
  - Segurança da informação e segurança cibernética;
  - Controles de segurança;
  - *Frameworks* de segurança;
  - Atividades e processos de negócio dos Tribunais;
  - Trabalhos correlatos.

- Capitulo 3 - Metodologia: descrição do método utilizado em cada etapa das três fases da pesquisa.
- Capítulo 4 - Análise e Discussão dos Resultados: apresentação das atividades principais, dos riscos de negócio, da análise de causas e consequências, dos riscos operacionais e dos controles de segurança recomendados pelo *framework* escolhido.
- Capítulo 5 - Conclusão: onde são apontadas as limitações do trabalho, as propostas de trabalhos futuros e as conclusões.
- Apêndice I.1 - Causas e consequências dos riscos de negócio: indicação da relação completa de todas as causas e consequências de cada risco de negócio.
- Apêndice I.2 - Classificações dos controles: apresentação da relação completa de todos os controles com a indicação em qual categoria este se enquadra, qual é o tipo de ativo relacionado ao controle, que função de segurança este exerce e qual é a prioridade de implantação da medida.

2 REFERENCIAL TEÓRICO

Neste capítulo, será desenvolvida uma exposição dos conceitos fundamentais que formam a base teórica deste trabalho. Inicialmente, será abordado o conceito de risco, explorando suas diversas categorias e a maneira como os riscos podem ser efetivamente gerenciados. Em seguida, discutiremos o processo de gestão de riscos, detalhando as etapas específicas que compõem esse processo.

Avançaremos para uma análise do conceito de segurança da informação e de segurança cibernética, enfatizando a importância dos controles e dos *frameworks* de segurança na proteção de dados e sistemas. Serão também exploradas os processos e atividades de negócio principais dos tribunais, destacando como estes se interconectam com as práticas de segurança da informação.

Por fim, apresentaremos uma revisão de trabalhos correlatos, proporcionando uma visão contextualizada das pesquisas e das práticas existentes no campo da segurança da informação e da gestão de riscos. Esta revisão visa não apenas estabelecer um ponto de referência para o presente estudo, mas também identificar lacunas de conhecimento e oportunidades para contribuições originais.

2.1 RISCO

O risco é um elemento que permeia todas as esferas da vida humana. Desde ações cotidianas, como se deslocar para o trabalho ou estudar, até decisões de maior envergadura, a natureza onipresente do risco é evidente. Esta exposição ao risco varia em intensidade; alguns riscos são mínimos, enquanto outros têm o potencial de alterar significativamente o curso da vida das pessoas [36].

Por outro lado, história humana é marcada por indivíduos e grupos que, ao enfrentarem riscos, impulsionaram a inovação. Para alcançar grandes feitos, muitas vezes é necessário se expor a um considerável nível de incerteza [37]. O desejo de eliminar riscos, tanto quanto a disposição para aproveitar oportunidades incertas, geraram muitas das invenções mais duradouras e avanços civilizatórios mais significativos [36].

Risco pode ser definido como o efeito da incerteza nos objetivos [38] [27]. Este efeito pode ser entendido como um desvio em relação a uma expectativa estabelecida. Importante destacar que o risco possui uma natureza dualística: pode ser positivo, o que indica uma oportunidade potencial, ou negativo, sugerindo uma ameaça. Portanto, os riscos envolvem os fatores e influências que criam incerteza quanto à realização dos objetivos pretendidos.

No contexto de segurança da informação, os riscos são frequentemente associados apenas a aspectos negativos. Os riscos se referem ao potencial de ameaças que podem explorar vulnerabilidades em um ativo ou conjunto de ativos de informação, resultando em danos para a organização [38] ou como a medida em que uma entidade está ameaçada por uma circunstância ou evento potencial [39].

No campo do estudo de risco existe também o entendimento de que a definição universal e unificada

de risco é irrealístico e que variações das definições devem ser aceitas e que podem variar conforme o contexto [40]. Este entendimento foi aplicado pela *Society for Risk Analysis (SRA)* durante a elaboração de seu glossário. A SRA [41] adota uma abordagem que reconhece a necessidade de definições oficiais, mas também aceita a variação dessas definições de acordo com o contexto. Algumas definições aceitas são:

- A possibilidade de ocorrências infelizes.
- O potencial de concretização de consequências negativas e indesejadas resultantes de um evento.
- A exposição a proposições incertas.
- As consequências e as incertezas associadas a uma atividade.
- A incerteza e a gravidade das consequências de uma atividade em relação a valores humanos.
- A ocorrência de consequências específicas de uma atividade e as incertezas relacionadas.
- O desvio em relação a um valor de referência e as incertezas associadas.

Esta abordagem multifacetada destaca a necessidade de compreender o risco em diferentes contextos e perspectivas. Essas definições refletem a compreensão de que o risco geralmente envolve a avaliação de atividades futuras e suas consequências potenciais, especialmente aquelas negativas ou indesejadas, em relação a valores importantes [40].

Portanto, sempre que um objetivo é estabelecido e existe algum grau de incerteza associado a ele, inevitavelmente, surge o risco [28]. Esta associação sublinha que o risco é um elemento inerente a qualquer planejamento ou decisão que envolva incertezas, não importa quão pequenas sejam.

2.2 CATEGORIAS DE RISCO

Os riscos nas organizações podem ser classificados em várias categorias principais. Essas categorias, ilustradas na Figura 2.1, refletem os diferentes aspectos e origens dos riscos que podem afetar uma organização [37].

Algumas das categorias de risco mencionadas por Crouhy et al. [37], que são diretamente relevantes para o escopo desta pesquisa, incluem:

- **Riscos operacionais:** abrangem perdas potenciais devido a sistemas inadequados, falhas de gerenciamento, controles deficientes, fraudes, erros humanos e riscos tecnológicos.
- **Riscos legais e regulatórios:** avaliam o impacto de mudanças legislativas e a possibilidade de contrapartes não terem autorização legal ou regulatória para transações específicas. Estes riscos estão intimamente relacionados aos riscos operacionais e de reputação.
- **Riscos de reputação:** são aqueles associados à confiança de que uma organização cumprirá seus compromissos, bem como a credibilidade quanto a execução de práticas justas

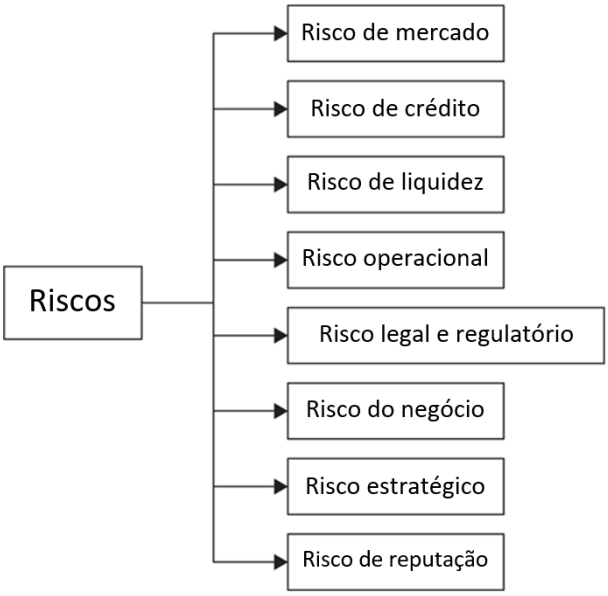


Figura 2.1: Categorias de risco.
Fonte: Adaptado de *The Essentials of Risk Management* [37].

e éticas. Envolvem a percepção pública da organização, podendo ser afetados por boatos na internet, notícias virais e comentários em plataformas digitais.

- **Riscos estratégicos:** envolvem os riscos relacionados a investimentos de alto valor com incertezas sobre sucesso e lucratividade, bem como mudanças estratégicas em relação aos concorrentes. Erros estratégicos geralmente prejudicam a reputação.
- **Riscos de negócio:** dizem respeito aos riscos clássicos do mundo dos negócios, como a incerteza sobre a demanda, o preço que pode ser cobrado ou o custo de produção e entrega. A gestão desses riscos em *frameworks* formais de gerenciamento pode ser desafiadora. Embora certamente devam ser avaliados e monitorados, não é óbvio identificar como fazê-lo.

É importante destacar que os riscos de negócio são profundamente influenciados por uma variedade de fatores, incluindo a qualidade da estratégia organizacional e a reputação da empresa no mercado. Uma prática comum na gestão de riscos é agrupar riscos estratégicos e riscos de reputação sob o amplo espectro dos riscos de negócio [37]. Esta abordagem enfatiza a natureza intrínseca e a interdependência entre estas categorias de risco, todas vitais para o sucesso e a sustentabilidade da organização, sugerindo que a análise e gestão de riscos devem considerar não apenas os elementos tangíveis e financeiros, mas também as complexas interações entre a estratégia adotada e a percepção da organização no cenário empresarial. Essa abordagem abrangente fortalece a compreensão das dinâmicas que moldam a resiliência e a sustentabilidade organizacional diante dos desafios inerentes ao ambiente de negócios.

Outra categorização de riscos é apresentada pelo *Risk Management Framework* do NIST RMF [39] que divide os riscos nas categorias descritas na Figura 2.2.

Os riscos operacionais são o tipo de risco associado a perdas diretas ou indiretas resultantes de pro-

Figura 2.2: Tipos de risco
Fonte: Adaptado de NIST *Risk Management Framework* [39]

cessos internos inadequados, falhas humanas ou sistêmicas, ou eventos externos [42]. Ou seja, abrange aspectos que não estejam diretamente ligados aos seus objetivos e atividades primários da instituição [43]. Por exemplo, em organizações bancárias todo e qualquer risco não relacionado à aspectos financeiros são definidos como risco operacional [44]. Os riscos relacionados aos objetivos das atividades de apoio ou secundárias são os riscos operacionais.

2.3 GESTÃO DE RISCOS

A gestão de riscos é definida de maneira geral como o conjunto de atividades coordenadas destinadas a orientar e controlar uma organização com relação aos riscos que enfrenta [45] [38].

Trata-se de um conjunto de ações proativas na qual as empresas conscientemente escolhem o tipo e o nível de risco que estão dispostas a aceitar. Semelhante à maioria das decisões de negócios, envolve o comprometimento de recursos atuais em antecipação a benefícios futuros incertos. A capacidade de fazer escolhas, avaliando o risco frente à potencial recompensa, está no centro do processo de gestão de todas as corporações de sucesso duradouro [37].

O processo decisório bem estruturado e informado por riscos, equilibra adequadamente os recursos disponíveis com os objetivos e aspirações de longo prazo da organização, sendo um significativo contribuinte para a formulação e o refinamento de estratégias.[46]. A gestão de riscos é parte intrínseca da governança e liderança organizacional, desempenhando um papel crucial na definição de estratégias, na realização de objetivos e na tomada fundamentada de decisões [27]. A Figura 2.3 representa visualmente este processo decisório que considera a integração da missão, visão e valores fundamentais com a gestão de riscos para impulsionar os objetivos e resultados globais das organizações [46] .

Figura 2.3: Visão COSO da gestão de riscos alinhada à estratégia e aos resultados.
Fonte: Tribunal de Contas da União [47]

A instituição de um programa robusto de gestão de riscos, juntamente com seus processos de apoio, é vital para o manejo efetivo dos riscos inerentes à segurança da informação dentro das operações da organização. A interconexão complexa entre as missões da organização, os processos de negócios relacionados e os sistemas de informação que dão suporte a essas atividades exige uma abordagem organizacional integrada para o gerenciamento destes riscos [48] [30]. Tal abordagem deve considerar não apenas os riscos individuais, mas também as suas inter-relações e o impacto cumulativo no alcance dos objetivos estratégicos da organização como um todo [46] [39].

Esta abordagem abrangente, que transcende as atividades operacionais, administrativas e de suporte e permeia a formulação estratégica da organização, é essencial para alinhar as práticas de gestão de riscos com a direção da entidade e envolver todos os níveis hierárquicos da organização [47] [30].

No topo da hierarquia, estão os executivos seniores e líderes, responsáveis pela visão e definição de metas e objetivos de alto nível. Estes indivíduos desempenham um papel crucial na orientação da estratégia de gestão de riscos, garantindo que ela esteja alinhada com os objetivos gerais da organização. No nível intermediário, encontram-se os líderes que são responsáveis pelo planejamento, execução e gestão de áreas ou projetos específicos. Estes gerentes intermediários atuam como um elo vital entre a estratégia de alto nível e a implementação prática no terreno, traduzindo os objetivos estratégicos em ações concretas e gerenciáveis. Por fim, no nível operacional, estão os indivíduos que implementam e mantêm os sistemas que suportam as missões e funções de negócios da organização. Estes colaboradores são os responsáveis por executar as políticas e procedimentos estabelecidos, desempenhando um papel crítico na mitigação dos riscos no dia a dia das operações [39].

A Figura 2.4 demonstra que a gestão de riscos afeta todos os aspectos das organizações e envolve as atividades de todos os níveis organizacionais [30]. Tornando-se a comunicação e os relatórios os fluxos de informação bidirecional multinível para garantir que o risco seja tratado em nível estratégico, tático e operacional.

Atuando dessa forma, a gestão de riscos torna-se um fator crucial para impulsionar resultados globais

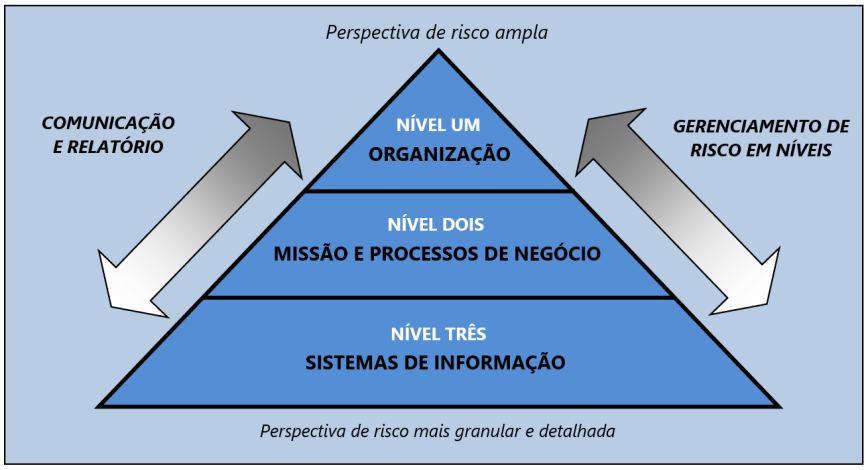


Figura 2.4: Abordagem de gestão de risco em toda organização
Fonte: NIST *Risk Management Framework* [39]

da organização e se torna um instrumento valioso para mitigar fatores que poderiam interferir no alcance dos resultados estratégicos pretendidos, oferecendo um retorno positivo frente aos investimentos realizados [46] [30].

Como destacado na Figura 2.5, a eficácia da gestão de riscos depende crucialmente da interdependência entre três componentes centrais [27]: *princípios*, localizados no círculo superior; *estrutura*, situada no círculo à esquerda; e *processo*, no círculo à direita. Os **princípios** são a base que define a abordagem de gerenciamento de riscos, enfatizando que o propósito principal é a criação e proteção de valor para a organização, mais do que ser um objetivo isolado. Esses princípios estabelecem a cultura e a mentalidade de risco dentro da organização, orientando todas as atividades relacionadas à gestão de riscos.

A **estrutura**, por sua vez, é um componente crítico para a eficácia da gestão de riscos, dependendo significativamente do comprometimento e da liderança da alta direção [27]. Esta estrutura proporciona a fundação e os arranjos organizacionais necessários para entender, gerenciar e comunicar efetivamente os riscos. Ela abrange políticas, responsabilidades e procedimentos que garantem a integração da gestão de riscos nas operações e processos organizacionais.

Finalmente, o *processo* de gestão de riscos, ilustrado no círculo à direita, envolve a aplicação prática dos princípios e estrutura. O **processo de gestão de riscos**, em sua aplicação prática, é direcionado para responder as seguintes perguntas fundamentais, conforme delineado pela ABNT NBR ISO/IEC 31010:2012 [49]:

- Quais eventos podem ocorrer e quais são suas causas subjacentes?
- Quais podem ser as consequências desses eventos?
- Qual é a probabilidade de ocorrência desses eventos?
- Existem estratégias ou medidas capazes de mitigar o impacto ou a probabilidade desses riscos?
- Até que ponto a organização está preparada para tolerar esses riscos?

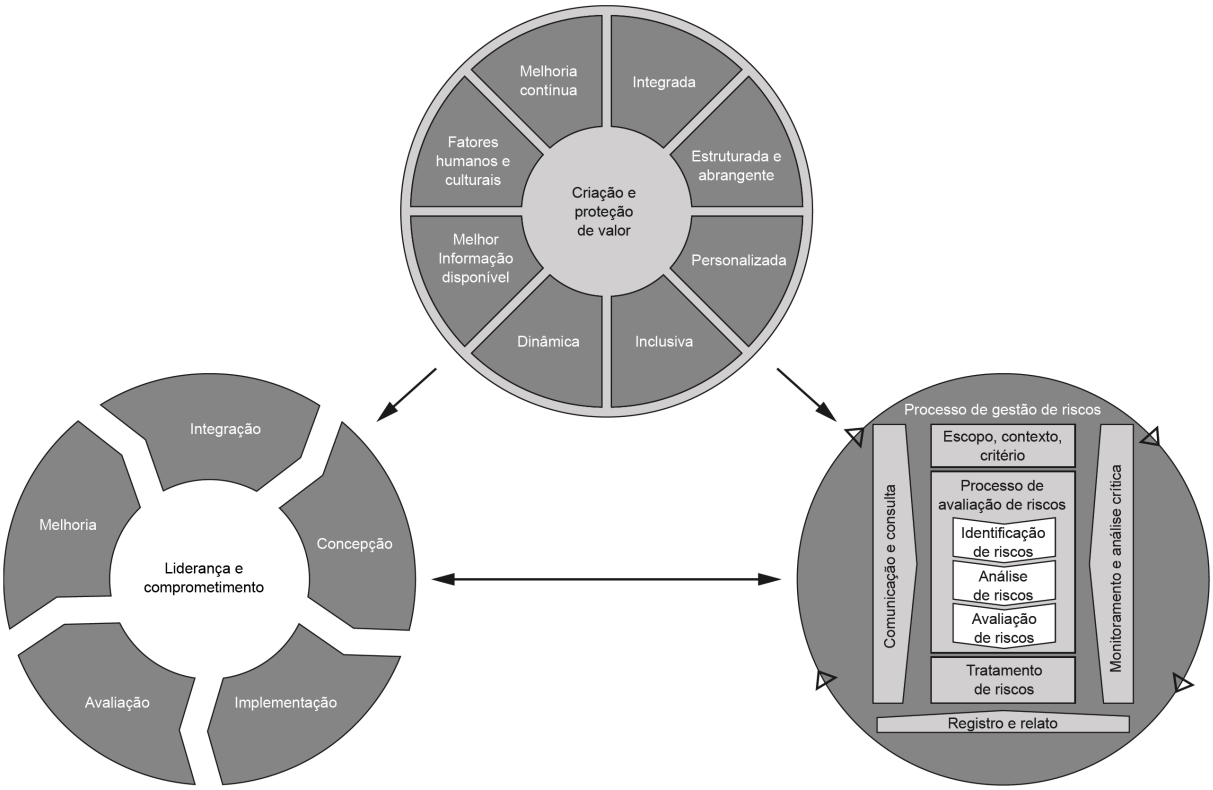


Figura 2.5: Princípios, estrutura e processo de gestão de risco.
Fonte: Norma NBR ISO 31000 [27].

Este processo - ou programa e conjunto de processos [48] - envolve a identificar dos riscos, estimar ou mensurar a probabilidade de ocorrência de eventos, analisar os impactos resultantes, avaliar a exposição e os controles em termos de custos e benefícios para estabelecer uma estratégia de resposta, tratamento ou mitigação, bem como o monitoramento contínuo dos riscos [27] [49] [37] [44]. Com base nessas informações, as organizações são capacitadas a determinar seus níveis aceitáveis de risco, isto é, a definir sua tolerância ao risco [32].

Estas etapas são representadas na Figura 2.6

O sucesso da gestão de riscos depende de alguns outros fatores adicionais. De acordo com o *The Standard for Risk Management in Portfolios, Programs, and Projects*, publicado pelo Project Management Institute - PMI [30], a gestão de riscos é uma responsabilidade compartilhada, cabendo a cada indivíduo aceitar e se comprometer pessoalmente com suas atividades relacionadas a riscos. Uma comunicação eficaz dos riscos é fundamental. Qualquer ação ou atitude que a obstrua pode diminuir significativamente a eficácia da gestão de riscos, impactando negativamente a proatividade e a capacidade de tomada de decisão.

Ademais, a gestão de riscos se tornar um compromisso institucional. Uma abordagem isolada para a gestão de riscos é inviável. Ela deve estar integrada a outros processos e projetos organizacionais, incluindo a alocação apropriada de recursos para garantir a efetiva implementação das práticas de gestão de risco. Por fim, é vital adaptar o esforço despendido nas atividades de gestão de riscos aos valores da organização, aos níveis de risco aceitáveis e às diversas restrições existentes [30].

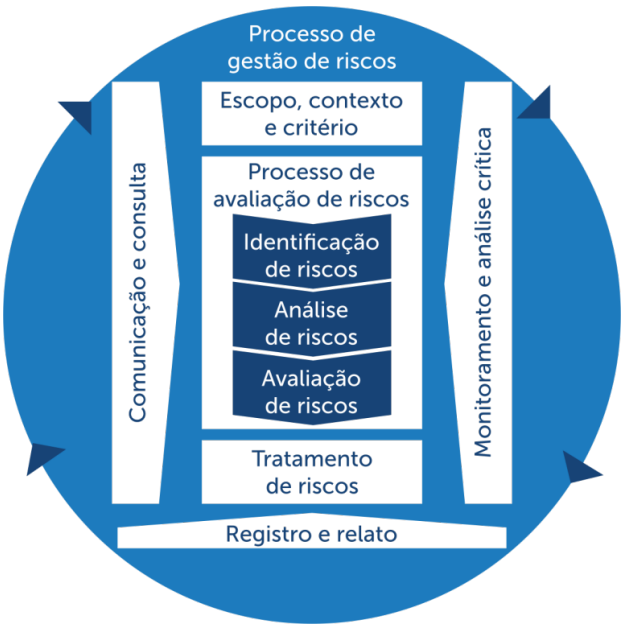


Figura 2.6: Processo de gestão de risco.
Fonte: Norma NBR ISO 31000 [27]

A Figura 2.7 ilustra alguns dos fatores-chave de sucesso para a gestão de riscos.

Figura 2.7: Fatores-chave de sucesso para a gestão de riscos.
Fonte: *The standard for risk management in portfolios, programs, and projects* do PMI [30].

Aven [40] argumenta que a gestão de riscos precisa estar em equilíbrio com outras preocupações também relevantes e que as decisões devem ser baseadas na avaliação das vantagens e desvantagens, com foco nos valores e prioridades dos tomadores de decisão. Para isso, é recomendada a adoção de padrões mínimos de segurança com o objetivo de simplificar o julgamentos e garantir a conformidade organizacional.

Esses critérios de restrição geralmente são chamados de critérios de risco, critérios de aceitação de risco ou critérios de tolerância. Um princípio comumente utilizado nesse contexto é o ALARP (*As Low As Reasonably Practicable*), que busca balancear os cuidados e precauções necessários na redução do risco até um ponto em que os custos não superem os benefícios.

O *framework* NIST CSF [32] ressalta a importância crítica de uma compreensão e definição adequadas da tolerância ao risco por parte das organizações, especialmente no contexto da segurança cibernética. Esta abordagem é essencial para a priorização eficaz das atividades de segurança cibernética. Devido aos custos elevados associados à implementação de medidas de segurança e obtenção de um nível aprimorado de segurança, as decisões se tornam mais razoáveis quando baseadas no nível de risco que se pretende aceitar. A gestão de risco oferece a possibilidade de quantificar e guiar a gestão da segurança cibernética, permitindo a comunicação e priorização de decisões bem como a validação de indicadores de negócio e o direcionamento de ações que favoreçam o alcance dos resultados negócio desejados.

2.4 PROCESSO DE AVALIAÇÃO DE RISCOS

A avaliação de riscos (*risk assessment*) é um dos componentes fundamentais de um processo de gerenciamento de riscos organizacionais [48] [49]. As avaliações de risco visam identificar, estimar e priorizar o risco para as funções institucionais [50]. O processo ou sub-processo de avaliação de riscos consiste na realização das três etapas fundamentais: identificação de riscos, análise de riscos e avaliação de riscos [45] [27] [38]. A Figura 2.8 detalha visualmente este processo.

Figura 2.8: Processo de avaliação de riscos.
Fonte: Adaptado de Norma NBR ISO 31000 [27].

A avaliação de riscos (*risk assessment*) pode ser definida também como a ciência dedicada ao entendimento e controle de riscos associados a eventos acidentais, permitindo facilitar a gestão racional e o entendimento sistêmico dos perigos. A ideia básica é estruturar, de forma sistemática, as informações e conhecimentos à disposição para avaliar os riscos [51].

O *Guide for Conducting Risk Assessments* [48] do NIST e a Norma ABNT NBR ISO/IEC 31010

[49] indicam que o objetivo principal das avaliações de risco são fornecer aos tomadores de decisão e às partes interessadas informações baseadas em evidências para a tomada de decisão e subsidiar as ações de resposta aos riscos dentre as opções disponíveis, identificando ameaças relevantes ou direcionadas às organizações. Shameli-Sendi et al. [52] argumentam que a finalidade da avaliação de riscos também é identificar vulnerabilidades e ameaças que possam comprometer recursos valiosos - sejam ativos, processos ou serviços - e avaliar com precisão como mitigá-los de forma eficaz. Os autores indicam que o risco se manifesta quando uma vulnerabilidade, ou fragilidade, se conecta com um agente de ameaça.

Os principais benefícios do processo de avaliação de riscos incluem [49] :

- Entender o risco e o impacto potencial sobre os objetivos.
- Subsidiar a tomada de decisão.
- Contribuir para o entendimento dos riscos visando selecionar as opções de tratamento.
- Identificar fatores de risco e elos fracos em sistemas e organizações.
- Comparar riscos entre as alternativas possíveis.
- Implementar a comunicação dos riscos.
- Auxiliar no estabelecimento de prioridades.
- Contribuir para a prevenção de incidentes com base em eventos anteriores.
- Selecionar as formas de tratamento dos riscos.
- Atender a requisitos regulatórios e de conformidade.
- Subsidiar a aceitação de riscos.

A Figura 2.9 apresenta uma representação gráfica das interações e papéis desempenhados por especialistas em riscos e tomadores de decisão. Neste contexto, a avaliação de riscos atua como um elo crucial, equilibrando fatos e valores e facilitando o julgamento informado sobre os riscos em questão. Essa avaliação deve levar em consideração não apenas os valores dos tomadores de decisão, mas também a quantidade e a qualidade das evidências disponíveis.

Entretanto, é fundamental que os tomadores de decisão não se baseiem exclusivamente na avaliação de riscos. Eles devem, de forma integral, considerar e integrar essas informações com dados e *insights* provenientes de outras fontes e áreas relevantes para uma compreensão abrangente e uma tomada de decisão eficaz [40].

Bernard (2007) enfatiza a importância de um processo de avaliação de riscos multidisciplinar e abrangente, estendendo-se além das unidades de segurança tradicionais [53]. A eficácia deste processo depende da inclusão de diversos setores organizacionais, como recursos humanos, jurídico, conformidade, auditoria e gestão de risco. No entanto, mesmo com a contribuição destes departamentos, a percepção do panorama de riscos permanece limitada.

O autor defende a necessidade de envolver diretamente unidades de negócio variadas, haja vista que possuem maior entendimento das funções críticas, como as informações são acessadas e onde estão localizadas. Os usuários e gestores dessas unidades, mesmo que não possuam conhecimento técnico aprofundado em segurança da informação, são essenciais no processo.

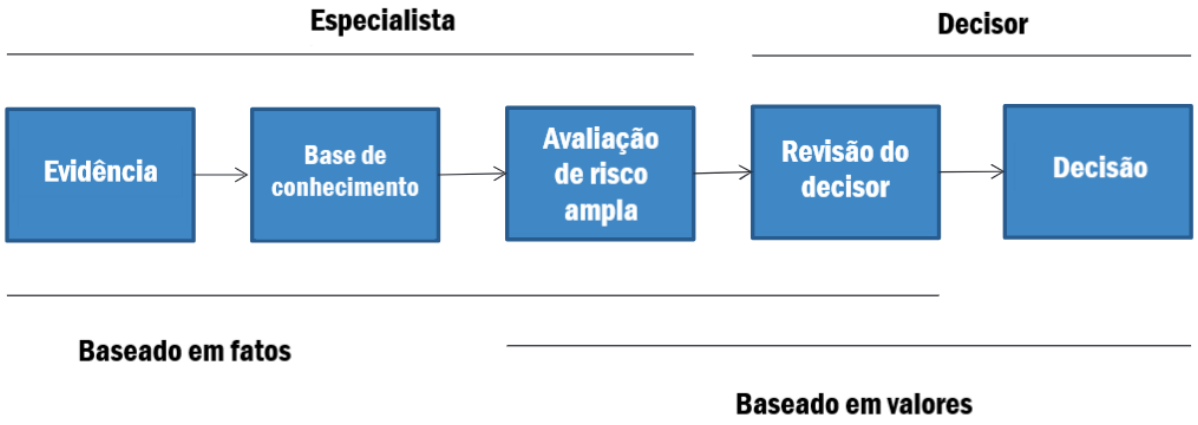


Figura 2.9: Modelo de interligação dos estágios de informação dos riscos de decisão.
Fonte: *Risk assessment and risk management: Review of recent advances on their foundation* [40]

O envolvimento ativo desses usuários e gestores de negócios é crucial para otimizar a priorização de medidas de segurança, avaliar o equilíbrio entre custos e impacto potencial no negócio e a fomentar a defesa da segurança dos ativos. Com uma compreensão mais ampla do impacto dos riscos nos objetivos institucionais, eles se tornam defensores efetivos da segurança da informação dentro da organização [53].

É importante destacar que o processo de avaliação de riscos possui limitações inerentes, particularmente evidentes em casos de eventos raros, mas com potenciais consequências devastadoras. A avaliação em tais cenários frequentemente depende de julgamentos subjetivos feitos por especialistas, que se baseiam em observações indiretas ou em modelos preditivos. A detecção e análise desses eventos são especialmente desafiadoras devido à escassez de dados históricos e ao entendimento limitado sobre como o sistema em questão pode reagir. Eventos dessa natureza, extremamente raros e de difícil previsibilidade, são frequentemente referidos como eventos *black swan*, um termo que ilustra a complexidade e a imprevisibilidade intrínsecas a esses tipos de riscos [54].

Para mitigar estas incertezas e aprimorar o processo de identificação de riscos, uma variedade de técnicas e métodos está disponível. Estas abordagens, que variam em complexidade e aplicabilidade. As técnicas de avaliação de riscos constituem um conjunto de métodos ou procedimentos empregados com o intuito de identificar, analisar e avaliar riscos em variados contextos, incluindo projetos, processos operacionais e sistemas organizacionais [49] [55].

Na escolha de técnicas de avaliação de riscos, é imperativo considerar uma série de fatores para assegurar que a técnica selecionada seja a mais apropriada ao contexto específico em questão. Estes fatores abrangem os objetivos da avaliação, o tipo e a extensão dos riscos a serem examinados, a disponibilidade e a qualidade dos dados, os recursos à disposição (tais como tempo, orçamento e expertise especializada), e o grau de detalhamento necessário para embasar decisões estratégicas [56].

A Norma NBR ISO/IEC 31010 [49] apresenta uma relação de 31 técnicas ou ferramentas distintas para o processo de avaliação de riscos. Cada técnica é categorizada conforme sua aplicabilidade - *Fortemente Aplicável (FA)*, *Não Aplicável (NA)* ou *Aplicável (A)* - em cada etapa do processo de avaliação de riscos.

Essas etapas incluem a identificação do risco, a análise de consequências, a análise de probabilidade, a análise do nível de risco e, finalmente, a avaliação do risco em si.

Diversas técnicas são empregadas na avaliação de riscos, abrangendo desde *brainstorming*, entrevistas estruturadas ou semiestruturadas, e listas de verificação, até métodos mais complexos como a Análise Preliminar de Perigos (APP), a análise de dados históricos, a HAZOP (Análise de Perigos e Operabilidade) e o método Delphi, entre outras. Estas técnicas, juntamente com muitas outras, compõem um leque extenso de opções para a identificação e avaliação eficaz de riscos, adaptadas ao contexto específico de cada organização. Elas são instrumentais para uma compreensão aprofundada dos riscos enfrentados e para o desenvolvimento de estratégias de gestão de riscos eficientes [55] [49].

Nas próximas subseções serão abordadas cada uma das etapas do processo de avaliação de riscos.

2.4.1 Identificação de riscos

A identificação de riscos é uma etapa crucial no processo de avaliação de riscos, na qual se busca descobrir e descrever os riscos dentro do escopo estabelecido previamente na fase de contexto. Esta fase pode envolver a análise de cenários ou situações potenciais que podem afetar o alcance dos objetivos, comprometendo valores ou ativos [52] [57] [49].

Para alcançar uma identificação eficaz de riscos, é essencial reconhecer as diversas fontes de risco, os próprios eventos de risco, suas causas e as potenciais consequências que eles podem acarretar. Este processo de identificação deve incorporar uma variedade de insumos, incluindo dados históricos, que fornecem *insights* valiosos sobre riscos passados, análises teóricas para compreender as possibilidades futuras, opiniões de especialistas que podem oferecer perspectivas aprofundadas e especializadas, e as necessidades e preocupações das partes interessadas. Essa abordagem multifacetada amplia a visão e a abrangência dos riscos [38] [56].

O Referencial Básico de Gestão de Risco do Tribunal de Contas da União recomenda que a identificação de riscos seja conduzida em vários fases ou níveis para assegurar uma maior eficácia [56]. O processo deve iniciar com uma abordagem preliminar e abrangente, que se concentra na identificação de riscos prioritários com potencial impacto nos objetivos estratégicos da organização. Após essa etapa inicial, é crucial adotar uma abordagem mais detalhada e específica, focada em identificar riscos associados aos processos prioritários previamente reconhecidos.

O objetivo desta fase é compilar uma lista abrangente de riscos, incluindo as causas e fontes dos eventos de risco, que possam impactar nos objetivos definidos na fase de estabelecimento do contexto. Nessa relação devem ser incluídos tanto os fatores humanos e organizacionais quanto os componentes relacionados a equipamentos e sistemas [27] [49] [56].

De acordo com a Norma NBR ISO/IEC 27005 [58], que aborda a gestão de riscos de segurança da informação, é fundamental, nesta fase, realizar um inventário de ativos e identificar seus responsáveis. Essa etapa inclui a identificação de ameaças, baseada na análise de incidentes anteriores, e a identificação de controles existentes. Além disso, é necessário estabelecer a relação entre as vulnerabilidades que podem ser exploradas por ameaças e a forma como essas ameaças podem comprometer os ativos. O processo

também envolve a identificação das consequências potenciais.

Dada a complexidade crescente dos ataques cibernéticos, a identificação abrangente de cenários de risco apresenta-se como um desafio significativo. Esta dificuldade decorre, em parte, da multidimensionalidade dos riscos cibernéticos e das limitações dos tomadores de decisão em prever completamente os diferentes cenários possíveis [59]. A incerteza não se limita apenas aos ataques conhecidos, mas também abrange aqueles ainda desconhecidos.

Diversas técnicas podem ser empregadas na identificação de riscos, cada uma com suas especificidades e vantagens. Entre os métodos baseados em evidências estão as listas de verificação e as análises críticas de dados históricos, que fornecem *insights* baseados em experiências e ocorrências anteriores. Outra abordagem envolve a formação de uma equipe de especialistas que sistematiza um conjunto de instruções ou perguntas direcionadas, facilitando a identificação de riscos de maneira estruturada [49].

Além disso, técnicas de raciocínio indutivo são utilizadas para derivar generalizações a partir de observações específicas, contribuindo para a identificação de novos riscos. Técnicas colaborativas como *brainstorming* e *Delphi* também são valiosas, pois permitem a geração e a consolidação de ideias a partir de diferentes perspectivas, enriquecendo o processo de identificação de riscos [49].

2.4.2 Análise de riscos

A fase de análise de riscos, que se posiciona como a segunda etapa no processo de avaliação de riscos, tem como objetivo central compreender a natureza e determinar a magnitude dos riscos previamente identificados. A qualidade das informações obtidas durante a identificação de riscos é um fator determinante para a eficácia dos resultados obtidos na subsequente análise de riscos [38] [42] [60] [41].

Durante a fase de análise de riscos, é crucial estabelecer um forma para medir o nível de risco e estabelecer o nível específico de cada risco. Tal compreensão é essencial, pois fundamenta as decisões estratégicas relacionadas ao tratamento dos riscos que são explorados na etapa subsequente do processo [27] [56] [61].

Para essa medição existem diversos modelos e abordagens. Alguns modelos levam em consideração fatores como o valor do ativo, o efeito da vulnerabilidade, o impacto potencial e a probabilidade da ameaça ou do impacto sobre o negócio [52] [39]. Outros modelos focam mais diretamente no impacto e na probabilidade de ocorrência do risco, bem como as relações de causa e efeito [56].

É importante reconhecer que um evento de risco pode ter várias causas e consequências, podendo influenciar diversos objetivos dentro da organização [49]. A escolha do modelo de medição de risco deve, portanto, refletir a natureza complexa e multifacetada dos riscos, garantindo uma avaliação abrangente e alinhada aos objetivos e contextos específicos [56].

A análise de riscos, uma etapa crucial no processo de avaliação, varia em termos de profundidade e complexidade. Essas variações dependem dos objetivos específicos da avaliação, bem como da disponibilidade e confiabilidade das informações e dos recursos disponíveis [49]. Esta análise abrangente inclui a avaliação das consequências dos riscos, a exploração de cenários variados, e a investigação das múltiplas causas dos riscos e dos impactos que podem gerar.

As consequências identificadas podem ser tanto tangíveis, como perdas financeiras ou danos físicos a equipamentos, quanto intangíveis, incluindo efeitos adversos na reputação ou na confiabilidade da organização. Independentemente da natureza, essas consequências têm o potencial de afetar parcial ou totalmente diversas funções e serviços dentro da organização [39].

De modo geral há três métodos para avaliação de impacto, probabilidade e na determinação do nível resultantes para fins de avaliação de riscos [49] [58] [56]:

- **Qualitativos**: definidos em termos de significância com base na percepção de pessoas. É recomendada a utilização de uma relação de critérios ou explicações de referências que auxiliem na dedução dos níveis para reduzir a subjetividade. Por exemplo: muito alto, alto, médio e baixo.
- **Semiquantitativos**: utilizam escalas numéricas previamente estabelecidas em que se avalia o nível de risco com base em uma fórmula. Por exemplo: escala de 0 a 10.
- **Quantitativos**: baseiam-se em fatores objetivos e mensuráveis para definir os níveis de probabilidade e impacto. Esta abordagem pode ser limitada ou não utilizada em função da insuficiência de informações detalhadas sobre o objeto de análise.

Existem análises sobre a escolha entre abordagens qualitativas e quantitativas para a avaliação de riscos, focando em quando é mais apropriado adotar cada uma delas. Evrin [61] ressalta que a análise qualitativa de riscos é rápida e flexível, porém subjetiva, sendo amplamente usada por organizações para avaliações rápidas e fáceis. Já a análise quantitativa, embora mais detalhada e objetiva, é opcional devido à sua complexidade, custo e tempo requerido. Esta abordagem de modo geral fornece dados mais precisos para decisões críticas, mas enfrenta desafios como a dificuldade de coleta de dados quantitativos de qualidade e a potencial imprecisão desses dados [60].

O *The standard for risk management in portfolios, programs, and projects* do PMI orienta que a análise qualitativa de riscos é apropriada para analisar individualmente a probabilidade e o impacto de cada risco nos objetivos do portfólio, programa ou projeto. Em contraste, a análise quantitativa de riscos foca no efeito combinado de todos os riscos identificados, incorporando elementos probabilísticos e interdependências. Assim, a análise qualitativa prioriza riscos individuais, a análise quantitativa estima o risco global, ajudando a diferenciar entre riscos que excedem a tolerância das partes interessadas e aqueles dentro de limites aceitáveis. O entendimento detalhado dos riscos individuais é crucial para esta avaliação global e para a priorização de respostas a riscos específicos que ameaçam objetivos críticos [30].

É importante salientar que, independentemente do modelo adotado, há de se reconhecer que os níveis de risco são estimativas e não devem ser atribuídos níveis de exatidão ou precisão incompatíveis com a disponibilidade de dados ou com o método utilizado [49].

Nesta fase é conveniente que as salvaguardas ou controles existentes sejam relacionados e avaliados quanto a sua eficácia para o tratamento do risco. O risco anterior a consideração dos controles é chamado de *risco inerente*. *Risco residual* é o nível de risco que permanece mesmo após a aplicação dos controles e proteções para o tratamento do risco [56].

As técnicas qualitativas, exemplificadas pela análise SWOT (Strengths, Weaknesses, Opportunities,

Threats) e pela análise de cenários, se concentram na descrição e interpretação dos riscos. Por outro lado, as técnicas quantitativas, como a análise estatística e a modelagem de riscos, baseiam-se em dados numéricos para a estimativa de probabilidades e impactos. Estas abordagens são fundamentais para um eficiente gerenciamento de riscos [40] [49].

2.4.3 Avaliação de riscos

É fundamental esclarecer a diferença entre o processo de avaliação de riscos (*risk assessment*) e a etapa de avaliação de riscos (*risk evaluation*), pois, apesar de serem frequentemente traduzidos de maneira similar, os termos têm origens e significados distintos na língua inglesa, refletindo contextos e conotações semânticas diferentes.

O termo ***assessment*** está associado à coleta e análise de informações para entender e interpretar um tópico ou área. Este processo é exploratório e diagnóstico por natureza, geralmente contínuo e formativo, com o objetivo de monitorar progresso e realizar ajustes ao longo do tempo [62] [63].

Por outro lado, ***evaluation*** envolve fazer julgamentos sobre o valor, qualidade ou importância de algo. Este termo está mais ligado à conclusão e ao julgamento. "*Evaluation*"é frequentemente um processo realizado ao final de um período, com o objetivo de sumarizar ou emitir uma opinião sobre o sucesso ou a eficácia de uma iniciativa [62] [63].

Em resumo, enquanto "*assessment*"está associado a um processo de exploração e diagnóstico, "*evaluation*"foca em julgamentos e conclusões com base nas informações coletadas.

A etapa de avaliação de riscos representa a fase final do processo de avaliação de riscos e consiste na comparação dos resultados obtidos na análise de riscos com critérios de tolerância ou aceitação do risco que foram estabelecidos anteriormente no contexto da organização. Baseado nessa comparação, decide-se quais riscos requerem tratamento [38] [27] [41] [56].

Este limites de tolerância aos riscos representam o nível acima do qual o tratamento do risco é desejável para que o risco real fique abaixo dele. A avaliação segue etapas como identificar na matriz de probabilidade x impacto os riscos acima do limite de exposição, entender as fontes, causas e consequências desses riscos para a organização, e avaliar os riscos abaixo do limite para monitoramento ou aceitação [56].

De acordo com o Manual de Gestão de Riscos do TCU [56], a análise de risco segue etapas como avaliar o impacto do risco sobre os objetivos, medindo o potencial comprometimento, e a probabilidade de ocorrência do risco. O nível do risco comumente é definido usando uma matriz de probabilidade x impacto, combinando escalas de probabilidade e impacto, geralmente qualitativas. Conforme demonstrado na Figura 2.10, a matriz ajuda a priorizar riscos. Gestores podem definir quais riscos devem ser tratados, considerando a situação real com os controles existentes.

Os riscos em um contexto da avaliação geralmente se enquadram em três categorias principais. A primeira é a dos *riscos intoleráveis*, que exigem medidas de tratamento imediatas devido ao seu alto nível de gravidade. A segunda categoria é a *zona indefinida* ou zona cinzenta, onde se faz necessário equilibrar os custos dos controles com os impactos potenciais para decidir se o risco deve ser tratado. A terceira categoria é a dos *riscos desprezíveis*, considerados de baixa prioridade e que, portanto, não requerem

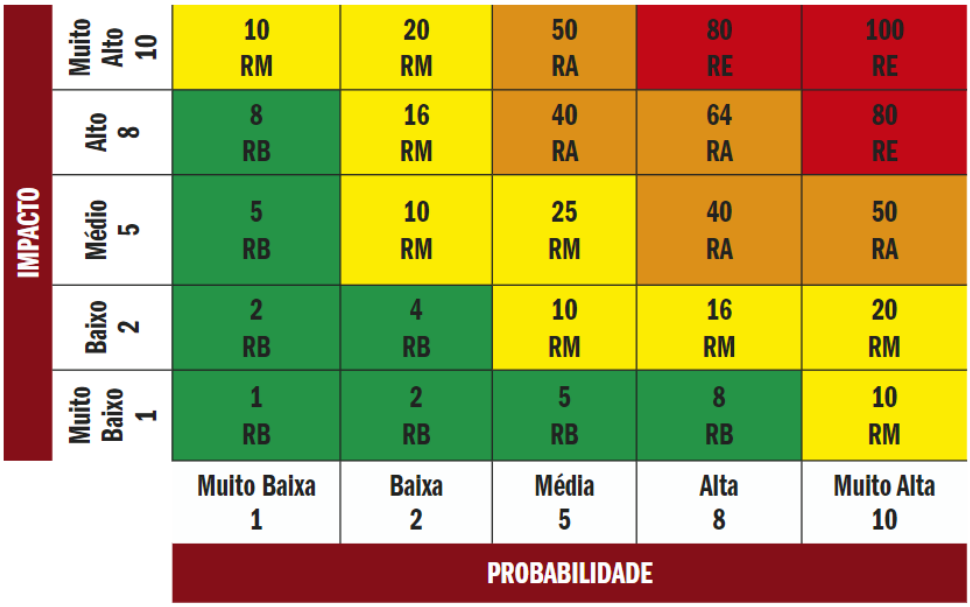


Figura 2.10: Exemplo de matriz de risco resultante da análise de riscos.
Fonte: Tribunal de Contas da União [56]

medidas de tratamento específicas. A classificação dos riscos nessas categorias é crucial para a definição de prioridades no processo de gestão de riscos [49].

Na priorização e tratamento dos riscos, é possível adotar critérios adicionais além daqueles definidos no contexto interno e externo. Estes critérios devem abranger tanto os objetivos organizacionais quanto as expectativas das partes interessadas. Isso implica em especificar qual nível hierárquico na organização deve ser informado ou assumir a responsabilidade pelas decisões relativas ao tratamento dos riscos. Um fator crítico é a definição de prazos para a implementação das medidas de tratamento. Adicionalmente, é importante considerar a necessidade de um monitoramento contínuo ou acompanhamento especializado dos riscos, assegurando que as medidas tomadas sejam não apenas eficazes, mas também alinhadas com as necessidades e expectativas das partes interessadas [58] [56].

Além disso, para a priorização e o tratamento dos riscos, é possível adotar critérios adicionais que complementam aqueles estabelecidos na definição do contexto interno e externo. Estes critérios adicionais devem considerar não apenas os objetivos organizacionais, mas também as perspectivas das partes interessadas. Isso inclui determinar qual nível hierárquico dentro da organização deve ser notificado ou responsável por decidir sobre as ações de tratamento do risco. Outro aspecto relevante é a definição do prazo para a implementação das medidas de tratamento. Além disso, deve-se avaliar a necessidade de monitoramento adicional ou acompanhamento especial do risco, garantindo que as ações tomadas sejam eficazes e alinhadas com as expectativas e necessidades das partes interessadas [58] [56].

A avaliação de riscos desempenha um papel crucial ao fornecer informações essenciais para uma tomada de decisão informada. No entanto, ela não é o único fator determinante no processo de tratamento de riscos. O gestor tem a responsabilidade de decidir, entre uma lista priorizada de riscos, quais demandam ações de tratamento específicas para sua mitigação [56].

Conforme exposto por Zio [51], a avaliação de riscos historicamente tem se baseado na análise probabilística para quantificar os riscos. Entretanto, essa abordagem mostra limitações, especialmente para eventos de baixa probabilidade, mas com consequências extremamente graves. Para superar essas limitações, Zio enfatiza a necessidade de adotar uma abordagem integral que combine tanto avaliações qualitativas quanto quantitativas. Apesar disso, ele reconhece que sempre existe a possibilidade de um resultado ou decisão ruim em razão das limitações de informações e de conhecimento do avaliador dos riscos. A imprecisão nas avaliações geralmente é resultado das limitações nos dados disponíveis e no conhecimento do avaliador. Portanto, a avaliação de riscos é melhor entendida, segundo Zio, como uma "análise estruturada do sistema de interesse para descrever qualitativa e quantitativamente o risco, com base nos conhecimentos disponíveis"

Al-Safwani destaca que a avaliação de riscos no campo da Tecnologia da Informação ainda não tem recebido a atenção necessária [64]. Apesar de muitas metodologias de análise de riscos empregarem abordagens qualitativas e quantitativas para contornar essa questão, os modelos de avaliação de riscos existentes são frequentemente vistos como insuficientes. Essa insuficiência é frequentemente atribuída a uma tomada de decisão que não considera adequadamente todos os critérios relevantes e à falta de uma análise detalhada sobre a relação custo-efetividade.

2.5 TRATAMENTO DE RISCOS

O tratamento de risco é definido como o ato de modificar o risco [65] [41] [38] [65].

O termo *tratamento de riscos*, conforme definido nas normas ISO [38] [27] [58], refere-se a uma etapa crucial do processo de gestão de riscos. Essa etapa envolve a implementação de estratégias diversas para abordar riscos potenciais. Estas estratégias podem incluir: evitar o risco, optando por não iniciar ou continuar atividades que o geram; aceitar ou aumentar o risco para capitalizar oportunidades; eliminar a fonte do risco; modificar a probabilidade ou impacto do risco; compartilhar o risco com terceiros, seja por meio de contratos ou financiamento; e a retenção consciente do risco após uma análise criteriosa.

Estratégias que se concentram em atenuar impactos negativos são comumente classificadas como 'mitigação de risco', 'eliminação de risco', 'prevenção de risco' e 'redução de risco'. É importante notar que, ao tratar riscos, pode haver a criação de novos riscos ou alterações em riscos já existentes. O objetivo principal do tratamento de riscos é selecionar e implementar ações efetivas para controlar, minimizar ou evitar riscos dentro das opções disponíveis"[38].

Por outro lado, o NIST em seus normativos [65] [39] nomeia esta fase como "*processo de resposta aos riscos*". as organizações podem optar por diversas respostas, incluindo a aceitação ou mitigação do risco. Os resultados da avaliação e as técnicas utilizadas orientam a escolha da resposta mais adequada. Na mitigação, as ações planejadas são incluídas no plano de ação, monitoradas e reavaliadas para assegurar a implementação e eficácia adequadas, cumprindo os requisitos de segurança e privacidade.

Este enfoque inclui um monitoramento e reavaliação contínuos das ações de mitigação para assegurar a eficácia e o cumprimento dos requisitos de segurança e privacidade. Quando o risco é aceito, as deficiências identificadas são documentadas e monitoradas para identificação de alterações nos fatores de

risco [66]. O responsável pela avaliação e os planos de ação determina se é necessário mitigar os riscos antes da autorização superior, considerando a priorização baseada na gravidade e impacto dos riscos. A resposta ao risco, seja mitigação ou aceitação, implica sempre em algum grau de risco residual. Este grau é determinado pela tolerância ao risco da organização.

O PMI [30], por sua vez, descreve o "*processo de resposta a riscos*"como a determinação das melhores ações para lidar com riscos identificados, analisados e priorizados. Este processo enfatiza a formulação de planos de resposta detalhados e a implementação das ações acordadas. O PMI destaca a importância de comunicar os planos de resposta aos stakeholders, gerenciar eficientemente a comunicação e considerar os custos de resposta ao risco.

O processo de tratamento de riscos engloba algumas ações essenciais que incluem não apenas aplicar as medidas escolhidas para o tratamento, mas avaliar a efetividade das medidas aplicadas. Ademais, decidir se o risco residual, aquele que permanece após a implementação das medidas de tratamento, está em patamares aceitáveis. Caso não esteja, realizar o tratamento adicional para que o risco fique dentro do aceitável. Convêm ainda avaliar se alguns controles existentes excedem as necessidades atuais e, portanto, podem ser considerados para remoção, especialmente se tiverem altos custos de manutenção. [27] [58].

2.6 SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Há debates em curso acerca dos conceitos de segurança da informação e segurança cibernética. Enquanto alguns os consideram como subconjunto do outro, outros os veem como conceitos complementares ou até utilizam como sendo sinônimos.

A definição de segurança da informação do NIST [65], que é utilizado como fonte de diversas outras referências, é a "*proteção de informações e sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição, a fim de fornecer confidencialidade, integridade e disponibilidade*".

De acordo com o NIST [65], "informação"é definida como qualquer comunicação ou representação de conhecimento, como fatos, dados ou opiniões, em qualquer meio ou forma. Isso inclui formas textuais, numéricas, gráficas, cartográficas, narrativas, eletrônicas ou audiovisuais. A definição abrange fatos e ideias que podem ser representados como várias formas de dados e conhecimento em qualquer meio ou forma que possa ser comunicado entre entidades de sistema. A definição ressalta as diversas maneiras pelas quais a informação pode ser transmitida e compreendida.

A segurança cibernética, por sua vez, conforme a definição do NIST [65], é a capacidade de proteger ou defender o uso do ciberespaço, ou espaço cibernético, contra ataques cibernéticos. O "ciberespaço"ou "espaço cibernético"é definido como um domínio de informação que consiste na rede interdependente de sistemas de informação, incluindo a internet, redes de telecomunicações, sistemas informáticos e processadores incorporados.

Stanger [67] apresenta a visão da organização CompTIA, que demonstra utilizar o NIST como referência, como a **segurança da informação** sendo um conceito abrangente que engloba a segurança cibernética,

segurança física e privacidade. Este conceito é visto como um "guarda-chuva"sob o qual diversos elementos de segurança se alinham, incluindo a proteção de dados tanto físicos (como papéis e dispositivos físicos) quanto digitais. Assim, entende-se que a segurança cibernética é um subconjunto de segurança da informação. Stanger observa que lentamente se percebe uma mudança da compreensão de que a segurança abrange não apenas a proteção de equipamentos, servidores e redes, mas principalmente a proteção de informações e pessoas.

O fabricante de segurança Check Point [68] destaca a inter-relação, mas também a distinção entre segurança cibernética e segurança da informação. A segurança da informação é mais abrangente e concentra-se na proteção das informações ou dados, enquanto a segurança cibernética se concentra também na proteção de ativos de TI contra ameaças. Incluindo redes e de aplicativos. A Check Point salienta que um incêndio em uma sala de arquivos pode ser tão prejudicial quanto um ataque de sequestro de dados (*ransomware*), dependendo dos dados envolvidos, ressaltando a necessidade de uma estratégia de segurança da informação que considere todos os riscos potenciais.

O CyBOK (*The Cyber Security Body of Knowledge*) [69] oferece uma definição de segurança cibernética focada na proteção de sistemas de informação (hardware, software e infraestrutura relacionada) e dos dados e serviços relacionados contra acessos não autorizados, danos ou utilização indevida. Esta definição considera danos tanto intencionais quanto acidentais e enfatiza a importância dos comportamentos humanos no contexto da segurança cibernética. O CyBOK também sublinha que a segurança cibernética deve ser equilibrada com outros riscos e requisitos, principalmente humanos, incluindo a necessidade de não perturbar tarefas principais.

O CyBOK [69] utiliza a série de normas NBR ISO/IEC 27000 para o conceito de segurança da informação, considerando a segurança da informação como a preservação da confidencialidade, integridade e disponibilidade das informações. Enfatiza também que, ao longo do desenvolvimento da era digital, vários termos, como segurança informática e segurança de redes e segurança de sistema ganharam destaque. A base de conhecimento aborda que os dois termos são frequentemente confundidos ou usados de forma intercambiável, e como, historicamente, houve uma ênfase excessiva nos controles técnicos, focados na informação. Aborda também a necessidade de abarcar sistema de segurança física.

Adicionalmente, o CyBOK [69]aborda que o ciberespaço é descrito como um "lugar"onde ocorrem diversas atividades humanas, como negócios, comunicações, arte e relações sociais. Dentro deste espaço, podem ocorrer crimes cibernéticos, terrorismo cibernético e guerra cibernética, com impactos tanto no mundo real quanto no virtual.

Bernard [53] aborda a questão da segurança da informação, destacando a tendência de os profissionais dessa área concentrarem-se principalmente a sistemas de dados eletrônicos, deixando de fora as formas não eletrônicas de dados. O autor ressalta que a inclusão da segurança física e ambiental em normas, não garante que os profissionais de segurança da informação possuam o conhecimento ou os meios para implementar controles de segurança para dados não eletrônicos. Para uma abordagem abrangente da segurança da informação, é essencial considerar todas as formas de dados, exigindo o envolvimento de profissionais capazes de identificar e mitigar riscos em diferentes tipos de informação. Destaca-se que a colaboração eficaz entre profissionais de segurança de dados eletrônicos e aqueles envolvidos na segurança física é viabilizada pela perspectiva de risco. Ao adotar uma abordagem do ciclo de vida da informação, que cobre

desde a criação até a destruição da informação, torna-se possível identificar todas as formas que a informação pode assumir, tanto eletrônicas quanto físicas. Isso resulta em um processo abrangente de avaliação de risco de informação, englobando todas as suas dimensões.

A maior parte das definições sugerem que a segurança cibernética foca na proteção dos dados em formato eletrônico ou digital e na proteção de dispositivos tecnológicos de atacantes cibernéticos pela descoberta de vulnerabilidades ou falhas de configuração, enquanto a segurança da informação é mais abrangente e inclui dados físicos e outros processos relacionados a controle de acesso e conformidade. Sendo a segurança cibernética um subconjunto da segurança da informação destinado a proteção da informação digital bem como a proteção dos ativos tecnológicos que manipulam a informação. Em alguns casos se coloca a segurança de TI como sinônimo de segurança cibernética e em outros se entende que a segurança cibernética se refere aos ativos conectados à internet, conforme a Figura 2.11 [70] [71] [72] [73] [74] [75].

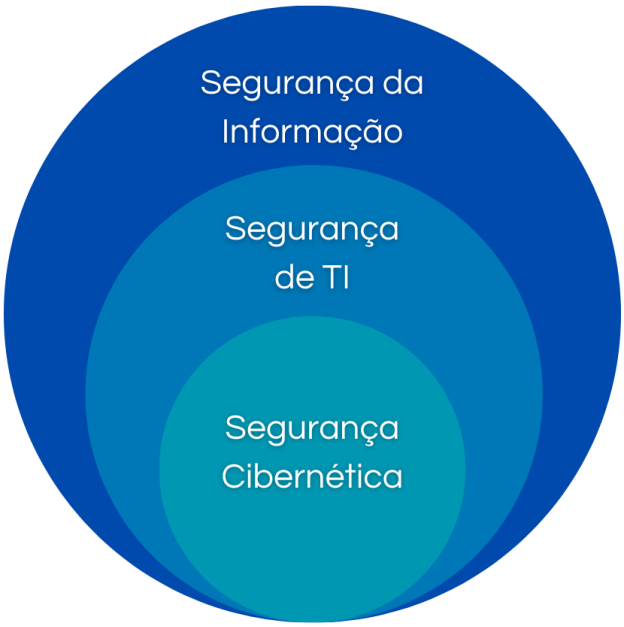


Figura 2.11: Relacionamento entre segurança de TI, segurança da informação e segurança cibernética.
Fonte: adaptado de ISC² [75]

No entanto, Solms e Niekerk [76] propõem outra abordagem. Embora a concordem que segurança da informação e a segurança da TIC sejam inter-relacionadas, entendem que elas se concentram em aspectos diferentes. A segurança da informação lidaria com a proteção da própria informação, enquanto a segurança da TIC foca na proteção dos sistemas que armazenam e processam essa informação. De acordo com essa definição, a segurança de Tecnologia da Informação e Comunicações (TIC) pode ser considerada uma subcomponente da segurança da informação, mas com características adicionais que se concentram mais nos aspectos técnicos e operacionais dos sistemas de informação. Os autores defendem que a segurança da cibernética abrange a proteção do próprio ciberespaço, da informação eletrônica, das tecnologias que apoiam o ciberespaço e dos usuários do ciberespaço. A segurança cibernética não se limitaria apenas à proteção da informação, mas também inclui a proteção de indivíduos, organizações e nações que operam no ciberespaço. Esta abordagem mais abrangente considera tanto ativos tangíveis quanto intangíveis, in-

cluindo questões éticas e a confiança dos cidadãos no uso do ciberespaço. A Figura 2.12 demonstra a essa visão de que a segurança cibernética se trata de uma expansão da segurança da informação.

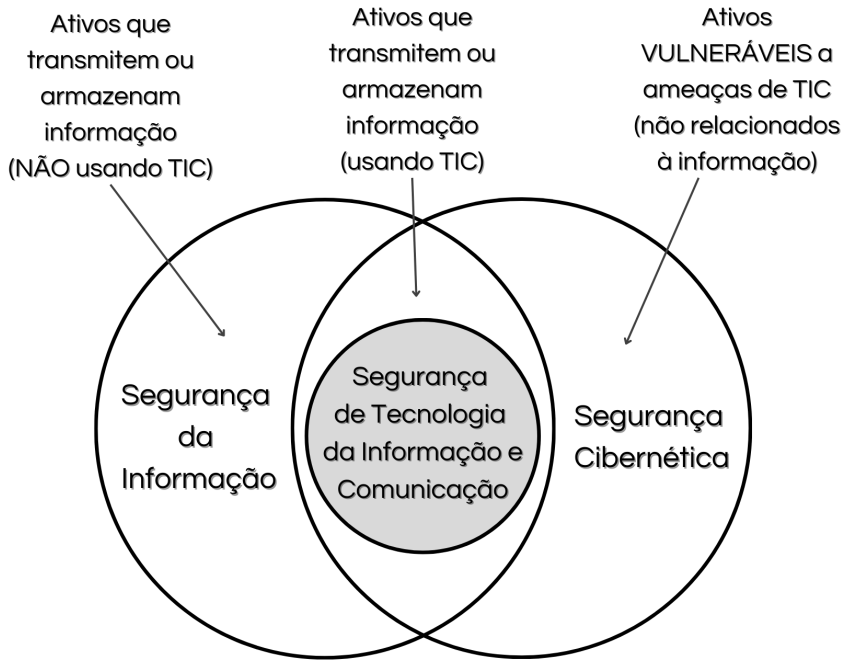


Figura 2.12: Relacionamento entre segurança de TI, segurança da informação e segurança cibernética.
Fonte: adaptado de Solms e Niekerk [76]

As Normas ABNT NBR ISO/IEC 27001 e 27002 [77] [78], que tratam, respectivamente, sobre sistemas de gestão de segurança da informação e orientam as práticas necessárias para a segurança da informação, definem que um ativo é qualquer coisa que possui valor para a organização. A Norma 27002 estabelece adicionalmente que existem diversos tipos de ativos, incluindo: ativos de informação, ativos de software, ativos físicos, serviços, pessoas e suas qualificações e habilidades bem como ativos intangíveis, tais como reputação e imagem. Devendo todos os ativos serem inventariados e protegidos quanto à sua segurança, por meio da aplicação de controles de segurança. Aparentemente, a divergência de entendimento apresentados por Solms e Niekerk está relacionada ao entendimento do que é um ativo de informação, pois entendem que a segurança da informação se aplica apenas à informação e não aos ativos que manipulam a informação.

A *European Union Agency for Network and Information Security - ENISA* [79] criou um relatório que objetiva avaliar o uso do termo "cybersecurity"e determinar um entendimento apropriado para o conceito. A ENISA destaca que os termos *Cyber Security* ou *Cybersecurity* são recentes e que evoluíram a partir do conceito de *cyberspace*. A ENISA reconhece a dificuldade de se estabelecer uma definição única de cibersegurança, dada sua natureza abrangente e em constante evolução. Em vez disso, propõe uma abordagem contextual e adaptativa, usando definições relevantes e apropriadas, dependendo do contexto e da organização em questão.

A Tabela 2.1 mostra um resumo das origens do termo cibersegurança e seus usos.

Tabela 2.1: Sumário de uso do termo *cybersecurity*

Origem	**Documento**	**Grafia**	**CID***	**Significado**	**Motivação**	**Ameaça**
ISO/IEC JTC1/SC27	27032	Cybersecurity	SIM	Somente ativos destinados à internet	Nenhuma diferenciação entre malicioso ou não intencional	Somente ativos virtuais conectados à internet, sem ativos físicos
ISO/IEC JTC1/SC27	27000		SIM	Qualquer origem de risco no ciberespaço	Nenhuma diferenciação entre malicioso ou não intencional	Qualquer ativo
ITU-T	X.1205	cybersecurity	SIM	Qualquer origem de risco no ciberespaço	Nenhuma diferenciação entre malicioso ou não intencional	Qualquer ativo
NIST	SP 800-39	cybersecurity	NÃO	Risco originado SOMENTE no espaço cibernético	Cobre apenas origens maliciosas (ataques cibernéticos)	Somente ativos virtuais conectados à internet, sem ativos físicos
OTAN	National Cyber Security Framework Manual	–	NÃO	Qualquer origem de Risco no Espaço Cibernético (Ameaça Cibernética)	Cobre apenas origens maliciosas (ataques cibernéticos)	Qualquer ativo
Committee on National Security Systems	CNSSI No. 4009	Cyber security	SIM	Qualquer risco	Nenhuma diferenciação entre malicioso ou não intencional	Qualquer ativo

*Confidencialidade, Integridade e Confidencialidade.

A ENISA define que a "segurança cibersegurança refere-se à segurança do ciberespaço, onde o próprio ciberespaço se refere ao conjunto de ligações e relações entre objetos acessíveis através de uma rede generalizada de telecomunicações, e ao conjunto dos próprios objetos onde apresentam interfaces que permitem o seu controle remoto, acesso remoto a dados, ou a sua participação em ações de controle dentro desse ciberespaço"[79] .

Com relação aos esforços de padronização do termos, a organização entende-se que pode não ser necessário uma definição única para segurança cibernética, tal como aplicado a outras definições e que pode não ser possível definir universalmente toda a extensão de coisas que a segurança cibernética cobre [79].

2.7 CONTROLES DE SEGURANÇA

Para Galegale et. al [31], os controles possuem um papel relevante na segurança da informação, pois é por meio deles que a segurança é obtida. Os controles possibilitam o gerenciamento dos riscos de proteção da informação por meio de procedimentos, estruturas organizacionais e práticas de natureza administrativa, técnica ou legal. Os controles selecionados e declarados na política são derivados dos requisitos de segurança da informação de cada organização. Após ter definido tais requisitos, ao buscar elaborar sua política, a organização se depara com uma grande quantidade de controles na literatura. Muitas vezes os controles são equivalentes, geralmente focada na descrição dos aspectos técnicos e operacionais da implementação, tratando todos os controles de forma igualitária quanto à sua criticidade. A depender dos objetivos e cultura da organização, a Segurança da Informação pode ser entendida sob três aspectos: técnico, onde se enfatiza a utilização de controles tecnológicos - social, motivação das pessoas e comportamento coletivos - sociotécnico, exploração das vantagens e minimização das desvantagens de forma simultânea. Embora se perceba a necessidade da segurança da informação, nem sempre há clareza sobre o que deve ser protegido e como fazer isso.

Bernard e Solms [34] discorrem que para as questões de segurança da informação serem endereçadas satisfatoriamente é necessário identificar, implementar e gerenciar um conjunto de controles eficazes capazes de fornecer um nível adequado de segurança. Identificar os controles mais eficazes sempre foi problemático e muitas abordagens e técnicas foram desenvolvidas com o objetivo de se fazer isso da forma mais objetiva possível. Sendo provavelmente a análise de risco a abordagem mais aceita e conhecida para se enfrentar tal desafio. Selecionar os controles de uma lista contida em *frameworks* ou manuais de boas práticas é problemático porque geralmente não é possível determinar quais são os controles de segurança mais recomendados para a situação particular de seu negócio, requisitos de segurança e dependência da tecnologia da informação no negócio.

Tradicionalmente, a seleção de controles é realizada por meio da gestão e análise de riscos. No entanto, uma linha base de controles mínimos de segurança deve ser definida com base em uma análise de negócios, sem que haja a dependência de uma análise de riscos prévia. Manuais de linha de base, com a definição de controles mínimos, surgiram como uma alternativa para eliminar a seleção aleatória ou a necessidade de um extenso e complexo processo de avaliação de risco para o estabelecimento de um nível mínimo de segurança [34].

A análise de negócios consiste em um conjunto de questões de alto nível relacionadas aos negócios que analisarão a situação específica da organização e determinarão a importância da segurança da informação e do gerenciamento da segurança da informação. Após essa determinação, os requisitos de segurança da organização podem ser estabelecidos, os quais serão diretamente refletidos na política de segurança da informação a ser implementada. Por exemplo, em uma instituição financeira, as informações financeiras são cruciais e devem ser protegidas a todo momento. Portanto, os requisitos de confidencialidade e seus controles serão altamente relevantes nesse caso. Esses requisitos de segurança, que fazem parte da política de segurança, serão aplicados por um ou mais controles de segurança [34].

No que diz respeito à avaliação dos controles, é necessário avaliar os aspectos relacionados à:

1. **Funcionalidade**: os controles estão realmente presentes?

2. **Correção**: os controles estão instalados e operando corretamente?
3. **Efetividade**: eles cumprem satisfatoriamente o seu propósito?
4. **Operação**: os procedimentos operacionais que suportam os controles são seguidos?

Para Al-Safwani [64] os métodos de avaliação de risco ajudam o processo de negócio em uma abordagem geral, mas não oferecem uma linha de base prática que seja clara e a seleção de controles é baseada na opinião e julgamento subjetivo de controles realizado com base na opinião de um especialista da área de segurança. A falta de objetividade na avaliação de risco afeta a priorização, a análise dos ativos vulneráveis e a seleção dos controles.

De acordo com Yevseyeva et al. [59], a identificação de riscos e o desenvolvimento de políticas de segurança na esfera da tecnologia da informação são primordialmente responsabilidades do *Chief Information Security Officer (CISO)*. A seleção de controles de segurança apresenta-se como um desafio significativo. A implementação de uma ampla gama de controles de segurança pode, por um lado, fortalecer a segurança organizacional, mas, por outro, pode impactar negativamente a produtividade devido à necessidade de se aderir a múltiplos procedimentos de segurança. Além disso, essa implementação é frequentemente limitada por restrições orçamentárias.

Yevseyeva et al. [59] entende que a avaliação dos riscos de segurança nas organizações está se tornando cada vez mais complexa e sofisticada, impulsionada pela intensificação do uso de informações e pelo surgimento contínuo de novas ameaças à segurança. Embora padrões de segurança internacionais, como ISO/IEC 27001/27002, forneçam diretrizes e requisitos gerais para o gerenciamento desses riscos, na prática, o CISO enfrenta o desafio de escolher entre centenas de controles possíveis para proteger eficazmente a organização. Embora existam diversas referências sobre aspectos financeiros e análises de custo-benefício na seleção de controles de segurança, é crucial considerar também fatores não monetários. Estes incluem aspectos operacionais e impactos na produtividade. Portanto, a escolha dos controles de segurança deve ser abordada como uma decisão multiobjetivos ou multicritério.

2.8 FRAMEWORKS DE SEGURANÇA

A norma NBR ISO/IEC 27001 [77], estabelecida pela ABNT, destaca-se como um dos guias de segurança mais amplamente reconhecidos e utilizados. Proporciona um modelo abrangente para a criação e operação de um Sistema de Gestão de Segurança da Informação (SGSI). O framework abarca diversos elementos, incluindo políticas, procedimentos, processos e recursos. O diferencial do ISO/IEC 27001 reside na sua abordagem holística, considerando não apenas a tecnologia, mas também as pessoas e os processos [80].

A NBR ISO/IEC 27002 [78] é uma norma internacional que oferece diretrizes para a prática de gestão da segurança da informação. A norma é particularmente utilizada como um recurso complementar à ISO/IEC 27001 e está estruturada em diversos domínios que abordam vários aspectos da segurança da informação. Cada domínio contém objetivos de controle e controles específicos. Esses controles são basicamente as medidas, políticas, procedimentos ou estruturas que ajudam a gerir riscos, reduzindo a pro-

babilidade de um incidente de segurança ou minimizando o impacto de tais incidentes. A norma cobre uma ampla gama de tópicos de segurança da informação, tornando-a uma das diretrizes mais abrangentes disponíveis. A norma é projetada para ser adaptável a diferentes tipos e tamanhos de organizações, oferecendo uma estrutura abrangente que aborda uma variedade de controles de segurança, tornando-se um recurso para organizações que buscam referencias para aprimorar sua segurança [80].

Por sua vez, a NBR ISO/IEC 27002, estabelecida pela ABNT em 2005, representa uma norma internacional que fornece orientações práticas para a gestão da segurança da informação. Essa norma é frequentemente utilizada como um complemento à ISO/IEC 27001 e está organizada em vários domínios que abordam diversos aspectos da segurança da informação. Cada domínio engloba objetivos de controle e controles específicos, os quais compreendem medidas, políticas, procedimentos ou estruturas que auxiliam na gestão de riscos, reduzindo a probabilidade de incidentes de segurança ou minimizando seu impacto. A norma abrange uma extensa gama de tópicos de segurança da informação, consolidando-se como uma das diretrizes mais abrangentes disponíveis. Sua concepção flexível permite a adaptação a diferentes tipos e tamanhos de organizações, fornecendo uma estrutura abrangente que contempla diversos controles de segurança, sendo uma valiosa referência para organizações em busca de aprimorar sua segurança [80].

O NIST Cybersecurity Framework [32] foi desenvolvido pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST). Este framework é focado em ajudar as organizações a gerenciar riscos de segurança cibernética visando o aprimoramento da cibersegurança em infraestruturas críticas, concentra-se na gestão dos riscos cibernéticos associados à Tecnologia da Informação (TI), Sistemas de Controle Industrial (ICS), Sistemas Ciber-Físicos (CPS) e, de forma mais ampla, dispositivos interconectados [81]. Este modelo abrange cinco funções fundamentais (identificação, proteção, detecção, resposta e recuperação), as quais devem ser implementadas por meio de um conjunto de controles de segurança. Seu propósito é apoiar organizações, fornecendo uma linguagem padronizada para compreender, gerenciar e comunicar os riscos de cibersegurança a partes internas e externas. Ele foi criado para ser flexível e adaptável, permitindo que uma ampla gama de organizações o aplique de acordo com suas necessidades específicas. A flexibilidade é uma das características mais notáveis do NIST Cybersecurity Framework. Ele é projetado para ser aplicado a uma variedade de setores e é amplamente adotado em escala global [82].

Os Controles CIS [83]constituem um conjunto de medidas destinadas à defesa cibernética, oferecendo diretrizes específicas e práticas para o fortalecimento da segurança. Desenvolvido pelo Center for Internet Security (CIS), esse *framework* é notadamente orientado para a ação, caracterizando-se por uma abordagem altamente tática. Diferentemente de abordagens mais abstratas, o CIS Controls adota uma postura mais pragmática ao fornecer um conjunto de controles priorizados, derivados de recomendações do NIST, com o objetivo de listar as ações mais efetivas para aprimorar a postura de segurança organizacional [84] [29].

Este conjunto de controles não apenas representa uma compilação de melhores práticas, mas também se fundamenta na expertise do CIS para identificar e hierarquizar as ações de segurança mais impactantes. Cada controle abrange aspectos específicos, abordando desde a identificação de vulnerabilidades até a resposta a incidentes, proporcionando assim uma estrutura abrangente para aprimorar a resiliência cibernética das organizações. A abordagem tática do CIS Controls, baseada na seleção criteriosa e priorização de ações, ressalta sua utilidade prática para organizações que buscam melhorar proativamente sua postura de segurança cibernética em um cenário dinâmico e desafiador [84] [29].

O NIST Special Publication 800-53, conforme documentado por NIST [66], figura como uma das publicações mais abrangentes no que tange aos controles de segurança em sistemas de informação. Cada controle é categorizado em famílias e minuciosamente descrito, incluindo diretrizes pormenorizadas sobre sua implementação e orientações acerca da mensuração de sua eficácia. A publicação NIST SP 800-53 aborda cada controle de segurança de maneira detalhada, proporcionando um elevado nível de especificidade.

É notável que o NIST SP 800-53 pode ser empregado de forma sinérgica com o framework Risk Management Framework [39] (NIST, 2018) para a gestão de riscos, oferecendo, assim, uma abordagem abrangente para a segurança da informação e a gestão de riscos. Embora inicialmente concebido para sistemas de informação federais nos Estados Unidos, o NIST SP 800-53 transcende suas fronteiras originais, sendo adotado como referência por diversas instituições internacionais e outros *frameworks*. Essa universalidade destaca a relevância e a aplicabilidade do NIST SP 800-53 em contextos globais, consolidando sua posição como um recurso fundamental para a implementação de práticas robustas de segurança da informação em nível internacional e como referência para outros modelos de referência [85] [86].

O COBIT, um framework de governança de Tecnologia da Informação, amplamente reconhecido por sua abordagem abrangente, que também abrange áreas diversas áreas da segurança da informação. Desenvolvido pela ISACA, este framework proporciona uma perspectiva integrada e de alto nível para a governança e gerenciamento das demandas organizacionais em um contexto de TI. O framework COBIT destaca-se por oferecer um conjunto de princípios e diretrizes que orientam as práticas de governança e gestão de TI, proporcionando uma estrutura consolidada para alinhar os objetivos de TI com os objetivos organizacionais mais amplos. Ao enfatizar a governança como um elemento fundamental, o COBIT oferece um roteiro valioso para o estabelecimento de controles, processos e métricas, visando otimizar o valor gerado pelos investimentos em TI. A sua aplicação não apenas facilita a conformidade com regulamentações, mas também promove a eficiência operacional e a resiliência diante de desafios cibernéticos em um ambiente tecnologicamente dinâmico. Dessa forma, o COBIT emerge como uma ferramenta significativa para organizações que buscam aprimorar a governança e gestão de TI em consonância com as metas estratégicas e operacionais [87].

O MITRE ATT&CK (*Adversarial Tactics, Techniques, and Common Knowledge*) é comumente designado como um framework, no entanto, uma descrição mais precisa seria a de um "modelo de conhecimento"que detalha o comportamento das ameaças cibernéticas. O ATT&CK oferece uma matriz minuciosa de táticas e técnicas que adversários podem empregar para comprometer, operar e movimentar-se dentro de redes. Este modelo revela-se particularmente valioso para a compreensão do ciclo de vida de um ataque e dos métodos que um adversário pode adotar. A matriz ATT&CK é estruturada conforme as fases de um ataque cibernético, iniciando-se pelo reconhecimento e estendendo-se até a exfiltração de dados e o comando e controle [33]. O diferencial do ATT&CK reside na sua ênfase em compreender como os adversários realmente conduzem suas operações, permitindo, assim, uma abordagem mais proativa e adaptativa à defesa cibernética. Este modelo pode ser instrumental na identificação de lacunas e no aprimoramento da postura de defesa. Embora o MITRE ATT&CK não se configure exatamente como um *framework* de segurança destinado a estabelecer políticas e procedimentos, constitui-se como uma ferramenta que complementa outros *framework* de segurança, fortalecendo, consequentemente, a postura de segurança cibernética de uma organização [88].

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

A Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), instituída pelo Conselho Nacional de Justiça (CNJ) em 2021 [89], constitui uma abordagem contextualizada ao cenário brasileiro, visando estabelecer diretrizes e ações específicas para salvaguardar o Poder Judiciário de ameaças cibernéticas. Importante ressaltar que muitos dos controles de segurança implementados na ENSEC-PJ foram inspirados ou adaptados a partir do CIS Controls v7. Esta estratégia propõe a integração de um modelo de governança em segurança cibernética com a estrutura de governança corporativa existente, alinhando suas diretrizes e ações com práticas gerais de governança e estratégia organizacional. As áreas temáticas abrangidas pela ENSEC-PJ incluem a proteção de infraestruturas críticas, avaliações de risco, implementação de controles de segurança, gestão de identidade e acesso, resiliência cibernética, capacitação e estratégias para gestão de crises cibernéticas.

Em complemento, o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ), instituído pela Portaria CNJ n. 162 de 10 de junho de 2021 [35], enfatiza a necessidade de uma avaliação contínua dos riscos associados às atividades críticas dos órgãos judiciários, essenciais para a manutenção dos seus produtos e serviços. A gestão adequada desses riscos, orientada em parte pelos princípios do CIS Controls v7, é crucial para garantir a continuidade operacional e a integridade dos serviços prestados pelo Poder Judiciário.

2.9 ATIVIDADES E PROCESSOS DE NEGÓCIO DOS TRIBUNAIS

A Cadeia de Valor é uma ferramenta de gestão empregada para representar de forma gráfica os macroprocessos e os principais processos desenvolvidos por uma organização no cumprimento de sua missão institucional. Este instrumento, ao ilustrar visualmente o conjunto de atividades executadas, facilita a compreensão de como valor é agregado aos produtos e serviços oferecidos. Ele permite uma análise abrangente tanto dos processos finalísticos quanto dos processos de apoio, destacando suas inter-relações e dependências [90].

As Cadeias de Valor dos diversos tribunais, conforme ilustrado nas figuras correspondentes, são reflexos distintos das estruturas e dinâmicas organizacionais de cada instituição. Por exemplo, a Cadeia de Valor do Supremo Tribunal Federal (STF) é detalhadamente apresentada na Figura 2.13. De forma similar, a Figura 2.16 desvenda a Cadeia de Valor do Superior Tribunal de Justiça (STJ). Além disso, o terceiro nível dos processos finalísticos do Tribunal de Justiça do Paraná (TJPR) é enfatizado na Figura 2.14, enquanto a Cadeia de Valor do Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT) é ilustrada na Figura 2.15. Cada uma dessas representações gráficas não apenas destaca os eixos de atuação, macroprocessos, processos e atividades principais inerentes a cada tribunal, mas também sublinha a importância de tais elementos na geração de valor organizacional.

Através da análise comparativa das Cadeias de Valor dos tribunais STF, TJPR, TJDFT e STJ, uma característica comum e essencial torna-se evidente: a predominância das atividades jurisdicionais, que formam o núcleo das suas missões institucionais. Essas atividades, cruciais para a administração da justiça, permanecem como elementos centrais e decisivos em todas as cadeias de valor, independentemente das

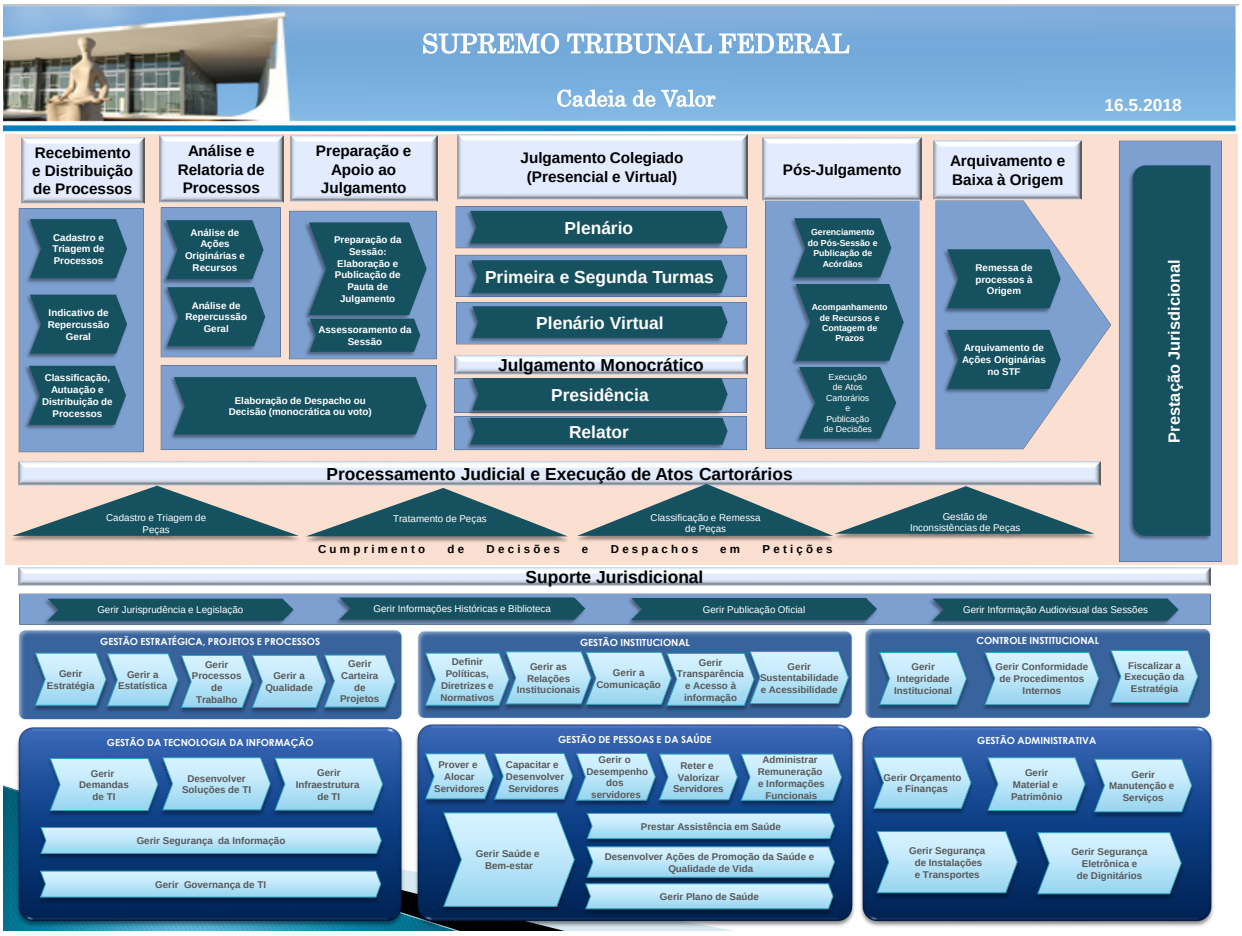


Figura 2.13: Cadeia de Valor do STF.
Fonte: Supremo Tribunal Federal [90]

Figura 2.14: 3º Nível da Cadeia de Valor do TJPR.
Fonte: Tribunal de Justiça do Paraná [91]

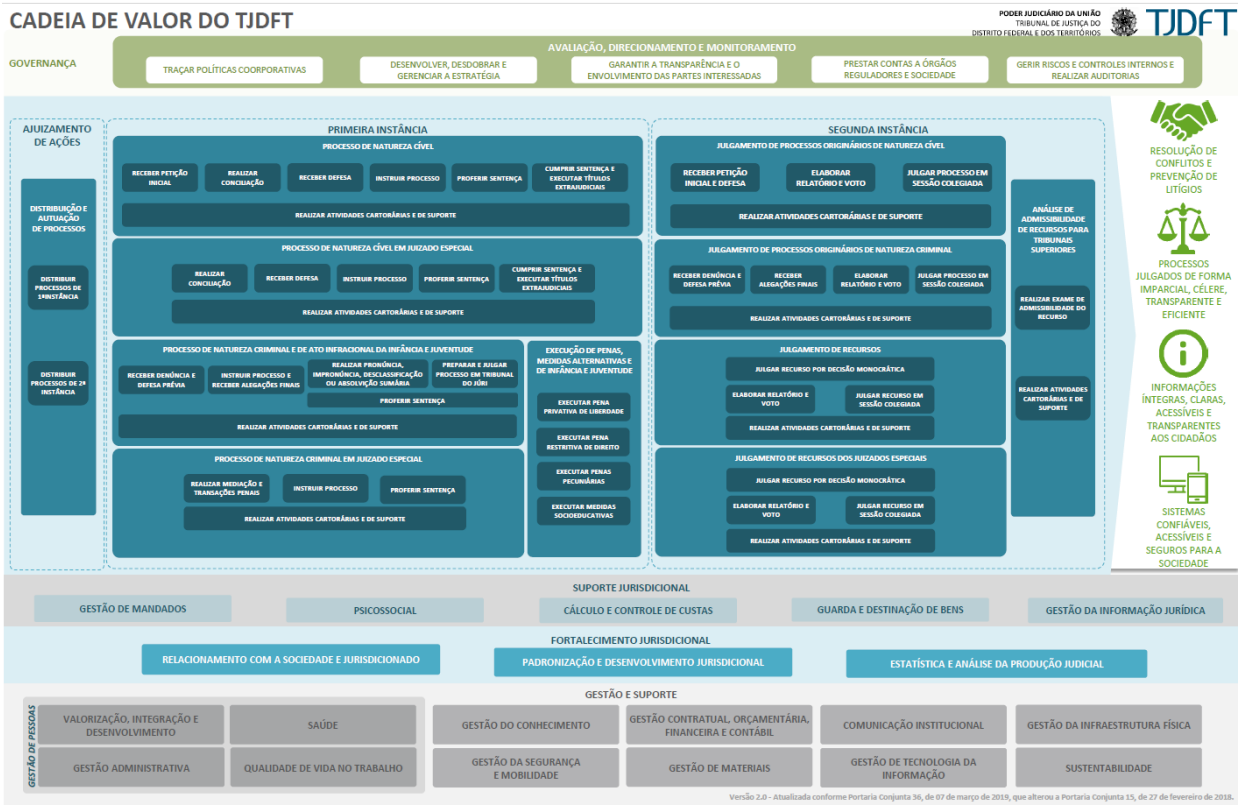


Figura 2.15: Cadeia de Valor do TJDFT.
Fonte: Tribunal de Justiça do Distrito Federal e Territórios [92]

Figura 2.16: Cadeia de Valor do STJ.
Fonte: Superior Tribunal de Justiça [93]

diferenças estruturais e operacionais específicas de cada tribunal.

2.10 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 [94] 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".

Wanderley [95] 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 [43], traçando paralelo com área bancária e a adoção pelo Banco Central do Brasil da categorização de riscos operacionais previstos na "Basileia II", propôs a definição de uma taxonomia para a categorização de riscos operacionais do Poder Judiciário que pudesse servir como linguagem comum aos órgãos do Poder Judiciário para a identificação e categorização dos riscos operacionais.

No estudo conduzido por Costa [96], a dinâmica de comunicação entre membros de equipes que operam de maneira remota no âmbito judicial é analisada. Costa explora não apenas o compartilhamento de informações, mas também avalia os riscos associados e propõe formas de estruturação efetiva das atividades judiciais em um contexto virtual. A pesquisa de Costa destaca a importância crítica de estabelecer uma padronização na gestão do conhecimento e nas práticas de comunicação. Para isso, sugere a necessidade de uma regulamentação mais abrangente por parte da alta gestão do Judiciário e a estruturação de canais virtuais dedicados para centralizar e facilitar o compartilhamento de informações entre os membros das equipes. Além disso, enfatiza a importância da utilização de instrumentos tecnológicos que sejam autorizados pelo respectivo Tribunal, como uma medida para garantir a segurança e a eficiência da comunicação.

Leite [97] 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.

Barrêto [98] pesquisou sobre como ocorreu a implantação dos processos de segurança, a criação do Comitê Gestor de Segurança e da Política de Segurança da Informação no âmbito do Tribunal de Justiça do Estado do Tocantins. Tendo utilizado a Norma da ABNT NBR ISO/IEC 27002 como um instrumento para identificação e análise dos processos adotados na Política de Segurança da Informação e avaliação do grau de maturidade em segurança da informação.

Schwaitzer [99] foca nos desafios de garantir a confidencialidade, integridade e disponibilidade da informação arquivística digital produzida pelo Poder Judiciário e enfatiza que a principal dificuldade é proteger essas informações contra exposição indevida, alterações não autorizadas e obsolescência rápida. A pesquisa conclui que a falta de uma abordagem integrada para lidar com segurança, acesso e preservação da informação é um problema significativo. Sendo necessária a classificação adequada da informação, a partir da análise de seu valor e requisitos legais, para assim mitigar os riscos e garantir o acesso à informação.

Oliveira e Cunha [100] avaliam indicadores sobre o Poder Judiciário e discutem as limitações, os desafios e o uso da tecnologia. Os autores indicam que o foco principal do uso da tecnologia não tem sido a melhoria da prestação jurisdicional ou aprimoramento de políticas públicas a fim de incrementar a qualidade do serviço prestado ao cidadão. Ademais, formulam a necessidade de emprego de *big data* como ferramenta para monitoramento efetivo das instituições e troca de informações para garantir dados confiáveis.

Moura [101] realizou levantamento da gestão de segurança da informação do Poder Judiciário com base em levantamentos de Governança de Tecnologia da Informação do Tribunal de Contas da União de 2014 e de 2016. Foram analisados 21 subitens relacionados à gestão corporativa de segurança da informação. Os resultados indicam que, apesar dos avanços na evolução crescimento na consciência sobre a segurança da informação nos entes do Judiciário, desafios significativos persistem, especialmente na implementação efetiva de políticas e práticas. O autor sugere a continuidade dos esforços para alinhar as práticas de segurança da informação às melhores práticas internacionais.

Filho [102] analisa a maturidade das políticas de segurança da informação nos tribunais superiores do judiciário brasileiro, um aspecto crucial da Governança de TI. Avaliando a aderência dessas políticas às melhores práticas, o estudo revela variações significativas na maturidade entre os tribunais. Comparando com o Poder Executivo, o nível considerado alto no Poder Judiciário é apenas razoável no Executivo, indicando discrepâncias entre os poderes. Entre os tribunais superiores, o Superior Tribunal de Justiça (STJ) destaca-se com o maior nível de maturidade, enquanto o Superior Tribunal Militar (STM) apresenta o menor, não possuindo sequer uma política de segurança da informação vigente. Aponta-se a necessidade de esforços concentrados em aprimorar as políticas de segurança da informação, buscando aumentar a efetividade e o cumprimento dessas políticas, fundamentais para a gestão de arquiteturas de informação em alinhamento com estratégias corporativas.

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 [103].

Gordon e Garrie [104] reforçam a importância da segurança cibernética para a proteção do processo judicial e indicam alguns princípios e 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.

O Escritório das Nações Unidas sobre Drogas e Crime no documento *Construindo uma gestão de riscos abrangente no Judiciário* [105] (em tradução livre) aborda a pouca atenção dada a questões de corrupção no sistema judicial, falta de política específicas anticorrupção e a gestão simplificada de riscos

no Judiciário. Se destacando a importância de se tratar riscos éticos e de integridade e estes resultam em baixo nível de confiança no sistema judicial. Indica-se ser imperativo promover uma abordagem holística para a construção da integridade judicial, que inclua a revisão de mecanismos de conflitos de interesse, a implementação de sistemas de gestão de casos eficazes, canais seguros de denúncia para delatores e treinamento especializado. Além disso, as políticas anticorrupção setoriais devem ser desenvolvidas em coordenação com organismos nacionais anticorrupção. O compromisso da liderança é um elemento crítico em qualquer programa de redução de riscos de corrupção.

Rast [2] discute ameaças cibernéticas enfrentadas pelo judiciário e profissionais da área legal. Aborda a sofisticação de ameaças que podem utilizar IA generativa, bem como *ransomware*, *phishing*, engenharia social, vazamento de dados, uso de redes inseguras, senhas fracas, *malwares*, vulnerabilidades de terceiros e ameaças internas podem ser utilizados por atacantes para roubar ou corromper dados. A autora destaca quem o primeiro passo deve ser identificar as causas potenciais dos riscos e que o tribunal deve realizar avaliação de riscos definir o acesso a dados críticos e sensíveis, incluindo arquivos judiciais, minutas, comunicações internas e informações de identificação pessoal e outras informações judiciais confidenciais. Sendo recomendada a implementação de boas práticas de segurança cibernética a avaliação de riscos, treinamento de pessoal e monitoramento de segurança para proteger dados judiciais sensíveis. Como controles se recomenda a autenticação multifatorial (MFA), VPNs, sistemas de detecção e resposta em endpoints (EDR), criptografia de dados e atualizações regulares de software, enfatizando a necessidade contínua de conscientização e treinamento.

Senécal e Benyekhlef [106], analisa os impactos e riscos jurídicos da integração de tecnologias de informação no sistema de justiça, denominada *cyberjustice*. Discute-se a transformação histórica dos sistemas legais com a evolução das mídias e a inclusão de tecnologias como arquivamento eletrônico e gestão de processos em procedimentos judiciais. A necessidade de uma avaliação abrangente dos riscos jurídicos associados a essas mudanças é um ponto crucial. Os autores propõem uma metodologia para essa avaliação, centrada na análise dos componentes informacionais dos sistemas, como fluxos de informação e processos. Esta abordagem tem como objetivo identificar e gerenciar os riscos potenciais aos princípios fundamentais da justiça. Enfatizam o impacto da justiça cibernética em direitos fundamentais e princípios do sistema de justiça, como equidade e acesso à justiça. Destaca-se a importância de pesquisas multidisciplinares para entender as consequências da justiça cibernética na sociedade, abarcando perspectivas culturais, econômicas, sociológicas e psicológicas. Os autores fornecem uma visão sobre como as tecnologias da informação estão remodelam o sistema de justiça e as complexas implicações legais que acompanham essa transformação, apontando para a necessidade de uma abordagem abrangente e multidisciplinar na avaliação dos riscos e oportunidades apresentados pela justiça cibernética.

A Comissão Europeia para a Eficiência da Justiça (CEPEJ) (em tradução livre) [107], no documento *Toolkit for supporting the implementation of the Guidelines on how to drive change towards Cyberjustice*, trata das diretrizes para o uso de tecnologias de informação e comunicação (TIC) no sistema de justiça para melhorar sua eficiência, acessibilidade e eficácia de administração da justiça. Dentre as premissas incluem a gestão eletrônica para o acompanhamento e a administração dos processos, realização videoconferência para conduzir audiências judiciais, digitalização de documentos judiciais e processos, plataformas de acesso público às informações jurídicas, uso de inteligência artificial e análise de dados e, por fim, a segurança cibernética e proteção de dados contra ataques cibernéticos e violações de dados.

Destaca-se no documento [107] a necessidade de um equilíbrio pragmático na segurança dos sistemas, evitando tanto a excessiva rigidez que inibe iniciativas quanto uma segurança frouxa que exponha o sistema a riscos. A análise e gestão de riscos de segurança são cruciais, exigindo avaliações periódicas que considerem a probabilidade e a gravidade dos danos potenciais. É enfatizada a importância da interoperabilidade dos sistemas e da circulação segura de informações e dados. Dentre os riscos que precisam ser avaliados, são incluídos ataques a sistemas de informação (ex: vírus, cavalos de troia), ataques de hackers a servidores web e sistemas internos, roubo de dados por e-mail (*phishing*), indisponibilidade de indivíduos-chave para a operação suave de sistemas de TI, perdas de dados devido a problemas técnicos ou operacionais, falhas elétricas, incêndios em centros de computação ou armazenamento de dados, danos por inundações e roubo de dados por funcionários. São estabelecidos também horários de operação e tempos de retorno à operação em caso de incidentes.

Observa-se adicionalmente existência de estudos voltados para a condução de avaliações de risco no contexto específico da justiça criminal nos EUA, haja vista a prática estabelecida de tomada de decisão da libertação de presos com base na avaliação de riscos que considere a probabilidade de reincidência de delitos. Assim, as decisões orientadas por avaliações de risco podem ser vistas como mais defensáveis e credíveis do que processos de tomada de decisão mais subjetivos e menos transparentes [108].

Apesar dessas contribuições, não se identificou estudos que objetivassem identificar de forma objetiva quais seriam os riscos de negócio ou operacionais das atividades principais do Poder Judiciário, bem como se observou uma lacuna no estudo dos controles de segurança da informação específicos que poderiam ser implantados para o tratamento de riscos do Poder Judiciário Brasileiro.

3 METODOLOGIA

O presente estudo caracteriza-se como uma pesquisa de natureza aplicada, com o objetivo principal de contribuir para a solução de problemas concretos e específicos. Esta classificação alinha-se com a definição de Silva e Menezes [109], que apontam a pesquisa aplicada como voltada para a aplicação prática e direta dos conhecimentos gerados.

Em termos metodológicos, o estudo adota uma abordagem qualitativa, buscando interpretar e compreender fenômenos complexos do mundo real que são intrinsecamente subjetivos e, portanto, dificilmente mensuráveis de forma quantitativa. A abordagem qualitativa oferece a flexibilidade necessária para investigar a profundidade e a complexidade das experiências e observações humanas. Se mostrando adequada para se a explorar as percepções e sentimentos dos atores envolvidos na definição de estratégias de segurança da informação, no desenvolvimento de táticas que visem aplicar tais ou na aplicação prática daquilo estabelecido em nível de gestão, que muitas vezes estão fora do escopo de estudos quantitativos [109].

O objetivo da pesquisa é descritivo e exploratório. Segundo Silva e Menezes [109], pesquisas com natureza descritiva buscam detalhar e elucidar as características específicas de uma determinada população ou fenômeno. Elas são fundamentais para obter uma visão mais completa e profunda sobre o assunto em estudo. Além disso, tais pesquisas podem também se concentrar no estabelecimento de relações entre variáveis, permitindo entender como uma variável pode influenciar ou estar associada a outra. Esse tipo de abordagem é essencial para identificar padrões, tendências e possíveis causalidades no cenário investigado. O método mais comum para a coleta de dados em pesquisas descritivas é o levantamento.

Pesquisas de natureza exploratória são essenciais quando se busca aprofundar na compreensão de um problema pouco estudado ou cujos conceitos relacionados ainda não estão bem estabelecidos. Considerando a constatação da escassez de trabalhos científicos que avaliassem os riscos de segurança da informação no Judiciário, a opção pela pesquisa exploratória se mostrou adequada pois esta tem como objetivo principal esclarecer e refinar conceitos, desenvolver hipóteses precisas ou descobrir novas intuições sobre o tema. Uma característica distintiva é a sua flexibilidade, permitindo ajustes e reorientações conforme novos dados são coletados. Para ganhar familiaridade com o problema e estabelecer bases para futuras investigações, tais pesquisas envolvem a coleta de dados por meio levantamento bibliográfico e documental, entrevistas semiestruturadas e a análise de estudos de caso [110].

Considerando que o objetivo geral deste estudo é propor uma relação de controles de segurança da informação que sirva de referência para a aplicação de medidas que tenham o potencial de reduzir as probabilidades de eventos de risco que impactem negativamente nas atividades essenciais do judiciário brasileiro, bem como os objetivos específicos descritos na subseção *1.3.2 Objetivos específicos*, este estudo foi realizado em três fases distintas. Conforme consta da Figura 3.1, foram estabelecidos objetivos para cada fase do estudo, a saber:

- Fase 1 - identificar os principais riscos de negócio das atividades primordiais do Poder Judiciário, que poderiam ser os fatores geradores de tais riscos e que consequências poderiam ser enfrentadas em caso de materialização do risco;

- Fase 2 - realizar o levantamento das medidas de segurança que, se aplicadas, poderiam tratar os riscos;
- Fase 3 - analisar os dados obtidos e buscar formas de apresentar os resultados de forma que auxiliasse os órgãos a definir responsáveis, ações prioritárias e melhorias que poderiam ser perseguidas.

Figura 3.1: Primeira fase da pesquisa.
Fonte: do Autor

Para o alcance da objetivo previsto para primeira fase da pesquisa, conforme ilustra a Figura 3.2, foi necessário realizar várias etapas metodológicas.

Realizou-se inicialmente pesquisa bibliográfica em periódicos e congressos acadêmicos e pesquisa documental de órgãos de controle externo, instâncias superiores do Poder Judiciário e padrões publicados por organizações internacionais. O objetivo da pesquisa era caracterizar as fases mandatórias para o processo de avaliação de riscos e a existência de trabalhos anteriores que identificassem quais seriam os riscos de negócio inerentes à atividade-fim do Poder Judiciário Brasileiro.

Para a definição das atividades principais do Poder Judiciário foram utilizadas as cadeias de valor de diferentes tribunais [90] [93] [91] [92].

Considerando os objetivos deste estudo e que Crouhy [37] declara que a literatura geralmente agrupa essas categoriais de risco, neste estudo a categoria **riscos de negócio** está englobando também a categoria de riscos legais e regulatórios, os riscos estratégicos e os riscos de reputação.

Salienta-se que o termo *business risk* também pode ser traduzido como risco empresarial. Contudo, esta expressão pode não representar o significado adequado para organizações públicas. Enquanto o objetivo principal de empresas é essencialmente o retorno sobre o investimento e a sua conservação em um ambiente competitivo, as instituições públicas visam a prestação de serviços essenciais à sociedade e o bem comum.

Para a identificação dos riscos de negócio, adotou-se uma técnica fortemente recomendadas pela norma ABNT NBR 31010 [49] para esse fim: entrevistas semiestruturadas.

Foram conduzidas entrevistas semiestruturadas com oito gestores públicos com vasta experiência e atuação em Tribunais Superiores e Regionais. Cada entrevistado respondeu a um conjunto de questões pré-definidas, destinadas a explorar as experiências profissionais relacionadas a situações de risco e a avaliar

Figura 3.2: Primeira fase da pesquisa.
Fonte: do Autor

cenários sob diferentes perspectivas [49]. Dos entrevistados, quatro possuem formação em direito e atuam no assessoramento de Ministros de Tribunais Superiores; três trabalham em áreas relacionadas à tecnologia da informação, e um está envolvido na gestão de riscos corporativos em seu respectivo órgão. O tempo médio de experiência desses profissionais no Judiciário é de aproximadamente 20 anos.

Na realização das entrevistas semiestruturadas, se seguiu o roteiro básico:

1. Apresentação do pesquisador e esclarecimento dos objetivos da pesquisa.
2. Esclarecimento sobre a estrutura da entrevista e garantia de anonimato das respostas, incentivando o entrevistado a discutir abertamente sobre situações de risco vivenciadas ou conhecidas, visando contribuir para o aprimoramento das instituições judiciárias.
3. Convite ao entrevistado para apresentar-se, indicando suas áreas de formação e atuação, além de compartilhar sua trajetória profissional.
4. Contextualização de incidentes de grande impacto ocorridos em órgãos do Poder Judiciário, ilustrados por meio de manchetes de matérias jornalísticas de veículos de comunicação.
5. **Pergunta 1**: Em sua opinião, é relevante identificar os riscos específicos inerentes ao negócio judiciário? Por quê?
6. **Pergunta 2**: Acha pertinente identificar as possíveis causas e/ou consequências desses riscos? Por quê?
7. **Pergunta 3**: Já presenciou alguma rotina ou evento que, na sua visão, represente um risco para a elaboração ou execução de um despacho ou decisão judicial? Se sim, poderia descrevê-los?
8. **Pergunta 4**: Acredita que existem controles adequados implementados para mitigar tais riscos?
9. Apresentação de uma lista inicial de riscos com base em eventos ocorridos, visando introduzir novos cenários e perspectivas sobre os riscos identificados.

10. **Pergunta 5**: Há algum risco adicional que gostaria de indicar ou gostaria de destacar quais riscos considera mais relevantes?
11. **Pergunta 6**: Os controles existentes na sua organização são considerados adequados para o tratamento desses riscos? Há algum controle adicional que sugeriria?
12. Agradecimento pela participação e questionamento sobre a indicação de outros possíveis participantes para a pesquisa.

Nas sessões de entrevistas foi permitindo que os entrevistados trouxessem novos aspectos sem se limitar aos aspectos relacionados no roteiro. As entrevistas tiveram duração entre 1 hora e meia e 2 horas. No decorrer das entrevistas se verificou que as respostas gradativamente se tornaram mais repetitivas e que a introdução de novos elementos ou aspectos decaía. Ao final da realização de oito entrevistas, entendeu-se que foi alcançada a saturação empírica e que o extenso volume dados coletados eram suficientes para compreender o fenômeno investigado [111].

Posteriormente, as informações coletadas foram analisadas e categorizadas. Utilizou-se o método *Bow Tie* descrito na Norma ABNT 31010 [49] para distinguir entre as causas, os riscos e as consequências identificadas durante as entrevistas. Cabe ressaltar que, nesta etapa inicial, foram registradas as medidas preventivas ou mitigatórias propostas pelos entrevistados para os riscos indicados, porém eles ainda não foram abordados nesta fase.

Finalmente, para a revisão e análise crítica dos resultados da Fase 1, foi realizada sessão de grupo focal composto por seis especialistas em gestão de riscos e segurança da informação, com experiências em diversas instituições judiciárias tais como TRF1, CJF, TST, STF, STJ e TSE. Durante esta oficina, apresentou-se uma proposta para a separação e categorização de causas, riscos e consequências, que foi então submetida à análise crítica do grupo.

Conforme descrito por Ribeiro et al. [112], o grupo focal é uma metodologia de coleta de dados qualitativos amplamente reconhecida e utilizada em pesquisa. Esse método consiste em reunir um conjunto de indivíduos que possuem conhecimento ou experiência sobre o tema em questão. O objetivo do grupo focal é enriquecer a pesquisa ao proporcionar um espaço para discussão focada, permitindo que o pesquisador obtenha *insights* mais profundos sobre percepções, sentimentos e atitudes dos participantes em relação ao tema estudado. Essa técnica é especialmente útil para captar a complexidade das opiniões e experiências dos participantes, fornecendo informações que podem ser fundamentais para a tomada de decisões organizacionais.

A Fase 1 da pesquisa é concluída após a obtenção da relação dos riscos de negócio relativos às atividades principais do Poder Judiciário, quais eventos podem fazer com que os riscos se materializem (causas) e quais consequências poderão ser observadas em caso da eventualidade do risco.

A segunda fase se iniciou por pesquisa bibliográfica com o objetivo de identificar estratégias e diretrizes de boas práticas para a implementação de medidas de segurança da informação, também conhecidas como controles de segurança. Esses controles têm o intuito de efetivamente proteger e mitigar riscos associados a confidencialidade, integridade e disponibilidade das informações. Com base nessa avaliação foi selecionado um *framework* de segurança para servir como base para a seleção dos controles.

A Figura 3.3 demonstra a sequência de etapas compreendidas na segunda fase da pesquisa.

Figura 3.3: Segunda fase da pesquisa.
Fonte: do Autor

Realizou-se a análise detalhada das causas dos riscos de negócio, comparando-as com a lista de controles recomendados pelo *framework* de segurança, e se relacionou os controles que potencialmente poderiam reduzir a probabilidade de ocorrência de cada risco ou o impacto decorrentes da materialização do evento de risco. Ademais, efetuou-se a revisão das respostas indicadas nas entrevistas e a complementação da relação de controles com aqueles que tinham sido propostos pelos entrevistados para o tratamento dos riscos sinalizados. Este procedimento resultou na identificação de um conjunto preliminar de controles aplicáveis a cada causa de risco específica.

Para aprimorar a qualidade e a abrangência da análise dos controles propostos, optou-se por utilizar a técnica de grupo focal para a revisão e crítica dos resultados obtidos. Para o contexto, o grupo focal foi composto por gestores de TI com experiência significativa em áreas como segurança da informação, segurança cibernética e gestão de riscos. Estes profissionais atuam como gestores de várias instituições judiciárias de importância, como TRF1, CJF, PF, TST, TSE, STJ e STF. Um total de oito sessões de grupo focal com duração média de duas horas cada, foram realizadas para avaliar e validar os controles identificados na fase de análise preliminar.

Na primeira sessão de grupo focal foi apresentada a planilha com a relação dos controles relacionados pelo pesquisador e se procedeu a análise e crítica ponto-a-ponto pelo grupo quanto a aplicabilidade da medida de segurança para o tratamento do risco operacional relacionado. Contudo, tal abordagem não se mostrou muito produtiva. Nas sessões subsequentes era previamente indicado quais grupos de controles seriam avaliados e se buscou discutir apenas os pontos que demandavam ajustes, seja pela remoção, modificação ou complementação de controles.

Durante estas sessões de grupo focal, ficou evidente que, embora o *framework* fosse um guia extenso e robusto, ele não cobria completamente alguns riscos operacionais críticos, particularmente aqueles que não estão estritamente ligados a questões tecnológicas. Nesses casos, os membros do grupo focal propuseram controles adicionais ou alternativos, baseados em suas próprias avaliações e experiências, para tratar as lacunas em relação às causas dos riscos de negócio identificados. Em alguns casos foi necessário pesquisar

fontes e referências adicionais de outros guias e normas de segurança que foram indicadas pelos integrantes do grupo focal, que serviram de base para a discussão conjunta das práticas identificadas e para a formação de entendimentos do grupo.

Portanto, essa fase é concluída com a relação de controles obtida pela combinação dos controles indicados nas entrevistas, com a análise preliminar de controles do *framework* e os *insights* qualitativos fornecido pelo grupo focal, resultando em uma abordagem de tratamento de riscos mais abrangente e adaptada às especificidades das instituições judiciárias.

Na Fase 3 da pesquisa, o principal objetivo foi realizar uma análise e revisão minuciosa dos dados coletados e avaliar formas de classificação das informações de forma que fosse possível identificar correlações e prioridades, conforme demonstra a Figura 3.4 com os passos seguidos durante a Fase 3 da pesquisa. Considerando o grande volume de informações, foi necessário também estabelecer técnicas de *Business Intelligence* para uma apresentação, acesso e interpretação dos dados de forma mais natural. Para este fim, foram empregados os softwares especializados *Power BI* e *Tableau*.

Figura 3.4: Terceira fase da pesquisa.
Fonte: do Autor

Primeiramente, os controles de segurança foram categorizados para fornecer uma compreensão mais clara sobre os tipos de medidas de segurança que poderiam ser aplicadas. Na classificação das **categorias de controles**, utilizou-se como uma das referências a taxonomia proposta por Machado [43] por se tratar de um estudo que foi direcionado para o contexto do Judiciário. No entanto, devido à extensão e diversidade das informações coletadas e à necessidade de sintetizar cada categoria de controle em um único termo descritivo, optou-se por adaptar esta taxonomia multicamadas para um sistema mais enxuto de categorização unidimensional.

A etapa subsequente implicou na classificação dos **tipos de ativos** associados a cada controle levantado durante a pesquisa. Essa classificação de ativos se mostrou necessária para servir como base orientativa e de identificação dos responsáveis que provavelmente serão responsáveis pela implementação dos controles, bem como para padronização das informações de cada controle pois o *framework* escolhido já implementa tal classificação em seus controles recomendados. Ademais, foi necessário classificar os controles de segurança adicionais para o padrão das **funções de segurança** utilizado pelo guia de referência.

O processo de categorização foi estendido ainda à determinação das **prioridades para a implementação** dos controles. Adotou-se o mesmo procedimento para classificação dos grupos de implementação (IG1, IG2 e IG3) dos controles utilizada no *framework* adotado para a definição das prioridades de implementação dos controles. É recomendado se iniciar a implementação dos controles pelo Grupo de Implementação 1 (IG1), que constitui as medidas de cibernética essenciais para qualquer organização pois se trata de uma lista de ações com menor complexidade e custo de implementação [113]. Além de serem medias basilares para a implementação de contramedidas mais complexas. Tendo em vista estes parâmetros, foi realizada essa classificação com relação aos controles adicionais propostos neste estudo.

Por fim, os resultados obtidos foram interpretados e comparados com os conceitos da literatura e revisão de estudos anteriores. Este último passo é essencial para entender o que os dados representavam, como poderiam ser aplicados para validar a confiabilidade dos resultados [114].

Ressalta-se que a metodologia adotada buscou propor diretrizes para a mitigação de riscos que pudessem ser utilizadas por todos os órgãos do Poder Judiciário, porém sem expor fragilidades ou riscos específicos das instituições envolvidas nas variadas etapas da pesquisa.

4 ANÁLISE DE RESULTADOS

Este estudo busca alcançar diversos objetivos interligados, visando uma compreensão integrada e aplicada ao cenário de riscos e controles de segurança da informação no contexto do Poder Judiciário. Primeiramente, o levantamento e a compreensão das atividades-chave deste ramo formam a base para a identificação dos riscos de negócio mais prementes. Uma vez identificados, esses riscos serão submetidos a uma análise aprofundada para mapear suas causas e consequências potenciais. Paralelamente, o estudo pretendia estabelecer um método para correlacionar esses riscos com controles de segurança cibernética, selecionando, nesse contexto, um *framework* de segurança cibernética que seja mais adequado às especificidades do Judiciário. A partir dessa escolha, a pesquisa visa mapear quais controles de segurança cibernética seriam mais eficazes na mitigação dos riscos de negócio identificados, contribuindo para uma estratégia de priorização na implementação desses controles. Por último, o estudo pretendia elucidar como as ações operacionais de segurança cibernética, ou a ausência delas, têm o potencial de impactar diretamente as atividades-fim do Poder Judiciário. Desse modo, os resultados esperados incluíam fornecer uma visão integrada e estratégica que favorecesse tanto a tomada de decisão informada quanto a eficácia operacional, em termos de segurança e integridade do sistema judicial. Foram obtidos os seguintes resultados.

4.1 FASE 1

4.1.1 Atividades principais

Dentro do contexto do Poder Judiciário, um conjunto de eixos de atuação, macroprocessos, processos e atividades se mostram essenciais para o funcionamento do sistema judicial. Conforme delineado pelas cadeias de valor do STF [115], STJ [93], TJPR [91] e TJDFT [92], há uma uniformidade básica nos processos de prestação jurisdicional, observada em todos os níveis do sistema judiciário brasileiro. As atividades relativas ao processamento judicial e execução de atos cartorários, diretamente relacionadas com a prestação jurisdicional, são os principais pilares dos tribunais.

Tal consistência não apenas reforça a importância central desses processos, mas também serve como um indicativo fundamental para direcionar as iniciativas de segurança da informação. Ao compreender as atividades jurisdicionais como essenciais, torna-se evidente que a segurança da informação deve ser priorizada nessas áreas, garantindo a proteção e integridade dos dados e procedimentos críticos ao funcionamento eficiente do judiciário.

A Tabela 4.1 relaciona esses agrupamentos de ações abrangentes para as todas as instituições judiciárias e que são fundamentais para a atividade finalística do Poder Judiciário.

Tabela 4.1: Atividades Principais do Poder Judiciário

Id	Atividades Principais
1	Recebimento e a Distribuição de Processos

Tabela 4.1: Atividades Principais do Poder Judiciário

Id	Atividades Principais
2	Análise e a Relatoria de Processos
3	Formulação das Decisões Judiciais
4	Julgamento Monocrático ou Colegiado
5	Processamento das Decisões
6	Execução dos Atos Cartorários
7	Cumprimento dos Despachos e Decisões

Este conjunto de atividades abrange a gama de operações judiciais, mas também reflete a complexidade inerente ao sistema judicial. Cada etapa possui seu próprio conjunto de desafios, requisitos e impactos, que, por sua vez, têm implicações diretas tanto para a eficiência operacional do Judiciário quanto para a unicidade do sistema como um todo. Compreender o valor intrínseco de cada processo de trabalho e as suas interconexões é vital para buscar formar de otimização da qualidade da prestação jurisdicional e da eficiência do Poder Judiciário.

O principal normativo de segurança da informação do Poder Judiciário, a Estratégia Nacional de Segurança Cibernética do Poder Judiciário - ENSEC-PJ [89], em seu Protocolo de Gestão de Crises Cibernéticas [35], corrobora com esse entendimento ao determinar que o primeiro passo basilar é justamente determinar as atividades essenciais que estão no cerne da razão de existir de cada órgão.

A partir da definição dessas prioridades vitais dos órgãos, deve-se reconhecer os ativos de informação indispensáveis para a sustentação das atribuições primárias – englobando equipe, procedimentos, infraestrutura e recursos tecnológicos – e se monitorar constantemente os riscos associados a essas atividades, levando em conta os possíveis impactos na continuidade do negócio [35].

O Manual de Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital da ENSEC-PJ[35], estabelece, ainda, que é fundamental identificar os ativos usados em funções essenciais do negócio ou que são utilizados em múltiplos serviços de negócio, visando o estabelecimento de planos de continuidade, recuperação e resposta aos ataques cibernéticos. Adicionalmente, define que é imperativo estabelecer um repositório centralizado dos processos organizacionais, assegurando que as funções essenciais sejam devidamente destacadas e priorizadas.

É importante notar que se buscou estabelecer as atividades principais mais abrangentes e comuns a todos os órgãos judiciários. Assim, todas as etapas subsequentes da pesquisa estão voltadas para o tratamento dos riscos relacionados a essas atividades primordiais e que possuem ampla aplicabilidade a todas as instituições de Justiça. Não se pretendeu abarcar a todas as especificidades de ramos especializados de Justiça ou de órgãos com objetivos majoritariamente administrativos.

4.1.2 Riscos de negócio

Por meio das entrevistas foi catalogado um conjunto de aproximadamente 110 potenciais riscos de negócio associados ao Poder Judiciário. Contudo, observou-se a necessidade de conduzir uma avaliação meticulosa e mais criteriosa a fim de determinar, com maior exatidão, quais destes constituiriam riscos

efetivos. Para enfrentar esta complexidade e alcançar um discernimento mais acurado, recorreu-se à técnica de análise de riscos denominada "*bow tie*". Esta metodologia permitiu isolar e categorizar os riscos autênticos, diferenciando-os de suas respectivas causas e impactos subsequentes.

As informações coletadas foram sistematizadas de maneira tabular e o resultado da análise realizada foi submetida à avaliação crítica de um painel composto por especialistas do Poder Judiciário. Para tal, empregou-se a técnica de grupo focal, proporcionando uma análise qualitativa e detalhada. Esta etapa objetivou não apenas identificar os riscos genuínos, mas também compreender suas causas e as potenciais consequências associadas.

Após a conclusão das fases de coleta de dados por meio de entrevistas, organização sistemática das informações, avaliação crítica dos elementos identificados como riscos, causas e consequências, e revisão por grupo focal, foi possível identificar e elencar 10 riscos de negócio críticos e pertinentes ao contexto do Poder Judiciário, conforme transcrito na Tabela 4.2.

Tabela 4.2: Riscos de Negócio do Poder Judiciário

	Riscos de Negócio
1	Divulgação antecipada de votos, determinações ou decisões
2	Vazamento de informações sigilosas, protegidas por segredo de Justiça ou dados pessoais
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, organizações criminosas ou grupos de influência ilegais

A primeira relação dos 10 riscos de negócio [10] previa que o risco de negócio seria denominado *Espionagem de outras nações e/ ou grupos de interesse*. Pierini [116] e Moura [117], revisam os conceitos existentes para grupos de interesse, grupos de pressão e *lobbying* como formas de representação de grupos civis e estabelecem as seguintes distinções:

- **Grupo de interesse** - se trata de um conjunto de pessoas com interesses comuns e que procuram por seus comportamentos obter resultados de suas reivindicações em relação a outros grupos sociais e a influenciar políticas públicas a favor de seus membros.
- **Grupo de pressão** - é um subconjunto do grupo de interesse que se caracteriza por uma maior ênfase na atuação direta junto à órgãos públicos e na mudança de políticas. Podendo variar a forma de abordagem, seja por partidos políticos ou atuação junto ao Poder Executivo e Judiciário.
- ***Lobby*** - é entendido como um instrumento de persuasão utilizado pelos grupos de pressão para participar da tomada de decisão que inclui um comportamento tático e bem planejado para defender seus interesses.

Após esta melhor compreensão, que surgiu no último ciclo sequencial de revisão incremental descrito na metodologia da pesquisa, ficou evidente que os mencionados grupos sociais não representam adequadamente o tipo de risco que se busca caracterizar. Mesmo o *lobby*, apesar de não regulamentado no Brasil, pode ser entendido como um instrumento democrático legítimo de representação de interesses [117]. O risco indicado busca alcançar ações que vão além da legítima atuação para a busca do alcance de interesses de grupos organizados. Assim, entendeu-se que a descrição *Espionagem de outras nações, organizações criminosas ou grupos de influência ilegais* retrata com maior exatidão o sentido original identificado nas etapas da Fase 1 da pesquisa.

4.1.3 Causas dos riscos de negócio

Chapelle [44] argumenta de maneira convincente que os riscos não existem isoladamente, mas devem ser compreendidos em relação aos objetivos de uma organização. Consequentemente, um risco só é considerado significativo se tiver o potencial de atingir adversamente uma atividade considerada crítica para a organização. Riscos que não influenciam os resultados desejados são, portanto, considerados irrelevantes para a análise de risco de uma organização. Considerando a relevância dos riscos de negócio identificados neste estudo, torna-se imperativo compreender os fatores que podem desencadear tais riscos, com o intuito de mitigá-los de forma eficaz.

Prosseguindo na investigação, realizou-se uma análise detalhada das causas ou fontes potenciais de riscos. Esta análise culminou na elaboração da Tabela 4.3 que relaciona as causas identificadas para os riscos de negócio pertinentes, possibilitando uma melhor compreensão de como certos eventos podem levar à materialização desses riscos.

Tabela 4.3: Causas dos Riscos de Negócio

	Causas e Fontes	**Riscos de Negócio**
1	Cópia de minutas ou processos em computadores e meios de armazenamento pessoais	1, 2
2	Vazamento intencional por pessoas que tenham acesso às minutas ou processos (espionagem)	1, 2, 10
3	Comprometimento de credenciais de acesso dos usuários	1, 2, 3, 8, 9, 10
4	Comprometimento de credenciais privilegiadas	1, 2, 3, 4, 5, 6, 8, 9, 10
5	Utilização de computadores pessoais desprotegidos ou em redes inseguras	1, 2, 3, 8, 9, 10
6	Descarte indevido ou extravio de documentos temporários (papel, CD, pendrive etc.)	1, 2, 10
7	Acesso físico não autorizado	1, 2, 3, 4, 6, 10
8	Código-fonte do sistema judicial com vulnerabilidades de segurança	1, 2, 3, 4, 5, 6, 7, 8, 9, 10
9	Falhas de configuração do ambiente de infraestrutura tecnológica	1, 2, 3, 4, 5, 6, 7, 8, 9, 10
10	Privilégios excessivos no sistema, em que qualquer usuário pode ter acesso de leitura das minutas	1, 2, 10

Tabela 4.3: Causas dos Riscos de Negócio

	Causas e Fontes	Riscos de Negócio
11	Ataques cibernéticos ou engenharia social	1, 2, 3, 4, 5, 6, 7, 8, 9, 10
12	Compartilhamento de senhas dos decisores	1, 2, 3, 7, 8
13	Ataques de sequestro de dados (ransomware de dupla extorsão)	1, 2, 4, 6, 10
14	Indisponibilidade de pessoas-chave	4, 6
15	Ataques de negação de serviço distribuídos (DDoS) com o objetivo de prejudicar a imagem de gestores ou autoridades em (ou cotados para) cargos de relevância	4, 7
16	Indisponibilidade de sistemas críticos ou falhas massivas de estruturas de armazenamento por falhas de infraestrutura de TI	4, 6
17	Fragilidade do algoritmo de sorteio	5, 7, 9
18	Modificação de informações na cadeia de fornecimento (MPF, AGU, Caixa etc.)	7, 9
19	Dependência de tecnologia de hardware e software estrangeiros	4, 5, 6, 10
20	Vazamentos ou espionagem em nível de hardware	1, 2, 10
21	Distribuição dos sistemas judiciais eletrônicos, dificultando o controle da segurança do código-fonte	1, 2, 3, 5, 7, 10
22	Complexidade do controle de segurança de todas as camadas tecnológicas que utilizam tecnologias estrangeiras (banco de dados, middleware, linguagem de programação, rede etc.)	2, 3, 5, 7, 10
23	Catástrofes naturais	4, 6
24	Processo inadequado de elaboração ou revisão de votos, decisões ou determinações	3, 7, 8, 9
25	Indisponibilidade de recursos humanos	1, 2, 3, 4, 5, 6, 8, 9, 10
26	Indisponibilidade de recursos materiais	1, 2, 3, 4, 5, 6, 7, 8, 9, 10
27	Regra de negócio que preveja a mesma carga de trabalho em cada gabinete, fazendo com que a distribuição de processos seja previsível	5, 7
28	Possibilidade de modificação de partes, classe processual ou petição inicial após a distribuição do processo	5, 7, 9
29	Entrada de uma mesma ação várias vezes até que o processo seja distribuído ao julgador desejado, desistindo das demais ações	5, 7
30	Entrada de uma mesma ação em diferentes jurisdições (litispendência)	5, 7
31	Volume excessivo de demandas que comprometem a capacidade de resposta dos tribunais (litigância predatória)	4, 7
32	Incapacidade técnica para assuntos de alta complexidade	1, 2, 4, 5, 9, 10
33	Falha na verificação de autenticidade de documentos externos que são inseridos no processo	7, 9
34	Modificação intencional de informação por pessoas que tem acesso ao processo	7, 9

Tabela 4.3: Causas dos Riscos de Negócio

	Causas e Fontes	Riscos de Negócio
35	Tráfico de influência (lobby judicial)	1, 2, 7, 10
36	Nepotismo	7
37	Suspeições de integrantes do gabinete	1, 2, 3, 7, 9
38	Descumprimento de prazos processuais	7, 9
39	Desconhecimento de todas as peças processuais necessárias para a análise e julgamento	7, 8, 9
40	Uso de ferramentas de IA generativa de forma não autorizada para apoio na elaboração de despachos e decisões	2, 8

No decorrer desta pesquisa, identificou-se a necessidade de refinar a lista preliminar de causas de riscos de negócios, conforme inicialmente mapeada [10]. Durante as revisões subsequentes, constatou-se que duas causas apresentavam substancial sobreposição, o que justificou sua consolidação na causa *16 - Indisponibilidade de sistemas críticos ou falhas massivas de estruturas de armazenamento por falhas de infraestrutura de TI*. Ademais, ajustes descritivos adicionais foram realizados para aprimorar a precisão das causas listadas. A relação atualizada incorpora esses refinamentos e reflete a compreensão ampliada adquirida nas etapas avançadas da pesquisa.

Uma vez observados os riscos de negócio e as causas desses riscos, se faz necessário entender as relações entre essas informações. A primeira análise diz respeito à compreensão dos tipos de riscos existentes e suas categorizações. Conforme descrito no capítulo da metodologia, os riscos relacionados às incertezas legais e regulatórias, bem como a falhas de estratégica e os eventos que podem conduzir a danos de reputação, podem todos ser agrupados como **riscos de negócio** [37].

Os riscos operacionais são compreendidos através de diversas perspectivas e contribuições. Segundo Jallow [42], esses riscos estão associados a perdas, tanto diretas quanto indiretas, decorrentes de processos internos ineficazes ou defeituosos, falhas humanas, sistemas inadequados ou eventos externos. Chapelle [44], de forma didática, define o risco operacional em instituições bancárias como sendo qualquer risco que não se enquadre nas categorias de crédito ou mercado, abrangendo, portanto, todos os aspectos não financeiros. Esta definição implica que, para uma instituição financeira, o risco operacional engloba os elementos não diretamente ligados aos seus objetivos primários ou à sua sustentabilidade no mercado competitivo.

Assim, essa concepção permite assimilar que o risco de negócio está associado às funções primárias da instituição, enquanto o risco operacional está relacionado com as funções de suporte ou apoio. Esta visão pode ser extrapolada para outras áreas de atuação sugerindo uma compreensão facilitada do conceito de risco operacional e o seu relacionamento com o risco de negócio.

Traçando um paralelo com o Poder Judiciário, sugere-se que os riscos de negócio são aqueles intrinsecamente ligados à missão institucional primária dos órgãos de Justiça. Uma análise detalhada das causas dos riscos de negócio revela que estas são predominantemente relacionadas a processos internos, recursos humanos e sistemas de informação. Desta forma, as causas dos riscos de negócio são riscos operacionais

que estão mais próximos e relacionados com os riscos das atividades principais do Judiciário.

Consequentemente, é razoável categorizar as causas dos riscos de negócios associados às funções centrais como riscos operacionais, originados de fontes variadas. A Figura 4.1 evidencia, em formato *bow-tie*, o encadeamento básico entre as diversas causas e consequências de um risco de negócio e indica que os riscos operacionais também possuem as suas próprias causas.

A implementação de controles de segurança da informação adequados é vital para mitigar esses riscos operacionais intermediários, os quais influenciam diretamente nos riscos de negócio de maior impacto potencial. Uma compreensão detalhada dessas relações causais é fundamental e será explorada na Fase 2 deste estudo, onde medidas de controle específicas serão discutidas em maior profundidade.

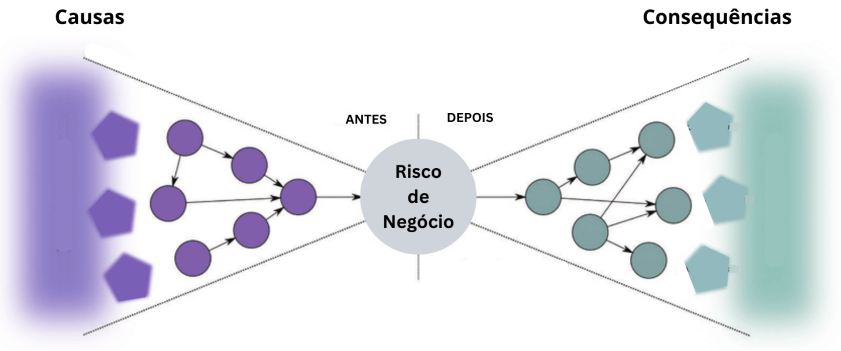


Figura 4.1: Causas e consequências de um risco de negócio.
Fonte: do Autor

A Figura 4.2 ilustra o encadeamento proposto entre controles de segurança da informação, riscos operacionais que são causas dos riscos de negócio e as consequências.

Com base na análise das inter-relações, distribuição e frequência dos riscos operacionais da tabela sugerem uma concentração de riscos operacionais que têm um efeito transversal sobre múltiplos riscos de negócio. Por exemplo, **vulnerabilidades no código-fonte do sistema judicial**, **falhas na configuração do ambiente de infraestrutura tecnológica**, **ataques cibernéticos ou engenharia social** e **indisponibilidade de recursos materiais voltados à segurança** aparecem como fatores recorrentes. Este padrão indica áreas críticas que requerem atenção prioritária, dado o seu amplo impacto potencial em todos os riscos de negócio.

Dentro do escopo desta análise, destaca-se um segundo conjunto de fatores críticos, constituído por dois controles de segurança: o **comprometimento de credenciais privilegiadas** e a **indisponibilidade de recursos humanos**. Estes elementos emergem como significativos, dada a sua influência em nove dos dez riscos de negócio identificados. Esta constatação não apenas sublinha também a relevância desses fatores, mas também indica a interconexão sistêmica com uma ampla gama de riscos operacionais e de negócio.

Se identifica também uma preponderância de riscos relacionados à Segurança da Informação. Esta observação sugere uma interconexão profunda entre a segurança da informação e a estabilidade estratégica das instituições judiciais. Essa interdependência ressalta a necessidade crítica de integrar a segurança da informação como um componente central do funcionamento institucional no judiciário.

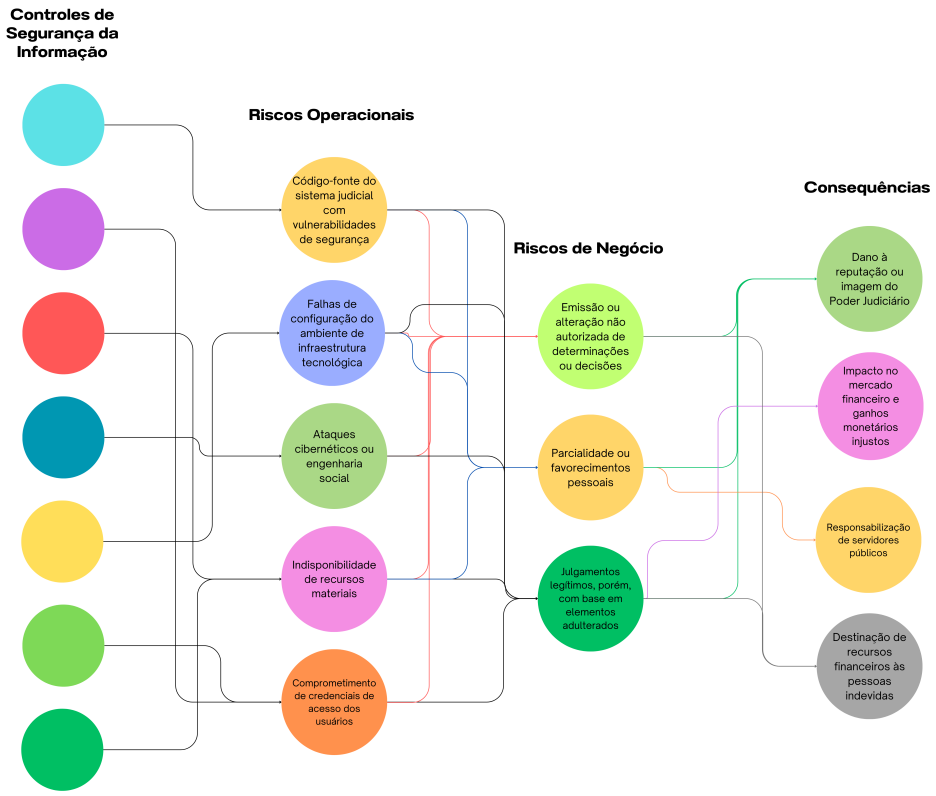


Figura 4.2: Relacionamento entre controles de segurança da informação e consequências dos riscos de negócio.
Fonte: do Autor

4.1.4 Consequências dos riscos de negócio

A avaliação e gestão de riscos é um aspecto fundamental em qualquer organização, mas assume uma importância crítica no sistema judiciário, onde as consequências das ações podem ter um alcance abrangente e significativo. Este processo permite que as entidades governamentais não só antecipem e preparem-se para potenciais adversidades, mas também priorizem e respondam de maneira eficaz, preservando assim a ordem e a confiança públicas.

Nem todos os riscos são igualmente prováveis ou têm o mesmo impacto. Avaliar as consequências potenciais permite às organizações priorizar riscos com base na severidade dos seus impactos potenciais [118]. Ao identificar quais riscos podem ter o maior impacto, as organizações podem direcionar seus recursos e esforços de maneira estratégica e eficiente para os pontos mais críticos [119].

Manter a continuidade de serviços é crucial, especialmente em serviços judiciais. Avaliar as consequências dos riscos permite antecipar as ameaças que possam gerar interrupções significativas. Compreender a gama de consequências possíveis ajuda no desenvolvimento de planos de resposta e contingência mais eficazes [120]. Isso envolve a criação de protocolos para responder a incidentes e minimizar danos e a desenvolver planos detalhados para mitigar danos e manter as operações essenciais em andamento, mesmo diante de eventos inesperados [121].

Tendo em vista a demonstração da relevância da identificação das consequências dos riscos para fins de avaliação e priorização das ações de prevenção e tratamento, foram identificadas as seguintes consequên-

cias dos riscos descritas na Figura 4.4 para melhor avaliação dos riscos.

Tabela 4.4: Consequências dos Riscos de Negócio

Riscos de Negócio		Consequências
1, 2, 3, 4, 5, 6, 7, 8, 9, 10	1	Dano à reputação ou imagem do Poder Judiciário
1, 9	2	Impacto no mercado financeiro e ganhos monetários injustos
1	3	Pressão político-partidária sobre o julgador
1	4	Comercialização de influência para obter resultados favoráveis, independentemente de influenciar diretamente nas decisões judiciais
2, 6, 7, 9, 10	5	Possibilidade de compensação financeira para as pessoas envolvidas
1, 2, 6, 7, 8, 10	6	Responsabilização de servidores públicos
3, 9	7	Liberação indevida de indivíduos detidos
3, 9	8	Destinação de recursos financeiros às pessoas indevidas
3	9	Inconsistências entre o que é apresentado em sessão pública e o registro eletrônico do processo
3, 4, 5, 7, 8, 9, 10	10	Abalo da confiança nas instituições judiciais
4	11	Impedimento do acesso à Justiça
2	12	Tentativa de extorsão por criminosos para não divulgar as informações
2, 4, 6, 10	13	Danos ao erário
4	14	Prejuízo pessoal de autoridades ou gestores em indicações para cargos relevantes
5, 10	15	Violação da garantia de que um juiz imparcial seja designado (princípio do juiz natural)
5, 10	16	Atribuição de processos a juízes que possuem conflitos de interesse ou suspeição
4, 6, 10	17	Impacto social sobre a sociedade em geral
2, 6, 7, 9	18	Dano irreparável para as partes envolvidas
2, 10	19	Acesso indevido a segredos industriais ou estratégicos de empresas ou instituições brasileiras
10	20	Prejuízo da capacidade competitiva da economia nacional
10	21	Comprometimento de objetivos estratégicos nacionais nas relações internacionais
10	22	Desvantagens de natureza política, geopolítica, militar, econômica, tecnológica ou científica

Uma análise quantitativa das relações entre os riscos de negócio e suas potenciais consequências, revela alguns *insights* interessantes. Notavelmente, a consequência **dano à reputação ou imagem do Poder Judiciário** aparece em todos os riscos listados. A presença universal desta categoria de consequências em todos os riscos sugere que, independentemente da natureza específica de um risco - seja ele relacionado à espionagem, vazamento de informações, interrupção dos serviços, ou manipulação processual - o impacto na reputação e imagem do Poder Judiciário é uma preocupação constante. Isto indica que a reputação e a

imagem do Judiciário são ativos particularmente vulneráveis e provavelmente os mais suscetíveis a serem afetados por uma variedade de eventos de risco.

O **abalo da confiança nas instituições judiciais** também aparece várias vezes como uma consequência de diferentes riscos. Isso sugere que a confiança da sociedade e de demais entes públicos nas instituições judiciais é muito relevante e deve ser uma área focal visando a implementação de um conjunto de ações protetivas. Percebe-se que a concretização desse grupo de riscos negociais possui o potencial de impactar mais gravemente na imagem da Justiça e gerar um dano ainda mais prejudicial, a descredibilização da Justiça. Isso demonstra a necessidade de uma abordagem de gestão de riscos que não apenas enderece os aspectos técnicos ou operacionais dos riscos, mas também considere estratégias para proteger e fortalecer a percepção pública do Judiciário.

Uma outra análise diz respeito à dispersão das consequências de cada risco. O risco **10 - espionagem de outras nações, organizações criminosas ou grupos de influência ilegais** é o que apresenta a maior diversidade de consequências, com doze possíveis repercussões. Isso indica a natureza complexa e multifacetada deste risco e que provavelmente apresenta maiores impactos em caso de ocorrência, que abrangem desde a reputação até a segurança nacional.

Seguindo na avaliação destes aspectos, os riscos **2 - vazamento de informações sigilosas, protegidas por segredo de Justiça ou dados pessoais**, com sete consequências identificadas, e **9 - julgamentos legítimos, porém, com base em elementos adulterados** possuem seis consequências. Estes riscos também possuem uma diversidade de consequências e mostram que problemas com segurança da informação e integridade dos julgamentos são críticos não apenas por suas implicações diretas, mas também pelo potencial dano que podem causar ao Judiciário.

E importante considerar não apenas a recorrência de consequências e a diversidade dos efeitos negativos potenciais, mas que mesmo um único evento pode ser mais danoso a um órgão. Ou seja, a quantidade de efeitos pode não representar o real nível de impacto. Enquanto não existe algum instrumento que defina em nível geral quais riscos ou impactos são mais relevantes aos órgãos do Poder Judiciário, é necessário que cada órgão avalie qualitativamente em que nível cada um desses eventos lhe impactam particularmente. Assim, a gestão eficaz desses riscos requer uma abordagem holística que leve em conta tanto os impactos tangíveis quanto intangíveis, com especial atenção ao ativo frequentemente afetado: a reputação e a imagem da instituição.

Há de se ponderar, no entanto, que sob à ótica da sociedade como um todo a concretização de um risco com consequências críticas em um órgão repercute na imagem de todas as instituições do sistema de justiça, mesmo que tenha sido um evento isolado. Isso demonstra que as ações de segurança da informação devem ser iniciativas amplamente estruturadas e preferencialmente patrocinadas pelos órgãos centrais que possuam uma visão ampliada dos objetivos estratégicos do Poder Judiciário, tais como os Tribunais e Conselhos Superiores.

A confiabilidade conferida ao Poder Judiciário constitui um elemento vital para a manutenção da harmonia social e para a legitimação do próprio Estado. Nesse contexto, antevê-se que a gestão estratégica de riscos emerge como um mecanismo primordial, que pode servir de instrumento facilitador para a comunicação transparente e inequívoca entre este pilar do Estado de Direito e as principais partes interessadas (*stakeholders*), a saber, o cidadão e seus representantes eleitos.

A observação da relação apresentada oferece adicionalmente uma visão aguçada sobre a natureza dos riscos em diferentes tipos de organizações. Se identifica que em organizações governamentais a maioria das consequências dos riscos está intrinsecamente ligada a questões de reputação. Este fato ressalta a importância crítica da imagem pública e da confiança na eficácia e na integridade dessas instituições. Em contraste, nas instituições privadas as consequências dos riscos tendem a estar mais diretamente relacionadas a perdas financeiras [37]. Esta diferença reflete as prioridades e os objetivos distintos desses dois tipos de organizações. Enquanto as entidades governamentais são primariamente orientadas para o serviço público e a manutenção da confiança social, as instituições privadas focam predominantemente na sua sustentabilidade financeira e na viabilidade econômica do investimento aplicado. A compreensão dessa distinção é fundamental para o desenvolvimento de estratégias de gestão de riscos adequadas a cada contexto organizacional.

Aprofundamento ainda mais na análise, se observa que outra consequência relevante identificada é a possibilidade de *responsabilização de servidores públicos*. Este é um resultado comum para vários riscos diferentes. O que indica que a falha na adoção de medidas adequadas para prevenir ou remediar os eventos de risco podem ser reflexo de omissão ou ineficiência de gestores e servidores públicos em agir com a devida diligência em identificar, prevenir ou remediar os eventos de risco com efeitos extremamente adversos. Sendo que essas situações que podem levar a medidas de apuração de eventuais omissões e à possibilidade de penalização.

Conforme exposto por Queiroz [122], uma estrutura em três linhas com atuação em primeiro nível nas áreas de tecnologia da informação, um segundo nível fora da TI apoiando e acompanhando como os riscos estão sendo tratados e uma terceira linha de auditoria independente. Este pode ser um meio para se estruturar a gestão de segurança da informação e de riscos entre diversos atores e de diminuir a dependência da atuação individual de gestores públicos. Nunes [28] defende ainda que a gestão de riscos pode ser uma forma de se viabilizar o equilíbrio entre os princípios da eficiência e da legalidade, por subsidiar decisões justificadas em diversas instâncias. Contribuindo para a redução da "cultura do controle"e do medo de responsabilização dos gestores em detrimento de se buscar as soluções mais eficientes.

Nesta mesmo gênero de consequências, existe ainda a possível necessidade de compensação financeira às pessoas ou empresas que tenham tido suas informações sensíveis indevidamente expostas ou modificadas ou que tenham sido alvo de desvio criminoso de valores que estão sob guarda do Judiciário. Tais eventos sugerem que há implicações financeiras significativas ao erário público associadas a estes riscos.

Se constata que alguns riscos podem levar a consequências que vão além do sistema de justiça, podendo gerar impactos sociais e econômicos mais amplos, afetando o mercado financeiro, segredos industriais e até mesmo relações internacionais.

Alguns dos riscos envolvem questões profundas sobre integridade e ética dos atores do sistema de Justiça e que comumente não são objeto de estudo. O Escritório das Nações Unidas sobre Drogas e Crime [105] alerta para este problema, que ocorre em âmbito internacional:

> *Na última década, as associações de juízes e os criadores das políticas judiciais têm-se centrado nas questões de promoção da independência ou em questões éticas, mas geralmente pouca atenção tem sido dada às questões da corrupção no sistema judicial. Como resultado,*

verifica-se frequentemente uma ausência de políticas setoriais anticorrupção e de gestão de riscos simplificadas no sistema judiciário, uma falta de práticas de medição da integridade e da corrupção e uma comunicação insuficiente com as partes interessadas relevantes, os meios de comunicação social e o público.

Portanto, é razoável propor que os resultados da primeira fase da pesquisa evidenciaram uma ampla gama de riscos operacionais, os riscos de negócio dos processos finalísticos da Justiça e como que consequências poderão ser enfrentadas e os relacionamentos entre todos estes aspectos.

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. Alcançou-se nesta fase do estudo uma forma de 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.

Contudo, uma análise detalhada revela que a correlação imediata entre os riscos de negócio e os riscos associados à segurança cibernética não é trivial. Essa dificuldade na interconexão entre diferentes categorias de risco é um fenômeno reconhecido na literatura especializada. Eling et. al. [123] discorrem sobre essa problemática, destacando a complexidade intrínseca em harmonizar o gerenciamento de riscos cibernéticos com as estratégias corporativas de gestão de riscos (*ERM - Enterprise Risk Management*). Observam que o risco cibernético frequentemente permanece isolado dentro das organizações, operando em um 'silo funcional' distinto das estruturas convencionais de ERM. Esse isolamento não apenas impede uma abordagem integrada e holística à gestão de riscos, mas também contribui para falhas significativas na governança de riscos, limitando assim a capacidade das organizações de responder de maneira eficaz às ameaças cibernéticas multifacetadas e em constante evolução.

Embora a importância dos riscos de segurança cibernética esteja ganhando reconhecimento nos escalões superiores da administração empresarial, muitos conselhos de administração ainda se encontram despreparados para incorporá-los adequadamente nas suas estratégias de tomada de decisão. Essa lacuna de preparação resulta frequentemente em que decisões críticas relacionadas ao risco corporativo sejam relegadas a níveis hierárquicos inferiores, comprometendo uma gestão eficaz e integrada de tais riscos. Neste contexto, se enfatiza a necessidade de pesquisas adicionais focadas na inclusão efetiva do risco cibernético nas deliberações e na governança de alto nível [123]. A implementação de tal inclusão não apenas reforçaria as estratégias de gestão de riscos corporativos, mas também asseguraria uma resposta mais ágil e informada frente aos desafios dinâmicos impostos pela segurança cibernética no ambiente empresarial contemporâneo.

Após a identificação dos riscos e a análise das suas respectivas relações de causa e efeito, torna-se imperativo aprofundar a compreensão das estratégias e medidas efetivas para mitigar a probabilidade de sua manifestação ou para minimizar os impactos adversos potenciais nos objetivos estratégicos da organização. Este processo envolve a implementação de controles preventivos e compensatórios que são essenciais para o tratamento eficiente dos riscos considerados prioritários. A aplicação destes controles fortalece a resiliência organizacional diante das ameaças e assegura uma gestão de riscos mais alinhada com as estratégicas das instituições.

A relação completa de todas as causas e consequências para cada risco de negócio consta do Apêndice I.1 - Causas e consequências dos riscos de negócio.

4.2 FASE 2

4.2.1 Seleção de *Framework*

Após uma análise, concluiu-se que o *framework* **CIS Controls**, em sua versão 8 mais recente, é a referência mais apropriada para a implementação de ações de segurança capazes de reduzir adequadamente a probabilidade e o impacto dos riscos identificados.

A seleção do *framework* CIS Controls foi fundamentada em uma variedade de fatores decisivos. Inicialmente, destaca-se que o CIS afirma adotar o princípio de Pareto, por meio da maximização da eficiência por meio da implementação dos controles mais efetivos e relevantes, evitando assim uma proliferação de medidas potencialmente desnecessárias [84]. Essa abordagem permite que as organizações busquem o maior nível de segurança enquanto evita uma quantidade extensiva de controles, os quais poderiam sobrecarregar a gestão e comprometer a eficácia da segurança.

Ademais, o CIS Controls tem sido amplamente reconhecido e adotado como um guia de referência nas principais iniciativas de segurança governamentais e no setor privado. Exemplificando, o Tribunal de Contas da União - TCU utiliza este *framework* como base fundamental para seu programa de auditorias em segurança cibernética [124]. Similarmente, a Secretaria de Governo Digital incorpora o CIS Controls no Framework de Privacidade e Segurança da Informação que é principal referência para mais de 250 órgãos vinculados ao Gov.br [125], e a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) emprega a versão 7 dos controles do CIS como parte de suas medidas para proteção de infraestruturas críticas e para a gestão de identidades e controle de acesso [35].

A escolha específica dos controles de segurança presentes no CIS Controls focou na mitigação direta das causas associadas aos riscos de negócio identificados no estudo. Cada controle foi criteriosamente selecionado para abordar ameaças ou vulnerabilidades específicas que, se exploradas, poderiam impactar diretamente a nos riscos operacionais identificados.

4.2.2 Controles de Segurança da Informação

Nesta fase do estudo, foram propostas **232 medidas de segurança da informação**. Destas, **133 (57,33%)** foram selecionadas a partir dos controles estabelecidos pelo **CIS Controls v8**. Além disso, **99 (42,67%)** representam controles complementares, introduzidos neste estudo, com o objetivo de mitigar riscos que não foram inicialmente cobertos pelo **CIS Controls v8**.

A Tabela 4.5 lista todos os controles que foram selecionados nesta pesquisa, a partir do CIS Controls, e que podem ser utilizados no tratamento de quais riscos operacionais ou causas de riscos de negócio.

Tabela 4.5: Controles de Segurança oriundos do CIS Controls

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
1.1	Estabelecer e manter um inventário detalhado de ativos corporativos	Estabeleça e mantenha um inventário preciso, detalhado e atualizado de todos os ativos corporativos com potencial para armazenar ou processar dados, incluindo: dispositivos de usuário final (incluindo portáteis e móveis), dispositivos de rede, dispositivos não computacionais/IoT e servidores. Certifique-se de que o inventário registre o endereço de rede (se estático), endereço de hardware, nome da máquina, proprietário do ativo de dados, departamento para cada ativo e se o ativo foi aprovado para se conectar à rede. Para dispositivos móveis de usuário final, as ferramentas do tipo MDM podem oferecer suporte a esse processo, quando apropriado. Este inventário inclui ativos conectados à infraestrutura fisicamente, virtualmente, remotamente e aqueles dentro dos ambientes de nuvem. Além disso, inclui ativos que são regularmente conectados à infraestrutura de rede corporativa, mesmo que não estejam sob o controle da empresa. Revise e atualize o inventário de todos os ativos corporativos semestralmente ou com mais frequência.	7, 9, 11, 15, 16, 23
1.2	Endereçar ativos não autorizados	Assegure que exista um processo para lidar com ativos não autorizados semanalmente. A empresa pode escolher remover o ativo da rede, negar que o ativo se conecte remotamente à rede ou colocar o ativo em quarentena.	7, 9, 11
1.3	Usar uma ferramenta de descoberta ativa	Utilize uma ferramenta de descoberta ativa para identificar ativos conectados à rede corporativa. Configure a ferramenta de descoberta ativa para executar diariamente ou com mais frequência.	7, 11
1.4	Usar o Dynamic Host Configuration Protocol (DHCP) para atualizar o inventário de ativos corporativos	Use o log do DHCP em todos os servidores DHCP ou ferramentas de gestão de endereço Internet Protocol (IP) para atualizar o inventário de ativos corporativos. Revise e use logs para atualizar o inventário de ativos corporativos semanalmente ou com mais frequência.	11
1.5	Usar uma ferramenta de descoberta passiva	Use uma ferramenta de descoberta passiva para identificar ativos conectados à rede corporativa. Revise e use varreduras para atualizar o inventário de ativos corporativos pelo menos semanalmente ou com mais frequência.	11
2.1	Estabelecer e manter um inventário de software	Estabeleça e mantenha um inventário detalhado de todos os softwares licenciados instalados em ativos corporativos. O inventário de software deve documentar o título, editor, data inicial de instalação/uso e objetivo de negócio de cada entrada; quando apropriado, inclua o Uniform Resource Locator(URL), app store(s), versão(ões), mecanismo de implantação e data de desativação. Revise e atualize o inventário de software semestralmente ou com mais frequência.	2, 9, 11, 15, 16, 23

Tabela 4.5: Controles de Segurança oriundos do CIS Controls

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
2.2	Assegurar que o software autorizado seja atualmente suportado	Assegure que apenas software atualmente suportado seja designado como autorizado no inventário de software para ativos corporativos. Se o software não é suportado, mas é necessário para o cumprimento da missão da empresa, documente uma exceção detalhando os controles de mitigação e a aceitação do risco residual. Para qualquer software não suportado sem uma documentação de exceção, designe como não autorizado. Revise o inventário de software para verificar o suporte do software pelo menos uma vez por mês ou com mais frequência.	2, 9, 11
2.3	Endereçar o software não autorizado	Assegure que o software não autorizado seja retirado de uso em ativos corporativos ou receba uma exceção documentada. Revise mensalmente ou com mais frequência.	2, 3, 4, 9, 11, 13
2.4	Utilizar ferramentas automatizadas de inventário de software	Utilize ferramentas de inventário de software, quando possível, em toda a empresa para automatizar a descoberta e documentação do software instalado.	2, 3, 4, 9, 11, 13
2.5	Lista de permissões de Software autorizado	Use controles técnicos, como a lista de permissões de aplicações, para garantir que apenas o software autorizado possa ser executado ou acessado. Reavalie semestralmente ou com mais frequência.	2, 3, 4, 9, 11, 13
2.6	Lista de permissões de bibliotecas autorizadas	Use os controles técnicos para garantir que apenas as bibliotecas de software autorizadas, como arquivos .dll, .ocx, .so, etc. específicos, tenham permissão para carregar em um processo do sistema. Impedir que bibliotecas não autorizadas sejam carregadas em um processo do sistema. Reavalie semestralmente ou com mais frequência.	8, 11, 13, 17
2.7	Lista de permissões de Scripts autorizados	Use controles técnicos, como assinaturas digitais e controle de versão, para garantir que apenas scripts autorizados, como arquivos .ps1, .py, etc. específicos, tenham permissão para executar. Bloqueie a execução de scripts não autorizados. Reavalie semestralmente ou com mais frequência.	9, 11, 13
3.01	Estabelecer e manter um processo de gestão de dados	Estabeleça e mantenha um processo de gestão de dados. No processo, trate a sensibilidade dos dados, o proprietário dos dados, o manuseio dos dados, os limites de retenção de dados e os requisitos de descarte, com base em padrões de sensibilidade e retenção para a empresa. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	1, 2, 5, 6, 24, 34
3.02	Estabelecer e manter um inventário de dados	Estabeleça e mantenha um inventário de dados, com base no processo de gestão de dados da empresa. No mínimo, inventarie os dados sensíveis. Revise e atualize o inventário anualmente, no mínimo, com prioridade para os dados sensíveis.	1, 2, 6, 24, 34

Tabela 4.5: Controles de Segurança oriundos do CIS Controls

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
3.03	Configurar listas de controle de acesso a dados	Configure listas de controle de acesso a dados com base na necessidade de conhecimento do usuário. Aplique listas de controle de acesso a dados, também conhecidas como permissões de acesso, a sistemas de arquivos, bancos de dados e aplicações locais e remotos.	1, 2, 5, 6, 10, 24, 34
3.04	Aplicar retenção de dados	Retenha os dados de acordo com o processo de gestão de dados da empresa. A retenção de dados deve incluir prazos mínimos e máximos.	6
3.05	Descartar dados com segurança	Descarte os dados com segurança conforme descrito no processo de gestão de dados da empresa. Certifique-se de que o processo e o método de descarte sejam compatíveis com a sensibilidade dos dados.	6
3.06	Criptografar dados em dispositivos de usuário final	Criptografe os dados em dispositivos de usuário final que contenham dados sensíveis. Exemplos de implementações podem incluir: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	1, 5, 34
3.07	Estabelecer e manter um esquema de classificação de dados	Estabeleça e mantenha um esquema geral de classificação de dados para a empresa. As empresas podem usar rótulos, como “Sensível”, “Confidencial” e “Público”, e classificar seus dados de acordo com esses rótulos. Revise e atualize o esquema de classificação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	1, 2, 6, 24, 34
3.08	Documentar Fluxos de Dados	Documente fluxos de dados. A documentação do fluxo de dados inclui fluxos de dados do provedor de serviços e deve ser baseada no processo de gestão de dados da empresa. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança	24, 34
3.09	Criptografar dados em mídia removível	Criptografe os dados em mídia removível.	1, 20, 22
3.1	Criptografar dados sensíveis em trânsito	Criptografe dados sensíveis em trânsito. Exemplos de implementações podem incluir: Transport Layer Security (TLS) e Open Secure Shell (OpenSSH).	5, 20, 22
3.11	Criptografar dados sensíveis em repouso	Criptografe dados sensíveis em repouso em servidores, aplicações e bancos de dados que contenham dados sensíveis. A criptografia da camada de armazenamento, também conhecida como criptografia do lado do servidor, atende ao requisito mínimo desta medida de segurança. Métodos de criptografia adicionais podem incluir criptografia de camada de aplicação, também conhecida como criptografia do lado do cliente, onde o acesso ao(s) dispositivo(s) de armazenamento de dados não permite o acesso aos dados em texto simples.	20, 22, 34

Tabela 4.5: Controles de Segurança oriundos do CIS Controls

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
3.12	Segmentar o processamento e o armazenamento de dados com base na sensibilidade	Segmente o processamento e o armazenamento de dados com base na sensibilidade dos dados. Não processe dados sensíveis em ativos corporativos destinados a dados de menor sensibilidade.	1, 2, 5, 6, 24, 34
3.13	Implantar uma solução de prevenção contra perda de dados	Implementar uma ferramenta automatizada, como uma ferramenta de prevenção de perda de dados (DLP) baseada em host para identificar todos os dados sensíveis armazenados, processados ou transmitidos por meio de ativos corporativos, incluindo aqueles localizados no site local ou em um provedor de serviços remoto, e atualizar o inventário de dados sensíveis da empresa.	1, 2, 5
3.14	Registrar o acesso a dados sensíveis	Registre o acesso a dados sensíveis, incluindo modificação e descarte.	1, 2, 6, 24, 34
4.01	Estabelecer e manter um processo de configuração segura	Estabeleça e mantenha um processo de configuração segura para ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos não computacionais/IoT; e servidores) e software (sistemas operacionais e aplicações). Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	5, 9, 11
4.02	Estabelecer e Manter um Processo de Configuração Segura para a Infraestrutura de Rede	Estabeleça e mantenha um processo de configuração segura para dispositivos de rede. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	9, 11, 34
4.04	Implementar e gerenciar um firewall nos servidores	Implemente e gerencie um firewall nos servidores, onde houver suporte. Exemplos de implementações incluem um firewall virtual, firewall do sistema operacional ou um agente de firewall de terceiros.	11
4.05	Implementar e gerenciar um firewall nos dispositivos de usuário final	Implemente e gerencie um firewall baseado em host ou uma ferramenta de filtragem de porta nos dispositivos de usuário final, com uma regra de negação padrão que bloqueia todo o tráfego, exceto os serviços e portas que são explicitamente permitidos.	5, 11
4.06	Gerenciar com segurança os ativos e software corporativos	Gerencie com segurança os ativos e software corporativos. Exemplos de implementações incluem gestão de configuração por meio de version-controlled-infrastructure-as-code e acesso a interfaces administrativas por meio de protocolos de rede seguros, como Secure Shell (SSH) e Hypertext Transfer Protocol Secure (HTTPS). Não use protocolos de gestão inseguros, como Telnet (Teletype Network) e HTTP, a menos que seja operacionalmente essencial.	4, 9, 11

Tabela 4.5: Controles de Segurança oriundos do CIS Controls

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
4.07	Gerenciar contas padrão nos ativos e software corporativos	Gerencie contas padrão nos ativos e software corporativos, como root, administrador e outras contas de fornecedores pré-configuradas. Exemplos de implementações podem incluir: desativar contas padrão ou torná-las inutilizáveis.	4, 9, 34
4.08	Desinstalar ou desativar serviços desnecessários nos ativos e software corporativos	Desinstale ou desative serviços desnecessários nos ativos e software corporativos, como um serviço de compartilhamento de arquivos não utilizado, módulo de aplicação da web ou função de serviço.	9
4.1	Impor o bloqueio automático de dispositivos nos dispositivos portáteis do usuário final	Imponha o bloqueio automático do dispositivo seguindo um limite pré-determinado de tentativas de autenticação local com falha nos dispositivos portáteis de usuário final, quando compatível. Para laptops, não permita mais de 20 tentativas de autenticação com falha; para tablets e smartphones, não mais do que 10 tentativas de autenticação com falha. Exemplos de implementações incluem Microsoft® InTune Device Lock e Apple® Configuration Profile maxFailedAttempts.	5
4.11	Impor a capacidade de limpeza remota nos dispositivos portáteis do usuário final	Limpe remotamente os dados corporativos de dispositivos portáteis de usuário final de propriedade da empresa quando for considerado apropriado, como dispositivos perdidos ou roubados, ou quando um indivíduo não trabalha mais na empresa.	1, 6
4.12	Separar os Espaços de Trabalho Corporativos nos dispositivos móveis	Certifique-se de que a separação de espaços de trabalho corporativos seja usada nos dispositivos móveis de usuário final, onde houver suporte. Exemplos de implementações incluem o uso de um Apple® Configuration Profile ou Android ™ Work Profile para separar aplicações e dados corporativos de aplicações e dados pessoais.	1, 6
5.1	Estabelecer e manter um inventário de contas	Estabeleça e mantenha um inventário de todas as contas gerenciadas na empresa. O inventário deve incluir contas de usuário e administrador. O inventário, no mínimo, deve conter o nome da pessoa, nome de usuário, datas de início/ término e departamento. Valide se todas as contas ativas estão autorizadas, em uma programação recorrente, no mínimo trimestralmente ou com mais frequência.	3, 4, 13
5.2	Usar senhas exclusivas	Use senhas exclusivas para todos os ativos corporativos. As melhores práticas de implementação incluem, no mínimo, uma senha de 8 caracteres para contas que usam MFA e uma senha de 14 caracteres para contas que não usam MFA.	3, 4, 13
5.3	Desabilitar contas inativas	Exclua ou desabilite quaisquer contas inativas após um período de 45 dias de inatividade, onde for suportado.	3, 4, 13

Tabela 4.5: Controles de Segurança oriundos do CIS Controls

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
5.4	Restringir privilégios de administrador a contas de Administrador dedicadas	Restrinja os privilégios de administrador a contas de administrador dedicadas nos ativos corporativos. Realize atividades gerais de computação, como navegação na Internet, e-mail e uso do pacote de produtividade, a partir da conta primária não privilegiada do usuário.	4, 13
5.5	Estabelecer e manter um inventário de contas de serviço	Estabeleça e mantenha um inventário de contas de serviço. O inventário, no mínimo, deve conter departamento proprietário, data de revisão e propósito. Realize análises de contas de serviço para validar se todas as contas ativas estão autorizadas, em uma programação recorrente, no mínimo trimestralmente ou com mais frequência.	4, 13
5.6	Centralizar a gestão de contas	Centralize a gestão de contas por meio de serviço de diretório ou de identidade.	3, 4, 13
6.1	Estabelecer um Processo de Concessão de Acesso	Estabeleça e siga um processo, de preferência automatizado, para conceder acesso aos ativos corporativos mediante nova contratação, concessão de direitos ou mudança de função de um usuário.	1, 2, 3, 4, 10, 12, 24
6.2	Estabelecer um Processo de Revogação de Acesso	Estabeleça e siga um processo, de preferência automatizado, para revogar o acesso aos ativos corporativos, por meio da desativação de contas imediatamente após o encerramento, revogação de direitos ou mudança de função de um usuário. Desativar contas, em vez de excluí-las, pode ser necessário para preservar as trilhas de auditoria.	1, 2, 3, 4, 10, 12, 24
6.3	Exigir MFA para aplicações expostas externamente	Exija que todas as aplicações corporativas ou de terceiros expostas externamente apliquem o MFA, onde houver suporte. Impor o MFA por meio de um serviço de diretório ou provedor de SSO é uma implementação satisfatória desta medida de segurança.	3, 4, 11, 12
6.4	Exigir MFA para acesso remoto à rede	Exija MFA para acesso remoto à rede.	3, 4, 11, 12
6.5	Exigir MFA para acesso administrativo	Exija MFA para todas as contas de acesso administrativo, onde houver suporte, em todos os ativos corporativos, sejam gerenciados no site local ou por meio de um provedor terceirizado.	4, 11, 13
6.6	Estabelecer e manter um inventário de sistemas de autenticação e autorização	Estabeleça e mantenha um inventário dos sistemas de autenticação e autorização da empresa, incluindo aqueles hospedados no site local ou em um provedor de serviços remoto. Revise e atualize o inventário, no mínimo, anualmente ou com mais frequência.	10
6.7	Centralizar o controle de acesso	Centralize o controle de acesso para todos os ativos corporativos por meio de um serviço de diretório ou provedor de SSO, onde houver suporte.	10, 24

Tabela 4.5: Controles de Segurança oriundos do CIS Controls

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
6.8	Definir e manter o controle de acesso baseado em funções	Defina e mantenha o controle de acesso baseado em funções, determinando e documentando os direitos de acesso necessários para cada função dentro da empresa para cumprir com sucesso suas funções atribuídas. Realize análises de controle de acesso de ativos corporativos para validar se todos os privilégios estão autorizados, em uma programação recorrente, no mínimo uma vez por ano ou com maior frequência.	10, 12, 24
7.1	Estabelecer e manter um processo de gestão de vulnerabilidade	Estabeleça e mantenha um processo de gestão de vulnerabilidade documentado para ativos corporativos. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	9, 11, 13
7.2	Estabelecer e manter um processo de remediação	Estabeleça e mantenha uma estratégia de remediação baseada em risco documentada em um processo de remediação, com revisões mensais ou mais frequentes.	9, 11, 13
7.3	Executar a gestão automatizada de patches do sistema operacional	Realize atualizações do sistema operacional em ativos corporativos por meio da gestão automatizada de patches mensalmente ou com mais frequência.	9, 11, 13
7.4	Executar a gestão automatizada de patches de aplicações	Realize atualizações de aplicações em ativos corporativos por meio da gestão automatizada de patches mensalmente ou com mais frequência.	9, 11, 13
7.5	Realizar varreduras automatizadas de vulnerabilidade em ativos corporativos internos	Realize varreduras automatizadas de vulnerabilidade em ativos corporativos internos trimestralmente ou com mais frequência. Realize varreduras autenticadas e não autenticadas, usando uma ferramenta de varredura de vulnerabilidade compatível com o SCAP.	11, 13
7.6	Realizar varreduras automatizadas de vulnerabilidade em ativos corporativos expostos externamente	Execute varreduras de vulnerabilidade automatizadas de ativos corporativos expostos externamente usando uma ferramenta de varredura de vulnerabilidade compatível com o SCAP. Execute varreduras mensalmente ou com mais frequência.	11, 13
7.7	Corrigir vulnerabilidades detectadas	Corrija as vulnerabilidades detectadas no software por meio de processos e ferramentas mensalmente, ou mais frequentemente, com base no processo de correção.	11, 13
8.01	Estabelecer e manter um processo de gestão de log de auditoria	Estabeleça e mantenha um processo de gestão de log de auditoria que defina os requisitos de log da empresa. No mínimo, trate da coleta, revisão e retenção de logs de auditoria para ativos corporativos. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	2, 9, 11, 13, 24, 34

Tabela 4.5: Controles de Segurança oriundos do CIS Controls

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
8.02	Coletar logs de auditoria	Colete logs de auditoria. Certifique-se de que o log, de acordo com o processo de gestão de log de auditoria da empresa, tenha sido habilitado em todos os ativos.	2, 11, 13, 24, 34
8.03	Garantir o armazenamento adequado do registro de auditoria	Certifique-se de que os destinos dos logs mantenham armazenamento adequado para cumprir o processo de gestão de log de auditoria da empresa.	2, 11, 13, 24, 34
8.04	Padronizar a sincronização de tempo	Padronize a sincronização de tempo. Configure pelo menos duas fontes de tempo sincronizadas nos ativos corporativos, onde houver suporte.	2, 11, 13, 34
8.05	Coletar logs de auditoria detalhados	Configure o log de auditoria detalhado para ativos corporativos contendo dados sensíveis. Inclua a origem do evento, data, nome de usuário, carimbo de data/hora, endereços de origem, endereços de destino e outros elementos úteis que podem ajudar em uma investigação forense.	2, 11, 13, 24, 34
8.09	Centralizar os logs de auditoria	Centralize, na medida do possível, a coleta e retenção de logs de auditoria nos ativos corporativos.	2, 11, 13, 24, 34
8.1	Reter os logs de auditoria	Reter os logs de auditoria em ativos corporativos por no mínimo 90 dias.	2, 11, 13, 24, 34
8.11	Conduzir revisões de log de auditoria	Realize análises de logs de auditoria para detectar anomalias ou eventos anormais que possam indicar uma ameaça potencial. Realize revisões semanalmente ou com mais frequência.	2, 11, 13, 24, 34
9.1	Garantir o uso apenas de navegadores e clientes de e-mail suportados plenamente	Certifique-se de que apenas navegadores e clientes de e-mail suportados plenamente tenham permissão para executar na empresa, usando apenas a versão mais recente dos navegadores e clientes de e-mail fornecidos pelo fornecedor.	5, 9
9.2	Usar serviços de filtragem de DNS	Use os serviços de filtragem de DNS em todos os ativos corporativos para bloquear o acesso a domínios mal-intencionados conhecidos.	5
9.3	Manter e impor filtros de URL baseados em rede	Imponha e atualize filtros de URL baseados em rede para limitar um ativo corporativo de se conectar a sites potencialmente maliciosos ou não aprovados. Exemplos de implementações incluem filtragem baseada em categoria, filtragem baseada em reputação ou através do uso de listas de bloqueio. Aplique filtros para todos os ativos corporativos.	5
9.4	Restringir extensões de cliente de e-mail e navegador desnecessárias ou não autorizadas	Restrinja, seja desinstalando ou desabilitando, quaisquer plug-ins de cliente de e-mail ou navegador, extensões e aplicações complementares não autorizados ou desnecessários.	5, 9
9.5	Implementar o DMARC	Para diminuir a chance de e-mails forjados ou modificados de domínios válidos, implemente a política e verificação DMARC, começando com a implementação dos padrões Sender Policy Framework (SPF) e DomainKeys Identified Mail (DKIM).	9

Tabela 4.5: Controles de Segurança oriundos do CIS Controls

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
9.6	Bloquear tipos de arquivo desnecessários	Bloqueie tipos de arquivo desnecessários que tentem entrar no gateway de e-mail da empresa.	9, 11
10.1	Instalar e manter um software anti-malware	Instale e mantenha um software anti-malware em todos os ativos corporativos.	5, 11, 13
10.2	Configurar atualizações automáticas de assinatura anti-malware	Configure atualizações automáticas para arquivos de assinatura anti-malware em todos os ativos corporativos.	5, 11, 13
10.3	Desabilitar a execução e reprodução automática para mídias removíveis	Desabilitar a funcionalidade de execução e reprodução automática para mídias removíveis.	5, 9, 11, 13
10.4	Configurar a varredura anti-malware automática de mídia removível	Configure o software anti-malware para verificar automaticamente a mídia removível.	5, 9, 11, 13
10.5	Habilitar recursos anti-exploração	Habilite recursos anti-exploração em ativos e software corporativos, onde possível, como Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), ou Apple® System Integrity Protection (SIP) e Gatekeeper™.	5, 11, 13
10.6	Gerenciar o software anti-malware de maneira centralizada	Gerencie o software anti-malware de maneira centralizada.	5, 9, 11, 13
10.7	Usar software anti-malware baseado em comportamento	Use software anti-malware baseado em comportamento.	5, 11, 13
11.1	Estabelecer e manter um processo de recuperação de dados	Estabeleça e mantenha um processo de recuperação de dados. No processo, aborde o escopo das atividades de recuperação de dados, a priorização da recuperação e a segurança dos dados de backup. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	13
11.2	Executar backups automatizados	Execute backups automatizados de ativos corporativos dentro do escopo. Execute backups semanalmente ou com mais frequência, com base na sensibilidade dos dados.	13, 16, 23
11.3	Proteger os dados de recuperação	Proteja os dados de recuperação com controles equivalentes dos dados originais. Referencie o uso de criptografia ou separação de dados, com base nos requisitos.	13
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	Estabeleça e mantenha uma instância isolada de dados de recuperação. Exemplos de implementações incluem controle de versão de destinos de backup por meio de sistemas ou serviços offline, na nuvem ou fora do site local.	13

Tabela 4.5: Controles de Segurança oriundos do CIS Controls

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
11.5	Testar os dados de recuperação	Teste a recuperação do backup trimestralmente, ou com mais frequência, para uma amostra dos ativos corporativos dentro do escopo.	13, 16, 23
12.1	Assegurar que a infraestrutura de rede esteja atualizada	Assegure que a infraestrutura de rede seja mantida atualizada. Exemplos de implementações incluem a execução da versão estável mais recente do software e/ou o uso de ofertas de network-as-a-service (NaaS) atualmente suportadas. Revise as versões do software mensalmente, ou com mais frequência, para verificar o suporte do software.	9, 11, 13, 16
12.2	Estabelecer e manter uma arquitetura de rede segura	Estabeleça e mantenha uma arquitetura de rede segura. Uma arquitetura de rede segura deve abordar segmentação, privilégio mínimo e disponibilidade, no mínimo.	9, 11, 13
12.3	Gerenciar infraestrutura de rede com segurança	Gerencie com segurança a infraestrutura de rede. Exemplos de implementações incluem versão controlada de infraestrutura como código e o uso de protocolos de rede seguros, como SSH e HTTPS.	9
12.5	Centralizar a autenticação, autorização e auditoria (AAA) de rede	Centralize AAA de rede.	3, 4, 11
12.6	Usar protocolos de comunicação e gestão de rede seguros	Use protocolos de comunicação e gestão de rede seguros (por exemplo, 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise ou superior).	3, 4, 5, 11
12.7	Assegurar que os dispositivos remotos utilizem uma VPN e estejam se conectando a uma infraestrutura AAA da empresa	Exigir que os usuários se autentiquem em serviços de autenticação e VPN gerenciados pela empresa antes de acessar os recursos da empresa em dispositivos de usuário final.	3, 4, 5
12.8	Estabelecer e manter recursos de computação dedicados para todo o trabalho administrativo	Estabeleça e mantenha recursos de computação dedicados, fisicamente ou logicamente separados, para todas as tarefas administrativas ou tarefas que requeiram acesso administrativo. Os recursos de computação devem ser segmentados da rede primária da empresa e não deve ser permitido o acesso à Internet.	4
13.01	Centralizar o alerta de eventos de segurança	Centralize os alertas de eventos de segurança em ativos corporativos para correlação e análise de log. A melhor prática requer o uso de um SIEM, que inclui alertas de correlação de eventos definidos pelo fornecedor. Uma plataforma de análise de log configurada com alertas de correlação relevantes para a segurança também atende a esta medida de segurança.	11, 20, 22

Tabela 4.5: Controles de Segurança oriundos do CIS Controls

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
13.02	Implantar solução de detecção de intrusão baseada em host	Implante uma solução de detecção de intrusão baseada em host em ativos corporativos, quando apropriado e/ou com suporte.	11
13.03	Implantar uma solução de detecção de intrusão de rede	Implante uma solução de detecção de intrusão de rede em ativos corporativos, quando apropriado. Exemplos de implementações incluem o uso de um Network Intrusion Detection System (NIDS) ou serviço de provedor de serviço de nuvem equivalente (CSP).	11, 20, 22
13.04	Realizar filtragem de tráfego entre segmentos de rede	Execute a filtragem de tráfego entre segmentos de rede, quando apropriado.	13
13.05	Gerenciar controle de acesso para ativos remotos	"Gerencie o controle de acesso para ativos que se conectam remotamente aos recursos da empresa. Determine a quantidade de acesso aos recursos da empresa com base em: software anti-malware atualizado instalado, conformidade de configuração com o processo de configurações seguras da empresa e garantia de que o sistema operacional e as aplicações estão atualizados."	13
13.06	Coletar logs de fluxo de tráfego da rede	Colete logs de fluxo de tráfego de rede e/ou tráfego de rede para revisar e alertar sobre dispositivos de rede.	11, 20, 22
13.07	Implantar solução de prevenção de intrusão baseada em host	Implante uma solução de prevenção de intrusão baseada em host em ativos corporativos, quando apropriado e/ou com suporte. Exemplos de implementações incluem o uso de um cliente Endpoint Detection and Response (EDR) ou agente IPS baseado em host.	11
13.08	Implantar uma solução de prevenção de intrusão de rede	Implante uma solução de prevenção de intrusão de rede, quando apropriado. Exemplos de implementações incluem o uso de um Network Intrusion Prevention System (NIPS) ou serviço CSP equivalente.	11, 20, 22
13.09	Implantar controle de acesso no nível de porta	Implante o controle de acesso no nível de porta. O controle de acesso no nível de porta utiliza 802.1x ou protocolos de controle de acesso à rede semelhantes, como certificados, e pode incorporar autenticação de usuário e/ou dispositivo.	11, 20, 22
13.1	Executar filtragem da camada de aplicação	Execute a filtragem da camada de aplicação. Exemplos de implementações incluem um proxy de filtragem, firewall de camada de aplicação ou gateway.	11, 13
14.1	Estabelecer e manter um programa de conscientização de segurança	Estabeleça e mantenha um programa de conscientização de segurança. O objetivo de um programa de conscientização de segurança é educar a força de trabalho da empresa sobre como interagir com ativos e dados corporativos de maneira segura. Realize o treinamento na contratação e, no mínimo, anualmente. Revise e atualize o conteúdo anualmente ou quando ocorrerem mudanças significativas na empresa que possam afetar esta proteção.	11, 12, 13, 27

Tabela 4.5: Controles de Segurança oriundos do CIS Controls

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
14.2	Treinar membros da força de trabalho para reconhecer ataques de engenharia social	Treine os membros da força de trabalho para reconhecer ataques de engenharia social, como phishing, pretexto e uso não autorizado.	3, 4, 5, 6, 11
14.3	Treinar membros da força de trabalho nas melhores práticas de autenticação	Treine os membros da força de trabalho nas melhores práticas de autenticação. Exemplos de tópicos incluem MFA, composição de senha e gestão de credenciais.	3, 4, 11, 12
14.4	Treinar a força de trabalho nas Melhores Práticas de Tratamento de Dados	Treine os membros da força de trabalho sobre como identificar, armazenar, transferir, arquivar e destruir dados sensíveis de maneira adequada. Isso também inclui o treinamento de membros da força de trabalho em práticas recomendadas de mesa e tela limpas, como bloquear a tela quando eles se afastam de seus ativos corporativos, apagar quadros brancos físicos e virtuais no final das reuniões e armazenar dados e ativos com segurança.	1, 5, 6, 11, 12, 32
14.5	Treinar membros da força de trabalho sobre as causas da exposição não intencional de dados	Treine os membros da força de trabalho para estarem cientes das causas da exposição não intencional de dados. Exemplos de tópicos incluem entrega incorreta de dados sensíveis, perda de um dispositivo de usuário final portátil ou publicação de dados para públicos indesejados.	1, 6, 11, 32
14.6	Treinar Membros da força de trabalho no Reconhecimento e Comunicação de Incidentes de Segurança	Treine os membros da força de trabalho para serem capazes de reconhecer um incidente em potencial e relatar tal incidente.	11
14.7	Treinar a força de trabalho sobre como identificar e comunicar se o seus ativos corporativos estão faltando atualizações de segurança	Treine a força de trabalho para entender como verificar e relatar patches de software desatualizados ou quaisquer falhas em ferramentas e processos automatizados. Parte desse treinamento deve incluir a notificação do pessoal de TI sobre quaisquer falhas em processos e ferramentas automatizadas.	5
14.8	Treinar a força de trabalho sobre os perigos de se conectar e transmitir dados corporativos em redes inseguras	Treine os membros da força de trabalho sobre os perigos de se conectar e transmitir dados em redes inseguras para atividades corporativas. Se a empresa tiver funcionários remotos, o treinamento deve incluir orientação para garantir que todos os usuários configurem com segurança sua infraestrutura de rede doméstica.	4, 5, 32

Tabela 4.5: Controles de Segurança oriundos do CIS Controls

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
14.9	Conduzir treinamento de competências e conscientização de segurança para funções específicas	Conduza treinamento de conscientização de segurança e de competências específicas para funções. Exemplos de implementações incluem cursos de administração de sistema seguro para profissionais de TI, treinamento de conscientização e prevenção de vulnerabilidades para desenvolvedores de aplicações da web do OWASP® Top 10 aplicações e treinamento avançado de conscientização de engenharia social para funções de perfil alto.	4, 8, 9, 17, 27, 28, 32
15.4	Garantir que os contratos do provedor de serviços incluam requisitos de segurança	Certifique-se de que os contratos do provedor de serviços incluem requisitos de segurança. Requisitos de exemplo podem incluir requisitos mínimos do programa de segurança, notificação e resposta de incidente de segurança e/ou de violação de dados, requisitos de criptografia de dados e compromissos de descarte de dados. Esses requisitos de segurança devem ser consistentes com a política de gestão do provedor de serviços da empresa. Revise os contratos do provedor de serviços anualmente para garantir que os contratos não estejam perdendo os requisitos de segurança.	9
15.7	Descomissionar com segurança os provedores de serviços	Descomissione os prestadores de serviços com segurança. Considerações de exemplo incluem desativação de contas de usuário e serviço, encerramento de fluxos de dados e descarte seguro de dados corporativos em sistemas de provedores de serviços.	9
16.01	Estabelecer e manter um processo seguro de desenvolvimento de aplicações	Estabeleça e mantenha um processo seguro de desenvolvimento de aplicações. No processo, trate de itens como: padrões de design de aplicação seguro, práticas de codificação seguras, treinamento de desenvolvedor, gestão de vulnerabilidade, segurança de código de terceiros e procedimentos de teste de segurança de aplicação. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	8, 17, 28

Tabela 4.5: Controles de Segurança oriundos do CIS Controls

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
16.02	Estabelecer e manter um processo para aceitar e endereçar vulnerabilidades de software	Estabelecer e manter um processo para aceitar e endereçar relatórios de vulnerabilidades de software, incluindo um meio para que as entidades externas relatem. O processo deve incluir itens como: uma política de tratamento de vulnerabilidade que identifica o processo de relatar, a parte responsável por lidar com os relatórios de vulnerabilidade e um processo de entrada, atribuição, correção e teste de correção. Como parte do processo, use um sistema de rastreamento de vulnerabilidade que inclua classificações de gravidade e métricas para medir o tempo de identificação, análise e correção de vulnerabilidades. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança. Os terceiros desenvolvedores de aplicações precisam considerar esta política para o exterior que ajuda a definir as expectativas para as partes interessadas externas.	8, 17, 28
16.03	Executar análise de causa raiz em vulnerabilidades de segurança	Execute a análise de causa raiz em vulnerabilidades de segurança. Ao revisar as vulnerabilidades, a análise da causa raiz é a tarefa de avaliar os problemas subjacentes que criam vulnerabilidades no código e permite que as equipes de desenvolvimento vão além de apenas corrigir vulnerabilidades individuais conforme elas surgem.	8, 17, 28
16.04	Estabelecer e gerenciar um inventário de componentes de software de terceiros	Estabeleça e gerencie um inventário atualizado de componentes de terceiros usados no desenvolvimento, geralmente chamados de “lista de materiais”, bem como componentes programados para uso futuro. Este inventário deve incluir quaisquer riscos que cada componente de terceiros possa representar. Avalie a lista pelo menos uma vez por mês para identificar quaisquer mudanças ou atualizações nesses componentes e valide se o componente ainda é compatível.	8, 17, 28
16.05	Usar componentes de software de terceiros atualizados e confiáveis	Use componentes de software de terceiros atualizados e confiáveis. Quando possível, escolha bibliotecas e estruturas estabelecidas e comprovadas que forneçam segurança adequada. Adquira esses componentes de fontes confiáveis ou avalie o software quanto a vulnerabilidades antes de usá-los.	8, 17, 28

Tabela 4.5: Controles de Segurança oriundos do CIS Controls

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
16.06	Estabelecer e manter um sistema de classificação de gravidade e processo para vulnerabilidades de aplicações	Estabeleça e mantenha um sistema de classificação de gravidade e processo para vulnerabilidades de aplicações que facilitem a priorização da ordem em que as vulnerabilidades descobertas são corrigidas. Esse processo inclui a definição de um nível mínimo de aceitabilidade de segurança para a liberação de código ou aplicações. As classificações de gravidade trazem uma forma sistemática de triagem de vulnerabilidades que melhora o gestão de riscos e ajuda a garantir que os bugs mais graves sejam corrigidos primeiro. Revise e atualize o sistema e processo anualmente.	8
16.07	Usar modelos de configurações de segurança padrão para infraestrutura de aplicações	Use modelos de configuração de segurança padrão recomendados pelo setor para componentes de infraestrutura de aplicações. Isso inclui servidores subjacentes, bancos de dados e servidores web e se aplica a contêineres de nuvem, componentes de Platform as a Service (PaaS) e componentes de SaaS. Não permita que o software desenvolvido internamente enfraqueça as configurações de segurança.	9, 11
16.08	Separar sistemas de produção e não produção	Mantenha ambientes separados para sistemas de produção e não produção.	8, 9, 11
16.09	Treinar desenvolvedores em conceitos de segurança de aplicações e codificação segura	Certifique-se de que todo o pessoal de desenvolvimento de software receba treinamento para escrever código seguro para seu ambiente de desenvolvimento e responsabilidades específicas. O treinamento pode incluir princípios gerais de segurança e práticas padrão de segurança de aplicações. Conduza o treinamento pelo menos uma vez por ano e projete de forma a promover a segurança dentro da equipe de desenvolvimento e construir uma cultura de segurança entre os desenvolvedores.	8, 17, 28
16.1	Aplicar princípios de design seguro em arquiteturas de aplicações	Aplique princípios de design seguro em arquiteturas de aplicações. Os princípios de design seguro incluem o conceito de privilégio mínimo e aplicação de mediação para validar cada operação que o usuário faz, promovendo o conceito de "nunca confiar nas entradas do usuário". Os exemplos incluem garantir que a verificação explícita de erros seja realizada e documentada para todas as entradas, incluindo tamanho, tipo de dados e intervalos ou formatos aceitáveis. O design seguro também significa minimizar a superfície de ataque da infraestrutura da aplicação, como desligar portas e serviços desprotegidos, remover programas e arquivos desnecessários e renomear ou remover contas padrão.	8, 9, 11

Tabela 4.5: Controles de Segurança oriundos do CIS Controls

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
16.11	Aproveitar os módulos ou serviços controlados para componentes de segurança de aplicações	Aproveite os módulos ou serviços controlados para os componentes de segurança da aplicação, como gestão de identidade, criptografia e auditoria e log. O uso de recursos da plataforma em funções críticas de segurança reduzirá a carga de trabalho dos desenvolvedores e minimizará a probabilidade de erros de design ou implementação. Os sistemas operacionais modernos fornecem mecanismos eficazes para identificação, autenticação e autorização e disponibilizam esses mecanismos para as aplicações. Use apenas algoritmos de criptografia padronizados, atualmente aceitos e amplamente revisados. Os sistemas operacionais também fornecem mecanismos para criar e manter logs de auditoria seguros.	8
16.12	Implementar verificações de segurança em nível de código	Aplique ferramentas de análise estáticas e dinâmicas dentro do ciclo de vida da aplicação para verificar se as práticas de codificação seguras estão sendo seguidas.	8, 17, 28
16.13	Realizar teste de invasão de aplicação	Realize teste de invasão das aplicações. Para aplicações críticas, o teste de invasão autenticado é mais adequado para localizar vulnerabilidades de lógica de negócios do que a varredura de código e o teste de segurança automatizado. O teste de invasão depende da habilidade do testador para manipular manualmente um aplicação como um usuário autenticado e não autenticado.	8
16.14	Conduzir aplicações de modelagem de ameaças	Conduza a modelagem de ameaças. A modelagem de ameaças é o processo de identificar e abordar as falhas de design de segurança da aplicação em um design, antes que o código seja criado. É conduzido por pessoas especialmente treinadas que avaliam o design da aplicação e medem os riscos de segurança para cada ponto de entrada e nível de acesso. O objetivo é mapear a aplicação, a arquitetura e a infraestrutura de uma forma estruturada para entender seus pontos fracos.	8
17.1	Designar Pessoal para Gerenciar Tratamento de Incidentes	"Designe uma pessoa-chave e pelo menos uma backup para gerenciar o processo de tratamento de incidentes da empresa. A equipe de gestão é responsável pela coordenação e documentação dos esforços de resposta e recuperação a incidentes e pode consistir em funcionários internos da empresa, fornecedores terceirizados ou uma abordagem híbrida. Se estiver usando um fornecedor terceirizado, designe pelo menos uma pessoa interna da empresa para supervisionar qualquer trabalho terceirizado. Revise anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança."	11, 13

Tabela 4.5: Controles de Segurança oriundos do CIS Controls

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
17.2	Estabelecer e manter informações de contato para relatar incidentes de segurança	Estabeleça e mantenha as informações de contato das partes que precisam ser informadas sobre os incidentes de segurança. Os contatos podem incluir funcionários internos, fornecedores terceirizados, policiais, provedores de seguros cibernéticos, agências governamentais relevantes, parceiros do Information Sharing and Analysis Center (ISAC) ou outras partes interessadas. Verifique os contatos anualmente para garantir que as informações estejam atualizadas.	11, 13
17.3	Estabelecer e manter um processo corporativo para relatar incidentes	Estabeleça e mantenha um processo corporativo para a força de trabalho relatar incidentes de segurança. O processo inclui cronograma de relatórios, pessoal para relatar, mecanismo para relatar e as informações mínimas a serem relatadas. Certifique-se de que o processo esteja publicamente disponível para toda a força de trabalho. Revise anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	11, 13
18.1	Estabelecer e manter um programa de teste de invasão	Estabeleça e mantenha um programa de teste de invasão adequado ao tamanho, complexidade e maturidade da empresa. As características do programa de teste de invasão incluem escopo, como rede, aplicação web, Application Programming Interface (API), serviços hospedados e controles de instalações físicas; frequência; limitações, como horas aceitáveis e tipos de ataque excluídos; informações do ponto de contato; remediação, por exemplo, como as descobertas serão encaminhadas internamente; e requisitos retrospectivos.	8, 9, 11, 13
18.2	Realizar testes de invasão externos periódicos	Realize testes de invasão externos periódicos com base nos requisitos do programa, pelo menos uma vez por ano. O teste de invasão externo deve incluir reconhecimento empresarial e ambiental para detectar informações exploráveis. O teste de invasão requer habilidades e experiência especializadas e deve ser conduzido por uma parte qualificada. O teste pode ser clear box ou opaque box.	9, 11, 13
18.3	Corrigir as descobertas do teste de invasão	Corrija as descobertas do teste de invasão com base na política da empresa para o escopo e a priorização da correção.	8, 9, 11, 13
18.4	Validar as Medidas de Segurança	Valide as medidas de segurança após cada teste de invasão. Se necessário, modifique os conjuntos de regras e recursos para detectar as técnicas usadas durante o teste.	9, 11, 13
18.5	Realizar testes de invasão internos periódicos	Realize testes de invasão internos periódicos com base nos requisitos do programa, pelo menos uma vez por ano. O teste pode ser clear box ou opaque box.	9, 11, 13

Apesar da adequabilidade da seleção do *framework* CIS Controls como linha de base (*baseline*) para a seleção dos controles de segurança cibernética parecesse adequada, uma análise mais profunda revelou a

existência de lacunas significativas. A abordagem do CIS, focada em estabelecer controles abrangentes e prioritários para mitigar a maioria dos riscos ou efeitos [84], resultou em vários riscos operacionais relevantes detectados na Fase 1 não estarem adequadamente cobertos pelos controles propostos, especialmente em áreas como segurança física e continuidade dos negócios. Além disso, a evolução tecnológica recente, exemplificada por inovações como *Secure Access Service Edge (SASE)*, acesso condicional baseado em padrões de comportamento e a tecnologia *blockchain* como ferramenta de controle de modificações de informações não eram abordados. Assim, ficou constatada a necessidade da indicação de medidas adicionais que poderiam ser importantes na mitigação dos riscos previamente identificados.

Dada a especificidade do setor judiciário e dos riscos associados à operação e gestão de dados sensíveis, tornou-se indispensável a proposição de controles personalizados. Pesquisa bibliográfica indicou que a personalização (*tailoring*) de medidas de segurança é uma prática recomendada e amplamente reconhecida. Este processo visa basicamente garantir a eficácia e adequação das medidas de segurança da informação em contextos específicos [126].

O processo de adaptação ou customização dos controles (*tailoring*) implica na personalização de controles preestabelecidos para atender às necessidades específicas de uma organização ou sistema. Essencialmente, esse processo permite que organizações ajustem os controles de segurança padrão para refletir seus próprios riscos, requisitos regulatórios e características operacionais. O *tailoring* envolve a avaliação de riscos, a identificação de controles relevantes e a modificação destes para se adequarem ao contexto específico. Isso inclui adicionar, modificar ou mesmo remover controles para garantir que a segurança seja eficaz, sem ser excessivamente restritiva ou inadequada para o ambiente em questão [127].

Assim, se buscou enriquecer o estudo com a inclusão de controles recomendados por participantes entrevistados e por membros dos grupos focais envolvidos na pesquisa. A contribuição multidisciplinar, envolvendo profissionais de diversas áreas, mas com atuação direta nos órgãos judiciais, proporcionou uma compreensão mais ampla e precisa dos riscos de negócio enfrentados pelo Poder Judiciário. A abordagem holística permitiu uma análise mais detalhada e contextualizada dos desafios e ameaças, refletindo na identificação de estratégias de mitigação mais eficazes e alinhadas com as demandas específicas e os riscos únicos enfrentados pelas instituições alvo deste estudo em suas singulares realidades.

Os controles adicionais propostos neste estudo foram agrupados em grupos com identificação de 19 a 28, conforme a categorização dos controles que será melhor abordada nos resultados da Fase 3, e na sequência da numeração utilizada pelo guia de linha de base adotado, conforme abaixo:

- Grupo 19: Ambiente Organizacional;
- Grupo 20: Competências;
- Grupo 21: Estratégia;
- Grupo 22: Estrutura;
- Grupo 23: Gestão;
- Grupo 24: Identidade e Acesso;
- Grupo 25: Inteligência;
- Grupo 26: Processos de Trabalho;

- Grupo 27: Segurança Física;
- Grupo 28: Tecnologia.

A Tabela 4.6 apresenta os controles complementares propostos neste estudo e como eles se relacionam com os riscos operacionais.

Tabela 4.6: Controles de Segurança Adicionais

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
19.1	Possuir um programa de saúde mental	Possuir um programa preventivo voltado para a saúde e o bem-estar emocional/ mental dos servidores e colaboradores, reduzindo as possibilidades de cooptação por agentes mal-intencionados.	2, 13, 17, 28, 34
19.2	Favorecer a comunicação entre peritos e julgadores para evitar equívocos interpretativos	Favoreça a aproximação e a comunicação entre peritos e julgadores para o esclarecimento de eventuais dúvidas e assim evitar equívocos interpretativos	32
19.3	Promover a cultura ética e de integridade	Promova a educação jurídica e a formação contínua para os profissionais do sistema de justiça, enfatizando a importância da ética, da imparcialidade e da integridade e dos limites de atuação do ator ou função.	35, 36, 37
19.4	Favorecer a correição e o controle independentes	Favoreça os órgãos independentes de supervisão e controle, exercendo o papel de supervisão pública para monitorar e investigar alegações de influência indevida.	35, 36, 37
20.01	Desenvolver planos de contingência e de sucessão	Identifique as funções e cargos críticos, avalie as habilidades e potencialidades dos servidores e defina estratégias de capacitação ou de equipes de trabalho multidisciplinares para que posições de liderança e de responsabilidade não fiquem descobertas em casos de ausências temporárias ou permanente (ex: férias, atestados, demissão, aposentadoria ou morte).	14, 25, 32
20.02	Comunicar eficazmente a falta de recursos humanos	Comunique-se de forma clara, concisa e frequente com a alta administração sobre os riscos e prioridades para ajudar a evitar a falta de recursos humanos para os projetos, programas e atividades prioritários.	25
20.03	Conscientizar a alta administração sobre as diferenças na distribuição dos processos	Conscientize a alta administração que um algoritmo aleatório pode ocorrer diferenças na distribuição dos processos, contudo no decorrer do tempo essas diferenças são equalizadas.	27
20.04	Flexibilizar a contratação de especialistas para lidar com assunto de alta complexidade técnica	Flexibilize a possibilidade de contratação de especialistas ou perito externo para atuar em assunto excepcional ou de alta complexidade técnica	32

Tabela 4.6: Controles de Segurança Adicionais

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
20.05	Capacitar tecnicamente magistrados e gestores para evitar falhas de interpretação	Capacite minimamente os magistrados e a alta administração para evitar problemas de comunicação e falhas de interpretação ao analisar laudos e perícias técnicas.	32
20.06	Avaliar criticamente a qualificação do perito contratado	Avalie criticamente a qualificação e o perfil profissional de prováveis peritos frente à sua área de atuação.	32
20.07	Investir na capacitação de servidores	Invista e priorize a capacitação de servidores visando a retenção e multiplicação do conhecimento.	32
20.08	Realizar avaliação psicológica	Realize a avaliação psicológica regular de pessoas que ocuparão cargos chave de assessoramento dos órgãos de cúpula, que desempenharão atividades críticas de inteligência ou que terão acesso a informações ultrassecretas.	2, 34
20.09	Oferecer treinamento sobre técnicas de gerenciamento de tempo	Ofereça treinamento sobre e a importância do cumprimento dos prazos, podendo incluir orientações sobre técnicas de gerenciamento de tempo e estratégias para lidar com prazos exíguos. Certifique-se de que todos os envolvidos estejam cientes dos prazos estabelecidos e da necessidade de ser pontual.	38
20.1	Selecionar assessores jurídicos qualificados	Selecione assessores jurídicos qualificados para auxiliar os julgadores na revisão das peças processuais, pesquisa legal e preparação de minutas de decisões. A equipe de apoio pode fornecer informações adicionais e análises que permitiram ao julgador tomar decisões fundamentadas.	39
20.11	Promover a capacitação de usuários de IA sobre as capacidades, limitações e o uso ético da tecnologia	Promova programas de capacitação para os usuários da ferramenta, incluindo magistrados, servidores, estagiários e colaboradores dos órgãos, visando a compreensão das capacidades, limitações e o uso ético da Inteligência Artificial (IA).	40
21.01	Gerenciar os riscos para autoridades do Poder Judiciário e possuir protocolos de segurança	Gerencie os riscos de continuidade de negócios relacionados à segurança de autoridades do Poder Judiciário por meio de um processo que identifique, analise, avalie e trate esses riscos. O tratamento dos riscos pode incluir protocolos que prevejam o não compartilhamento de meios de transporte, hospedagens em locais diferentes, escolta, vigilância, rotas seguras, monitoramento de dark web, zonas de exclusão e varreduras de segurança em locais comuns.	14
21.02	Desenvolver estratégias de continuidade	Desenvolva planos de continuidade para antever e prevenir incidentes ou desastres, criar contingências e garantir a rápida recuperação.	16, 23
21.03	Fomentar parcerias entre órgãos públicos e a academia	Fomente parcerias entre os órgãos da Administração Pública e as universidades brasileiras para o desenvolvimento conjunto e a integração de soluções de tecnologia da informação, contribuindo para a produção mais eficiente e segura.	19, 22

Tabela 4.6: Controles de Segurança Adicionais

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
21.04	Estimular a produção nacional de tecnologia da informação	Estimule a produção e o desenvolvimento de soluções nacionais de tecnologia da informação com base em avaliação de riscos que considere a criticidade das informações, a possibilidade de espionagem por Estados estrangeiros e a demanda interna.	19, 22
21.05	Promover a criação de um laboratório nacional de testes de segurança cibernética	Promova a criação de um laboratório nacional com instrumental e pessoal adequados para a realização de testes avançados de segurança cibernética para a avaliação de equipamentos de tecnologia.	20, 22
21.06	Promover o intercâmbio internacional de tecnologias e a produção local de equipamentos	Promova a cooperação e o intercâmbio de tecnologias da informação com países amigos, objetivando o desenvolvimento conjunto de tecnologias próprias, a ampliação da oferta de soluções nacionais e a produção local de equipamentos, buscando evitar a quebra da produção em caso da deflagração de conflitos transnacionais.	19, 22
21.07	Possuir um repositório central do código-fonte dos sistemas judiciais em que se façam análises de segurança	Possua um repositório central das diversas versões em uso do Pje e dos demais sistemas judiciais e implemente rotinas automatizadas de detecção de vulnerabilidades que incluam a análise estática do código-fonte a fim de se avaliar se boas práticas de desenvolvimento seguro estão senso seguidas, se existem dependências de componentes ou bibliotecas inseguras, se utilizam linguagens de programação obsoletas e possivelmente rodam em ambientes que não recebem atualizações segurança.	21
21.08	Gerenciar os riscos relacionados a catástrofes naturais	Gerencie os riscos de continuidade de negócios relacionados aos desastres naturais por meio de um processo que identifique, analise, avalie e trate riscos de inundações, incêndios, terremotos, dentre outros, a que o órgão está exposto e desenvolva estratégias de mitigação dos riscos para evitar danos físicos ou a interrupção da prestação jurisdicional.	23
21.09	Aprimorar a governança corporativa e a gestão de pessoas	Defina claramente os objetivos estratégicos e o escopo dos projetos para garantir que os recursos humanos necessários sejam alocados adequadamente, levando em conta os possíveis riscos que podem impactar no alcance dos resultados pretendidos.	25
21.1	Aprimorar a governança corporativa e a gestão orçamentária	Defina claramente os objetivos estratégicos e o escopo dos projetos para garantir que os recursos financeiros necessários sejam alocados adequadamente, levando em conta os possíveis riscos que podem impactar no alcance dos resultados pretendidos.	26

Tabela 4.6: Controles de Segurança Adicionais

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
21.11	Estabelecer códigos de conduta ética e de limites de comunicação entre os atores do sistema de Justiça	Estabeleça códigos de conduta ética para juízes, promotores, procuradores e advogados que definam padrões claros sobre conflitos de interesse, aceitação de presentes ou benefícios e os limites para comunicações permitidas entre os atores do sistema de justiça.	35
21.12	Regulamentar limites para as formas de convencimento e persuasão judicial	Regulamente claramente limites para as atividades de convencimento e persuasão judicial permitidas, incluindo a possibilidade de participação em eventos, seminários ou conferências patrocinados por grupos de interesse.	35
21.13	Dar transparência e publicidade das comunicações com as partes e a participação em eventos	Dê transparência e publicidade das comunicações com as partes quando um envolvido no processo pedir audiência particular ou tornar pública a agenda dos julgadores e divulgar a participação em eventos, seminários e conferências patrocinados por terceiros.	35
21.14	Estabelecer regras para a nomeação de parentes	Estabeleça regras para nomear parentes próximos para cargos de assessoria ou apoio em gabinetes	36
21.15	Definir regras para gerenciar conflitos de interesse de julgadores	Defina diretrizes e regras para identificar e gerenciar conflitos de interesse reais ou aparentes quando da atuação de parentes ou pessoas com relações pessoais como advogados ou partes em processos sob competência de julgadores.	36
21.16	Definir regras para gerenciar conflitos de interesse de assessores e analistas judiciários	Defina diretrizes e regras para identificar e gerenciar conflitos de interesse reais ou aparentes quando da atuação de parentes ou pessoas com relações pessoais, como advogados ou partes, em processos sob análise, revisão ou minuta de decisões de assessores e analistas judiciários.	37
21.17	Estabelecer políticas e diretrizes claras sobre o uso de IA para a elaboração de despachos e decisões	Estabeleça políticas e diretrizes claras sobre como e quando o uso de Inteligência Artificial (IA) para a elaboração de despachos e decisões é apropriado, incluindo regras sobre como evitar a exposição de dados pessoais e informações protegidas por segredo de Justiça e preveja a necessidade de capacitação para os autorizados a utilizar a tecnologia.	40
22.1	Priorizar a utilizar servidores públicos com boas recomendações que lidem com informações sigilosas	Priorize a utilização de servidores públicos com boas recomendações e busque reduzir o acesso de estagiários e terceirizados às informações de grande relevância ou sigilosas.	2, 34
22.2	Possuir quadro de pessoal compatível	Possua quadro de pessoal compatível com o volume de trabalho de forma que seja possível analisar com profundidade as peças processuais apresentadas pelas partes.	38, 39
22.3	Utilizar servidores públicos com boas recomendações no desenvolvimento de sistemas críticos	Priorize a utilização de servidores públicos com boas recomendações e busque reduzir a utilização de estagiários e terceirizados que atuam no desenvolvimento de sistemas críticos.	17, 28

Tabela 4.6: Controles de Segurança Adicionais

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
23.01	Realizar testes regulares de continuidade e integridade	Realize testes de integridade em equipamentos para detectar possíveis falhas e garantir a continuidades dos serviços.	16, 23
23.02	Criar programas de testes e de auditoria para aferir a aleatoriedade dos sorteios em sistemas judiciais	Crie programas de testes internos e de auditoria por órgãos de controle e correição para aferir a aleatoriedade do sorteio de processos em sistemas judiciais.	17, 28
23.03	Priorizar atividades e projetos e alocar pessoas conforme a criticidade	Priorize as atividades e projetos que são críticos para o alcance dos objetivos estratégicos, permitindo que os recursos humanos sejam alocados de forma mais eficiente e eficaz.	25
23.04	Estimar realisticamente as necessidades de recursos humanos	Estime de forma realista as necessidades de recursos humanos para evitar a falta de recursos. As estimativas devem ser baseadas em dados históricos e nas lições aprendidas de projetos anteriores semelhantes.	25
23.05	Priorizar atividades e projetos críticos e alocar recursos financeiros conforme a criticidade	Priorize os projetos e atividades que são críticas para o alcance dos objetivos estratégicos, permitindo que os recursos financeiros sejam alocados de forma mais eficiente e eficaz.	26
23.06	Estimar realisticamente as necessidades de recursos materiais e o seu custo	Estime de forma realista as necessidades de recursos materiais e o seu custo para evitar a falta de recursos. As estimativas devem ser baseadas em dados históricos e nas lições aprendidas de projetos anteriores semelhantes.	26
23.07	Gerir projetos e processos para detectar a falta de recursos humanos em tempo hábil	Monitore e controle os projetos e processos para evitar a falta de recursos humanos. Deve-se estabelecer indicadores de desempenho e acompanhar o progresso para identificar problemas e tomar ações corretivas em tempo hábil.	25
23.08	Gerir projetos e processos para detectar a falta de recursos materiais em tempo hábil	Monitore e controle os projetos e processos para evitar a falta de recursos financeiros. Deve-se estabelecer indicadores de desempenho e acompanhar o progresso para identificar problemas e tomar ações corretivas em tempo hábil.	26
23.09	Estabelecer uma política de gestão de pessoas para reter talentos e desenvolver habilidades	Estabeleça uma política de gestão de pessoas que defina as diretrizes e práticas para atrair e reter talentos, desenvolver habilidades, manter a remuneração e benefícios atrativos e contribuir para a saúde e bem-estar dos membros, servidores e colaboradores.	25
23.1	Racionalizar investimentos em segurança cibernética com base em gestão de riscos	Racionalize os investimentos em soluções de segurança cibernética, de forma que os controles de segurança sejam priorizados e implementados para o tratamentos dos riscos mais relevantes, em conformidade com processo de avaliação de riscos.	26

Tabela 4.6: Controles de Segurança Adicionais

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
23.11	Padronizar diretrizes e procedimentos para lidar com ações duplicadas	Padronize as diretrizes e os procedimentos para a identificação de ações duplicadas e que medidas devem ser tomadas	29, 30, 31
23.12	Estabelecer medidas disciplinares ou sanções para o descumprimento injustificado de prazos	Estabeleça medidas disciplinares ou sanções cabíveis para os casos de descumprimento injustificado dos prazos processuais.	38
24.1	Utilizar mecanismos de detecção de comportamentos padrão de acessos e estabeleça políticas de acesso condicional	Utilize mecanismos que tracem uma linha padrão de acessos dos usuários e estabeleçam condições de segurança adicionais para os acessos fora de padrão (horários, origem geográfica, ações)	3, 4, 5, 12, 13
25.1	Avaliar a evolução profissional e econômica	Implemente ações de inteligência ou parcerias com autoridades competentes para avaliação da compatibilidade social, financeira, patrimonial e de ascensão profissional para cargos de assessoramento em órgãos de cúpula, que desempenharão atividades críticas de inteligência ou que terão acesso a dados ultrassecretos.	2, 17, 28, 34
25.2	Monitorar comunidades e fóruns	Monitore menções aos órgãos e autoridades em comunidades e fóruns fechados que indiquem a contratação de pessoas, a existência de insiders, a coordenação de ataques ou a venda de informações.	2, 4, 13, 17, 28, 34
25.3	Avaliar antecedentes de pessoas com acesso antecipado a decisões em Tribunais Superiores ou acesso a informações secretas	Implemente ações de inteligência ou parcerias com autoridades competentes para a avaliação de antecedentes para pessoas que tenham acesso antecipado a votos, determinações ou decisões em Tribunais Superiores ou que terão acesso a informações secretas. Podendo incluir a verificação de dados: pessoais, profissionais, comerciais, criminais, associações políticas e sociais.	2, 34
25.4	Investigar redes sociais e verificar de conflitos de interesse	Verifique atividades em redes sociais para obter informações adicionais sobre personalidade, comportamento e conexões. A verificação de conexões empresariais e de negócios passados podem também ajudar a identificar possíveis conflitos de interesse.	2, 17, 28, 34
25.5	Implementar monitoramento eletrônico	Realize atividades de inteligência ou parcerias com autoridades competentes para o monitoramento eletrônico regular de pessoas que ocuparão cargos chave de assessoramento dos órgãos de cúpula, que desempenharão atividades críticas de inteligência ou que terão acesso a dados ultrassecretos para detectar de atividades ou ligações suspeitas.	2, 34

Tabela 4.6: Controles de Segurança Adicionais

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
25.6	Avaliar antecedentes de desenvolvedores ou DBAs que atuam em sistemas judiciais ou sistemas críticos	Implemente ações de inteligência ou parcerias com autoridades competentes para a avaliação de antecedentes de pessoas que atuam no desenvolvimento ou gestão de banco de dados de sistemas judiciais ou críticos para a instituição. Podendo incluir a verificação de dados: pessoais, profissionais, comerciais, criminais, associações políticas e sociais.	17, 28
26.01	Segregar funções de programação, avaliação de qualidade e auditoria de código-fonte sensível	Segregue as funções de programação, avaliação de qualidade e auditoria de código-fonte sensível, evitando que uma mesma pessoa ou equipe seja responsável por todas as etapas de programação para diminuir a probabilidade de fraudes ou favorecimentos.	17, 28
26.02	Evitar inserir notas ou comentários internos em minutas de documentos	Evite inserir notas ou comentários internos da equipe ou direcionados ao decisor no corpo do documento que está em elaboração, evitando que acidentalmente esses comentários sejam mantidos na versão final.	24
26.03	Implementar dupla aprovação para ações críticas nos sistemas de informação	Implemente processo no qual sejam segregadas as funções críticas e que não seja possível que apenas uma pessoa finalize, aprove ou modifique documentos sensíveis, tais como levantamento de valores elevados ou a expedição de decisões relevantes	24, 34
26.04	Comunicar eficazmente a falta de recursos financeiros	Comunique-se de forma clara, concisa e frequente com a alta administração sobre os riscos e prioridades para ajudar a evitar a falta de recursos financeiros para os projetos, programas e atividades prioritários.	26
26.05	Solicitar a suspensão dos processos quando identificada a duplicidade de ações	Solicite a suspensão dos processos quando identificada a duplicidade de ações até que se decida o juízo competente para julgar o caso, evitando o prosseguimento simultâneo.	29, 30
26.06	Verificar visualmente o documento físico e validar assinaturas físicas	Verifique o documento em busca de características físicas que possam indicar sua autenticidade, como marca d'água, hologramas, selos, assinaturas originais, carimbos oficiais ou elementos de segurança específicos para o tipo de documento, quando aplicável. Exemplo: autenticação em cartório.	33
26.07	Comparar informações com documentos de referência	Compare as cópias ou informações fornecidas com os documentos autênticos de referência. Por exemplo, ao receber uma identificação pessoal, compare com uma identificação emitida oficialmente pelo órgão competente.	33
26.08	Utilizar métodos de validação de documentos digitais	Utilize mecanismos de validação de documentos digitais e não presuma que são autênticos. Sempre que possível, verifique assinaturas digitais em software confiável, faça o checksum de arquivos, acesse o link ou QR code de validação dos emissores e comparece com as informações fornecidas.	33

Tabela 4.6: Controles de Segurança Adicionais

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
26.09	Consultar o emissor do documento	Consulte a instituição ou a pessoa responsável pela emissão do documento e verifique diretamente a sua autenticidade. A depender da natureza do documento e do contexto utilizado, a verificação pode ser por telefone, e-mail ou pessoalmente.	33
26.1	Consultar especialistas em caso de dúvidas quanto a autenticidade de documentos	Consulte especialistas em casos complexos ou de alta relevância. Pode-se utilizar da opinião de especialistas forenses, peritos em caligrafia ou outros profissionais qualificados para verificar a autenticidade.	33
26.11	Sistematizar e monitorar o controle de prazos processuais	Sistematize e monitore de forma eficiente o controle dos prazos processuais, utilize calendários ou softwares específicos para acompanhar e alertar sobre prioridades e evitar que prazos sejam esquecidos ou negligenciados.	38
26.12	Validar informações de resumos elaborados por partes interessadas	Valide as informações apresentadas em resumos de processos volumosos e que passaram por diversas instâncias pois informações relevantes podem ter sido omitidas para conduzir a uma avaliação parcial e conveniente para uma das partes.	39
26.13	Segmentar funções e revisar análises preliminares	Segmente em diferentes etapas as funções de análise, elaboração e revisão de minutas com o objetivo de reduzir o risco de incorreções de linguagem, erros materiais, equívocos interpretativos e falta de alinhamento com o posicionamento do julgador.	39
26.14	Realizar audiências e exposições orais para a melhor compreensão do caso	Realize audiências e exposições orais para que as partes destaquem informações contidas nas peças processuais, proporcionando a compreensão mais completa do caso previamente à decisão.	39
26.15	Solicitar esclarecimentos adicionais	Solicite esclarecimentos adicionais em caso de dúvidas ou informações insuficientes, requisitando documentos complementares ou pedindo esclarecimentos sobre pontos específicos.	39
26.16	Estabelecer um processo de supervisão e revisão humana de decisões ou documentos gerados por IA	Estabeleça um processo de supervisão humana, em que as decisões ou documentos gerados por Inteligência Artificial (IA) sejam revisados por profissionais qualificados para garantir que os documentos estejam adequados do ponto de vista legal e com princípios éticos.	40
27.1	Implementar barreiras físicas adicionais e a identificação e autorização específicas para acesso às áreas sensíveis	Implemente barreiras físicas adicionais, tais como portas, catracas, fechaduras magnéticas, coletores biométricos e alarmes, e a necessidade de identificação e autorização adicionais para acesso às áreas sensíveis das instalações internas (ex: gabinetes, datacenter, infraestrutura elétrica). Esses sistemas podem ser integrados com câmeras de vigilância e alarmes e serem utilizados no monitoramento ativo.	7

Tabela 4.6: Controles de Segurança Adicionais

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
27.2	Proteger o perímetro das instalações	Proteja o perímetro das instalações com cercas e portões de acesso, podendo ser implementados proteções adicionais como detectores de metal, aparelhos de raio-x, sensores de movimento e alarmes para detectar intrusões.	7
27.3	Instalar vigilância por câmeras	Instale câmeras de vigilância para monitorar o perímetro e as instalações internas de intrusos e mantenho registro das gravações por tempo adequado. Preferencialmente utilize equipamentos com recursos de detecção de movimento, visão noturna, com alta qualidade de vídeo e capacidade de aproximação (zoom).	7
27.4	Possuir equipe de segurança monitorar ativamente as atividades suspeitas	Possuir equipe de segurança para monitorar ativamente as atividades suspeitas dentro e fora das instalações.	7
27.5	Realizar varreduras ambientais em ambientes críticos	Realize varreduras ambientais em ambiente críticos tais como datacenters ou gabinetes de desembargadores e ministros a fim de encontrar escutas ou dispositivos físicos de captura de comunicações ou dados.	7
27.6	Monitorar condições climáticas do ambiente	Monitore as condições climáticas do ambiente para evitar que temperaturas elevadas ou umidade excessiva possam danificar equipamentos eletrônicos resultando em falhas ou perda de dados.	16, 23
28.01	Configurar limites de banda de tráfego	Configure limites de largura de banda consumida, quantidade de conexões simultâneas abertas ou de requisições por usuário para ajudar a limitar a quantidade de tráfego enviado ao servidor, reduzindo o impacto de um ataque de DDoS.	15
28.02	Implementar abordagens de confiança zero (zero trust)	Implemente abordagens de confiança zero (zero trust) para que mesmo os usuários, os dispositivos e as comunicações internos sejam continuamente avaliados e protegidos.	3, 4, 5
28.03	Controlar alterações e garantir a custódia do código-fonte	Controle as alterações software, mantenha o histórico de cada versão modificada e verifique a integridade do código-fonte para garantir que não tenha sido indevidamente modificado. Pode ser utilizada função hash, sistema de controle de versão ou assinatura do código para garantir que o código-fonte não foi adulterado.	8, 17, 21
28.04	Microssegmentar comunicações de rede	Microssegmente as comunicações de rede para reduzir movimentações laterais e conter a propagação de malwares	13
28.05	Monitorar o tráfego e estabelecer padrões	Monitore o tráfego de rede, estabeleça padrões e crie alertas para desvios incomuns de tráfego que indiquem um ataque de DDoS.	15
28.06	Balancear a carga entre equipamentos de infraestrutura	Balanceie e distribua a carga entre vários equipamentos de infraestrutura para evitar a sobrecarga de um único ponto. Utilize hardware dedicado ou software de balanceamento de carga.	15

Tabela 4.6: Controles de Segurança Adicionais

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
28.07	Utilizar infraestrutura elástica	Utilize arquitetura em que os recursos de computação, armazenamento e rede são dimensionados automaticamente de acordo com as necessidades de processamento e de tráfego de dados em tempo real. Reduzindo ou escalando a infraestrutura conforme a demanda e sem a necessidade de intervenção humana. Sendo importante definir limite aceitável de recursos alocados para evitar o esgotamento total de recursos de infraestrutura on premisses ou a grande elevação de custos de serviços em nuvem.	15
28.08	Filtrar tráfego malicioso	Filtre e bloqueie tráfego suspeito, malicioso ou oriundo de botnets, com base na reputação dos endereços IP, filtragem de portas e protocolos.	15
28.09	Prevenir falsificação de endereço IP (spoofing)	Previna spoofing de IP para ajudar a reduzir ataques de DDoS. Utilize técnicas de autenticação de origem, como a verificação de roteamento de pacotes (RPV) ou a autenticação de mensagens de domínio baseada em assinatura (DomainKeys Identified Mail - DKIM).	15
28.1	Sanitizar o tráfego na operadora	Sanitize o tráfego ainda na operadora, evitando a saturação da capacidade de tráfego dos enlaces de comunicação.	15
28.11	Utilizar serviço de sanitização de tráfego em ambiente de terceiro	Utilize serviço de sanitização de tráfego em provedor de serviço de borda de acesso seguro (SASE) de forma que apenas o tráfego legítimo seja direcionado para o ambiente da instituição.	15
28.12	Monitorar os recursos de infraestrutura	Implemente sistemas de monitoramento para alertar sobre a elevação de consumo de recursos que poderão levar a uma falha, caso a equipe de TI não atue, bem alertar sobre possíveis falhas em componentes de hardware (ex: discos, processadores, fontes de alimentação).	16
28.13	Manter infraestrutura crítica em redundância	Mantenha sistemas de redundância para garantir que, caso ocorra a falha de um elemento crítico de infraestrutura (hardware e software), outro possa assumir a carga de trabalho automaticamente.	16, 23
28.14	Realizar atualizações preventivas e de segurança em ativos de infraestrutura	Realize atualizações regulares de firmware e software bem como a manutenção preventiva em equipamentos para evitar falhas devido a problemas de compatibilidade ou degradação pelo uso.	16
28.15	Utilizar fontes de aleatoriedade confiáveis	Avalie se o algoritmo utiliza uma fonte de aleatoriedade confiável e imprevisível. Geradores de números aleatórios e criptograficamente seguros podem ser produzidos em software ou hardware e utilizar fontes de ruído térmico em circuitos eletrônicos, ruído atmosférico captado ou funções matemáticas em cadeia, dentre outros. Esta avaliação deve ocorrer periodicamente considerando as evoluções constantes nesse campo de estudo.	17

Tabela 4.6: Controles de Segurança Adicionais

Id	Controle	Descrição da Medida de Segurança	Risco Operacional
28.16	Verificar a integridade dos documentos transmitidos eletronicamente	Verifique se os webservices, APIs ou sistemas possuem regras para atestar a integridade dos documentos transmitidos eletronicamente. Podem ser implementadas verificações de hash, de metadados dos arquivos e a assinatura digital para a verificação da integridade dos documentos eletrônicos.	18
28.17	Adaptar os sistemas judiciais para utilização da tecnologia blockchain	Adapte os sistemas judiciais para a utilização da tecnologia blockchain para o registro de transações e informações de forma segura e descentralizada, validando e registrando as informações de forma transparente e imutável. O blockchain pode garantir a integridade dos dados, a autenticidade da origem e a transparência da troca.	18, 34
28.18	Priorizar a transferência eletrônica de documentos pela integração de sistemas de órgãos da administração pública	Priorize a transferência eletrônica de documentos realizada por meio da integração de sistemas de órgãos da Administração Pública. A verificação de autenticidade de documentos físicos ou de documentos eletrônicos enviados por e-mail é mais difícil e requer conhecimentos específicos das várias técnicas de falsificação utilizadas, demandando a capacitação de muitas pessoas, de dupla verificação e da possibilidade de ataques de engenharia social.	18
28.19	Analisar a emissão eletromagnética	Analise a emissão eletromagnética para identificar a comunicação de possíveis dispositivos de comunicação. Envolve a utilização de equipamentos especializados para detectar a emissão eletromagnética.	20
28.2	Automatizar a verificação de ações semelhantes por meio de robôs ou IA	Automatize a consulta e verificação de processos em outros tribunais ou em uma base central de processos que possuam as mesmas partes, classes, subclasses ou assuntos processuais por meio do uso de robôs ou utilize inteligência artificial para comparar o teor das petições iniciais e indicar a possibilidade da duplicidade de ações no mesmo órgão.	29, 30, 31
28.21	Integrar a comunicação entre os sistemas judiciais ou criar base nacional de processos judiciais	Integre a comunicação entre os sistemas judiciais e compartilhe informações sobre as ações no acervo de cada órgão ou a manutenção de base nacional de processos judiciais, possibilitando a consulta e a identificação de processos semelhantes.	30, 31
28.22	Automatizar a execução dos atos processuais decorrentes do descumprimento de prazos	Automatize no sistema judicial a execução dos atos processuais decorrentes do descumprimento injustificado do prazos pelas partes.	38
28.23	Desmontar o dispositivo e analisar os componentes	Desmonte o dispositivo e analise os componentes que poderiam permitir a captura ou gravação de áudio ou vídeo, transmissões de rádio ou a comunicação remota	20

Percebe-se que a segurança da informação não se limita apenas aos departamentos tradicionalmente associados a essa área. É imprescindível o envolvimento integrado de setores como Gestão de Pessoas,

Jurídico, Conformidade, Auditoria e Gestão de Riscos. Estas áreas, ao atuarem de maneira sinérgica, desempenham um papel crucial na identificação, avaliação e mitigação de riscos. Esta abordagem integral permite uma compreensão mais ampla e efetiva dos riscos, contribuindo para a implementação de estratégias de segurança mais abrangentes. A colaboração interdepartamental eleva a capacidade de uma organização em prevenir, detectar e responder a ameaças potenciais, otimizando a gestão de riscos em todos os níveis da organização.

Bernard [53] confirma esse entendimento e complementa que os usuários da informação em diferentes unidades de negócio desempenham um papel fundamental, compreendendo suas funções críticas e o impacto da perda de informações. Os gerentes responsáveis pelas unidades de negócios dependentes de ativos de informação também são partes interessadas na segurança da informação. Embora não compreendam, e nem precisem conhecer completamente, o funcionamento da segurança ao serem apresentados a uma visão clara dos riscos e a um plano de tratamento de riscos priorizado, eles podem avaliar facilmente o custo das medidas de redução de riscos em relação ao impacto potencial dos eventos de risco no negócio. Isso os capacita a se tornarem defensores da segurança dos ativos pelos quais são responsáveis ou dos quais dependem.

Dentre os diversos controles se observa controles voltados para riscos de integridade e ética. Pesquisa bibliográfica confirma a existência desses riscos no âmbito do Poder Judiciário e que a gestão de riscos abrangente é a melhor forma de identificar e tratar tais aspectos. A importância da indicação de controles para gestão de destes riscos é apresentada pelo Escritório das Nações Unidas para Drogas e Crime [105]. Este organismo reforça que existem riscos de corrupção com relação a condutas de juízes e responsáveis pela definição de políticas judiciais, incluindo: condutas dos juízes podem gerar suspeitas de corrupção, descumprimento dos requisitos de um julgamento justo, a privação do tempo adequado para preparação da defesa, a ausência de fundamentação jurídica, práticas de condenação questionáveis, manipulação de declarações de bens, a não declaração de presentes, aceitação de hospitalidade, adiamento de procedimentos de apelação e promoções judiciais após casos politicamente sensíveis.

Além disso, o Escritório das Nações Unidas indica riscos de presidentes dos tribunais alterarem deliberadamente a composição das câmaras, manipulação do sistema de distribuição de casos, investigações inadequadas de alegações de má conduta e tolerância à corrupção. Nos conselhos judiciais, os riscos incluem processos de nomeação e promoção questionáveis, processos disciplinares seletivos e falta de controle e revisão regulares. No tocante aos riscos externos e de influência política, estes podem ser identificados em normas jurídicas ambíguas, promoções judiciais baseadas em critérios subjetivos, amnistias em processos criminais e esforços para reabrir casos politicamente sensíveis [105].

Portanto, o envolvimento de diversas áreas de atuação e de conhecimento na construção os resultados apresentados na Fase 2, que complementam a indicação dos riscos de negócio, suas causas e consequências, com a indicação de uma abrangente relação de possíveis medidas de segurança necessárias para evitar os aspectos indesejados para os órgãos de Justiça pode se tornar um instrumento relevante para que as unidades de negócio possam colaborativamente atuem em prol da visão e defesa da segurança da organização como um todo.

4.3 FASE 3

4.3.1 Funções de segurança

O CIS Controls adotou a abordagem de definição de 5 funções de segurança inicialmente desenvolvida pelo NIST no *CyberSecurity Framework*. As funções básicas de segurança são o nível mais alto de abstração previsto no NIST CSF e atual como a espinha dorsal em torno do qual todos os outros elementos são organizados. As cinco funções representam os pilares principais para um programa de segurança cibernética abrangente e auxiliam a expressar de forma facilitada e em alto nível a função de segurança cibernética no tratamento de riscos para os tomadores de decisão [128].

O NIST define cada uma das cinco funções da seguinte forma [128]:

- ***Identificar****: auxilia no desenvolvimento de um entendimento organizacional para gerir o risco de segurança cibernética em sistemas, pessoas, ativos, dados e capacidades, permitindo que a organização foque e priorize seus esforços de acordo com sua estratégia de gestão de riscos e necessidades de negócios.*
- ***Proteger****: define salvaguardas adequadas para garantir a entrega de serviços de infraestrutura crítica, limitando ou contendo o impacto de um possível evento de segurança cibernética. A função*
- ***Detectar*** *estabelece atividades apropriadas para identificar a ocorrência de um evento de segurança cibernética, possibilitando a descoberta oportuna desses eventos.*
- ***Responder****: inclui atividades apropriadas para agir em relação a um incidente de segurança cibernética detectado, apoiando a capacidade de conter seu impacto.*
- ***Recuperar****: identifica atividades apropriadas para manter planos de resiliência e restaurar capacidades ou serviços prejudicados devido a um incidente de segurança cibernética, apoiando a recuperação oportuna para operações normais e reduzindo o impacto do incidente.*

Tendo em vista esta relevância desta visão de alto nível, foi aplicada a mesma metodologia avaliação de funções de segurança para os controles adicionais propostos neste estudo, que resultaram na distribuição descrita na Figura 4.3

4.3.2 Categorização dos controles

Para melhorar a eficácia na aplicação de medidas de segurança, foi imprescindível categorizar a ampla gama de controles existentes, incluindo aqueles relativos ao CIS Controls. Esta categorização é útil para facilitar a identificação e o agrupamento das ações de segurança mais relevantes que poderão ser aplicadas conforme os propósitos e contextos de implementação. Bem como fornecendo uma visão por área temática dos diferentes tipos de controles disponíveis, orientando os gestores na seleção das medidas mais pertinentes para atingir objetivos específicos.

Além disso, essa estrutura de categorização é benéfica para a condução de autoavaliações e auditorias,

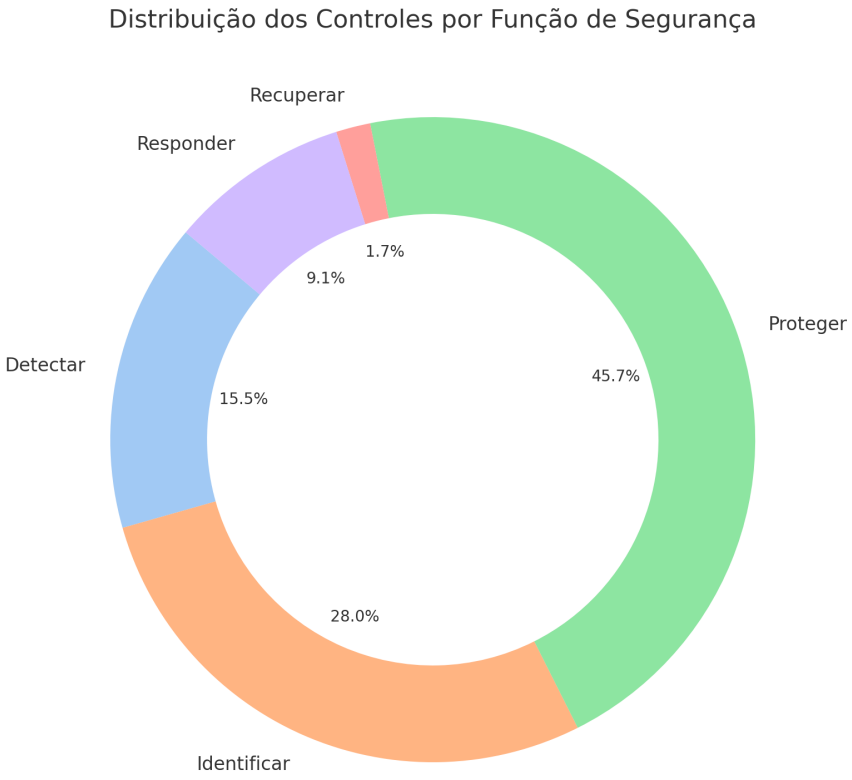


Figura 4.3: Distribuição dos controles conforme a sua função.
Fonte: do Autor

facilitando uma análise objetiva das práticas atuais e a identificação de áreas que necessitam de melhorias em setores específicos. Verificou-se que Angelini [129] suporta a relevância de realizar a classificação dos controles de segurança como primeiro ato ao se buscar definir uma metodologia de avaliação de risco cibernético. O autor destaca que a classificar os controles com base em suas características é fundamental para que clarificar o seu propósito e facilitar a interpretação para a sua implementação.

Para a elaboração desta classificação, se observou como uma das referências a taxonomia de controles de risco operacional no Poder Judiciário proposta por Machado [43]. Entretanto, verificou-se que a taxonomia proposta não atenderia às especificidades deste estudo. Buscou-se estabelecer uma nomenclatura original de categorias dos controles em único nível para que os gestores pudessem selecionar mais rapidamente a área temática de cada controle. Essa avaliação resultou em uma classificação que compreende onze categorias distintas de controles, conforme descrição a seguir:

1. **Ambiente organizacional**: refere-se ao conjunto de aspectos que definem a cultura ou clima organizacional, envolvendo aspectos éticos, conflitos pessoais e as condições que influenciam a maneira como as pessoas se relacionam e as decisões são tomadas.
2. **Competências**: engloba as habilidades, conhecimentos, atitudes e experiências necessárias para que as pessoas desempenhem suas funções de trabalho.
3. **Estratégia**: relacionada à definição de objetivos de longo prazo e à formulação de planos

para alcançá-los. A definição clara de objetivos e metas ajudam a orientar os planejamentos e ações dos demais níveis organizacionais, para que se alinhem às prioridades gerais da instituição.

4. **Estrutura**: refere-se à maneira como a organização é organizada, incluindo a hierarquia, a distribuição de atribuições e responsabilidades e os mecanismos de coordenação entre diferentes unidades organizacionais.
5. **Fornecedores**: envolve a gestão das relações com fornecedores, incluindo a seleção, o monitoramento e a avaliação deles. Isso é crucial para garantir a qualidade da entrega de produtos e serviços adquiridos e a aplicação de eventuais sanções, quando necessário.
6. **Gestão**: abrange o conjunto de planos e ações voltadas para a execução e acompanhamento da estratégia organizacional em áreas temáticas específicas - geralmente em unidades organizacionais - visando garantir a eficiência, eficácia e conformidade regulamentar. Engloba a ações gerenciais em nível tático.
7. **Identidade e acesso**: relacionado aos controles para gerenciar a identificação das pessoas quem tem acesso a quais informações e sistemas dentro da organização. Alcança todo o ciclo de vida da gestão de autorizações de pessoas, incluindo o ingresso, cadastro, mudança de lotação e o desligamento de magistrados, servidores estagiários e terceirizados e suas respectivas autorizações de acesso.
8. **Inteligência**: trata da inteligência de ameaças humanas e que envolvem a coleta, análise e utilização de informações sigilosas ou abertas para antecipar tendências e riscos institucionais para a tomada de decisões informadas.
9. **Processos de trabalho**: referem-se aos controles relativos ao conjunto de atividades organizadas e sequenciais que são realizadas para atingir objetivos específicos uma organização. Os processos de trabalho estruturam como o trabalho é feito, garantindo que as tarefas sejam realizadas de maneira eficiente e eficaz, ao mesmo tempo em que contribuem para o alcance dos objetivos organizacionais.
10. **Segurança física**: Esta categoria engloba as medidas destinadas a proteger as instalações físicas da organização e os ativos nela contidos. Inclui controles como sistemas de vigilância, controle de acesso, proteção contra incêndios e segurança para prevenir o acesso não autorizado a áreas sensíveis.
11. **Tecnologia**: Refere-se ao conjunto de ferramentas, sistemas, e infraestruturas tecnológicas utilizadas pela organização. Inclui serviços, hardware e software utilizados para a transmissão, armazenamento ou modificação de informação.

A Figura 4.4 representa visualmente a distribuição geral dos controles de segurança da informação em cada uma das categorias descritas.

A análise dos dados revela uma predominância marcante da categoria *Tecnologia*, com um volume significativamente maior de controles quando comparado às outras categorias. Esta tendência pode ser atribuída a diversos fatores. Inicialmente, a interpretação desse fenômeno pode ser vinculada ao elevado nível de digitalização de serviços no âmbito do Poder Judiciário. A crescente dependência de soluções

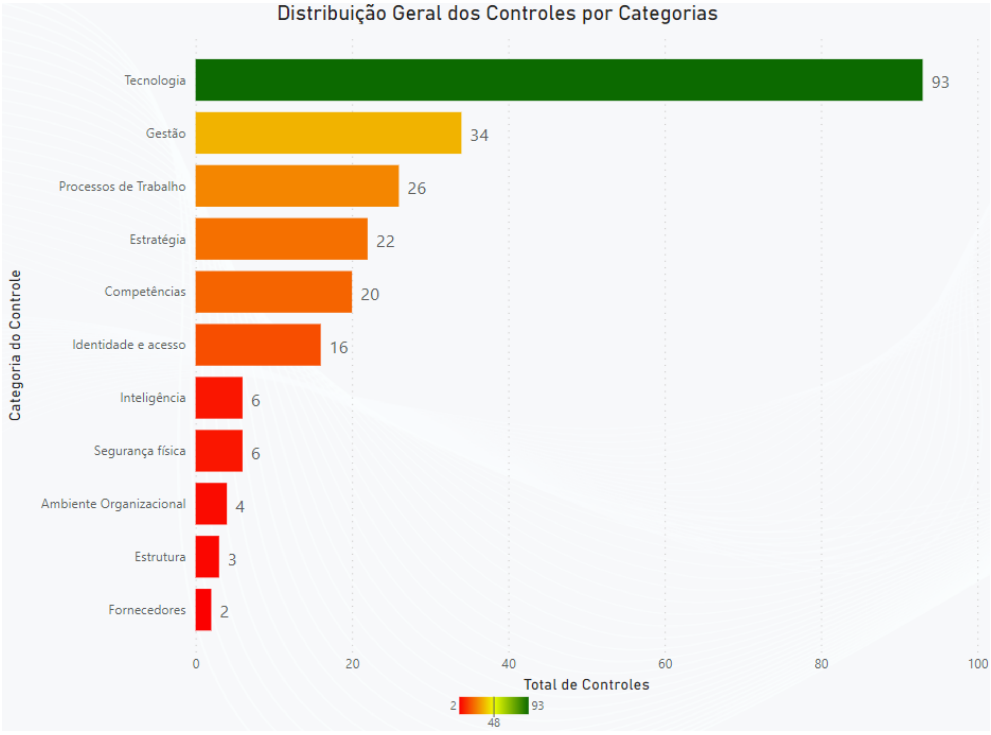


Figura 4.4: Distribuição dos controles por categoria.
Fonte: do Autor

tecnológicas para atingir objetivos estratégicos amplia a exposição a riscos cibernéticos, tornando imperativo o fortalecimento de medidas de segurança para proteger esses ativos críticos. Essa realidade se reflete em um foco acentuado nos controles de segurança cibernética, superando outras áreas em número e complexidade.

A representatividade de aproximadamente 40% dos controles voltados para aspectos tecnológicos não só ressalta a importância da segurança cibernética no cenário atual, mas também reflete a complexidade inerente à gestão da segurança em ambientes tecnológicos. A área de tecnologia da informação, caracterizada pela constante evolução e diversidade, exige uma gama abrangente de controles para mitigar uma vasta gama de ameaças potenciais. Além disso, incidentes de segurança relacionados à tecnologia tendem a ser mais evidentes e geram impactos imediatos e significativos, justificando a necessidade de uma atenção mais intensiva e, consequentemente, de um maior número de controles nesta área.

Contudo, a predominância quantitativa de controles tecnológicos não implica automaticamente que estes sejam os mais relevantes em todos os contextos. É imperativo que cada organização conduza uma avaliação qualitativa de quais riscos são mais sensíveis para o seu contexto, determinando com base nessas premissas a relevância relativa de cada controle para a redução dos riscos críticos da instituição [130]. Tal abordagem é fundamental para alcançar um equilíbrio entre a implementação de controles de segurança tecnológicos e aqueles pertinentes a outras áreas operacionais e estratégicas.

Outra análise diz respeito à comparação entre a categorização dos controles oriundos do guia de referência e os controles adicionais propostos. Conforme evidenciam as Figuras 4.5 e 4.6, observa-se que o *CIS Controls* possui um enfoque majoritariamente tecnológico, enquanto os controles adicionais propostos

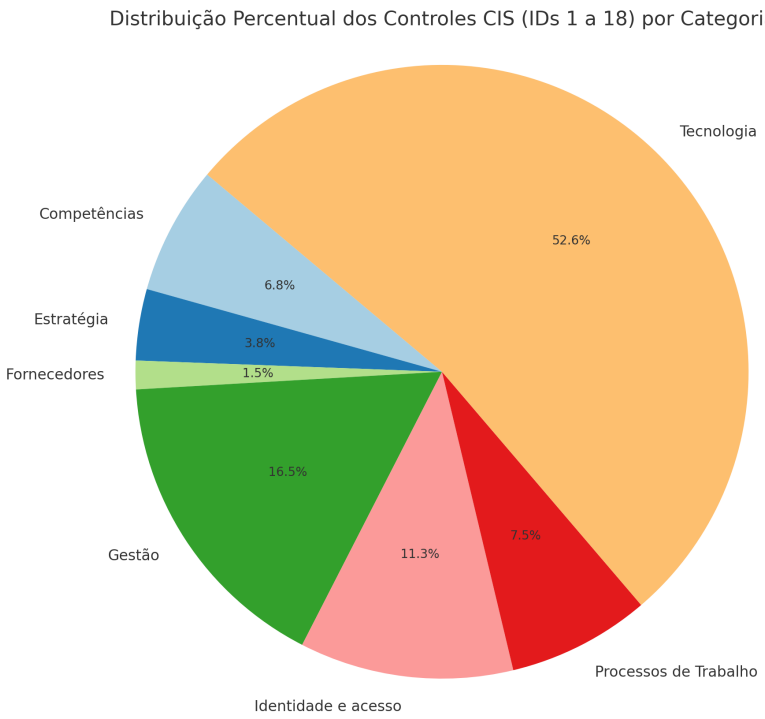


Figura 4.5: Distribuição das categorias dos controles CIS.
Fonte: do Autor

neste estudo apresentaram menor variação quantitativa entre as várias categorias. Entretanto, a distribuição mais equilibrada das categorias de controles de segurança de tecnologia controles adicionais (19 a 28) somente foi possível em função do CIS Controls previamente ter endereçado a maioria das medidas técnicas.

Importante ressaltar que os controles adicionais foram construídos por gestores do Poder Judiciário com ampla vivência prática e são direcionados para o tratamento de riscos específicos e relevantes neste contexto. Estes controles representam uma fonte valiosa de medidas abrangentes e alinhadas às necessidades específicas do setor judiciário.

Além disso, a análise das categorias *Estratégia*, *Gestão* e *Processos de Trabalho* sugere uma forte interconexão e complementaridade entre as categorias. Os controles voltados para a **estratégia** se concentram na governança, definição de direções de longo prazo e na formulação de planos para alcançar objetivos organizacionais. Controles estratégicos incluem políticas, planejamento estratégico e metas organizacionais. Os controles de **gestão** estão mais relacionados à supervisão e implementação das estratégias definidas em nível estratégico. Esta categoria pode incluir controles relacionados à administração diária, gerenciamento de recursos, tomada de decisão e controle operacional. O gerenciamento de **processos de trabalho** foca no fluxo de trabalho e na entrega de valor por meio da execução de diversas atividades e interação entre variados atores. Os controles são mais práticos e orientados para a execução, abordando como as tarefas são realizadas cotidianamente, garantindo eficiência e a segurança dos processos.

Todas as categorias são interdependentes e complementares para a proteção das organizações. No entanto, essas três categorias são ainda mais relacionadas e poderiam até mesmo ser vistas como partes de

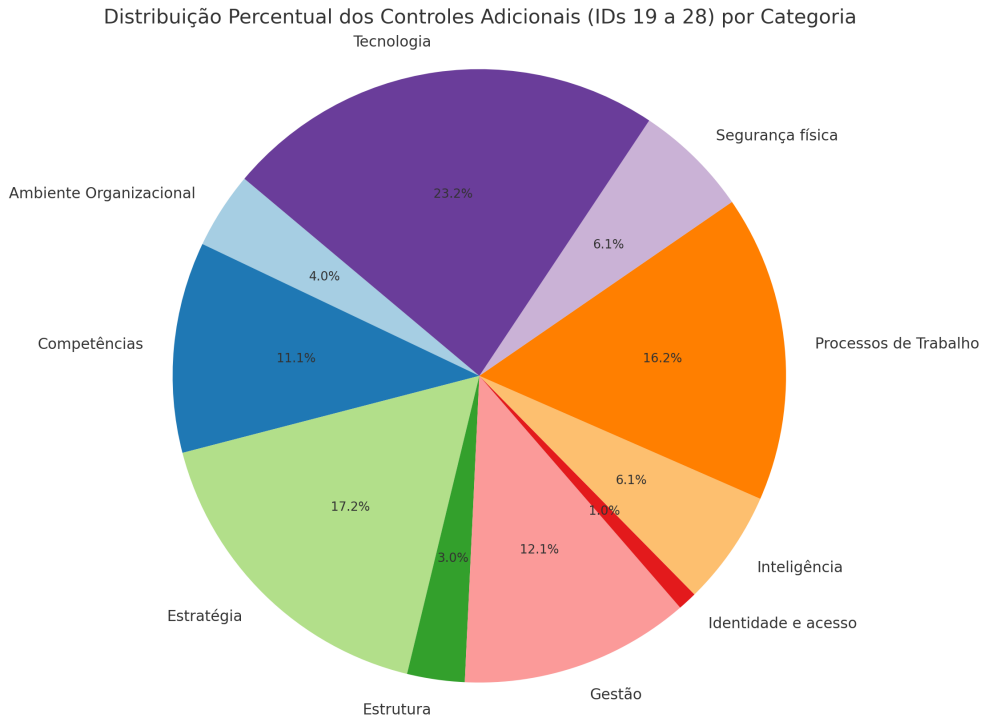


Figura 4.6: Distribuição das categorias dos controles adicionais.
Fonte: do Autor

um sistema interconectado que podem fornecer uma visão abrangente de como a organização opera, desde o nível estratégico até a execução prática. Se as categorias *Estratégia*, *Gestão* e *Processos de Trabalho* fossem em uma única categoria, denominada **Estratégia, Gestão e Processos de Trabalho**, a distribuição percentual dos controles por categoria demonstrada na Figura 4.7.

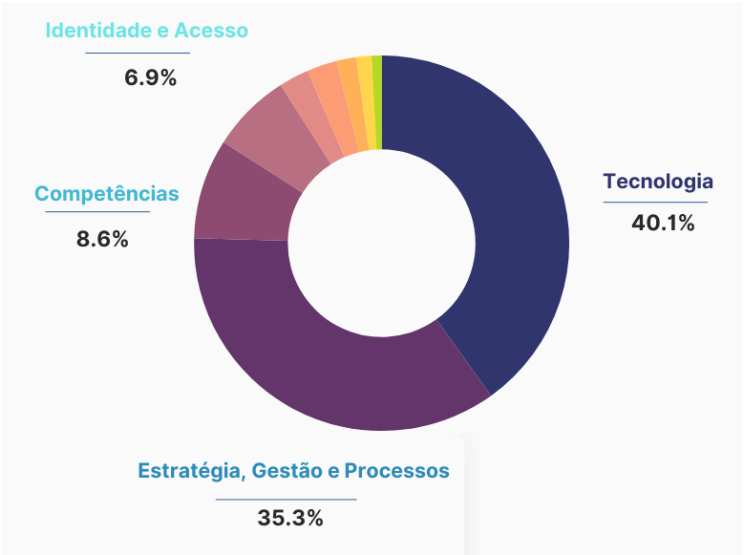


Figura 4.7: Visão alternativa das categorias agrupando Estratégia, Gestão e Processos.
Fonte: do Autor

Esta visão da categoria agrupada "Estratégia, Gestão e Processos de Trabalho"representa uma parcela

significativa do total de controles, ficando próxima da quantidade de controles de tecnologia. Demonstrando que a obtenção da segurança da informação nas instituições depende da atuação de várias unidades organizacionais e da implementação de uma quantidade relevante de ações, que vão além das atribuições e de ações vinculadas exclusivamente às áreas de Tecnologia da Informação.

Essas observações podem ser usadas para entender as prioridades e focos do conjunto de controles analisado, além de ser referência para indicar áreas que requerer mais atenção ou aprimoramento.

4.3.3 Tipos de ativos

Para a avaliação de riscos de segurança da informação é fundamental considerar o valor ou a relevância dos ativos envolvidos para que seja possível avaliar impactos em caso da ocorrência de incidentes. A gestão de ativos é relevante pois permite à organização identificar quais recursos precisam de proteção, avaliar os riscos associados e implementar medidas de segurança apropriadas para protegê-los. A identificação, avaliação e categorização dos ativos são etapas críticas para se estabelecer e implementar os controles de segurança adequados para a mitigação dos riscos [130] [131] [39]. O CIS Controls utiliza uma classificação de tipos de ativos envolvidos em cada um de seus controles. Porém, é possível identificar que em alguns casos se adota a tipo de ativo "N/A"quando não se trata de controles diretamente ligados à aspectos de tecnologia da informação. Considerando os objetivos deste trabalho, aplicou-se a classificação dos ativos relacionados a cada controle, inclusive nos controles adicionais e nos casos em que o CIS Controls entendeu que não era aplicável. Desta forma, foram feitos os seguintes ajustes nos controles de referência nos casos em que não havia atribuição do tipo de ativo:

1. O grupo de controles 14, que trata de conscientização, foram adequados para a classificação *pessoas*. Observa-se que o CIS Controls utiliza o tipo de ativo similar denominado *usuários*, porém verificou-se que ele é utilizado quando se pretende abordar controles relacionados às *contas de usuários*.
2. Os controles 15.4 e 15.7 foram ajustados de N/A para *informação*. Apesar de existir a categoria "dados"no CIS Controles, esse tipo de ativo é atribuído somente para controles relacionados à proteção e restauração de dados, geralmente a funções de backup.
3. Para os controles 17.1 e 17.2, que tratam da definição de responsáveis e contatos na resposta a incidentes, foi atribuído o tipo de ativo *pessoas*.
4. Os controles 17.3, 18.1 e 18.8 receberam a atribuição de ativo do tipo *processo*.

Entende-se que a visão de não identificar ativos para os casos mencionados revela uma visão excessivamente centrada em aspectos tecnológicos, negligenciando a grande importância das pessoas e processos para a segurança da informação. É imprescindível reconhecer a existência e o valor dos ativos intangíveis, os quais também necessitam de proteção adequada, conforme estabelecido na norma ABNT ISO/IEC 27002 [78]. Nos controles onde o tipo de ativo é categorizado como *informação*, percebe-se a possibilidade de subdivisão em outros ativos que, de forma integrada, são fundamentais para a proteção efetiva da informação. Um exemplo claro é o controle *21.2*, que aborda o desenvolvimento de planos de continuidade para prevenir incidentes ou desastres, estabelecendo contingências e assegurando a rápida recuperação.

Além disso, é necessário refletir sobre a utilização da classificação de processos como um ativo. Um processo não deve ser visto apenas como um objetivo em si, mas como um meio para gerar valor e alcançar metas específicas dentro de uma organização. Essa abordagem ressalta que o valor de um processo está em sua capacidade de contribuir eficazmente para o alcance de resultados desejados. Por exemplo, o princípio de segregação de funções, que fundamenta o controle 26.1 relacionado à separação das funções de programação, avaliação de qualidade do código e auditoria, é um processo que adiciona valor ao incrementar a segurança e integridade dos procedimentos operacionais, prevenindo conflitos de interesse e fraudes. Portanto, se um processo cria valor de maneira tangível, entende-se que ele pode ser considerado um ativo para a organização, pois contribui para sua eficiência, eficácia e segurança. Ao reconhecer processos valiosos como ativos, as organizações podem direcionar recursos adequados para sua manutenção e aprimoramento, garantindo que continuem a agregar valor ao longo do tempo.

Há de se destacar como a classificação de ativos é relevante sobre diversos aspectos e pode auxiliar outros processos sob as seguintes perspectivas [78]:

- **Priorização de recursos**: ao identificar os tipos de ativos, as organizações podem priorizar quais ativos precisam de mais proteção. Isso é crucial porque os recursos de segurança são muitas vezes limitados, e é importante focar nos ativos mais críticos ou vulneráveis.
- **Gerenciamento de riscos**: Compreender os tipos de ativos ajuda na avaliação de riscos. Diferentes tipos de ativos têm diferentes níveis de risco associados, e a classificação ajuda a determinar onde estão as maiores ameaças e vulnerabilidades.
- **Desenvolvimento de estratégias de segurança**: A classificação de ativos é fundamental para determinar os papéis e responsabilidades pela segurança dos ativos de informação, dividindo as funções de proprietário e de custodiante do ativo.
- **Resposta a incidentes**: Em caso de um incidente de segurança, saber quais ativos foram afetados e como eles são classificados pode acelerar a resposta e a recuperação.
- **Continuidade de serviços**: Conhecer os tipos de ativos e as ameaças a que estão expostos, pode auxiliar na definição de estratégias de continuidade e recuperação de desastres.
- **Eficiência e performance**: Identificar os ativos e seus responsáveis auxilia a paralelizar a implementação das medidas protetivas, reduzindo o tempo total de tratamento dos riscos.

A Figura 4.8 evidencia a disposição geral dos tipos de ativos identificados na pesquisa.

Relacionando as informações apresentadas sobre as categorias de controles e os tipos de ativos, é possível identificar áreas que demandam maior atenção. Uma forma visual de representar essas relação é o mapa de calor. Esta representação pode oferecer *insights* valiosos para a priorização e compreensão da complexidade dos controles de risco. As áreas com maior concentração de controles indicam pontos de alta complexidade ou atenção intensa, possivelmente devido a multiplicidade de elementos que representam fontes de riscos. Esta distribuição pode também revelar se há um equilíbrio adequado entre as responsabilidades de aplicação de controles e até mesmo indicar necessidades de priorização.

Áreas com poucos controles sugerem potenciais lacunas de identificação de riscos ou menor relevância no risco geral da organização, demandando análise mais aprofundada e direcionada para garantir a gestão

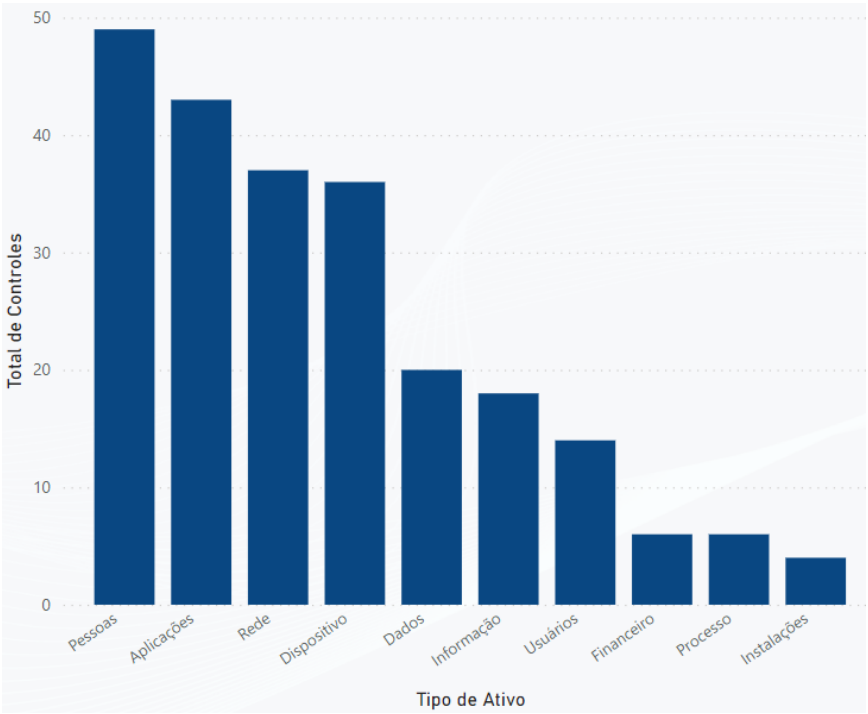


Figura 4.8: Tipos de ativo
Fonte: do Autor

dos riscos eficiente. Este panorama auxilia de forma relevante na alocação de recursos humanos e materiais, priorizando áreas de maior densidade de controles. Sendo estes indicativos de maior complexidade e necessidade de atenção para a redução do risco corporativo. Importante notar, contudo, que uma alta quantidade de controles não implica necessariamente em eficácia na gestão de riscos. Pode ser indicativo também da necessidade de reavaliação da estrutura corporativa ou de redefinição dos processos de trabalho.

O mapa também pode ser uma ferramenta estratégica para o estabelecimento de metas de aprimoramento futuros e revelar tendências e padrões no gerenciamento de riscos, fornecendo uma visão abrangente da gestão de riscos, permitindo avaliar e refinar estratégias com base em uma compreensão clara de onde os controles estão concentrados e onde podem existir lacunas.

Com base na Figura 4.9 se observa a necessidade de **priorização de ações relacionadas à configuração de ativos de rede, de dispositivos e de aplicações** de Tecnologia da Informação. Destaca-se também a importância do **desenvolvimento de competências em segurança das pessoas**.

Portanto, a compreensão dos tipos de ativos envolvidos em cada controles é relevante para a gestão de riscos e para a eficácia da gestão de segurança da informação, permitindo uma abordagem mais focada e eficiente em termos de proteção e resposta a ameaças.

4.3.4 Prioridades de implantação

Neste estudo, adotou-se o conceito de Grupo de Implementação (*IG - Implementation Group*) do CIS Controls como uma ferramenta auxiliar na priorização da implementação de controles de segurança. Esta

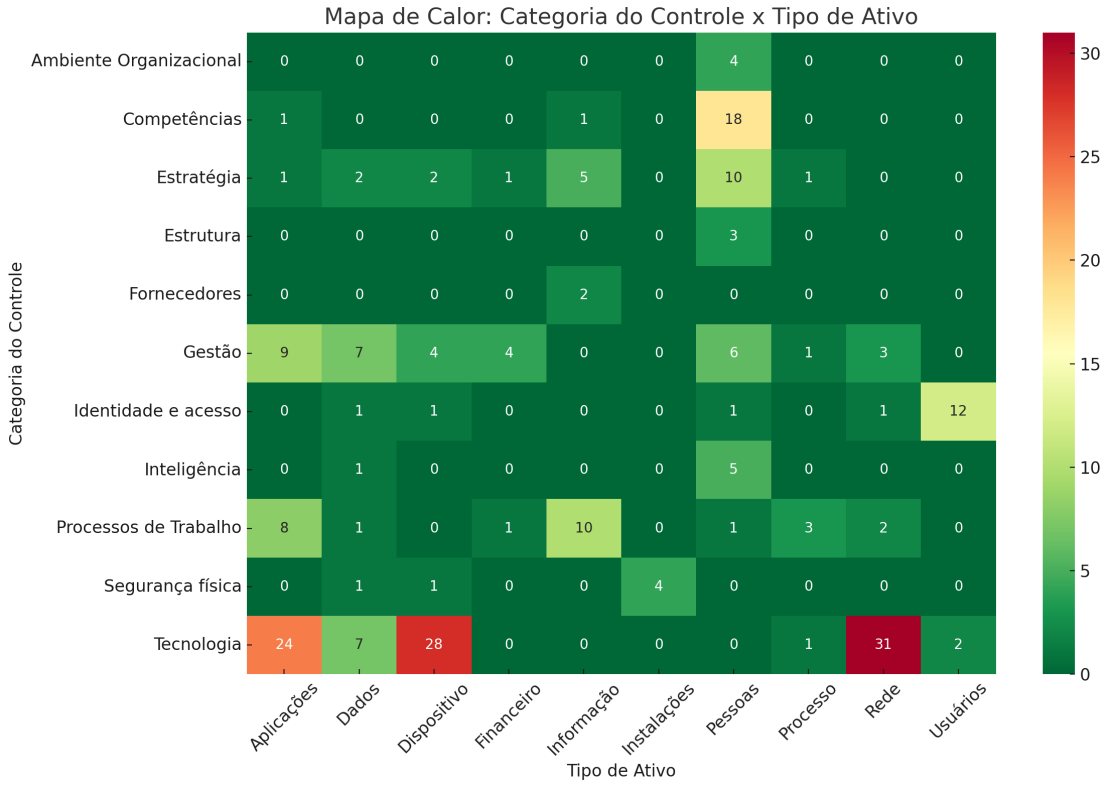


Figura 4.9: Relação entre os tipos de ativos e as categorias dos controles
Fonte: do Autor

abordagem é particularmente útil em empresas de menor porte, onde a implementação até mesmo dos controles básicos de segurança, como estratégias de backup para recuperação de dados em caso de ataques de *ransomware*, pode ser desafiadora. Os grupos de implementação são classificados em IG1, IG2 e IG3, baseando-se em fatores como a complexidade das medidas de segurança, o tamanho da organização e suas necessidades específicas de segurança [113].

Os grupos de implementação oferecem uma visão modular dos Controles CIS, adaptável a diferentes perfis empresariais. O IG1, conhecido como 'higiene cibernética básica', consiste em um conjunto fundamental de medidas de segurança aplicáveis a qualquer organização para defesa contra os ataques frequentes. Cada grupo subsequente (IG2 e IG3) expande sobre o anterior, incorporando todas as medidas de segurança listadas nos grupos anteriores [83].

A análise da frequência dos controles por prioridade de implantação revelou que **107 controles estão categorizados no grupo de implantação 1, 87 como grupo 2, e 38 como grupo 3**, conforme proporção apresentada na Figura 4.10.

A adoção desses grupos permite que as organizações concentrem seus esforços nos aspectos mais críticos de segurança e nos controles de maior relevância. Iniciando com o IG1, as organizações podem progredir para os níveis IG2 e IG3 à medida que a maturidade em segurança cibernética aumenta, permitindo a implementação de controles adicionais e mais complexos. Importante destacar que esses grupos não são prescritivos, podendo ser ajustados conforme as necessidades de cada organização [83].

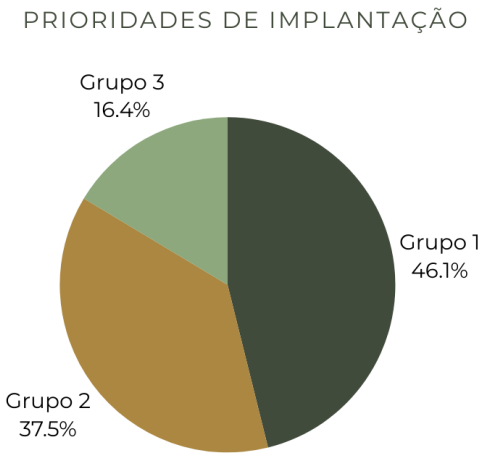


Figura 4.10: Distribuição dos controles por prioridade de implantação.
Fonte: do Autor

Para aprimorar o entendimento das relações entre os diferentes elementos analisados até o momento, foi criada a matriz apresentada na Figura 4.11 que mostram a relação entre os três elementos: categoria de controle, tipo de ativo e prioridade de implantação.

Observa-se que dentre os controles cuja implementação é prioritária (IG1), as principais medidas de segurança, com menor complexidade de implementação e maior resultado, são aquelas voltadas para a capacitação de pessoas. Ao analisar esses controles constata-se ser fundamental a capacitação em segurança da informação. Indo da capacitação básica para reconhecer e alertar ataques aos usuários e profissionais de tecnologia da informação até o nível avançado e direcionado profissionais da área em segurança cibernética. Cada grupo conforme a sua necessidade e especificidade.

Figura 4.12 mostra o segundo grupo de implementação e as relações com os tipos de ativos e os tipos de ativos, onde se destaca a implementação de controles de tecnologia de redes como prioritários do grupo 2.

Figura 4.13 apresenta o mapa de calor que relaciona os controles de maior complexidade ou custo de implementação, as categorias de controle e os tipos de ativos. Para esse cenário de implementação de controles, há um maior equilíbrio da distribuição das medidas de segurança entre configurações de dispositivos, de aplicativos e de redes. Se destacam também nesse grupos de controles aqueles relacionados às medidas de inteligência.

A análise da distribuição dos controles com base em várias visões e abordagens fornecem *insights* valiosos. Por exemplo, a identificação de tipos de ativos frequentemente associados a altas prioridades de implantação sugere áreas que demandam atenção imediata ou são críticas para a organização. Além disso, auxilia no planejamento estratégico e na alocação de recursos para implementação de controles, indicando as categorias que requerem mais atenção ou recursos. A análise pode refletir a avaliação de risco subjacente da organização, ajudando na alocação de recursos e no planejamento estratégico.

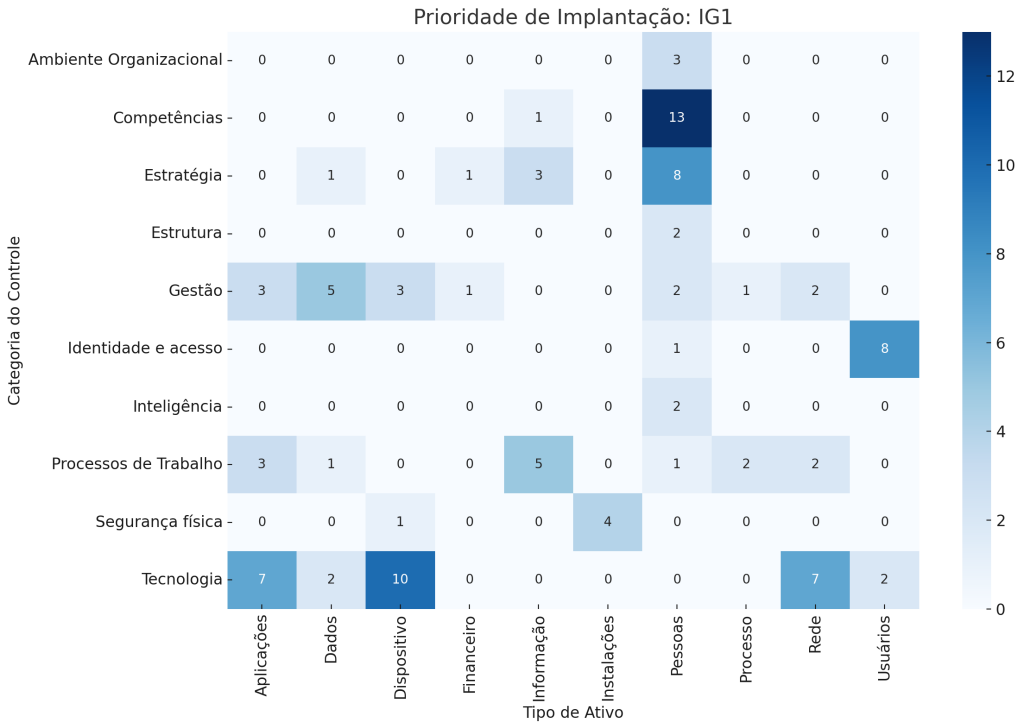


Figura 4.11: Relações entre controles do grupo 1, categorias e ativos
Fonte: do Autor

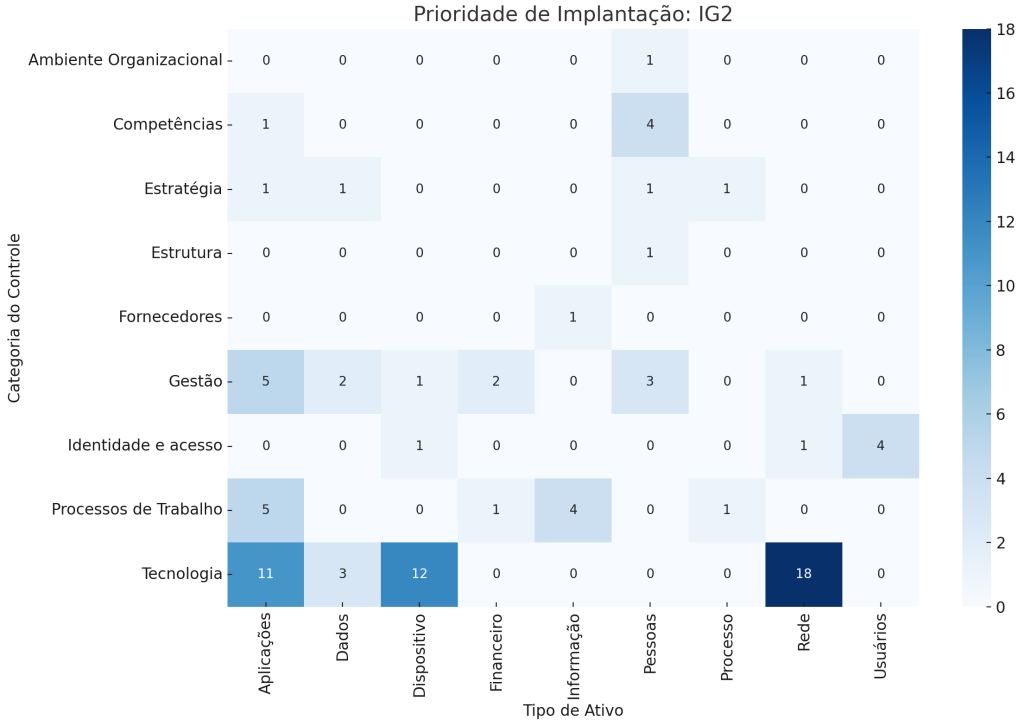


Figura 4.12: Relações entre controles do grupo 2, categorias e ativos
Fonte: do Autor

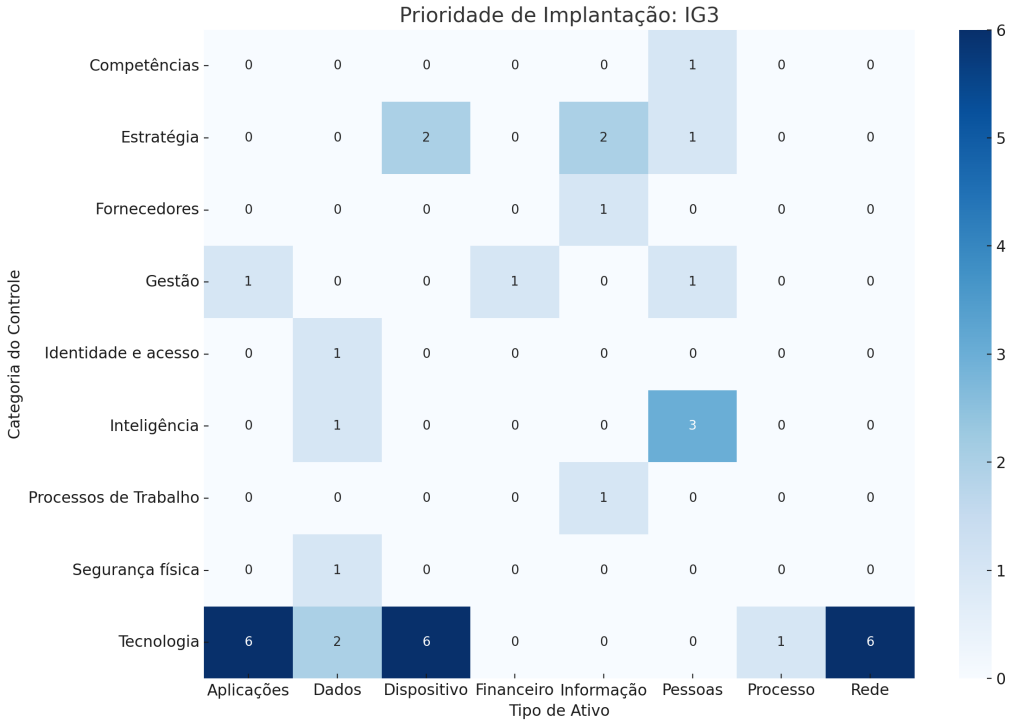


Figura 4.13: Relações entre controles do grupo 3, categorias e ativos
Fonte: do Autor

É importante ressaltar que a análise das prioridades de implantação pode ser ajustada ao contexto específico da organização por meio da combinação de outras informações ou avaliações, tais como em avaliações de risco da instituição, custos de implementação dos controles, dentre outros.

Portanto, o cruzamento de informações do grupo de implementação (IG) do CIS Controls, categorias dos controles e tipos de ativos se mostra como uma útil referência para a priorização na adoção de controles de segurança, oferecendo uma estrutura modular e escalável que pode ser personalizada de acordo com as especificidades de cada órgão.

A relação completa de todos os controles com a indicação em qual categoria este se enquadra, qual é o tipo de ativo relacionado ao controle, que função de segurança este exerce e qual é a prioridade de implantação da medida consta do Apêndice I.2 - Classificações dos controles.

4.4 AVALIAÇÃO E APLICAÇÃO DA PROPOSTA

Este trabalho de pesquisa estabeleceu inicialmente a seguinte hipótese:

> *A definição de controles tecnológicos não é suficiente para a mitigação dos riscos de segurança da informação associados às atividades principais do Poder Judiciário.*

Este estudo culminou em uma ampla relação de medidas de segurança da informação que poderiam

auxiliar no tratamento dos riscos das atividades principais do Poder Judiciário. O estudo evidenciou que estes controles se enquadram em diversas áreas temáticas, separam-se em cinco funções basilares de segurança, visam proteger ativos de segurança específicos e são separados em três níveis de prioridade de implantação. Assim, fica demonstrado que a hipótese prevista no início da pesquisa foi validada e os resultados evidenciaram que os controles propostos para o tratamento dos riscos de negócio vão além das medidas tecnológicas de segurança, apontando a relevância de uma abordagem multidisciplinar.

Embora a proposta seja passível de aplicação em todos os órgãos do Judiciário, é fundamental realizar uma avaliação qualitativa e contextualizada dos riscos e suas consequências em cada organização para garantir a eficácia da proposta. Esta avaliação deve considerar aspectos específicos de cada órgão, como a cultura organizacional, a posição e função dentro da estrutura do Poder Judiciário, além do seu apetite ao risco. Tais fatores são cruciais para assegurar que a proposta seja adequadamente adaptada às necessidades e particularidades de cada órgão, proporcionando uma abordagem mais direcionada e eficiente na gestão de riscos.

Adicionalmente, a lista de controles de segurança proposta pode funcionar como uma fonte para avaliação e aperfeiçoamento contínuo das práticas de segurança da informação. A aderência a esses controles, expressa em termos percentuais, pode indicar um índice de maturidade, auxiliando os órgãos do Judiciário a mensurar e evoluir suas competências em segurança da informação. Contudo, é importante que a aplicação desta avaliação seja adaptada às características particulares e ao contexto de cada órgão para garantir resultados relevantes, conforme a compreensão qualitativa dos riscos e consequências para cada instituição.

Acredita-se, portanto, que a metodologia proposta permite conectar toda a cadeia de riscos, deste o negócio ao controle de segurança cibernética. Potencialmente atendendo ao proposto por Eling et al. [123] quanto a necessidade de integrar o risco cibernético à estrutura de gestão de riscos corporativos – ERM. Gerando uma abordagem integrada que une a compreensão dos riscos em múltiplos níveis, associada à gestão efetiva dos controles de segurança da informação, são capazes de aprimorar a segurança da Justiça.

5 CONSIDERAÇÕES FINAIS

No início deste estudo, observou-se a alta incidência de ataques cibernéticos bem-sucedidos contra órgãos do Poder Judiciário. Esses ataques não apenas paralisaram as atividades essenciais de diversas instituições, mas também levaram à alteração indevida de informações em sistemas de informação. Tais incidentes resultaram em desvios significativos de recursos provenientes de depósitos judiciais. Essa situação evidenciava a importância de se investigar formas de aprimorar a segurança das informações gerenciadas pelos órgãos de justiça no Brasil.

Diante disso, a pesquisa teve como objetivo geral construir uma lista de controles de segurança da informação que sirva de referência para a aplicação de medidas que reduzam as probabilidades de eventos de risco que possam impactar negativamente nas atividades principais do judiciário brasileiro. Verifica-se que este propósito geral foi alcançado, pois efetivamente o trabalho conseguiu identificar os principais riscos de negócio, relacionar os riscos de negócio com os riscos operacionais e apresentar uma multifacetada gama de controles de segurança que abrangem diversas áreas de conhecimento e atuação. Esta proposta de medidas fornece um guia prático para a implementação de estratégias de segurança no contexto específico do Judiciário.

O primeiro objetivo específico consistia em *identificar as atividades principais do Poder Judiciário e que necessitam de maior proteção*. Este objetivo foi atingido, conforme demonstrado na seção 4.1.1. Nesta seção, foram destacadas as seguintes atividades principais: recebimento e a distribuição de processos; análise e a relatoria de processos; formulação das decisões judiciais; julgamento monocrático ou colegiado; processamento das decisões; execução dos atos cartorários e o cumprimento de despachos e decisões.

O segundo objetivo previsto era *compreender os principais riscos de negócio associados a estas atividades*. Este objetivo foi alcançado, evidenciado pela identificação detalhada de 10 riscos de negócio principais, 40 causas desses riscos e 22 consequências que poderiam impactar às instituições. Estes achados estão descritos nas subseções *4.1.3*, *4.1.4* e *4.1.5*.

O terceiro objetivo específico consistia em *entender a relação entre ações operacionais de segurança da informação e os riscos de negócio*. Foi possível estabelecer um entendimento claro da dinâmica existente entre os riscos de negócio, suas causas subjacentes e a percepção de que eles constituíam riscos operacionais. Esta compreensão permitiu identificar que tais riscos poderiam ser mitigados por meio da aplicação de medidas operacionais adequadas, oriundas de diversas áreas organizacionais.

O quarto objetivo específico tratava-se de *apontar, a partir de um framework internacional de referência, os controles de segurança que possuem o potencial de mitigar os riscos de negócio identificados*. Este objetivo foi parcialmente alcançado com a escolha do guia *CIS Controls*, versão 8, que proporcionou uma lista inicial de 133 medidas de segurança. No entanto, observou-se que esta lista não cobria todos os riscos identificados. Por isso, foi necessária uma etapa adicional, que incluiu a contribuição de gestores, servidores e especialistas do Poder Judiciário, além de outras referências internacionais e de mercado. Esta fase complementar resultou na proposição de 99 controles adicionais. Assim, a soma total chegou a 232 medidas de segurança, detalhadas nas subseções 4.2.1 e 4.2.2. Portanto, conclui-se que a combinação das

ações iniciais e adicionais possibilitou atingir plenamente o quarto objetivo específico estabelecido.

O último objetivo específico visava *auxiliar os órgãos judiciais na identificação de papéis, responsabilidades e ações prioritárias*. Este fim foi alcançado pela realização de diversas interpretações, que incluíram a criação de categorias, a identificação de tipos de ativos relacionados, a definição da função de segurança e a determinação de grupos prioritários para a implementação de cada controle. A utilização de análise de dados e técnicas de *business intelligence* permitiu ainda fornecer diferentes perspectivas sobre os controles sugeridos. Essas abordagens permitem a cada instituição a coordenação das ações prioritárias de mitigação entre várias equipes ou unidades organizacionais, de acordo com suas habilidades, conhecimentos ou responsabilidades específicas.

Portanto, ao considerar o problema de pesquisa estabelecido: *"quais são os controles de segurança da informação que devem ser implementados para prevenir a ocorrência de eventos de risco que afetem as atividades principais do Poder Judiciário?"*, pode-se afirmar que a questão foi respondida.

A pesquisa partiu da hipótese de que *a definição de controles tecnológicos não é suficiente para a mitigação dos riscos de segurança da informação associados às atividades principais do Poder Judiciário*. Os resultados apresentados e classificações dos controles demonstraram que a importância da atuação integral e multi-departamental para a segurança da informação no contexto da pesquisa, confirmando que hipótese proposta foi validada.

Contudo, considerando a natureza dinâmica da segurança da informação, bem como o surgimento constante de novas tecnologias, regulamentações e ameaças que podem modificar o cenário de riscos, torna-se imprescindível a realização de revisões periódicas. Tal processo de revisão é fundamental para assegurar que as estratégias de segurança adotadas mantenham sua relevância e eficácia diante das mudanças contínuas no ambiente de segurança da informação.

A pesquisa apresentou algumas limitações ou dificuldades que necessitam ser pontuadas. Primeiramente, a escolha dos entrevistados, embora tenha incluído gestores com experiências muito relevantes, não abrangeu gestores atuantes no 1º grau de jurisdição. A inclusão desses profissionais poderia ter proporcionado uma perspectiva mais ampla sobre os riscos específicos dessa esfera de atuação, enriquecendo a análise dos riscos inerentes ao Judiciário em seu nível mais básico.

Uma limitação adicional surgiu na formação do grupo focal destinado à revisão dos controles de segurança propostos. Dada a extensa quantidade de medidas de segurança a serem analisadas, constituiu-se um grupo com a capacidade de abordar a maior parte dessas medidas. No entanto, o grupo enfrentou dificuldades para avaliar adequadamente aspectos específicos relacionados a questões jurídicas. Além disso, as reuniões semanais de revisão dos controles, que se estenderam por vários meses, não permitiram tempo suficiente para organizar um segundo grupo focal especializado na avaliação de temas jurídicos.

Outra limitação inerente à pesquisa derivou dos objetivos estabelecidos, que se concentravam em identificar os riscos comuns às atividades principais das instituições do Judiciário. Consequentemente, optou-se por limitar intencionalmente o escopo do estudo, excluindo detalhes e particularidades de segmentos especializados da Justiça, como a Justiça Eleitoral ou a Justiça Militar. Estes segmentos possuem características e necessidades próprias que demandam adaptações específicas nas estratégias de segurança da informação. A pesquisa não se dedicou a explorar como essas peculiaridades poderiam influenciar a identificação de

riscos e nas medidas de mitigação. A inclusão destas peculiaridades poderia ter levado a uma ampliação da lista de atividades principais e uma compreensão mais especializada dos riscos de negócio e suas inter-relações de causa e consequências em ramos especializados da justiça.

Outro aspecto limitante foi a limitação de prazo para a conclusão do estudo. A limitação temporal demanda a definição de uma linha de corte no qual seriam satisfeitos os objetivos da pesquisa. Durante a realização da pesquisa, novas visões e possibilidades se abriram diante do pesquisador, porém foi necessário não incluir novos objetivos da pesquisa e limitar o teste da hipótese original para a conclusão do ciclo atual de pesquisa.

Desta forma, a pesquisa adotou uma abordagem predominantemente quantitativa na definição das prioridades dos controles de segurança da informação. Apesar de essa metodologia fornecer *insights* importantes, métodos quantitativos podem não captar completamente a complexidade e a nuance de certos aspectos da segurança da informação. Por exemplo, não foi possível determinar, dentre as 22 consequências dos riscos de negócio, se existem consequências mais indesejadas do que outras. A avaliação qualitativa dos impactos dos riscos poderia determinar riscos de negócio prioritários e modificar o direcionamento das medidas de segurança mais relevantes. Uma abordagem que combinasse métodos quantitativos e qualitativos poderia oferecer uma base mais sólida e abrangente para a priorização dos controles.

Em relação a diretrizes para pesquisas futuras, sugere-se ampliar o escopo de profissionais e órgãos participantes das entrevistas para aprofundar a identificação dos riscos de negócio do Poder Judiciário, incluindo gestores do primeiro grau, tribunais estaduais ou análises focadas em ramos especializados de Justiça.

Propõe-se, ainda, avaliar qualitativamente, por meio de múltiplos critérios, quais controles de segurança da informação são mais relevantes e prioritários. A continuidade da análise dos riscos operacionais e seus controles, com base em uma escala de criticidade dos riscos de negócio, seriam úteis na priorização dos controles de segurança da informação mais relevantes para os objetivos de negócio.

Outra possibilidade seria o desenvolvimento de uma metodologia ágil destinada à avaliação e quantificação do nível de risco associado à segurança da informação nos órgãos do Poder Judiciário. Esta metodologia seria centrada em um processo de autoavaliação, que se basearia na implementação efetiva dos controles de segurança propostos neste estudo. Adicionalmente, o referido método permitiria a identificação de controles prioritários, cuja implementação resultaria em uma otimização do nível de risco de acordo com as necessidades e particularidades de cada órgão judiciário.

Se vislumbra ainda a possibilidade de comparação dos controles propostos neste trabalho com os controles previstos na Estratégia Nacional de Segurança Cibernética do Poder Judiciário- ENSEC-PJ. Esta comparação poderia indicar possíveis aprimoramentos e atualizações para revisões futuras do normativo do CNJ.

Este estudo oferece contribuições para o campo da gestão de riscos e definição de estratégias de segurança da informação, especialmente no contexto do Poder Judiciário, frente aos desafios impostos por ataques cibernéticos. As descobertas aqui apresentadas podem auxiliar a comunicação e compreensão mútua entre as áreas técnicas e a alta administração e apontam estratégias e ações preventivas ou mitigatórias voltadas para a segurança das instituições e autoridades judiciais. Adicionalmente, este trabalho oferece

uma perspectiva sobre o direcionamento e otimização dos investimentos em segurança da informação, que são desafios frequentemente enfrentados pelos órgãos governamentais. Este estudo contribui para a literatura existente, fornece sugestões práticas e abre caminho para pesquisas futuras que possam explorar a implementação e a avaliação das medidas de segurança propostas, bem como sua adaptação para aplicação em diferentes contextos institucionais.

REFERÊNCIAS BIBLIOGRÁFICAS

1 AMARAL, D. M. O poder judiciário, estrutura e principais funções. *Jus Brasil*, 2020. Disponível em: <https://www.jusbrasil.com.br/artigos/o-poder-judiciario-estrutura-e-principais-funcoes/861564653>.

2 RAST, C. *Cybersecurity Threats to the Judiciary*. 2023. Disponível em: <https://www.americanbar.org/groups/judicial/publications/judges_journal/2023/summer/cybersecurity-threats-to-judiciary/>.

3 ALVARES, N. O. *A informatização do processo judicial e o acesso à justiça*. 2011. Disponível em: <https://repositorio.uniceub.br/jspui/handle/123456789/506>.

4 HINO, M. C.; CUNHA, M. A. Adoption of technology in the legal professionals' perspective. In: . [S.l.]: Fundacao Getulio Vargas, Escola de Direito de Sao Paulo, 2020. v. 16. ISSN 23176172.

5 STF. Stf abre seminário internacional sobre segurança cibernética. 2023. Disponível em: <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=512828&ori=1>.

6 ELTIS, K. The judicial system in the digital age: Revisiting the relationship between privacy and accessibility in the cyber context. *McGill Law Journal*, Consortium Erudit, v. 56, p. 289–316, 4 2011. ISSN 0024-9041.

7 FAUSTINO, R. *Uso de recursos digitais cresce na Justiça e deixa tribunais mais ágeis*. 2018. Disponível em: <https://epocanegocios.globo.com/amp/Tecnologia/noticia/2018/09/uso-de-recursos-digitais-cresce-na-justica-e-deixa-tribunais-mais-ageis.html>.

8 MARTINS, T. do C. Acesso à justiça e pandemia. *Revista Jus Navigandi*, v. 6412, 1 2021. ISSN 1518-4862. Disponível em: <https://jus.com.br/artigos/88048.Acessoem:23dez.2022>.

9 JUSTIçA 4.0 - Portal CNJ. *Portal CNJ*. Disponível em: <https://www.cnj.jus.br/tecnologia-da-informacao-e-comunicacao/justica-4-0/>.

10 ALVES, R. S.; GEORG, M. A. C.; NUNES, R. R. Judiciário sob ataque hacker: riscos de negócio para segurança cibernética em tribunais brasileiros. *RISTI*, 2023. Disponível em: <https://doi.org/10.5281/zenodo.7920441>.

11 MOREIRA, F. R.; FILHO, D. A. D. S.; NZE, G. D. A.; JUNIOR, R. T. de S.; NUNES, R. R. Evaluating the performance of nist's framework cybersecurity controls through a constructivist multicriteria methodology. In: . Piscataway: IEEE, 2021. v. 9, p. 129605–129618. ISSN 2169-3536.

12 KRUMAY, B.; BERNROIDER, E. W. N.; WALSER, R. Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the nist cybersecurity framework. In: GRUSCHKA, N. (Ed.). *Secure IT Systems*. Cham: Springer International Publishing, 2018. p. 369–384. ISBN 978-3-030-03638-6.

13 INTERNET Crime Report 2021. *Federal Bureaus of Investigation - FBI*, 2021. Disponível em: <https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf>.

14 ENISA THREAT LANDSCAPE 2022. 11 2022. Disponível em: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>.

15 MOURA, R. M.; BORGES, L. A impunidade dos hackers que colocaram o judiciário de joelhos. *Veja*, 2022. Disponível em: <https://veja.abril.com.br/politica/a-impunidade-dos-hackers-que-colocaram-o-judiciario-de-joelhos/>.

16 REINA, E. *Ameaça Virtual - Em 18 meses, hackers violaram sistemas de tribunais no Brasil a cada 41 dias*. 2022. Acessado em 22 de maio de 2022. Disponível em: <https://www.conjur.com.br/2022-abr-15/onda-invasoes-hackers-estruturas-tecnologicas-tribunais>.

17 HIRATA, A.; OLIVEIRA, C. G. B. de. 39 dias após o ataque cibernético ao stj - reflexões e desafios. *Migalhas*, v. 5505, 12 2020. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/337701/39-dias-apos-o-ataque-cibernetico-ao-stj--reflexoes-e-desafios>.

18 REINA, E. A onda de invasões hackers às estruturas tecnológicas dos tribunais. *Revista Consultor Jurídico*, 4 2022. Disponível em: <https://www.conjur.com.br/2022-abr-15/onda-invasoes-hackers-estruturas-tecnologicas-tribunais>.

19 TJ do Distrito Federal segue fora do ar após ataque no domingo. *Ciso Advisor*, 2022. Disponível em: <https://www.cisoadvisor.com.br/tj-do-distrito-federal-segue-fora-do-ar-apos-ataque-no-domingo/>.

20 JUSTIçA Federal condena hackers por falsificação de documento público em sistema processual. *Portal do TRF3*, 12 2021. Disponível em: <https://web.trf3.jus.br/noticias-sjms/Noticiar/ExibirNoticia/48-justica-federal-condena-hackers-por-falsificacao-de>.

21 LOBO, A. P. *TRT do Rio de Janeiro sofre golpe de R$ 4 milhões com certificados digitais falsos*. 2022.

22 FUCCIA, E. V. Fraudes em alvarás no trt-1 superam r$ 4 mi e sistema de pagamento é suspenso. *Revista Consultor Jurídico*, 11 2022. Disponível em: <https://www.conjur.com.br/2022-nov-13/fraudes-emissao-alvaras-trt-ultrapassam-milhoes>.

23 PINOTTI, F.; LOPES, L. *Invasão de sistema do CNJ e falso mandado de prisão contra Moraes: entenda o que levou à prisão do hacker*. 2023. Disponível em: <https://www.cnnbrasil.com.br/politica/invasao-de-sistema-do-cnj-e-falso-mandado-de-prisao-contra-moraes-entenda-o-que-levou-a-prisao-do-hacker/>.

24 RAYMOND, N. *Federal judiciary 'vulnerable' to cyberattacks, U.S. lawmakers told*. 2022. Disponível em: <https://www.reuters.com/legal/government/federal-judiciary-vulnerable-cyberattacks-us-lawmakers-told-2022-05-12/>.

25 GERSTEIN, J.; WARD, A. *Supreme Court has voted to overturn abortion rights, draft opinion shows*. 2022. Disponível em: <https://www.politico.com/news/2022/05/02/supreme-court-abortion-draft-opinion-00029473>.

26 BLAND, A. *Supreme court abortion law leak: what happened and why does it matter?* 2022. Disponível em: <https://www.theguardian.com/world/2022/may/03/supreme-court-abortion-law-leak-roe-v-wade>.

27 NORMA ABNT NBR ISO 31000. 3 2018.

28 NUNES, R. R.; PERINI, M. T. B. S.; PINTO, I. E. M. M. A gestão de riscos como instrumento para a aplicação efetiva do princípio constitucional da eficiência. In: . [S.l.]: Centro Universitario de Brasilia, 2021. v. 11, p. 260–281. ISSN 22361677.

29 LIMA, E. de O.; MOREIRA, F. R.; DEUS, F. E.; DEUS, F. E.; NZE, D. G. A. Avaliação da rotina operacional do operador nacional do sistema elétrico brasileiro (ons) em relação às ações de gerenciamento de riscos associados à segurança cibernética-sistema de gestão de pessoas view project signal processing for 5g wireless communications using massive mimo systems view project. In: . [S.l.: s.n.], 2022. E49, p. 301–312.

30 THE Standard for Risk Management in Portifolios, Programs, and Projects. [S.l.]: Project Management Institute, Inc.(PMI), 2019. ISBN 978-1-62825-565-2.

31 GALEGALE, N. V.; FONTES, E. L. G.; GALEGALE, B. P. Uma contribuição para a segurança da informação: um estudo de casos múltiplos com organizações brasileiras1. *Perspectivas em Ciência da Informação*, Escola de Ciência da Informação da UFMG, v. 22, n. 3, p. 75–97, Jul 2017. ISSN 1413-9936. Disponível em: <https://doi.org/10.1590/1981-5344/2866>.

32 FRAMEWORK for Improving Critical Infrastructure Cybersecurity, Version 1.1. 4 2018. Disponível em: <http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

33 MITRE ATT&CK. 2022. Disponível em: <https://attack.mitre.org/versions/v12/matrices/enterprise/>.

34 BARNARD, L.; von Solms, R. A formalized approach to the effective selection and evaluation of information security controls. *Computers & Security*, v. 19, n. 2, p. 185–194, 2000. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404800878293>.

35 PROTOCOLOS e Manuais previstos na Estratégia Nacional de Segurança Cibernética. 2021. Disponível em: <https://atos.cnj.jus.br/files/compilado1402302021061460c7617672ec5.pdf>.

36 DAMODARAN, A. *Gestão Estratégica do Risco: uma referência para a tomada de riscos empresariais*. [S.l.]: Bookman, 2009. ISBN 978-0-13-199048-7.

37 CROUHY, M.; GALAI, D.; MARK, R. *The Essentials of Risk Management, Second Edition*. [S.l.]: McGraw Hill, 2014. ISBN 978-0-07-182115-5.

38 IEC, I. *International Standard ISO/IEC 27000*. 2018. Disponível em: <www.iso.org>.

39 RISK Management Framework for Information Systems and Organizations. 12 2018. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>.

40 AVEN, T. Risk assessment and risk management: Review of recent advances on their foundation. In: . [S.l.]: North-Holland, 2016. v. 253, p. 1–13. ISSN 0377-2217.

41 AVEN, T.; BEN-HAIM, Y.; ANDERSEN, B. H.; COX, T.; DROGUETT, E. L.; GREENBERG, M.; GUIKEMA, S.; KRöGER, W.; RENN, O.; THOMPSON, K. M.; ZIO, E. Society for risk analysis glossary. *Society for Risk Analysis*, 2018. Disponível em: <https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf>.

42 JALLOW, A. K.; MAJEED, B.; VERGIDIS, K.; TIWARI, A.; ROY, R. Operational risk analysis in business processes. *BT Technology Journal*, v. 25, n. 1, p. 168–177, 2007. ISSN 1573-1995. Disponível em: <https://doi.org/10.1007/s10550-007-0018-4>.

43 MACHADO, M. B. Taxonomia de eventos de risco operacional do poder judiciário. 2018. Disponível em: <http://repositorio.enap.gov.br/handle/1/3399>.

44 CHAPELLE, A. Front matter. In: ____. *Operational Risk Management*. John Wiley & Sons, Ltd, 2018. p. i–xxiv. ISBN 9781119548997. Disponível em: <https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119548997.fmatter>.

45 ROSS, R.; WINSTEAD, M.; MCEVILLEY, M. *Engineering trustworthy secure systems*. 2022. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf>.

46 COSO. Enterprise risk management integrating with strategy and performance. 2017. Disponível em: <https://www.coso.org/Shared%20Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf>.

47 MODELOS de referência de gestão corporativa de riscos. *Tribunal de Contas da União*. Disponível em: <https://portal.tcu.gov.br/planejamento-governanca-e-gestao/gestao-de-riscos/politica-de-gestao-de-riscos/modelos-de-referencia.htm>.

48 MANAGING Information Security Risk: Organization, Mission, and Information System View. 2011. Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf>.

49 NORMA ABNT NBR ISO/IEC 31010. 5 2012.

50 STANDARDS, N. I. of; TECHNOLOGY. *Guide for Conducting Risk Assessments - SP 800-30*. 2012. Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>.

51 ZIO, E. The future of risk assessment. In: . [S.l.]: Elsevier, 2018. v. 177, p. 176–190. ISSN 0951-8320.

52 SHAMELI-SENDI, A.; AGHABABAEI-BARZEGAR, R.; CHERIET, M. Taxonomy of information security risk assessment (isra). *Computers & Security*, Elsevier Advanced Technology, v. 57, p. 14–30, 3 2016. ISSN 0167-4048.

53 BERNARD, R. Information lifecycle security risk assessment: A tool for closing security gaps. *Computers and Security*, v. 26, p. 26–30, 2 2007. ISSN 01674048.

54 AVEN, T. On the meaning of a black swan in a risk context. *Safety Science*, v. 57, p. 44–51, 8 2013. ISSN 09257535.

55 LUKO, S. N. *Risk assessment techniques*. [S.l.]: Taylor and Francis Inc., 2014. 379-382 p.

56 REFERENCIAL básico de Gestão de Riscos. *Tribunal de Contas da União*, 2018. Disponível em: <https://portal.tcu.gov.br/referencial-basico-de-gestao-de-riscos.htm>.

57 MASTWIJK, K. Dealing with uncertainty: cybersecurity risk assessment approaches - a qualitative research on cyber risk assessment practices in organizations. *Universiteit Leiden*, 2020.

58 NORMA ABNT NBR ISO-IEC 27005 2019. 2019.

59 YEVSEYEVA, I.; BASTO-FERNANDES, V.; EMMERICH, M.; van Moorsel, A. Selecting optimal subset of security controls. *Procedia Computer Science*, v. 64, p. 1035–1042, 2015. ISSN 1877-0509. Conference on ENTERprise Information Systems/International Conference on Project MANagement/Conference on Health and Social Care Information Systems and Technologies, CENTERIS/ProjMAN / HCist 2015 October 7-9, 2015. Disponível em: <https://www.sciencedirect.com/science/article/pii/S187705091502760X>.

60 ATKINSON, S. *Quantitative Risk Analysis: Its Importance and Implications*. 2023. Disponível em: <https://www.cisecurity.org/insights/blog/quantitative-risk-analysis-its-importance-and-implications>.

61 EVRIN, V. Risk assessment and analysis methods: Qualitative and quantitative. *ISACA JOURNAL*, v. 2, 2021. Disponível em: <https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods>.

62 DIFFERENCE Between Assessment and Evaluation. 2016. Disponível em: <https://keydifferences.com/difference-between-assessment-and-evaluation.html>.

63 KARAN, R. *Difference Between Assessment and Evaluation*. 2023. Disponível em: <https://www.shiksha.com/online-courses/articles/difference-between-assessment-and-evaluation/>.

64 AL-SAFWANI, N.; FAZEA, Y.; IBRAHIM, H. Iscp: In-depth model for selecting critical security controls. *Computers & Security*, v. 77, p. 565–577, 2018. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404818305534>.

65 PAULSEN, C.; BYERS, R. Glossary of key information security terms. 7 2019. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf>.

66 SECURITY and Privacy Controls for Information Systems and Organizations. 2020. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>.

67 STANGER, J. *What Is the Difference Between IT Security and Cybersecurity?* 2023. Disponível em: <https://www.comptia.org/blog/what-is-the-difference-between-it-security-and-cybersecurity>.

68 CHECKPOINT. *Cybersecurity vs Information Security*. 2023. Disponível em: <https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/cybersecurity-vs-information-security/>.

69 MARTIN, A.; RASHID, A.; CHIVERS, H.; DANEZIS, G.; SCHNEIDER, S.; LUPU, E. The cyber security body of knowledge v1.1.0, 2021. In: ____. University of Bristol, 2021. cap. Introduction to CyBOK. Version 1.1.0. Disponível em: <https://www.cybok.org/>.

70 HOODA, S. *What is the Difference Between Information Security and Cybersecurity?* 2020. Disponível em: <https://cloudacademy.com/blog/cybersecurity-vs-information-security-is-there-a-difference/>.

71 MOORE, M.; BANE, C. *Cybersecurity vs. Information Security vs. Network Security*. Disponível em: <https://onlinedegrees.sandiego.edu/cyber-security-information-security-network-security/>.

72 GALARITA, B.; SWANSTON, B. *Information Security vs. Cybersecurity: What's Te Difference?* 2022. Disponível em: <https://www.forbes.com/advisor/education/information-security-vs-cyber-security/>.

73 IRWIN, L. *Information Security vs Cyber Security: The Difference*. 2022. Disponível em: <https://www.itgovernance.co.uk/blog/do-you-know-the-difference-between-cyber-security-and-information-security>.

74 REID, R.; NIEKERK, J. V. From information security to cyber security cultures: Organizations to societies. IEEE, 2014.

75 (ISC)² - International Information System Security Certification Consortium, Inc. *Classroom-Based CISSP Official (ISC)² Textbook*. 6th. ed. (ISC)² - International Information System Security Certification Consortium, Inc., 2023. Disponível em: <https://isc2.vitalsource.com/books/ISC2-CBCISSP-EB-6-EN-EPUB>.

76 SOLMS, R. V.; NIEKERK, J. V. From information security to cyber security. *Computers and Security*, Elsevier Ltd, v. 38, p. 97–102, 2013. ISSN 01674048.

77 ABNT. *NBR ISO/IEC 27001*. 2013.

78 ABNT. *NBR ISO/IEC 27002*. 2005.

79 BROOKSON, C.; CADZOW, S.; ECKMAIER, R.; ESCHWEILER, J.; GERBER, B.; GUARINO, A.; RANNENBERG, K.; SHAMAH, J.; GóRNIAK, S. *Definition of Cybersecurity: Gaps and overlaps in standardisation*. 2015. Disponível em: <www.enisa.europa.eu>.

80 MOREIRA, F. R.; DE, E.; LIMA, O.; NUNES, R. R. A utilização dos frameworks nist csf e da séria nbr abnt iso 27.000 no contexto da gestão da segurança da informação. Disponível em: <https://www.researchgate.net/publication/360082614>.

81 CORALLO, A.; LAZOI, M.; LEZZI, M. Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. In: . [S.l.]: Elsevier B.V., 2020. v. 114. ISSN 01663615.

82 ALMUHAMMADI, S.; ALSALEH, M. Information security maturity model for nist cyber security framework. In: . [S.l.]: Academy and Industry Research Collaboration Center (AIRCC), 2017. p. 51–62.

83 CONTROLS, C. *CIS Controls v8*. 2023. Disponível em: <https://www.cisecurity.org/controls/v8>.

84 SAGER, T.; MCCLAIN, S. *CIS Controls - Auditing, Assessing, Analyzing: A Prioritized Approach using the Pareto Principle*. 2020. <https://www.cisecurity.org/insights/white-papers/auditing-assessing-analyzing-a-prioritized-approach-using-the-pareto-principle>. Acessado em: 4 de outubro de 2023.

85 STINE, K.; QUINN, S.; WITTE, G.; GARDNER, R. K. *Integrating Cybersecurity and Enterprise Risk Management (ERM)*. 2020. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf>.

86 GUNAWAN, C. T. A.; SURYANTO, Y. Maturity level analysis of digital evidence handling on integrated criminal justice system based on nist sp800-53 revision 5 using nist maturity. *Budapest International Research and Critics Institute (BIRCI-Journal)*, Budapest International Research and Critics Institute, 2022.

87 ASTUTI, H. M.; MUQTADIROH, F. A.; DARMANINGRAT, E. W. T.; PUTRI, C. U. Risks assessment of information technology processes based on cobit 5 framework: A case study of its service desk. In: . [S.l.]: Elsevier B.V., 2017. v. 124, p. 569–576. ISSN 18770509.

88 GEORGIADOU, A.; MOUZAKITIS, S.; ASKOUNIS, D. Assessing mitre att&ck risk using a cyber-security culture framework. *Sensors*, MDPI AG, v. 21, 5 2021. ISSN 14248220.

89 Conselho Nacional de Justiça. *Estratégia Nacional de Segurança Cibernética do Poder Judiciário*. 2021. Disponível em: <https://atos.cnj.jus.br/files/compilado1402302021061460c7617672ec5.pdf>.

90 FEDERAL, S. T. *Acesso em 4 de fevereiro de 2024*. 2018. Acessado em 8 de setembro de 2022. Disponível em: <https://www.stf.jus.br/arquivo/cms/intranetAGE/anexo/MapProcessos/CadeiaValor/CadeiadevalorSTF2018.pdf>.

91 PARANá, T. de Justiça do. *Cadeia de Valor*. 2020. Acessado em 4 de fevereiro de 2024. Disponível em: <https://www.tjpr.jus.br/cadeia-valor>.

92 TERRITóRIOS, T. de Justiça do Distrito Federal e. *Cadeia de Valor*. 2018. Acessado em 4 de fevereiro de 2024. Disponível em: <https://www.tjdft.jus.br/institucional/governanca/cadeia-de-valor-1/copy_of_cadeiacompleta.pdf>.

93 JUSTIçA, S. T. de. *Cadeia de Valor*. 2023. Disponível em: <https://bdjur.stj.jus.br/jspui/bitstream/2011/176988/Prt_311_2023_GP.pdf>.

94 ROVER, A. J. O e-judiciário no brasil: Uma bibliometria temática. *Conpedi Law Review*, v. 1, p. p. 155, 2015.

95 WANDERLEY, D. L. *Um framework para o gerencimaento de riscos em segurança da informação no Poder Judiciário do Tocantins*. 2020. Disponível em: <http://hdl.handle.net/11612/2388>.

96 COSTA, R. L. D. 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, p. 76–96, 2021. ISSN 2525-9822.

97 LEITE, R. V. Poder judiciário e meio de comunicação: do dever de transparência aos riscos de exposição midiática. *ReJuB - Revista Judicial Brasileira*, v. 1, n. 1, p. 205–226, 2021.

98 BARRêTO, M. L. de A. *Estudo Sobre a Gestão da Política de Segurança da Informação no Poder Judiciário do Estado do Tocantins*. [S.l.]: Universidade Federal do Tocantins, 2021.

99 SCHWAITZER, L. de Beaurepaire da S. *Segurança, Acesso e Preservação da Informação Arquivística do Poder Judiciário*. 2016. 385-400 p.

100 OLIVEIRA, F. L. D.; CUNHA, L. G. The indicators on the brazilian judiciary: Limitations, challenges and the use of technology. *Revista Direito GV*, Fundacao Getulio Vargas, Escola de Direito de Sao Paulo, v. 16, 2020. ISSN 23176172.

101 MOURA, L. de C. *Gestão de Segurança da Informação no Poder Judiciário: estudo baseado nos levantamentos de Governança de Tecnologia da Informação do Tribunal de Contas da União de 2014 e de 2016*. 2017.

102 FILHO, L. G. L. dos S. *Análise da Maturidade da Política de Segurança da Informação dos Tribunais Superiores do Poder Judiciário Brasileiro*. 2016.

103 Joint Technology Committee. *Cybersecurity Basics for Courts*. 2019. Disponível em: <https://www.ncsc.org/__data/assets/pdf_file/0037/68887/JTC-2021-05-Cybersecurity-QR_Final-Clean.pdf>.

104 GORDON, D. L. M. *Cybersecurity & the Courthouse: Safeguarding the Judicial Process*. Wolters Kluwer, 2020. ISBN 9781543809756. Disponível em: <https://books.google.com.br/books?id=DHLJDwAAQBAJ>.

105 ARNAUDOVSKA, A. *Building a comprehensive risk management in the judiciary*. 2021. Disponível em: <https://www.unodc.org/dohadeclaration/en/news/2021/22/building-a-comprehensive-risk-management-in-the-judiciary.html>.

106 SENéCAL, F.; BENYEKHLEF, K. Groundwork for assessing the legal risks of cyberjustice. *Canadian Journal of Law and Technology*, p. 41–56, 9 2009. Risco legal e justiça cibernética. Disponível em: <https://ssrn.com/abstract=1477584>.

107 (CEPEJ), E. C. for the Efficiency of J. *Toolkit for supporting the implementation of the Guidelines on how to drive change towards Cyberjustice*. 2019.

108 BUREAU OF JUSTICE ASSISTANCE. *What is Risk Assessment?* 2023. <https://bja.ojp.gov/program/psrac/basics/what-is-risk-assessment>. Retrieved from Bureau of Justice Assistance.

109 SILVA, E. L.; MENEZES, E. M. *Metodologia da Pesquisa e Elaboração de Dissertação*. Florianópolis, Santa Catarina, Brasil: Universidade Federal de Santa Catarina, 2005.

110 GIL, A. C. *Como Elaborar Projetos de Pesquisa*. 6. ed. São Paulo: Atlas, 2018.

111 FONTANELLA, B. J. B.; LUCHESI, B. M.; SAIDEL, M. G. B.; RICAS, J.; TURATO, E. R.; MELO, D. G. Amostragem em pesquisas qualitativas: proposta de procedimentos para constatar saturação teórica. *Cadernos De Saúde Pública*, v. 27, n. 2, p. 388–394, 2011.

112 RIBEIRO, A. C.; DEMO, G.; SANTOS, C. D. dos. Grupo focal: Aplicações na pesquisa nacional em administração. *Pretexto*, v. 22, p. 108–128, 2021. ISSN 1984-6983.

113 STOCCHETTI, V.; SAGER, T. *The Cost of Cyber Defense - CIS Controls Implementation Group 1*. 2023. Disponível em: <https://www.cisecurity.org/insights/white-papers/the-cost-of-cyber-defense-cis-controls-ig1>.

114 BARDIN, L.; RETO, L. A.; PINHEIRO, A. *Analise de conteudo*. [S.l.]: Edicoes 70, 2000. ISBN 9724408981.

115 FEDERAL, S. T. *Acesso em 8 de setembro de 2022*. 2018. Acessado em 8 de setembro de 2022. Disponível em: <https://portal.stf.jus.br/textos/verTexto.asp?servico=centralDoCidadaoAcessoInformacaoGestaoEstrategica>.

116 PIERINI, A. J. Grupos de interesses, de pressão e lobbying - revisitando os conceitos. *REVISTA ELETRÔNICA DE CIÊNCIAS SOCIAIS*, v. 10, 2010. Disponível em: <https://periodicoshomolog.ufjf.br/index.php/csonline/article/view/17158>.

117 MOURA, K. R. C. *Os efeitos da não regulamentação do lobby no Brasil: Uma análise sobre o interesse dos atores do legislativo na aprovação do PL 1202/2017*. 2018. Disponível em: <https://bdm.unb.br/bitstream/10483/25444/1/2018_KarolinaReisCunhaMoura_tcc.pdf>.

118 QUANTITATIVE Risk Analysis: Its Importance and Implications. 2023. <https://www.cisecurity.org/white-papers/quantitative-risk-analysis/>. Retrieved from Center for Internet Security.

119 THE Ultimate Guide to Risk Prioritization. 2023. <https://hyperproof.io/resource/the-ultimate-guide-to-risk-prioritization/>. Retrieved from Hyperproof.

120 CONTINGENCY plan examples: A step-by-step guide to help your business prepare for the unexpected. 2023. <https://www.ibm.com/blog/contingency-plan-examples/>. Retrieved from IBM.

121 USE a Contingency Plan to Protect Your Business. 2023. <https://asana.com/resources/contingency-plan>. Retrieved from Asana.

122 QUEIROZ, C. E. M. *Análise das estruturas de segurança cibernética em tribunais do Distrito Federal: um estudo à luz das três linhas de defesa*. Dissertação (Trabalho de Conclusão de Curso) — Universidade de Brasília, 2022. Bacharelado em Administração.

123 ELING, M.; MCSHANE, M.; NGUYEN, T. Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, v. 10, n. 1, p. 93–125, 2021.

124 Tribunal de Contas da União. *Acompanhamento de SegCiber*. 2020. <https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/fiscalizacoes/>. Acessado em 4 de outubro de 2023.

125 ROBERTO, P.; GUEDES, N.; JOSé, L.; SULTANI, M.; ANDRé, F.; MITKIEWICZ, C.; FERREIRA, L. R.; MELO, L. A. V. D.; ANDRADE, A. D.; AFRâNIO, M.; TEIXEIRA, H.; BRUNO, M.; SOUSA, P. R. D.; DIAS, E.; IVALDO, M.; DE, J.; CASTRO, S.; MAGNO, F.; NOBRE, F.; RODRIGUES, J.; LEONARD, S.; YAMAOKA, K.; MARCUS, B.; BARBOSA, P.; RAFAEL, V.; RIBEIRO, S. *Guia do Framework de Privacidade e Segurança da Informação*. 2023. <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf>. Acessado em [12 de outubro de 2023].

126 NIST. *Glossary - NIST CSRC*. 2023. Disponível em: <https://csrc.nist.gov/glossary/term/tailoring>.

127 SECURITY, U. D. of H. *DHS 4300A Sensitive Systems Handbook - Attachment M - Tailoring NIST 800-53 Security Controls*. 2014.

128 NIST. *The Five Functions*. 2023. Disponível em: <https://www.nist.gov/cyberframework/online-learning/five-functions>.

129 ANGELINI, M.; BONOMI, S.; PALMA, A. A methodology to support automatic cyber risk assessment review. 7 2022. Disponível em: <http://arxiv.org/abs/2207.03269>.

130 KASSA, S. G. It asset valuation, risk assessment and control implementation. *ISACA Journal*, v. 3, p. 1–9, 5 2017. Disponível em: <https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/it-asset-valuation-risk-assessment-and-control-implementation-model>.

131 KWAN, T. W. *Navigating Security Threats with IT Inventory Management*. 2023. Disponível em: <https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/navigating-security-threats-with-it-inventory-management>.

APÊNDICES

I.1 CAUSAS E CONSEQUÊNCIAS DOS RISCOS DE NEGÓCIO

Tabela 1: Relação entre causas e consequências dos riscos de negócio

Causas	Risco de Negócio	Consequências
1 Cópia de minutas ou processos em computadores e meios de armazenamento pessoais		
2 Vazamento intencional por pessoas que tenham acesso às minutas ou processos (espionagem)		
3 Comprometimento de credenciais de acesso dos usuários		
4 Comprometimento de credenciais privilegiadas		
5 Utilização de computadores pessoais desprotegidos ou em redes inseguras		
6 Descarte indevido ou extravio de documentos temporários (papel, CD, pendrive etc.)		
7 Acesso físico não autorizado		1 Dano à reputação ou imagem do Poder Judiciário
8 Código-fonte do sistema judicial com vulnerabilidades de segurança	1 **Divulgação antecipada de votos, determinações ou decisões**	2 Impacto no mercado financeiro e ganhos monetários injustos
9 Falhas de configuração do ambiente de infraestrutura tecnológica		3 Pressão político-partidária sobre o julgador
10 Privilégios excessivos no sistema, em que qualquer usuário pode ter acesso de leitura das minutas		4 Comercialização de influência para obter resultados favoráveis, independentemente de influenciar diretamente nas decisões judiciais
11 Ataques cibernéticos ou engenharia social		6 Responsabilização de servidores públicos
12 Compartilhamento de senhas dos decisores		

Tabela 1 - continuação da página anterior

Causas	Risco de Negócio	Consequências
13 Ataques de sequestro de dados (ransomware de dupla extorsão) 20 Vazamentos ou espionagem em nível de hardware 21 Distribuição dos sistemas judiciais eletrônicos, dificultando o controle da segurança do código-fonte 25 Indisponibilidade de recursos humanos 26 Indisponibilidade de recursos materiais 32 Incapacidade técnica para assuntos de alta complexidade 35 Tráfico de influência (lobby judicial) 37 Suspeições de integrantes do gabinete		
1 Cópia de minutas ou processos em computadores e meios de armazenamento pessoais 2 Vazamento intencional por pessoas que tenham acesso às minutas ou processos (espionagem) 3 Comprometimento de credenciais de acesso dos usuários 4 Comprometimento de credenciais privilegiadas 5 Utilização de computadores pessoais desprotegidos ou em redes inseguras 6 Descarte indevido ou extravio de documentos temporários (papel, CD, pendrive etc.) 7 Acesso físico não autorizado 8 Código-fonte do sistema judicial com vulnerabilidades de segurança 9 Falhas de configuração do ambiente de infraestrutura tecnológica 10 Privilégios excessivos no sistema, em que qualquer usuário pode ter acesso de leitura das minutas	2 **Vazamento de informações sigilosas, protegidas por segredo de Justiça ou dados pessoais**	1 Dano à reputação ou imagem do Poder Judiciário 5 Possibilidade de compensação financeira para as pessoas envolvidas 6 Responsabilização de servidores públicos 12 Tentativa de extorsão por criminosos para não divulgar as informações

Tabela 1 - continuação da página anterior

Causas	Risco de Negócio	Consequências
11 Ataques cibernéticos ou engenharia social 12 Compartilhamento de senhas dos decisores 13 Ataques de sequestro de dados (ransomware de dupla extorsão) 20 Vazamentos ou espionagem em nível de hardware 21 Distribuição dos sistemas judiciais eletrônicos, dificultando o controle da segurança do código-fonte 22 Complexidade do controle de segurança de todas as camadas tecnológicas que utilizam tecnologias estrangeiras (banco de dados, middleware, linguagem de programação, rede etc.) 25 Indisponibilidade de recursos humanos 26 Indisponibilidade de recursos materiais 32 Incapacidade técnica para assuntos de alta complexidade 35 Tráfico de influência (lobby judicial) 37 Suspeições de integrantes do gabinete 40 Uso de ferramentas de IA generativa de forma não autorizada para apoio na elaboração de despachos e decisões		13 Danos ao erário 18 Dano irreparável para as partes envolvidas 19 Acesso indevido a segredos industriais ou estratégicos de empresas ou instituições brasileiras
3 Comprometimento de credenciais de acesso dos usuários 4 Comprometimento de credenciais privilegiadas 5 Utilização de computadores pessoais desprotegidos ou em redes inseguras 7 Acesso físico não autorizado 8 Código-fonte do sistema judicial com vulnerabilidades de segurança 9 Falhas de configuração do ambiente de infraestrutura tecnológica		1 Dano à reputação ou imagem do Poder Judiciário

Tabela 1 - continuação da página anterior

Causas	Risco de Negócio	Consequências
11 Ataques cibernéticos ou engenharia social 12 Compartilhamento de senhas dos decisores 21 Distribuição dos sistemas judiciais eletrônicos, dificultando o controle da segurança do código-fonte 22 Complexidade do controle de segurança de todas as camadas tecnológicas que utilizam tecnologias estrangeiras (banco de dados, middleware, linguagem de programação, rede etc.) 24 Processo inadequado de elaboração ou revisão de votos, decisões ou determinações 25 Indisponibilidade de recursos humanos 26 Indisponibilidade de recursos materiais 37 Suspeições de integrantes do gabinete	3 **Emissão ou alteração não autorizada de determinações ou decisões**	7 Liberação indevida de indivíduos detidos 8 Destinação de recursos financeiros às pessoas indevidas 9 Inconsistências entre o que é apresentado em sessão pública e o registro eletrônico do processo 10 Abalo da confiança nas instituições judiciais
4 Comprometimento de credenciais privilegiadas 7 Acesso físico não autorizado 8 Código-fonte do sistema judicial com vulnerabilidades de segurança 9 Falhas de configuração do ambiente de infraestrutura tecnológica 11 Ataques cibernéticos ou engenharia social 13 Ataques de sequestro de dados (ransomware de dupla extorsão) 14 Indisponibilidade de pessoas-chave 15 Ataques de negação de serviço distribuídos (DDoS) com o objetivo de prejudicar a imagem de gestores ou autoridades em (ou cotados para) cargos de relevância 16 Indisponibilidade de sistemas críticos ou falhas massivas de estruturas de armazenamento por falhas de infraestrutura de TI	4 **Interrupção da prestação jurisdicional**	1 Dano à reputação ou imagem do Poder Judiciário 11 Impedimento do acesso à Justiça 10 Abalo da confiança nas instituições judiciais 13 Danos ao erário

Tabela 1 - continuação da página anterior

Causas	Risco de Negócio	Consequências
19 Dependência de tecnologia de hardware e software estrangeiros 23 Catástrofes naturais 25 Indisponibilidade de recursos humanos 26 Indisponibilidade de recursos materiais 31 Volume excessivo de demandas que comprometem a capacidade de resposta dos tribunais (litigância predatória) 32 Incapacidade técnica para assuntos de alta complexidade		14 Prejuízo pessoal de autoridades ou gestores em indicações para cargos relevantes 17 Impacto social sobre a sociedade em geral
4 Comprometimento de credenciais privilegiadas 8 Código-fonte do sistema judicial com vulnerabilidades de segurança 9 Falhas de configuração do ambiente de infraestrutura tecnológica 11 Ataques cibernéticos ou engenharia social 17 Fragilidade do algoritmo de sorteio 19 Dependência de tecnologia de hardware e software estrangeiros 21 Distribuição dos sistemas judiciais eletrônicos, dificultando o controle da segurança do código-fonte 22 Complexidade do controle de segurança de todas as camadas tecnológicas que utilizam tecnologias estrangeiras (banco de dados, middleware, linguagem de programação, rede etc.) 25 Indisponibilidade de recursos humanos 26 Indisponibilidade de recursos materiais	5 **Previsibilidade ou manipulação da distribuição dos processos**	1 Dano à reputação ou imagem do Poder Judiciário 10 Abalo da confiança nas instituições judiciais 15 Violação da garantia de que um juiz imparcial seja designado (princípio do juiz natural) 16 Atribuição de processos a juízes que possuem conflitos de interesse ou suspeição

Tabela 1 - continuação da página anterior

Causas	Risco de Negócio	Consequências
27 Regra de negócio que preveja a mesma carga de trabalho em cada gabinete, fazendo com que a distribuição de processos seja previsível 28 Possibilidade de modificação de partes, classe processual ou petição inicial após a distribuição do processo 29 Entrada de uma mesma ação várias vezes até que o processo seja distribuído ao julgador desejado, desistindo das demais ações 30 Entrada de uma mesma ação em diferentes jurisdições (litispendência) 32 Incapacidade técnica para assuntos de alta complexidade		
4 Comprometimento de credenciais privilegiadas 7 Acesso físico não autorizado 8 Código-fonte do sistema judicial com vulnerabilidades de segurança 9 Falhas de configuração do ambiente de infraestrutura tecnológica 11 Ataques cibernéticos ou engenharia social 13 Ataques de sequestro de dados (ransomware de dupla extorsão) 14 Indisponibilidade de pessoas-chave 16 Indisponibilidade de sistemas críticos ou falhas massivas de estruturas de armazenamento por falhas de infraestrutura de TI 19 Dependência de tecnologia de hardware e software estrangeiros 23 Catástrofes naturais 25 Indisponibilidade de recursos humanos	6 **Perda de informações**	1 Dano à reputação ou imagem do Poder Judiciário 5 Possibilidade de compensação financeira para as pessoas envolvidas 6 Responsabilização de servidores públicos 13 Danos ao erário 17 Impacto social sobre a sociedade em geral 18 Dano irreparável para as partes envolvidas

Tabela 1 - continuação da página anterior

Causas	Risco de Negócio	Consequências
26 Indisponibilidade de recursos materiais		
8 Código-fonte do sistema judicial com vulnerabilidades de segurança 9 Falhas de configuração do ambiente de infraestrutura tecnológica 11 Ataques cibernéticos ou engenharia social 12 Compartilhamento de senhas dos decisores 15 Ataques de negação de serviço distribuídos (DDoS) com o objetivo de prejudicar a imagem de gestores ou autoridades em (ou cotados para) cargos de relevância 17 Fragilidade do algoritmo de sorteio 18 Modificação de informações na cadeia de fornecimento (MPF, AGU, Caixa etc.) 21 Distribuição dos sistemas judiciais eletrônicos, dificultando o controle da segurança do código-fonte 22 Complexidade do controle de segurança de todas as camadas tecnológicas que utilizam tecnologias estrangeiras (banco de dados, middleware, linguagem de programação, rede etc.) 24 Processo inadequado de elaboração ou revisão de votos, decisões ou determinações 26 Indisponibilidade de recursos materiais 27 Regra de negócio que preveja a mesma carga de trabalho em cada gabinete, fazendo com que a distribuição de processos seja previsível 28 Possibilidade de modificação de partes, classe processual ou petição inicial após a distribuição do processo 29 Entrada de uma mesma ação várias vezes até que o processo seja distribuído ao julgador desejado, desistindo das demais ações	7 **Parcialidade ou favorecimentos pessoais**	1 Dano à reputação ou imagem do Poder Judiciário 5 Possibilidade de compensação financeira para as pessoas envolvidas 6 Responsabilização de servidores públicos 10 Abalo da confiança nas instituições judiciais 18 Dano irreparável para as partes envolvidas

Tabela 1 - continuação da página anterior

Causas	Risco de Negócio	Consequências
30 Entrada de uma mesma ação em diferentes jurisdições (litispendência) 31 Volume excessivo de demandas que comprometem a capacidade de resposta dos tribunais (litigância predatória) 33 Falha na verificação de autenticidade de documentos externos que são inseridos no processo 34 Modificação intencional de informação por pessoas que tem acesso ao processo 35 Tráfico de influência (lobby judicial) 37 Nepotismo 37 Suspeições de integrantes do gabinete 38 Descumprimento de prazos processuais 39 Desconhecimento de todas as peças processuais necessárias para a análise e julgamento		
3 Comprometimento de credenciais de acesso dos usuários 4 Comprometimento de credenciais privilegiadas 5 Utilização de computadores pessoais desprotegidos ou em redes inseguras 8 Código-fonte do sistema judicial com vulnerabilidades de segurança 9 Falhas de configuração do ambiente de infraestrutura tecnológica 11 Ataques cibernéticos ou engenharia social 12 Compartilhamento de senhas dos decisores 24 Processo inadequado de elaboração ou revisão de votos, decisões ou determinações 25 Indisponibilidade de recursos humanos 26 Indisponibilidade de recursos materiais	8 **Assuntos indesejados ou inadequados em determinações e decisões**	1 Dano à reputação ou imagem do Poder Judiciário 6 Responsabilização de servidores públicos 10 Abalo da confiança nas instituições judiciais

Tabela 1 - continuação da página anterior

Causas	Risco de Negócio	Consequências
39 Desconhecimento de todas as peças processuais necessárias para a análise e julgamento 40 Uso de ferramentas de IA generativa de forma não autorizada para apoio na elaboração de despachos e decisões		
3 Comprometimento de credenciais de acesso dos usuários 4 Comprometimento de credenciais privilegiadas 5 Utilização de computadores pessoais desprotegidos ou em redes inseguras 8 Código-fonte do sistema judicial com vulnerabilidades de segurança 9 Falhas de configuração do ambiente de infraestrutura tecnológica 11 Ataques cibernéticos ou engenharia social 17 Fragilidade do algoritmo de sorteio 18 Modificação de informações na cadeia de fornecimento (MPF, AGU, Caixa etc.) 24 Processo inadequado de elaboração ou revisão de votos, decisões ou determinações 25 Indisponibilidade de recursos humanos 26 Indisponibilidade de recursos materiais 28 Possibilidade de modificação de partes, classe processual ou petição inicial após a distribuição do processo 32 Incapacidade técnica para assuntos de alta complexidade 33 Falha na verificação de autenticidade de documentos externos que são inseridos no processo	9 **Julgamentos legítimos, porém, com base em elementos adulterados**	1 Dano à reputação ou imagem do Poder Judiciário 2 Impacto no mercado financeiro e ganhos monetários injustos 5 Possibilidade de compensação financeira para as pessoas envolvidas 7 Liberação indevida de indivíduos detidos 8 Destinação de recursos financeiros às pessoas indevidas 10 Abalo da confiança nas instituições judiciais 18 Dano irreparável para as partes envolvidas

Tabela 1 - continuação da página anterior

Causas	Risco de Negócio	Consequências
34 Modificação intencional de informação por pessoas que tem acesso ao processo 38 Descumprimento de prazos processuais 39 Desconhecimento de todas as peças processuais necessárias para a análise e julgamento		
2 Vazamento intencional por pessoas que tenham acesso às minutas ou processos (espionagem) 3 Comprometimento de credenciais de acesso dos usuários 4 Comprometimento de credenciais privilegiadas 5 Utilização de computadores pessoais desprotegidos ou em redes inseguras 6 Descarte indevido ou extravio de documentos temporários (papel, CD, pendrive etc.) 7 Acesso físico não autorizado 8 Código-fonte do sistema judicial com vulnerabilidades de segurança 9 Falhas de configuração do ambiente de infraestrutura tecnológica 10 Privilégios excessivos no sistema, em que qualquer usuário pode ter acesso de leitura das minutas 11 Ataques cibernéticos ou engenharia social 13 Ataques de sequestro de dados (ransomware de dupla extorsão) 19 Dependência de tecnologia de hardware e software estrangeiros 20 Vazamentos ou espionagem em nível de hardware	10 **Espionagem de outras nações, organizações criminosas ou grupos de influência ilegais**	1 Dano à reputação ou imagem do Poder Judiciário 5 Possibilidade de compensação financeira para as pessoas envolvidas 6 Responsabilização de servidores públicos 10 Abalo da confiança nas instituições judiciais 13 Danos ao erário 15 Violação da garantia de que um juiz imparcial seja designado (princípio do juiz natural) 16 Atribuição de processos a juízes que possuem conflitos de interesse ou suspeição 17 Impacto social sobre a sociedade em geral 19 Acesso indevido a segredos industriais ou estratégicos de empresas ou instituições brasileiras

Tabela 1 - continuação da página anterior

Causas	Risco de Negócio	Consequências
21 Distribuição dos sistemas judiciais eletrônicos, dificultando o controle da segurança do código-fonte		20 Prejuízo da capacidade competitiva da economia nacional
22 Complexidade do controle de segurança de todas as camadas tecnológicas que utilizam tecnologias estrangeiras (banco de dados, middleware, linguagem de programação, rede etc.)		21 Comprometimento de objetivos estratégicos nacionais nas relações internacionais
25 Indisponibilidade de recursos humanos		22 Desvantagens de natureza política, geopolítica, militar, econômica, tecnológica ou científica
26 Indisponibilidade de recursos materiais		
32 Incapacidade técnica para assuntos de alta complexidade		
35 Tráfico de influência (lobby judicial)		
37 Suspeições de integrantes do gabinete		

I.2 CLASSIFICAÇÕES DOS CONTROLES

Tabela 2: Categorias dos controles

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
01.1	Estabelecer e manter um inventário detalhado de ativos corporativos	Estabeleça e mantenha um inventário preciso, detalhado e atualizado de todos os ativos corporativos com potencial para armazenar ou processar dados, incluindo: dispositivos de usuário final (incluindo portáteis e móveis), dispositivos de rede, dispositivos não computacionais/IoT e servidores. Certifique-se de que o inventário registre o endereço de rede (se estático), endereço de hardware, nome da máquina, proprietário do ativo de dados, departamento para cada ativo e se o ativo foi aprovado para se conectar à rede. Para dispositivos móveis de usuário final, as ferramentas do tipo MDM podem oferecer suporte a esse processo, quando apropriado. Este inventário inclui ativos conectados à infraestrutura fisicamente, virtualmente, remotamente e aqueles dentro dos ambientes de nuvem. Além disso, inclui ativos que são regularmente conectados à infraestrutura de rede corporativa, mesmo que não estejam sob o controle da empresa. Revise e atualize o inventário de todos os ativos corporativos semestralmente ou com mais frequência.	Gestão	Dispositivo	Identificar	IG1
01.2	Endereçar ativos não autorizados	Assegure que exista um processo para lidar com ativos não autorizados semanalmente. A empresa pode escolher remover o ativo da rede, negar que o ativo se conecte remotamente à rede ou colocar o ativo em quarentena.	Gestão	Dispositivo	Responder	IG1

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
01.3	Usar uma ferramenta de descoberta ativa	Utilize uma ferramenta de descoberta ativa para identificar ativos conectados à rede corporativa. Configure a ferramenta de descoberta ativa para executar diariamente ou com mais frequência.	Tecnologia	Dispositivo	Detectar	IG2
01.4	Usar o Dynamic Host Configuration Protocol (DHCP) para atualizar o inventário de ativos corporativos	Use o log do DHCP em todos os servidores DHCP ou ferramentas de gestão de endereço Internet Protocol (IP) para atualizar o inventário de ativos corporativos. Revise e use logs para atualizar o inventário de ativos corporativos semanalmente ou com mais frequência.	Tecnologia	Dispositivo	Identificar	IG2
01.5	Usar uma ferramenta de descoberta passiva	Use uma ferramenta de descoberta passiva para identificar ativos conectados à rede corporativa. Revise e use varreduras para atualizar o inventário de ativos corporativos pelo menos semanalmente ou com mais frequência.	Tecnologia	Dispositivo	Detectar	IG3
02.1	Estabelecer e manter um inventário de software	Estabeleça e mantenha um inventário detalhado de todos os softwares licenciados instalados em ativos corporativos. O inventário de software deve documentar o título, editor, data inicial de instalação/uso e objetivo de negócio de cada entrada; quando apropriado, inclua o Uniform Resource Locator(URL), app store(s), versão(ões), mecanismo de implantação e data de desativação. Revise e atualize o inventário de software semestralmente ou com mais frequência.	Gestão	Aplicações	Identificar	IG1

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
02.2	Assegurar que o software autorizado seja atualmente suportado	Assegure que apenas software atualmente suportado seja designado como autorizado no inventário de software para ativos corporativos. Se o software não é suportado, mas é necessário para o cumprimento da missão da empresa, documente uma exceção detalhando os controles de mitigação e a aceitação do risco residual. Para qualquer software não suportado sem uma documentação de exceção, designe como não autorizado. Revise o inventário de software para verificar o suporte do software pelo menos uma vez por mês ou com mais frequência.	Gestão	Aplicações	Identificar	IG1
02.3	Endereçar o software não autorizado	Assegure que o software não autorizado seja retirado de uso em ativos corporativos ou receba uma exceção documentada. Revise mensalmente ou com mais frequência.	Gestão	Aplicações	Responder	IG1
02.4	Utilizar ferramentas automatizadas de inventário de software	Utilize ferramentas de inventário de software, quando possível, em toda a empresa para automatizar a descoberta e documentação do software instalado.	Tecnologia	Aplicações	Detectar	IG2
02.5	Lista de permissões de Software autorizado	Use controles técnicos, como a lista de permissões de aplicações, para garantir que apenas o software autorizado possa ser executado ou acessado. Reavalie semestralmente ou com mais frequência.	Tecnologia	Aplicações	Proteger	IG2
02.6	Lista de permissões de bibliotecas autorizadas	Use os controles técnicos para garantir que apenas as bibliotecas de software autorizadas, como arquivos .dll, .ocx, .so, etc. específicos, tenham permissão para carregar em um processo do sistema. Impedir que bibliotecas não autorizadas sejam carregadas em um processo do sistema. Reavalie semestralmente ou com mais frequência.	Tecnologia	Aplicações	Proteger	IG2

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
02.7	Lista de permissões de Scripts autorizados	Use controles técnicos, como assinaturas digitais e controle de versão, para garantir que apenas scripts autorizados, como arquivos .ps1, .py, etc. específicos, tenham permissão para executar. Bloqueie a execução de scripts não autorizados. Reavalie semestralmente ou com mais frequência.	Tecnologia	Aplicações	Proteger	IG3
03.01	Estabelecer e manter um processo de gestão de dados	Estabeleça e mantenha um processo de gestão de dados. No processo, trate a sensibilidade dos dados, o proprietário dos dados, o manuseio dos dados, os limites de retenção de dados e os requisitos de descarte, com base em padrões de sensibilidade e retenção para a empresa. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Estratégia	Dados	Identificar	IG1
03.02	Estabelecer e manter um inventário de dados	Estabeleça e mantenha um inventário de dados, com base no processo de gestão de dados da empresa. No mínimo, inventarie os dados sensíveis. Revise e atualize o inventário anualmente, no mínimo, com prioridade para os dados sensíveis.	Gestão	Dados	Identificar	IG1
03.03	Configurar listas de controle de acesso a dados	Configure listas de controle de acesso a dados com base na necessidade de conhecimento do usuário. Aplique listas de controle de acesso a dados, também conhecidas como permissões de acesso, a sistemas de arquivos, bancos de dados e aplicações locais e remotos.	Gestão	Dados	Proteger	IG1
03.04	Aplicar retenção de dados	Retenha os dados de acordo com o processo de gestão de dados da empresa. A retenção de dados deve incluir prazos mínimos e máximos.	Gestão	Dados	Proteger	IG1

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
03.05	Descartar dados com segurança	Descarte os dados com segurança conforme descrito no processo de gestão de dados da empresa. Certifique-se de que o processo e o método de descarte sejam compatíveis com a sensibilidade dos dados.	Gestão	Dados	Proteger	IG1
03.06	Criptografar dados em dispositivos de usuário final	Criptografe os dados em dispositivos de usuário final que contenham dados sensíveis. Exemplos de implementações podem incluir: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	Tecnologia	Dispositivo	Proteger	IG1
03.07	Estabelecer e manter um esquema de classificação de dados	Estabeleça e mantenha um esquema geral de classificação de dados para a empresa. As empresas podem usar rótulos, como “Sensível”, “Confidencial” e “Público”, e classificar seus dados de acordo com esses rótulos. Revise e atualize o esquema de classificação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Estratégia	Dados	Identificar	IG2
03.08	Documentar Fluxos de Dados	Documente fluxos de dados. A documentação do fluxo de dados inclui fluxos de dados do provedor de serviços e deve ser baseada no processo de gestão de dados da empresa. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança	Gestão	Dados	Identificar	IG2
03.09	Criptografar dados em mídia removível	Criptografe os dados em mídia removível.	Tecnologia	Dados	Proteger	IG2
03.10	Criptografar dados sensíveis em trânsito	Criptografe dados sensíveis em trânsito. Exemplos de implementações podem incluir: Transport Layer Security (TLS) e Open Secure Shell (OpenSSH).	Tecnologia	Dados	Proteger	IG2

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
03.11	Criptografar dados sensíveis em repouso	Criptografe dados sensíveis em repouso em servidores, aplicações e bancos de dados que contenham dados sensíveis. A criptografia da camada de armazenamento, também conhecida como criptografia do lado do servidor, atende ao requisito mínimo desta medida de segurança. Métodos de criptografia adicionais podem incluir criptografia de camada de aplicação, também conhecida como criptografia do lado do cliente, onde o acesso ao(s) dispositivo(s) de armazenamento de dados não permite o acesso aos dados em texto simples.	Tecnologia	Dados	Proteger	IG2
03.12	Segmentar o processamento e o armazenamento de dados com base na sensibilidade	Segmente o processamento e o armazenamento de dados com base na sensibilidade dos dados. Não processe dados sensíveis em ativos corporativos destinados a dados de menor sensibilidade.	Tecnologia	Rede	Proteger	IG2
03.13	Implantar uma solução de prevenção contra perda de dados	Implementar uma ferramenta automatizada, como uma ferramenta de prevenção de perda de dados (DLP) baseada em host para identificar todos os dados sensíveis armazenados, processados ou transmitidos por meio de ativos corporativos, incluindo aqueles localizados no site local ou em um provedor de serviços remoto, e atualizar o inventário de dados sensíveis da empresa.	Tecnologia	Dados	Proteger	IG3
03.14	Registrar o acesso a dados sensíveis	Registre o acesso a dados sensíveis, incluindo modificação e descarte.	Tecnologia	Dados	Detectar	IG3

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
04.01	Estabelecer e manter um processo de configuração segura	Estabeleça e mantenha um processo de configuração segura para ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos não computacionais/IoT; e servidores) e software (sistemas operacionais e aplicações). Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Processos de Trabalho	Aplicações	Proteger	IG1
04.02	Estabelecer e Manter um Processo de Configuração Segura para a Infraestrutura de Rede	Estabeleça e mantenha um processo de configuração segura para dispositivos de rede. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Processos de Trabalho	Rede	Proteger	IG1
04.04	Implementar e gerenciar um firewall nos servidores	Implemente e gerencie um firewall nos servidores, onde houver suporte. Exemplos de implementações incluem um firewall virtual, firewall do sistema operacional ou um agente de firewall de terceiros.	Tecnologia	Dispositivo	Proteger	IG1
04.05	Implementar e gerenciar um firewall nos dispositivos de usuário final	Implemente e gerencie um firewall baseado em host ou uma ferramenta de filtragem de porta nos dispositivos de usuário final, com uma regra de negação padrão que bloqueia todo o tráfego, exceto os serviços e portas que são explicitamente permitidos.	Tecnologia	Dispositivo	Proteger	IG1
04.06	Gerenciar com segurança os ativos e software corporativos	Gerencie com segurança os ativos e software corporativos. Exemplos de implementações incluem gestão de configuração por meio de version-controlled-infrastructure-as-code e acesso a interfaces administrativas por meio de protocolos de rede seguros, como Secure Shell (SSH) e Hypertext Transfer Protocol Secure (HTTPS). Não use protocolos de gestão inseguros, como Telnet (Teletype Network) e HTTP, a menos que seja operacionalmente essencial.	Gestão	Rede	Proteger	IG1

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
04.07	Gerenciar contas padrão nos ativos e software corporativos	Gerencie contas padrão nos ativos e software corporativos, como root, administrador e outras contas de fornecedores pré-configuradas. Exemplos de implementações podem incluir: desativar contas padrão ou torná-las inutilizáveis.	Tecnologia	Usuários	Proteger	IG1
04.08	Desinstalar ou desativar serviços desnecessários nos ativos e software corporativos	Desinstale ou desative serviços desnecessários nos ativos e software corporativos, como um serviço de compartilhamento de arquivos não utilizado, módulo de aplicação da web ou função de serviço.	Tecnologia	Dispositivo	Proteger	IG2
04.10	Impor o bloqueio automático de dispositivos nos dispositivos portáteis do usuário final	Imponha o bloqueio automático do dispositivo seguindo um limite pré-determinado de tentativas de autenticação local com falha nos dispositivos portáteis de usuário final, quando compatível. Para laptops, não permita mais de 20 tentativas de autenticação com falha; para tablets e smartphones, não mais do que 10 tentativas de autenticação com falha. Exemplos de implementações incluem Microsoft® InTune Device Lock e Apple® Configuration Profile maxFailedAttempts.	Tecnologia	Dispositivo	Responder	IG2
04.11	Impor a capacidade de limpeza remota nos dispositivos portáteis do usuário final	Limpe remotamente os dados corporativos de dispositivos portáteis de usuário final de propriedade da empresa quando for considerado apropriado, como dispositivos perdidos ou roubados, ou quando um indivíduo não trabalha mais na empresa.	Tecnologia	Dispositivo	Proteger	IG2
04.12	Separar os Espaços de Trabalho Corporativos nos dispositivos móveis	Certifique-se de que a separação de espaços de trabalho corporativos seja usada nos dispositivos móveis de usuário final, onde houver suporte. Exemplos de implementações incluem o uso de um Apple® Configuration Profile ou Android ™ Work Profile para separar aplicações e dados corporativos de aplicações e dados pessoais.	Tecnologia	Dispositivo	Proteger	IG3

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
05.1	Estabelecer e manter um inventário de contas	Estabeleça e mantenha um inventário de todas as contas gerenciadas na empresa. O inventário deve incluir contas de usuário e administrador. O inventário, no mínimo, deve conter o nome da pessoa, nome de usuário, datas de início/ término e departamento. Valide se todas as contas ativas estão autorizadas, em uma programação recorrente, no mínimo trimestralmente ou com mais frequência.	Identidade e acesso	Usuários	Identificar	IG1
05.2	Usar senhas exclusivas	Use senhas exclusivas para todos os ativos corporativos. As melhores práticas de implementação incluem, no mínimo, uma senha de 8 caracteres para contas que usam MFA e uma senha de14 caracteres para contas que não usam MFA.	Identidade e acesso	Usuários	Proteger	IG1
05.3	Desabilitar contas inativas	Exclua ou desabilite quaisquer contas inativas após um período de 45 dias de inatividade, onde for suportado.	Identidade e acesso	Usuários	Responder	IG1
05.4	Restringir privilégios de administrador a contas de Administrador dedicadas	Restrinja os privilégios de administrador a contas de administrador dedicadas nos ativos corporativos. Realize atividades gerais de computação, como navegação na Internet, e-mail e uso do pacote de produtividade, a partir da conta primária não privilegiada do usuário.	Tecnologia	Usuários	Proteger	IG1
05.5	Estabelecer e manter um inventário de contas de serviço	Estabeleça e mantenha um inventário de contas de serviço. O inventário, no mínimo, deve conter departamento proprietário, data de revisão e propósito. Realize análises de contas de serviço para validar se todas as contas ativas estão autorizadas, em uma programação recorrente, no mínimo trimestralmente ou com mais frequência.	Identidade e acesso	Usuários	Identificar	IG2
05.6	Centralizar a gestão de contas	Centralize a gestão de contas por meio de serviço de diretório ou de identidade.	Identidade e acesso	Usuários	Proteger	IG2

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
06.1	Estabelecer um Processo de Concessão de Acesso	Estabeleça e siga um processo, de preferência automatizado, para conceder acesso aos ativos corporativos mediante nova contratação, concessão de direitos ou mudança de função de um usuário.	Identidade e acesso	Usuários	Proteger	IG1
06.2	Estabelecer um Processo de Revogação de Acesso	Estabeleça e siga um processo, de preferência automatizado, para revogar o acesso aos ativos corporativos, por meio da desativação de contas imediatamente após o encerramento, revogação de direitos ou mudança de função de um usuário. Desativar contas, em vez de excluí-las, pode ser necessário para preservar as trilhas de auditoria.	Identidade e acesso	Usuários	Proteger	IG1
06.3	Exigir MFA para aplicações expostas externamente	Exija que todas as aplicações corporativas ou de terceiros expostas externamente apliquem o MFA, onde houver suporte. Impor o MFA por meio de um serviço de diretório ou provedor de SSO é uma implementação satisfatória desta medida de segurança.	Identidade e acesso	Usuários	Proteger	IG1
06.4	Exigir MFA para acesso remoto à rede	Exija MFA para acesso remoto à rede.	Identidade e acesso	Usuários	Proteger	IG1
06.5	Exigir MFA para acesso administrativo	Exija MFA para todas as contas de acesso administrativo, onde houver suporte, em todos os ativos corporativos, sejam gerenciados no site local ou por meio de um provedor terceirizado.	Identidade e acesso	Usuários	Proteger	IG1
06.6	Estabelecer e manter um inventário de sistemas de autenticação e autorização	Estabeleça e mantenha um inventário dos sistemas de autenticação e autorização da empresa, incluindo aqueles hospedados no site local ou em um provedor de serviços remoto. Revise e atualize o inventário, no mínimo, anualmente ou com mais frequência.	Identidade e acesso	Usuários	Identificar	IG2

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
06.7	Centralizar o controle de acesso	Centralize o controle de acesso para todos os ativos corporativos por meio de um serviço de diretório ou provedor de SSO, onde houver suporte.	Identidade e acesso	Usuários	Proteger	IG2
06.8	Definir e manter o controle de acesso baseado em funções	Defina e mantenha o controle de acesso baseado em funções, determinando e documentando os direitos de acesso necessários para cada função dentro da empresa para cumprir com sucesso suas funções atribuídas. Realize análises de controle de acesso de ativos corporativos para validar se todos os privilégios estão autorizados, em uma programação recorrente, no mínimo uma vez por ano ou com maior frequência.	Identidade e acesso	Dados	Proteger	IG3
07.1	Estabelecer e manter um processo de gestão de vulnerabilidade	Estabeleça e mantenha um processo de gestão de vulnerabilidade documentado para ativos corporativos. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Processos de Trabalho	Aplicações	Proteger	IG1
07.2	Estabelecer e manter um processo de remediação	Estabeleça e mantenha uma estratégia de remediação baseada em risco documentada em um processo de remediação, com revisões mensais ou mais frequentes.	Processos de Trabalho	Aplicações	Responder	IG1
07.3	Executar a gestão automatizada de patches do sistema operacional	Realize atualizações do sistema operacional em ativos corporativos por meio da gestão automatizada de patches mensalmente ou com mais frequência.	Tecnologia	Aplicações	Proteger	IG1
07.4	Executar a gestão automatizada de patches de aplicações	Realize atualizações de aplicações em ativos corporativos por meio da gestão automatizada de patches mensalmente ou com mais frequência.	Tecnologia	Aplicações	Proteger	IG1

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
07.5	Realizar varreduras automatizadas de vulnerabilidade em ativos corporativos internos	Realize varreduras automatizadas de vulnerabilidade em ativos corporativos internos trimestralmente ou com mais frequência. Realize varreduras autenticadas e não autenticadas, usando uma ferramenta de varredura de vulnerabilidade compatível com o SCAP.	Tecnologia	Aplicações	Identificar	IG2
07.6	Realizar varreduras automatizadas de vulnerabilidade em ativos corporativos expostos externamente	Execute varreduras de vulnerabilidade automatizadas de ativos corporativos expostos externamente usando uma ferramenta de varredura de vulnerabilidade compatível com o SCAP. Execute varreduras mensalmente ou com mais frequência.	Tecnologia	Aplicações	Identificar	IG2
07.7	Corrigir vulnerabilidades detectadas	Corrija as vulnerabilidades detectadas no software por meio de processos e ferramentas mensalmente, ou mais frequentemente, com base no processo de correção.	Tecnologia	Aplicações	Responder	IG2
08.01	Estabelecer e manter um processo de gestão de log de auditoria	Estabeleça e mantenha um processo de gestão de log de auditoria que defina os requisitos de log da empresa. No mínimo, trate da coleta, revisão e retenção de logs de auditoria para ativos corporativos. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Processos de Trabalho	Rede	Proteger	IG1
08.02	Coletar logs de auditoria	Colete logs de auditoria. Certifique-se de que o log, de acordo com o processo de gestão de log de auditoria da empresa, tenha sido habilitado em todos os ativos.	Tecnologia	Rede	Detectar	IG1
08.03	Garantir o armazenamento adequado do registro de auditoria	Certifique-se de que os destinos dos logs mantenham armazenamento adequado para cumprir o processo de gestão de log de auditoria da empresa.	Tecnologia	Rede	Proteger	IG1
08.04	Padronizar a sincronização de tempo	Padronize a sincronização de tempo. Configure pelo menos duas fontes de tempo sincronizadas nos ativos corporativos, onde houver suporte.	Tecnologia	Rede	Proteger	IG2

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
08.05	Coletar logs de auditoria detalhados	Configure o log de auditoria detalhado para ativos corporativos contendo dados sensíveis. Inclua a origem do evento, data, nome de usuário, carimbo de data/hora, endereços de origem, endereços de destino e outros elementos úteis que podem ajudar em uma investigação forense.	Tecnologia	Rede	Detectar	IG2
08.09	Centralizar os logs de auditoria	Centralize, na medida do possível, a coleta e retenção de logs de auditoria nos ativos corporativos.	Tecnologia	Rede	Detectar	IG2
08.10	Reter os logs de auditoria	Reter os logs de auditoria em ativos corporativos por no mínimo 90 dias.	Tecnologia	Rede	Proteger	IG2
08.11	Conduzir revisões de log de auditoria	Realize análises de logs de auditoria para detectar anomalias ou eventos anormais que possam indicar uma ameaça potencial. Realize revisões semanalmente ou com mais frequência.	Tecnologia	Rede	Detectar	IG2
09.1	Garantir o uso apenas de navegadores e clientes de e-mail suportados plenamente	Certifique-se de que apenas navegadores e clientes de e-mail suportados plenamente tenham permissão para executar na empresa, usando apenas a versão mais recente dos navegadores e clientes de e-mail fornecidos pelo fornecedor.	Tecnologia	Aplicações	Proteger	IG1
09.2	Usar serviços de filtragem de DNS	Use os serviços de filtragem de DNS em todos os ativos corporativos para bloquear o acesso a domínios malintencionados conhecidos.	Tecnologia	Rede	Proteger	IG1
09.3	Manter e impor filtros de URL baseados em rede	Imponha e atualize filtros de URL baseados em rede para limitar um ativo corporativo de se conectar a sites potencialmente maliciosos ou não aprovados. Exemplos de implementações incluem filtragem baseada em categoria, filtragem baseada em reputação ou através do uso de listas de bloqueio. Aplique filtros para todos os ativos corporativos.	Tecnologia	Rede	Proteger	IG2

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
09.4	Restringir extensões de cliente de e-mail e navegador desnecessárias ou não autorizadas	Restrinja, seja desinstalando ou desabilitando, quaisquer plug-ins de cliente de e-mail ou navegador, extensões e aplicações complementares não autorizados ou desnecessários.	Tecnologia	Aplicações	Proteger	IG2
09.4	Restringir extensões de cliente de e-mail e navegador desnecessárias ou não autorizadas	Restrinja, seja desinstalando ou desabilitando, quaisquer plug-ins de cliente de e-mail ou navegador, extensões e aplicações complementares não autorizados ou desnecessários.	Tecnologia	Aplicações	Proteger	IG2
09.5	Implementar o DMARC	Para diminuir a chance de e-mails forjados ou modificados de domínios válidos, implemente a política e verificação DMARC, começando com a implementação dos padrões Sender Policy Framework (SPF) e DomainKeys Identified Mail (DKIM).	Tecnologia	Rede	Proteger	IG2
09.6	Bloquear tipos de arquivo desnecessários	Bloqueie tipos de arquivo desnecessários que tentem entrar no gateway de e-mail da empresa.	Tecnologia	Rede	Proteger	IG2
10.1	Instalar e manter um software anti-malware	Instale e mantenha um software anti-malware em todos os ativos corporativos.	Tecnologia	Dispositivo	Proteger	IG1
10.2	Configurar atualizações automáticas de assinatura anti-malware	Configure atualizações automáticas para arquivos de assinatura anti-malware em todos os ativos corporativos.	Tecnologia	Dispositivo	Proteger	IG1
10.3	Desabilitar a execução e reprodução automática para mídias removíveis	Desabilitar a funcionalidade de execução e reprodução automática para mídias removíveis.	Tecnologia	Dispositivo	Proteger	IG1
10.4	Configurar a varredura anti-malware automática de mídia removível	Configure o software anti-malware para verificar automaticamente a mídia removível.	Tecnologia	Dispositivo	Detectar	IG2

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
10.5	Habilitar recursos anti-exploração	Habilite recursos anti-exploração em ativos e software corporativos, onde possível, como Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), ou Apple® System Integrity Protection (SIP) e Gatekeeper™.	Tecnologia	Dispositivo	Proteger	IG2
10.6	Gerenciar o software anti-malware de maneira centralizada	Gerencie o software anti-malware de maneira centralizada.	Tecnologia	Dispositivo	Proteger	IG2
10.7	Usar software anti-malware baseado em comportamento	Use software anti-malware baseado em comportamento.	Tecnologia	Dispositivo	Detectar	IG2
11.1	Estabelecer e manter um processo de recuperação de dados	Estabeleça e mantenha um processo de recuperação de dados. No processo, aborde o escopo das atividades de recuperação de dados, a priorização da recuperação e a segurança dos dados de backup. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Processos de Trabalho	Dados	Recuperar	IG1
11.2	Executar backups automatizados	Execute backups automatizados de ativos corporativos dentro do escopo. Execute backups semanalmente ou com mais frequência, com base na sensibilidade dos dados.	Tecnologia	Dados	Recuperar	IG1
11.3	Proteger os dados de recuperação	Proteja os dados de recuperação com controles equivalentes dos dados originais. Referencie o uso de criptografia ou separação de dados, com base nos requisitos.	Tecnologia	Dados	Proteger	IG1
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	Estabeleça e mantenha uma instância isolada de dados de recuperação. Exemplos de implementações incluem controle de versão de destinos de backup por meio de sistemas ou serviços offline, na nuvem ou fora do site local.	Gestão	Dados	Recuperar	IG1

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
11.5	Testar os dados de recuperação	Teste a recuperação do backup trimestralmente, ou com mais frequência, para uma amostra dos ativos corporativos dentro do escopo.	Gestão	Dados	Recuperar	IG2
12.1	Assegurar que a infraestrutura de rede esteja atualizada	Assegure que a infraestrutura de rede seja mantida atualizada. Exemplos de implementações incluem a execução da versão estável mais recente do software e/ou o uso de ofertas de network-as-a-service (NaaS) atualmente suportadas. Revise as versões do software mensalmente, ou com mais frequência, para verificar o suporte do software.	Gestão	Rede	Proteger	IG1
12.2	Estabelecer e manter uma arquitetura de rede segura	Estabeleça e mantenha uma arquitetura de rede segura. Uma arquitetura de rede segura deve abordar segmentação, privilégio mínimo e disponibilidade, no mínimo.	Gestão	Rede	Proteger	IG2
12.3	Gerenciar infraestrutura de rede com segurança	Gerencie com segurança a infraestrutura de rede. Exemplos de implementações incluem versão controlada de infraestrutura como código e o uso de protocolos de rede seguros, como SSH e HTTPS.	Tecnologia	Rede	Proteger	IG2
12.5	Centralizar a autenticação, autorização e auditoria (AAA) de rede	Centralize AAA de rede.	Identidade e acesso	Rede	Proteger	IG2
12.6	Usar protocolos de comunicação e gestão de rede seguros	Use protocolos de comunicação e gestão de rede seguros (por exemplo, 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise ou superior).	Tecnologia	Rede	Proteger	IG2
12.7	Assegurar que os dispositivos remotos utilizem uma VPN e estejam se conectando a uma infraestrutura AAA da empresa	Exigir que os usuários se autentiquem em serviços de autenticação e VPN gerenciados pela empresa antes de acessar os recursos da empresa em dispositivos de usuário final.	Identidade e acesso	Dispositivo	Proteger	IG2

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
12.8	Estabelecer e manter recursos de computação dedicados para todo o trabalho administrativo	Estabeleça e mantenha recursos de computação dedicados, fisicamente ou logicamente separados, para todas as tarefas administrativas ou tarefas que requeiram acesso administrativo. Os recursos de computação devem ser segmentados da rede primária da empresa e não deve ser permitido o acesso à Internet.	Tecnologia	Dispositivo	Proteger	IG3
13.01	Centralizar o alerta de eventos de segurança	Centralize os alertas de eventos de segurança em ativos corporativos para correlação e análise de log. A melhor prática requer o uso de um SIEM, que inclui alertas de correlação de eventos definidos pelo fornecedor. Uma plataforma de análise de log configurada com alertas de correlação relevantes para a segurança também atende a esta medida de segurança.	Tecnologia	Rede	Detectar	IG2
13.02	Implantar solução de detecção de intrusão baseada em host	Implante uma solução de detecção de intrusão baseada em host em ativos corporativos, quando apropriado e/ou com suporte.	Tecnologia	Dispositivo	Detectar	IG2
13.03	Implantar uma solução de detecção de intrusão de rede	Implante uma solução de detecção de intrusão de rede em ativos corporativos, quando apropriado. Exemplos de implementações incluem o uso de um Network Intrusion Detection System (NIDS) ou serviço de provedor de serviço de nuvem equivalente (CSP).	Tecnologia	Rede	Detectar	IG2
13.04	Realizar filtragem de tráfego entre segmentos de rede	Execute a filtragem de tráfego entre segmentos de rede, quando apropriado.	Tecnologia	Rede	Proteger	IG2

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
13.05	Gerenciar controle de acesso para ativos remotos	"Gerencie o controle de acesso para ativos que se conectam remotamente aos recursos da empresa. Determine a quantidade de acesso aos recursos da empresa com base em: software anti-malware atualizado instalado, conformidade de configuração com o processo de configurações seguras da empresa e garantia de que o sistema operacional e as aplicações estão atualizados."	Gestão	Dispositivo	Proteger	IG2
13.06	Coletar logs de fluxo de tráfego da rede	Colete logs de fluxo de tráfego de rede e/ou tráfego de rede para revisar e alertar sobre dispositivos de rede.	Tecnologia	Rede	Detectar	IG2
13.07	Implantar solução de prevenção de intrusão baseada em host	Implante uma solução de prevenção de intrusão baseada em host em ativos corporativos, quando apropriado e/ou com suporte. Exemplos de implementações incluem o uso de um cliente Endpoint Detection and Response (EDR) ou agente IPS baseado em host.	Tecnologia	Dispositivo	Proteger	IG3
13.08	Implantar uma solução de prevenção de intrusão de rede	Implante uma solução de prevenção de intrusão de rede, quando apropriado. Exemplos de implementações incluem o uso de um Network Intrusion Prevention System (NIPS) ou serviço CSP equivalente.	Tecnologia	Rede	Proteger	IG3
13.09	Implantar controle de acesso no nível de porta	Implante o controle de acesso no nível de porta. O controle de acesso no nível de porta utiliza 802.1x ou protocolos de controle de acesso à rede semelhantes, como certificados, e pode incorporar autenticação de usuário e/ou dispositivo.	Tecnologia	Dispositivo	Proteger	IG3
13.10	Executar filtragem da camada de aplicação	Execute a filtragem da camada de aplicação. Exemplos de implementações incluem um proxy de filtragem, firewall de camada de aplicação ou gateway.	Tecnologia	Rede	Proteger	IG3

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
14.1	Estabelecer e manter um programa de conscientização de segurança	Estabeleça e mantenha um programa de conscientização de segurança. O objetivo de um programa de conscientização de segurança é educar a força de trabalho da empresa sobre como interagir com ativos e dados corporativos de maneira segura. Realize o treinamento na contratação e, no mínimo, anualmente. Revise e atualize o conteúdo anualmente ou quando ocorrerem mudanças significativas na empresa que possam afetar esta proteção.	Estratégia	Pessoas	Proteger	IG1
14.2	Treinar membros da força de trabalho para reconhecer ataques de engenharia social	Treine os membros da força de trabalho para reconhecer ataques de engenharia social, como phishing, pretexto e uso não autorizado.	Competências	Pessoas	Proteger	IG1
14.3	Treinar membros da força de trabalho nas melhores práticas de autenticação	Treine os membros da força de trabalho nas melhores práticas de autenticação. Exemplos de tópicos incluem MFA, composição de senha e gestão de credenciais.	Competências	Pessoas	Proteger	IG1
14.4	Treinar a força de trabalho nas Melhores Práticas de Tratamento de Dados	Treine os membros da força de trabalho sobre como identificar, armazenar, transferir, arquivar e destruir dados sensíveis de maneira adequada. Isso também inclui o treinamento de membros da força de trabalho em práticas recomendadas de mesa e tela limpas, como bloquear a tela quando eles se afastam de seus ativos corporativos, apagar quadros brancos físicos e virtuais no final das reuniões e armazenar dados e ativos com segurança.	Competências	Pessoas	Proteger	IG1
14.5	Treinar membros da força de trabalho sobre as causas da exposição não intencional de dados	Treine os membros da força de trabalho para estarem cientes das causas da exposição não intencional de dados. Exemplos de tópicos incluem entrega incorreta de dados sensíveis, perda de um dispositivo de usuário final portátil ou publicação de dados para públicos indesejados.	Competências	Pessoas	Proteger	IG1

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
14.6	Treinar Membros da força de trabalho no Reconhecimento e Comunicação de Incidentes de Segurança	Treine os membros da força de trabalho para serem capazes de reconhecer um incidente em potencial e relatar tal incidente.	Competências	Pessoas	Proteger	IG1
14.7	Treinar a força de trabalho sobre como identificar e comunicar se o seus ativos corporativos estão faltando atualizações de segurança	Treine a força de trabalho para entender como verificar e relatar patches de software desatualizados ou quaisquer falhas em ferramentas e processos automatizados. Parte desse treinamento deve incluir a notificação do pessoal de TI sobre quaisquer falhas em processos e ferramentas automatizadas.	Competências	Pessoas	Proteger	IG1
14.8	Treinar a força de trabalho sobre os perigos de se conectar e transmitir dados corporativos em redes inseguras	Treine os membros da força de trabalho sobre os perigos de se conectar e transmitir dados em redes inseguras para atividades corporativas. Se a empresa tiver funcionários remotos, o treinamento deve incluir orientação para garantir que todos os usuários configurem com segurança sua infraestrutura de rede doméstica.	Competências	Pessoas	Proteger	IG1
14.9	Conduzir treinamento de competências e conscientização de segurança para funções específicas	Conduza treinamento de conscientização de segurança e de competências específicas para funções. Exemplos de implementações incluem cursos de administração de sistema seguro para profissionais de TI, treinamento de conscientização e prevenção de vulnerabilidades para desenvolvedores de aplicações da web do OWASP® Top 10 aplicações e treinamento avançado de conscientização de engenharia social para funções de perfil alto.	Competências	Pessoas	Proteger	IG2

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
15.4	Garantir que os contratos do provedor de serviços incluam requisitos de segurança	Certifique-se de que os contratos do provedor de serviços incluem requisitos de segurança. Requisitos de exemplo podem incluir requisitos mínimos do programa de segurança, notificação e resposta de incidente de segurança e/ou de violação de dados, requisitos de criptografia de dados e compromissos de descarte de dados. Esses requisitos de segurança devem ser consistentes com a política de gestão do provedor de serviços da empresa. Revise os contratos do provedor de serviços anualmente para garantir que os contratos não estejam perdendo os requisitos de segurança.	Fornecedores	Informação	Proteger	IG2
15.7	Descomissionar com segurança os provedores de serviços	Descomissione os prestadores de serviços com segurança. Considerações de exemplo incluem desativação de contas de usuário e serviço, encerramento de fluxos de dados e descarte seguro de dados corporativos em sistemas de provedores de serviços.	Fornecedores	Informação	Proteger	IG3
16.01	Estabelecer e manter um processo seguro de desenvolvimento de aplicações	Estabeleça e mantenha um processo seguro de desenvolvimento de aplicações. No processo, trate de itens como: padrões de design de aplicação seguro, práticas de codificação seguras, treinamento de desenvolvedor, gestão de vulnerabilidade, segurança de código de terceiros e procedimentos de teste de segurança de aplicação. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Processos de Trabalho	Aplicações	Proteger	IG2

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
16.02	Estabelecer e manter um processo para aceitar e endereçar vulnerabilidades de software	Estabelecer e manter um processo para aceitar e endereçar relatórios de vulnerabilidades de software, incluindo um meio para que as entidades externas relatem. O processo deve incluir itens como: uma política de tratamento de vulnerabilidade que identifica o processo de relatar, a parte responsável por lidar com os relatórios de vulnerabilidade e um processo de entrada, atribuição, correção e teste de correção. Como parte do processo, use um sistema de rastreamento de vulnerabilidade que inclua classificações de gravidade e métricas para medir o tempo de identificação, análise e correção de vulnerabilidades. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança. Os terceiros desenvolvedores de aplicações precisam considerar esta política para o exterior que ajuda a definir as expectativas para as partes interessadas externas.	Processos de Trabalho	Aplicações	Proteger	IG2
16.03	Executar análise de causa raiz em vulnerabilidades de segurança	Execute a análise de causa raiz em vulnerabilidades de segurança. Ao revisar as vulnerabilidades, a análise da causa raiz é a tarefa de avaliar os problemas subjacentes que criam vulnerabilidades no código e permite que as equipes de desenvolvimento vão além de apenas corrigir vulnerabilidades individuais conforme elas surgem.	Gestão	Aplicações	Proteger	IG2

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
16.04	Estabelecer e gerenciar um inventário de componentes de software de terceiros	Estabeleça e gerencie um inventário atualizado de componentes de terceiros usados no desenvolvimento, geralmente chamados de "lista de materiais", bem como componentes programados para uso futuro. Este inventário deve incluir quaisquer riscos que cada componente de terceiros possa representar. Avalie a lista pelo menos uma vez por mês para identificar quaisquer mudanças ou atualizações nesses componentes e valide se o componente ainda é compatível.	Gestão	Aplicações	Proteger	IG2
16.05	Usar componentes de software de terceiros atualizados e confiáveis	Use componentes de software de terceiros atualizados e confiáveis. Quando possível, escolha bibliotecas e estruturas estabelecidas e comprovadas que forneçam segurança adequada. Adquira esses componentes de fontes confiáveis ou avalie o software quanto a vulnerabilidades antes de usá-los.	Gestão	Aplicações	Proteger	IG2
16.06	Estabelecer e manter um sistema de classificação de gravidade e processo para vulnerabilidades de aplicações	Estabeleça e mantenha um sistema de classificação de gravidade e processo para vulnerabilidades de aplicações que facilitem a priorização da ordem em que as vulnerabilidades descobertas são corrigidas. Esse processo inclui a definição de um nível mínimo de aceitabilidade de segurança para a liberação de código ou aplicações. As classificações de gravidade trazem uma forma sistemática de triagem de vulnerabilidades que melhora o gestão de riscos e ajuda a garantir que os bugs mais graves sejam corrigidos primeiro. Revise e atualize o sistema e processo anualmente.	Processos de Trabalho	Aplicações	Proteger	IG2

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
16.07	Usar modelos de configurações de segurança padrão para infraestrutura de aplicações	Use modelos de configuração de segurança padrão recomendados pelo setor para componentes de infraestrutura de aplicações. Isso inclui servidores subjacentes, bancos de dados e servidores web e se aplica a contêineres de nuvem, componentes de Platform as a Service (PaaS) e componentes de SaaS. Não permita que o software desenvolvido internamente enfraqueça as configurações de segurança.	Tecnologia	Aplicações	Proteger	IG2
16.08	Separar sistemas de produção e não produção	Mantenha ambientes separados para sistemas de produção e não produção.	Gestão	Aplicações	Proteger	IG2
16.09	Treinar desenvolvedores em conceitos de segurança de aplicações e codificação segura	Certifique-se de que todo o pessoal de desenvolvimento de software receba treinamento para escrever código seguro para seu ambiente de desenvolvimento e responsabilidades específicas. O treinamento pode incluir princípios gerais de segurança e práticas padrão de segurança de aplicações. Conduza o treinamento pelo menos uma vez por ano e projete de forma a promover a segurança dentro da equipe de desenvolvimento e construir uma cultura de segurança entre os desenvolvedores.	Competências	Aplicações	Proteger	IG2

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
16.10	Aplicar princípios de design seguro em arquiteturas de aplicações	Aplique princípios de design seguro em arquiteturas de aplicações. Os princípios de design seguro incluem o conceito de privilégio mínimo e aplicação de mediação para validar cada operação que o usuário faz, promovendo o conceito de "nunca confiar nas entradas do usuário". Os exemplos incluem garantir que a verificação explícita de erros seja realizada e documentada para todas as entradas, incluindo tamanho, tipo de dados e intervalos ou formatos aceitáveis. O design seguro também significa minimizar a superfície de ataque da infraestrutura da aplicação, como desligar portas e serviços desprotegidos, remover programas e arquivos desnecessários e renomear ou remover contas padrão.	Tecnologia	Aplicações	Proteger	IG2
16.11	Aproveitar os módulos ou serviços controlados para componentes de segurança de aplicações	Aproveite os módulos ou serviços controlados para os componentes de segurança da aplicação, como gestão de identidade, criptografia e auditoria e log. O uso de recursos da plataforma em funções críticas de segurança reduzirá a carga de trabalho dos desenvolvedores e minimizará a probabilidade de erros de design ou implementação. Os sistemas operacionais modernos fornecem mecanismos eficazes para identificação, autenticação e autorização e disponibilizam esses mecanismos para as aplicações. Use apenas algoritmos de criptografia padronizados, atualmente aceitos e amplamente revisados. Os sistemas operacionais também fornecem mecanismos para criar e manter logs de auditoria seguros.	Tecnologia	Aplicações	Proteger	IG2
16.12	Implementar verificações de segurança em nível de código	Aplique ferramentas de análise estáticas e dinâmicas dentro do ciclo de vida da aplicação para verificar se as práticas de codificação seguras estão sendo seguidas.	Tecnologia	Aplicações	Proteger	IG3

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
16.13	Realizar teste de invasão de aplicação	Realize teste de invasão das aplicações. Para aplicações críticas, o teste de invasão autenticado é mais adequado para localizar vulnerabilidades de lógica de negócios do que a varredura de código e o teste de segurança automatizado. O teste de invasão depende da habilidade do testador para manipular manualmente um aplicação como um usuário autenticado e não autenticado.	Tecnologia	Aplicações	Proteger	IG3
16.14	Conduzir aplicações de modelagem de ameaças	Conduza a modelagem de ameaças. A modelagem de ameaças é o processo de identificar e abordar as falhas de design de segurança da aplicação em um design, antes que o código seja criado. É conduzido por pessoas especialmente treinadas que avaliam o design da aplicação e medem os riscos de segurança para cada ponto de entrada e nível de acesso. O objetivo é mapear a aplicação, a arquitetura e a infraestrutura de uma forma estruturada para entender seus pontos fracos.	Gestão	Aplicações	Proteger	IG3
17.1	Designar Pessoal para Gerenciar Tratamento de Incidentes	"Designe uma pessoa-chave e pelo menos uma backup para gerenciar o processo de tratamento de incidentes da empresa. A equipe de gestão é responsável pela coordenação e documentação dos esforços de resposta e recuperação a incidentes e pode consistir em funcionários internos da empresa, fornecedores terceirizados ou uma abordagem híbrida. Se estiver usando um fornecedor terceirizado, designe pelo menos uma pessoa interna da empresa para supervisionar qualquer trabalho terceirizado. Revise anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança."	Estratégia	Pessoas	Responder	IG1

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
17.2	Estabelecer e manter informações de contato para relatar incidentes de segurança	Estabeleça e mantenha as informações de contato das partes que precisam ser informadas sobre os incidentes de segurança. Os contatos podem incluir funcionários internos, fornecedores terceirizados, policiais, provedores de seguros cibernéticos, agências governamentais relevantes, parceiros do Information Sharing and Analysis Center (ISAC) ou outras partes interessadas. Verifique os contatos anualmente para garantir que as informações estejam atualizadas.	Gestão	Pessoas	Responder	IG1
17.3	Estabelecer e manter um processo corporativo para relatar incidentes	Estabeleça e mantenha um processo corporativo para a força de trabalho relatar incidentes de segurança. O processo inclui cronograma de relatórios, pessoal para relatar, mecanismo para relatar e as informações mínimas a serem relatadas. Certifique-se de que o processo esteja publicamente disponível para toda a força de trabalho. Revise anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Processos de Trabalho	Processo	Responder	IG1
18.1	Estabelecer e manter um programa de teste de invasão	Estabeleça e mantenha um programa de teste de invasão adequado ao tamanho, complexidade e maturidade da empresa. As características do programa de teste de invasão incluem escopo, como rede, aplicação web, Application Programming Interface (API), serviços hospedados e controles de instalações físicas; frequência; limitações, como horas aceitáveis e tipos de ataque excluídos; informações do ponto de contato; remediação, por exemplo, como as descobertas serão encaminhadas internamente; e requisitos retrospectivos.	Estratégia	Processo	Identificar	IG2

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
18.2	Realizar testes de invasão externos periódicos	Realize testes de invasão externos periódicos com base nos requisitos do programa, pelo menos uma vez por ano. O teste de invasão externo deve incluir reconhecimento empresarial e ambiental para detectar informações exploráveis. O teste de invasão requer habilidades e experiência especializadas e deve ser conduzido por uma parte qualificada. O teste pode ser clear box ou opaque box.	Tecnologia	Rede	Identificar	IG2
18.3	Corrigir as descobertas do teste de invasão	Corrija as descobertas do teste de invasão com base na política da empresa para o escopo e a priorização da correção.	Tecnologia	Rede	Proteger	IG2
18.4	Validar as Medidas de Segurança	Valide as medidas de segurança após cada teste de invasão. Se necessário, modifique os conjuntos de regras e recursos para detectar as técnicas usadas durante o teste.	Tecnologia	Rede	Proteger	IG3
18.5	Realizar testes de invasão internos periódicos	Realize testes de invasão internos periódicos com base nos requisitos do programa, pelo menos uma vez por ano. O teste pode ser clear box ou opaque box.	Tecnologia	Processo	Identificar	IG3
19.1	Possuir um programa de saúde mental	Possuir um programa preventivo voltado para a saúde e o bem-estar emocional/ mental dos servidores e colaboradores, reduzindo as possibilidades de cooptação por agentes mal-intencionados.	Ambiente Organizacional	Pessoas	Identificar	IG1
19.2	Favorecer a comunicação entre peritos e julgadores para evitar equívocos interpretativos	Favoreça a aproximação e a comunicação entre peritos e julgadores para o esclarecimento de eventuais dúvidas e assim evitar equívocos interpretativos	Ambiente Organizacional	Pessoas	Responder	IG1
19.3	Promover a cultura ética e de integridade	Promova a educação jurídica e a formação contínua para os profissionais do sistema de justiça, enfatizando a importância da ética, da imparcialidade e da integridade e dos limites de atuação do ator ou função.	Ambiente Organizacional	Pessoas	Identificar	IG1

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
19.4	Favorecer a correição e o controle independentes	Favoreça os órgãos independentes de supervisão e controle, exercendo o papel de supervisão pública para monitorar e investigar alegações de influência indevida.	Ambiente Organizacional	Pessoas	Detectar	IG2
20.01	Desenvolver planos de contingência e de sucessão	Identifique as funções e cargos críticos, avalie as habilidades e potencialidades dos servidores e defina estratégias de capacitação ou de equipes de trabalho multidisciplinares para que posições de liderança e de responsabilidade não fiquem descobertas em casos de ausências temporárias ou permanente (ex: férias, atestados, demissão, aposentadoria ou morte).	Competências	Pessoas	Identificar	IG1
20.02	Comunicar eficazmente a falta de recursos humanos	Comunique-se de forma clara, concisa e frequente com a alta administração sobre os riscos e prioridades para ajudar a evitar a falta de recursos humanos para os projetos, programas e atividades prioritários.	Competências	Pessoas	Identificar	IG1
20.03	Conscientizar a alta administração sobre as diferenças na distribuição dos processos	Conscientize a alta administração que um algoritmo aleatório pode ocorrer diferenças na distribuição dos processos, contudo no decorrer do tempo essas diferenças são equalizadas.	Competências	Pessoas	Identificar	IG1
20.04	Flexibilizar a contratação de especialistas para lidar com assunto de alta complexidade técnica	Flexibilize a possibilidade de contratação de especialistas ou perito externo para atuar em assunto excepcional ou de alta complexidade técnica	Competências	Pessoas	Responder	IG2
20.05	Capacitar tecnicamente magistrados e gestores para evitar falhas de interpretação	Capacite minimamente os magistrados e a alta administração para evitar problemas de comunicação e falhas de interpretação ao analisar laudos e perícias técnicas.	Competências	Pessoas	Identificar	IG2

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
20.06	Avaliar criticamente a qualificação do perito contratado	Avalie criticamente a qualificação e o perfil profissional de prováveis peritos frente à sua área de atuação.	Competências	Pessoas	Detectar	IG1
20.07	Investir na capacitação de servidores	Invista e priorize a capacitação de servidores visando a retenção e multiplicação do conhecimento.	Competências	Pessoas	Identificar	IG1
20.08	Realizar avaliação psicológica	Realize a avaliação psicológica regular de pessoas que ocuparão cargos chave de assessoramento dos órgãos de cúpula, que desempenharão atividades críticas de inteligência ou que terão acesso a informações ultrassecretas.	Competências	Pessoas	Identificar	IG3
20.09	Oferecer treinamento sobre técnicas de gerenciamento de tempo	Ofereça treinamento sobre e a importância do cumprimento dos prazos, podendo incluir orientações sobre técnicas de gerenciamento de tempo e estratégias para lidar com prazos exíguos. Certifique-se de que todos os envolvidos estejam cientes dos prazos estabelecidos e da necessidade de ser pontual.	Competências	Pessoas	Proteger	IG2
20.10	Selecionar assessores jurídicos qualificados	Selecione assessores jurídicos qualificados para auxiliar os julgadores na revisão das peças processuais, pesquisa legal e preparação de minutas de decisões. A equipe de apoio pode fornecer informações adicionais e análises que permitiram ao julgador tomar decisões fundamentadas.	Competências	Pessoas	Identificar	IG1
20.11	Promover a capacitação de usuários de IA sobre as capacidades, limitações e o uso ético da tecnologia	Promova programas de capacitação para os usuários da ferramenta, incluindo magistrados, servidores, estagiários e colaboradores dos órgãos, visando a compreenção das capacidades, limitações e o uso ético da Inteligência Artificial (IA).	Competências	Informação	Identificar	IG1

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
21.01	Gerenciar os riscos para autoridades do Poder Judiciário e possuir protocolos de segurança	Gerencie os riscos de continuidade de negócios relacionados à segurança de autoridades do Poder Judiciário por meio de um processo que identifique, analise, avalie e trate esses riscos. O tratamento dos riscos pode incluir protocolos que prevejam o não compartilhamento de meios de transporte, hospedagens em locais diferentes, escolta, vigilância, rotas seguras, monitoramento de dark web, zonas de exclusão e varreduras de segurança em locais comuns.	Estratégia	Pessoas	Identificar	IG1
21.02	Desenvolver estratégias de continuidade	Desenvolva planos de continuidade para antever e prevenir incidentes ou desastres, criar contingências e garantir a rápida recuperação.	Estratégia	Informação	Identificar	IG1
21.03	Fomentar parcerias entre órgãos públicos e a academia	Fomente parcerias entre os órgãos da Administração Pública e as universidades brasileiras para o desenvolvimento conjunto e a integração de soluções de tecnologia da informação, contribuindo para a produção mais eficiente e segura.	Estratégia	Informação	Identificar	IG3
21.04	Estimular a produção nacional de tecnologia da informação	Estimule a produção e o desenvolvimento de soluções nacionais de tecnologia da informação com base em avaliação de riscos que considere a criticidade das informações, a possibilidade de espionagem por Estados estrangeiros e a demanda interna.	Estratégia	Informação	Identificar	IG3
21.05	Promover a criação de um laboratório nacional de testes de segurança cibernética	Promova a criação de um laboratório nacional com instrumental e pessoal adequados para a realização de testes avançados de segurança cibernética para a avaliação de equipamentos de tecnologia.	Estratégia	Dispositivo	Identificar	IG3

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
21.06	Promover o intercâmbio internacional de tecnologias e a produção local de equipamentos	Promova a cooperação e o intercâmbio de tecnologias da informação com países amigos, objetivando o desenvolvimento conjunto de tecnologias próprias, a ampliação da oferta de soluções nacionais e a produção local de equipamentos, buscando evitar a quebra da produção em caso da deflagração de conflitos transnacionais.	Estratégia	Dispositivo	Identificar	IG3
21.07	Possuir um repositório central do código-fonte dos sistemas judiciais em que se façam análises de segurança	Possua um repositório central das diversas versões em uso do Pje e dos demais sistemas judiciais e implemente rotinas automatizadas de detecção de vulnerabilidades que incluam a análise estática do código-fonte a fim de se avaliar se boas práticas de desenvolvimento seguro estão senso seguidas, se existem dependências de componentes ou bibliotecas inseguras, se utilizam linguagens de programação obsoletas e possivelmente rodam em ambientes que não recebem atualizações segurança.	Estratégia	Aplicações	Detectar	IG2
21.08	Gerenciar os riscos relacionados a catástrofes naturais	Gerencie os riscos de continuidade de negócios relacionados aos desastres naturais por meio de um processo que identifique, analise, avalie e trate riscos de inundações, incêndios, terremotos, dentre outros, a que o órgão está exposto e desenvolva estratégias de mitigação dos riscos para evitar danos físicos ou a interrupção da prestação jurisdicional.	Estratégia	Informação	Identificar	IG1
21.09	Aprimorar a governança coorporativa e a gestão de pessoas	Defina claramente os objetivos estratégicos e o escopo dos projetos para garantir que os recursos humanos necessários sejam alocados adequadamente, levando em conta os possíveis riscos que podem impactar no alcance dos resultados pretendidos.	Estratégia	Pessoas	Identificar	IG1

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
21.10	Aprimorar a governança coorporativa e a gestão orçamentária	Defina claramente os objetivos estratégicos e o escopo dos projetos para garantir que os recursos financeiros necessários sejam alocados adequadamente, levando em conta os possíveis riscos que podem impactar no alcance dos resultados pretendidos.	Estratégia	Financeiro	Identificar	IG1
21.11	Estabelecer códigos de conduta ética e de limites de comunicação entre os atores do sistema de Justiça	Estabeleça códigos de conduta ética para juízes, promotores, procuradores e advogados que definam padrões claros sobre conflitos de interesse, aceitação de presentes ou benefícios e os limites para comunicações permitidas entre os atores do sistema de justiça.	Estratégia	Pessoas	Identificar	IG1
21.12	Regulamentar limites para as formas de convencimento e persuasão judicial	Regulamente claramente limites para as atividades de convencimento e persuasão judicial permitidas, incluindo a possibilidade de participação em eventos, seminários ou conferências patrocinados por grupos de interesse.	Estratégia	Pessoas	Identificar	IG2
21.13	Dar transparência e publicidade das comunicações com as partes e a participação em eventos	Dê transparência e publicidade das comunicações com as partes quando um envolvido no processo pedir audiência particular ou tornar pública a agenda dos julgadores e divulgar a participação em eventos, seminários e conferências patrocinados por terceiros.	Estratégia	Pessoas	Identificar	IG3
21.14	Estabelecer regras para a nomeação de parentes	Estabeleça regras para nomear parentes próximos para cargos de assessoria ou apoio em gabinetes	Estratégia	Pessoas	Identificar	IG1
21.15	Definir regras para gerenciar conflitos de interesse de julgadores	Defina diretrizes e regras para identificar e gerenciar conflitos de interesse reais ou aparentes quando da atuação de parentes ou pessoas com relações pessoais como advogados ou partes em processos sob competência de julgadores.	Estratégia	Pessoas	Identificar	IG1

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
21.16	Definir regras para gerenciar conflitos de interesse de assessores e analistas judiciários	Defina diretrizes e regras para identificar e gerenciar conflitos de interesse reais ou aparentes quando da atuação de parentes ou pessoas com relações pessoais, como advogados ou partes, em processos sob análise, revisão ou minuta de decisões de assessores e analistas judiciários.	Estratégia	Pessoas	Identificar	IG1
21.17	Estabelecer políticas e diretrizes claras sobre o uso de IA para a elaboração de despachos e decisões	Estabeleça políticas e diretrizes claras sobre como e quando o uso de Inteligência Artificial (IA) para a elaboração de despachos e decisões é apropriado, incluindo regras sobre como evitar a exposição de dados pessoais e informações protegidas por segredo de Justiça e preveja a necessidade de capacitação para os autorizados a utilizar a tecnologia.	Estratégia	Informação	Identificar	IG1
22.1	Priorizar a utilizar servidores públicos com boas recomendações que lidem com informações sigilosas	Priorize a utilização de servidores públicos com boas recomendações e busque reduzir o acesso de estagiários e terceirizados às informações de grande relevância ou sigilosas.	Estrutura	Pessoas	Identificar	IG1
22.2	Possuir quadro de pessoal compatível	Possua quadro de pessoal compatível com o volume de trabalho de forma que seja possível analisar com profundidade as peças processuais apresentadas pelas partes.	Estrutura	Pessoas	Proteger	IG2
22.3	Utilizar servidores públicos com boas recomendações no desenvolvimento de sistemas críticos	Priorize a utilização de servidores públicos com boas recomendações e busque reduzir a utilização de estagiários e terceirizados que atuam no desenvolvimento de sistemas críticos.	Estrutura	Pessoas	Identificar	IG1
23.01	Realizar testes regulares de continuidade e integridade	Realize testes de integridade em equipamentos para detectar possíveis falhas e garantir a continuidades dos serviços.	Gestão	Dispositivo	Detectar	IG1

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
23.02	Criar programas de testes e de auditoria para aferir a aleatoriedade dos sorteios em sistemas judiciais	Crie programas de testes internos e de auditoria por órgãos de controle e correição para aferir a aleatoriedade do sorteio de processos em sistemas judiciais.	Gestão	Aplicações	Detectar	IG2
23.03	Priorizar atividades e projetos e alocar pessoas conforme a criticidade	Priorize as atividades e projetos que são críticos para o alcance dos objetivos estratégicos, permitindo que os recursos humanos sejam alocados de forma mais eficiente e eficaz.	Gestão	Pessoas	Identificar	IG1
23.04	Estimar realisticamente as necessidades de recursos humanos	Estime de forma realista as necessidades de recursos humanos para evitar a falta de recursos. As estimativas devem ser baseadas em dados históricos e nas lições aprendidas de projetos anteriores semelhantes.	Gestão	Pessoas	Identificar	IG2
23.05	Priorizar atividades e projetos críticos e alocar recursos financeiros conforme a criticidade	Priorize os projetos e atividades que são críticas para o alcance dos objetivos estratégicos, permitindo que os recursos financeiros sejam alocados de forma mais eficiente e eficaz.	Gestão	Financeiro	Identificar	IG1
23.06	Estimar realisticamente as necessidades de recursos materiais e o seu custo	Estime de forma realista as necessidades de recursos materiais e o seu custo para evitar a falta de recursos. As estimativas devem ser baseadas em dados históricos e nas lições aprendidas de projetos anteriores semelhantes.	Gestão	Financeiro	Identificar	IG2
23.07	Gerir projetos e processos para detectar a falta de recursos humanos em tempo hábil	Monitore e controle os projetos e processos para evitar a falta de recursos humanos. Deve-se estabelecer indicadores de desempenho e acompanhar o progresso para identificar problemas e tomar ações corretivas em tempo hábil.	Gestão	Pessoas	Responder	IG3
23.08	Gerir projetos e processos para detectar a falta de recursos materiais em tempo hábil	Monitore e controle os projetos e processos para evitar a falta de recursos financeiros. Deve-se estabelecer indicadores de desempenho e acompanhar o progresso para identificar problemas e tomar ações corretivas em tempo hábil.	Gestão	Financeiro	Responder	IG3

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
23.09	Estabelecer uma política de gestão de pessoas para reter talentos e desenvolver habilidades	Estabeleça uma política de gestão de pessoas que defina as diretrizes e práticas para atrair e reter talentos, desenvolver habilidades, manter a remuneração e benefícios atrativos e contribuir para a saúde e bem-estar dos membros, servidores e colaboradores.	Gestão	Pessoas	Identificar	IG2
23.10	Racionalizar investimentos em segurança cibernética com base em gestão de riscos	Racionalize os investimentos em soluções de segurança cibernética, de forma que os controles de segurança sejam priorizados e implementados para o tratamentos dos riscos mais relevantes, em conformidade com processo de avaliação de riscos.	Gestão	Financeiro	Identificar	IG2
23.11	Padronizar diretrizes e procedimentos para lidar com ações duplicadas	Padronize as diretrizes e os procedimentos para a identificação de ações duplicadas e que medidas devem ser tomadas	Gestão	Processo	Identificar	IG1
23.12	Estabelecer medidas disciplinares ou sanções para o descumprimento injustificado de prazos	Estabeleça medidas disciplinares ou sanções cabíveis para os casos de descumprimento injustificado dos prazos processuais.	Gestão	Pessoas	Identificar	IG2
24.1	Utilizar mecanismos de detecção de comportamentos padrão de acessos e estabeleça políticas de acesso condicional	Utilize mecanismos que tracem uma linha padrão de acessos dos usuários e estabeleçam condições de segurança adicionais para os acessos fora de padrão (horários, origem geográfica, ações)	Identidade e acesso	Pessoas	Proteger	IG1
25.1	Avaliar a evolução profissional e econômica	Implemente ações de inteligência ou parcerias com autoridades competentes para avaliação da compatibilidade social, financeira, patrimonial e de ascensão profissional para cargos de assessoramento em órgãos de cúpula, que desempenharão atividades críticas de inteligência ou que terão acesso a dados ultrassecretos.	Inteligência	Pessoas	Detectar	IG3

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
25.2	Monitorar comunidades e fóruns	Monitore menções aos órgãos e autoridades em comunidades e fóruns fechados que indiquem a contratação de pessoas, a existência de insiders, a coordenação de ataques ou a venda de informações.	Inteligência	Dados	Detectar	IG3
25.3	Avaliar antecedentes de pessoas com acesso antecipado a decisões em Tribunais Superiores ou acesso a informações secretas	Implemente ações de inteligência ou parcerias com autoridades competentes para a avaliação de antecedentes para pessoas que tenham acesso antecipado a votos, determinações ou decisões em Tribunais Superiores ou que terão acesso a informações secretas. Podendo incluir a verificação de dados: pessoais, profissionais, comerciais, criminais, associações políticas e sociais.	Inteligência	Pessoas	Identificar	IG1
25.4	Investigar redes sociais e verificar de conflitos de interesse	Verifique atividades em redes sociais para obter informações adicionais sobre personalidade, comportamento e conexões. A verificação de conexões empresariais e de negócios passados podem também ajudar a identificar possíveis conflitos de interesse.	Inteligência	Pessoas	Identificar	IG3
25.5	Implementar monitoramento eletrônico	Realize atividades de inteligência ou parcerias com autoridades competentes para o monitoramento eletrônico regular de pessoas que ocuparão cargos chave de assessoramento dos órgãos de cúpula, que desempenharão atividades críticas de inteligência ou que terão acesso a dados ultrassecretos para detectar de atividades ou ligações suspeitas.	Inteligência	Pessoas	Identificar	IG3
25.6	Avaliar antecedentes de desenvolvedores ou DBAs que atuam em sistemas judiciais ou sistemas críticos	Implemente ações de inteligência ou parcerias com autoridades competentes para a avaliação de antecedentes de pessoas que atuam no desenvolvimento ou gestão de banco de dados de sistemas judiciais ou críticos para a instituição. Podendo incluir a verificação de dados: pessoais, profissionais, comerciais, criminais, associações políticas e sociais.	Inteligência	Pessoas	Identificar	IG1

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
26.01	Segregar funções de programação, avaliação de qualidade e auditoria de código-fonte sensível	Segregue as funções de programação, avaliação de qualidade e auditoria de código-fonte sensível, evitando que uma mesma pessoa ou equipe seja responsável por todas as etapas de programação para diminuir a probabilidade de fraudes ou favorecimentos.	Processos de Trabalho	Aplicações	Identificar	IG2
26.02	Evitar inserir notas ou comentários internos em minutas de documentos	Evite inserir notas ou comentários internos da equipe ou direcionados ao decisor no corpo do documento que está em elaboração, evitando que acidentalmente esses comentários sejam mantidos na versão final.	Processos de Trabalho	Pessoas	Identificar	IG1
26.03	Implementar dupla aprovação para ações críticas nos sistemas de informação	Implemente processo no qual sejam segregadas as funções críticas e que não seja possível que apenas uma pessoa finalize, aprove ou modifique documentos sensíveis, tais como levantamento de valores elevados ou a expedição de decisões relevantes	Processos de Trabalho	Aplicações	Proteger	IG2
26.04	Comunicar eficazmente a falta de recursos financeiros	Comunique-se de forma clara, concisa e frequente com a alta administração sobre os riscos e prioridades para ajudar a evitar a falta de recursos financeiros para os projetos, programas e atividades prioritários.	Processos de Trabalho	Financeiro	Identificar	IG2
26.05	Solicitar a suspensão dos processos quando identificada a duplicidade de ações	Solicite a suspensão dos processos quando identificada a duplicidade de ações até que se decida o juízo competente para julgar o caso, evitando o prosseguimento simultâneo.	Processos de Trabalho	Informação	Responder	IG2

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
26.06	Verificar visualmente o documento físico e validar assinaturas físicas	Verifique o documento em busca de características físicas que possam indicar sua autenticidade, como marca d'água, hologramas, selos, assinaturas originais, carimbos oficiais ou elementos de segurança específicos para o tipo de documento, quando aplicável. Exemplo: autenticação em cartório.	Processos de Trabalho	Informação	Detectar	IG1
26.07	Comparar informações com documentos de referência	Compare as cópias ou informações fornecidas com os documentos autênticos de referência. Por exemplo, ao receber uma identificação pessoal, compare com uma identificação emitida oficialmente pelo órgão competente.	Processos de Trabalho	Informação	Detectar	IG1
26.08	Utilizar métodos de validação de documentos digitais	Utilize mecanismos de validação de documentos digitais e não presuma que são autênticos. Sempre que possível, verifique assinaturas digitais em software confiável, faça o checksum de arquivos, acesse o link ou QR code de validação dos emissores e comparece com as informações fornecidas.	Processos de Trabalho	Informação	Detectar	IG1
26.09	Consultar o emissor do documento	Consulte a instituição ou a pessoa responsável pela emissão do documento e verifique diretamente a sua autenticidade. A depender da natureza do documento e do contexto utilizado, a verificação pode ser por telefone, e-mail ou pessoalmente.	Processos de Trabalho	Informação	Detectar	IG2
26.10	Consultar especialistas em caso de dúvidas quanto a autenticidade de documentos	Consulte especialistas em casos complexos ou de alta relevância. Pode-se utilizar da opinião de especialistas forenses, peritos em caligrafia ou outros profissionais qualificados para verificar a autenticidade.	Processos de Trabalho	Informação	Responder	IG3

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
26.11	Sistematizar e monitorar o controle de prazos processuais	Sistematize e monitore de forma eficiente o controle dos prazos processuais, utilize calendários ou softwares específicos para acompanhar e alertar sobre prioridades e evitar que prazos sejam esquecidos ou negligenciados.	Processos de Trabalho	Processo	Identificar	IG2
26.12	Validar informações de resumos elaborados por partes interessadas	Valide as informações apresentadas em resumos de processos volumosos e que passaram por diversas instâncias pois informações relevantes podem ter sido omitidas para conduzir a uma avaliação parcial e conveniente para uma das partes.	Processos de Trabalho	Informação	Detectar	IG1
26.13	Segmentar funções e revisar análises preliminares	Segmente em diferentes etapas as funções de análise, elaboração e revisão de minutas com o objetivo de reduzir o risco de incorreções de linguagem, erros materiais, equívocos interpretativos e falta de alinhamento com o posicionamento do julgador.	Processos de Trabalho	Processo	Detectar	IG1
26.14	Realizar audiências e exposições orais para a melhor compreensão do caso	Realize audiências e exposições orais para que as partes destaquem informações contidas nas peças processuais, proporcionando a compreensão mais completa do caso previamente à decisão.	Processos de Trabalho	Informação	Identificar	IG2
26.15	Solicitar esclarecimentos adicionais	Solicite esclarecimentos adicionais em caso de dúvidas ou informações insuficientes, requisitando documentos complementares ou pedindo esclarecimentos sobre pontos específicos.	Processos de Trabalho	Informação	Identificar	IG2

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
26.16	Estabelecer um processo de supervisão e revisão humana de decisões ou documentos gerados por IA	Estabeleça um processo de supervisão humana, em que as decisões ou documentos gerados por Inteligência Artificial (IA) sejam revisados por profissionais qualificados para garantir que os documentos estejam adequados do ponto de vista legal e com princípios éticos.	Processos de Trabalho	Informação	Identificar	IG1
27.1	Implementar barreiras físicas adicionais e a identificação e autorização específicas para acesso às áreas sensíveis	Implemente barreiras físicas adicionais, tais como portas, catracas, fechaduras magnéticas, coletores biométricos e alarmes, e a necessidade de identificação e autorização adicionais para acesso às áreas sensíveis das instalações internas (ex: gabinetes, datacenter, infraestrutura elétrica). Esses sistemas podem ser integrados com câmeras de vigilância e alarmes e serem utilizados no monitoramento ativo.	Segurança física	Instalações	Proteger	IG1
27.2	Proteger o perímetro das instalações	Proteja o perímetro das instalações com cercas e portões de acesso, podendo ser implementados proteções adicionais como detectores de metal, aparelhos de raio-x, sensores de movimento e alarmes para detectar intrusões.	Segurança física	Instalações	Proteger	IG1
27.3	Instalar vigilância por câmeras	Instale câmeras de vigilância para monitorar o perímetro e as instalações internas de intrusos e mantenho registro das gravações por tempo adequado. Preferencialmente utilize equipamentos com recursos de detecção de movimento, visão noturna, com alta qualidade de vídeo e capacidade de aproximação (zoom).	Segurança física	Instalações	Detectar	IG1
27.4	Possuir equipe de segurança monitorar ativamente as atividades suspeitas	Possuir equipe de segurança para monitorar ativamente as atividades suspeitas dentro e fora das instalações.	Segurança física	Instalações	Detectar	IG1

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
27.5	Realizar varreduras ambientais em ambientes críticos	Realize varreduras ambientais em ambiente críticos tais como datacenters ou gabinetes de desembargadores e ministros a fim de encontrar escutas ou dispositivos físicos de captura de comunicações ou dados.	Segurança física	Dados	Detectar	IG3
27.6	Monitorar condições climáticas do ambiente	Monitore as condições climáticas do ambiente para evitar que temperaturas elevadas ou umidade excessiva possam danificar equipamentos eletrônicos resultando em falhas ou perda de dados.	Segurança física	Dispositivo	Detectar	IG1
28.01	Configurar limites de banda de tráfego	Configure limites de largura de banda consumida, quantidade de conexões simultâneas abertas ou de requisições por usuário para ajudar a limitar a quantidade de tráfego enviado ao servidor, reduzindo o impacto de um ataque de DDoS.	Tecnologia	Rede	Proteger	IG1
28.02	Implementar abordagens de confiança zero (zero trust)	Implemente abordagens de confiança zero (zero trust) para que mesmo os usuários, os dispositivos e as comunicações internos sejam continuamente avaliados e protegidos.	Tecnologia	Rede	Proteger	IG3
28.03	Controlar alterações e garantir a custódia do código-fonte	Controle as alterações software, mantenha o histórico de cada versão modificada e verifique a integridade do código-fonte para garantir que não tenha sido indevidamente modificado. Pode ser utilizada função hash, sistema de controle de versão ou assinatura do código para garantir que o código-fonte não foi adulterado.	Tecnologia	Aplicações	Proteger	IG1
28.04	Microssegmentar comunicações de rede	Microssegmente as comunicações de rede para reduzir movimentações laterais e conter a propagação de malwares	Tecnologia	Rede	Proteger	IG3
28.05	Monitorar o tráfego e estabelecer padrões	Monitore o tráfego de rede, estabeleça padrões e crie alertas para desvios incomuns de tráfego que indiquem um ataque de DDoS.	Tecnologia	Rede	Detectar	IG1

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
28.06	Balancear a carga entre equipamentos de infraestrutura	Balanceie e distribua a carga entre vários equipamentos de infraestrutura para evitar a sobrecarga de um único ponto. Utilize hardware dedicado ou software de balanceamento de carga.	Tecnologia	Dispositivo	Responder	IG1
28.07	Utilizar infraestrutura elástica	Utilize arquitetura em que os recursos de computação, armazenamento e rede são dimensionados automaticamente de acordo com as necessidades de processamento e de tráfego de dados em tempo real. Reduzindo ou escalando a infraestrutura conforme a demanda e sem a necessidade de intervenção humana. Sendo importante definir limite aceitável de recursos alocados para evitar o esgotamento total de recursos de infraestrutura on premisses ou a grande elevação de custos de serviços em nuvem.	Tecnologia	Dispositivo	Responder	IG2
28.08	Filtrar tráfego malicioso	Filtre e bloqueie tráfego suspeito, malicioso ou oriundo de botnets, com base na reputação dos endereços IP, filtragem de portas e protocolos.	Tecnologia	Rede	Proteger	IG1
28.09	Prevenir falsificação de endereço IP (spoofing)	Previna spoofing de IP para ajudar a reduzir ataques de DDoS. Utilize técnicas de autenticação de origem, como a verificação de roteamento de pacotes (RPV) ou a autenticação de mensagem de domínio baseada em assinatura (DomainKeys Identified Mail - DKIM).	Tecnologia	Rede	Proteger	IG2
28.10	Sanitizar o tráfego na operadora	Sanitize o tráfego ainda na operadora, evitando a saturação da capacidade de tráfego dos enlaces de comunicação.	Tecnologia	Rede	Responder	IG1
28.11	Utilizar serviço de sanitização de tráfego em ambiente de terceiro	Utilize serviço de sanitização de tráfego em provedor de serviço de borda de acesso seguro (SASE) de forma que apenas o tráfego legítimo seja direcionado para o ambiente da instituição.	Tecnologia	Rede	Proteger	IG3

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
28.12	Monitorar os recursos de infraestrutura	Implemente sistemas de monitoramento para alertar sobre a elevação de consumo de recursos que poderão levar a uma falha, caso a equipe de TI não atue, bem alertar sobre possíveis falhas em componentes de hardware (ex: discos, processadores, fontes de alimentação etc).	Tecnologia	Dispositivo	Detectar	IG1
28.13	Manter infraestrutura crítica em redundância	Mantenha sistemas de redundância para garantir que, caso ocorra a falha de um elemento crítico de infraestrutura (hardware e software), outro possa assumir a carga de trabalho automaticamente.	Tecnologia	Dispositivo	Responder	IG1
28.14	Realizar atualizações preventivas e de segurança em ativos de infraestrutura	Realize atualizações regulares de firmware e software bem como a manutenção preventiva em equipamentos para evitar falhas devido a problemas de compatibilidade ou degradação pelo uso.	Tecnologia	Dispositivo	Identificar	IG1
28.15	Utilizar fontes de aleatoriedade confiáveis	Avalie se o algoritmo utiliza uma fonte de aleatoriedade confiável e imprevisível. Geradores de números aleatórios e criptograficamente seguros podem ser produzidos em software ou hardware e utilizar fontes de ruído térmico em circuitos eletrônicos, ruído atmosférico captado ou funções matemáticas em cadeia, dentre outros. Esta avaliação deve ocorrer periodicamente considerando as evoluções constantes nesse campo de estudo.	Tecnologia	Aplicações	Proteger	IG1
28.16	Verificar a integridade dos documentos transmitidos eletronicamente	Verifique se os webservices, APIs ou sistemas possuem regras para atestar a integridade dos documentos transmitidos eletronicamente. Podem ser implementadas verificações de hash, de metadados dos arquivos e a assinatura digital para a verificação da integridade dos documentos eletrônicos.	Tecnologia	Aplicações	Detectar	IG1

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
28.17	Adaptar os sistemas judiciais para utilização da tecnologia blockchain	Adapte os sistemas judiciais para a utilização da tecnologia blockchain para o registro de transações e informações de forma segura e descentralizada, validando e registrando as informações de forma transparente e imutável. O blockchain pode garantir a integridade dos dados, a autenticidade da origem e a transparência da troca.	Tecnologia	Aplicações	Proteger	IG3
28.18	Priorizar a transferência eletrônica de documentos pela integração de sistemas de órgãos da administração pública	Priorize a transferência eletrônica de documentos realizada por meio da integração de sistemas de órgãos da Administração Pública. A verificação de autenticidade de documentos físicos ou de documentos eletrônicos enviados por e-mail é mais difícil e requer conhecimentos específicos das várias técnicas de falsificação utilizadas, demandando a capacitação de muitas pessoas, de dupla verificação e da possibilidade de ataques de engenharia social.	Tecnologia	Aplicações	Proteger	IG1
28.19	Analisar a emissão eletromagnética	Analise a emissão eletromagnética para identificar a comunicação de possíveis dispositivos de comunicação. Envolve a utilização de equipamentos especializados para detectar a emissão eletromagnética.	Tecnologia	Dispositivo	Detectar	IG2
28.20	Automatizar a verificação de ações semelhantes por meio de robôs ou IA	Automatize a consulta e verificação de processos em outros tribunais ou em uma base central de processos que possuam as mesmas partes, classes, subclasses ou assuntos processuais por meio do uso de robôs ou utilize inteligência artificial para comparar o teor das petições iniciais e indicar a possibilidade da duplicidade de ações no mesmo órgão.	Tecnologia	Aplicações	Responder	IG3
28.21	Integrar a comunicação entre os sistemas judiciais ou criar base nacional de processos judiciais	Integre a comunicação entre os sistemas judiciais e compartilhe informações sobre as ações no acervo de cada órgão ou a manutenção de base nacional de processos judiciais, possibilitando a consulta e a identificação de processos semelhantes.	Tecnologia	Aplicações	Identificar	IG2

Tabela 2 - continuação da página anterior

Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança	Categoria do Controle	Tipo de Ativo	Função de Segurança	Prioridade de Implantação
28.22	Automatizar a execução dos atos processuais decorrentes do descumprimento de prazos	Automatize no sistema judicial a execução dos atos processuais decorrentes do descumprimento injustificado do prazos pelas partes.	Tecnologia	Aplicações	Responder	IG3
28.23	Desmontar o dispositivo e analisar os componentes	Desmonte o dispositivo e analise os componentes que poderiam permitir a captura ou gravação de áudio ou vídeo, transmissões de rádio ou a comunicação remota	Tecnologia	Dispositivo	Detectar	IG3

.3 PAINÉIS DE BUSINESS INTELLIGENCE - BI

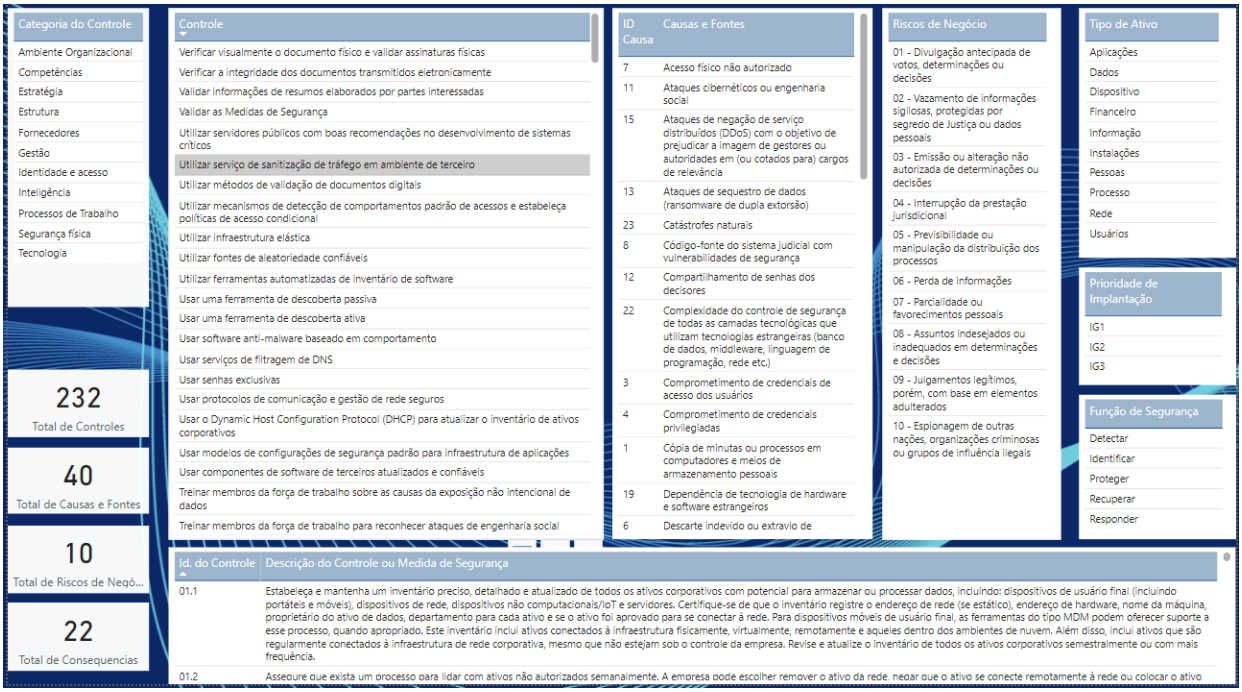


Figura 1: Visão geral
Fonte: do Autor

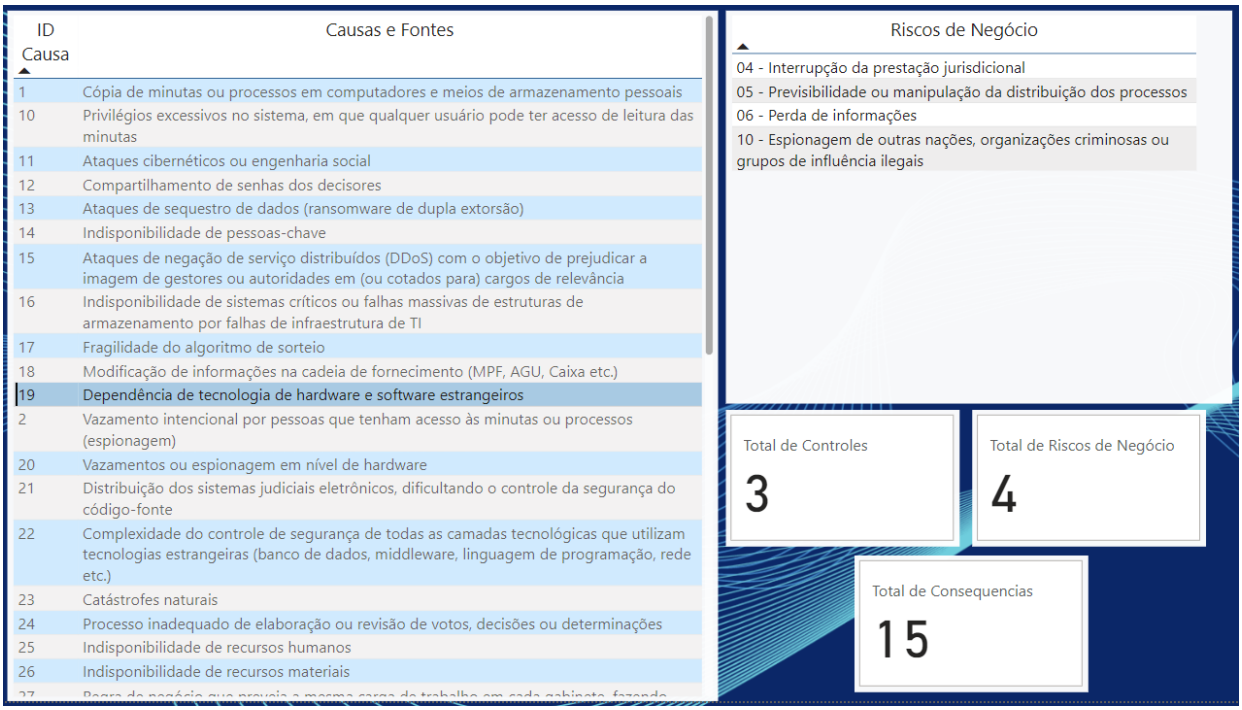


Figura 2: Relações das causas dos riscos de negócio
Fonte: do Autor

Figura 3: Total de consequências por risco de negócio
Fonte: do Autor

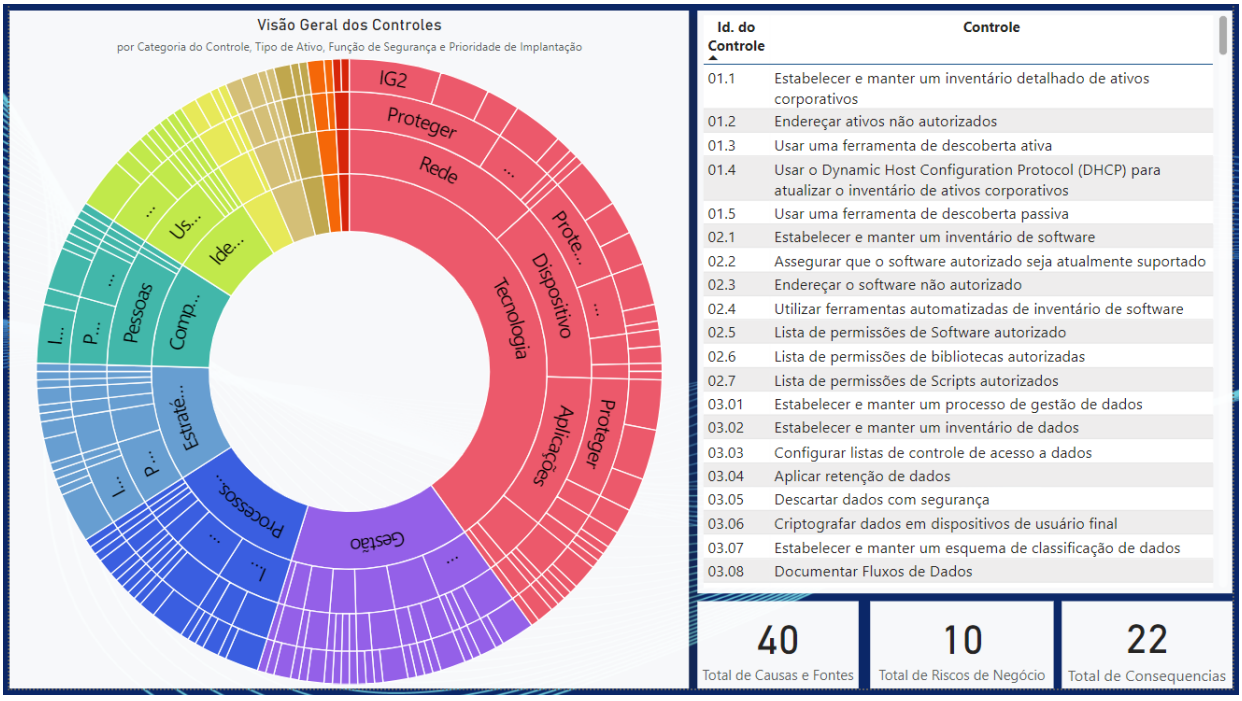
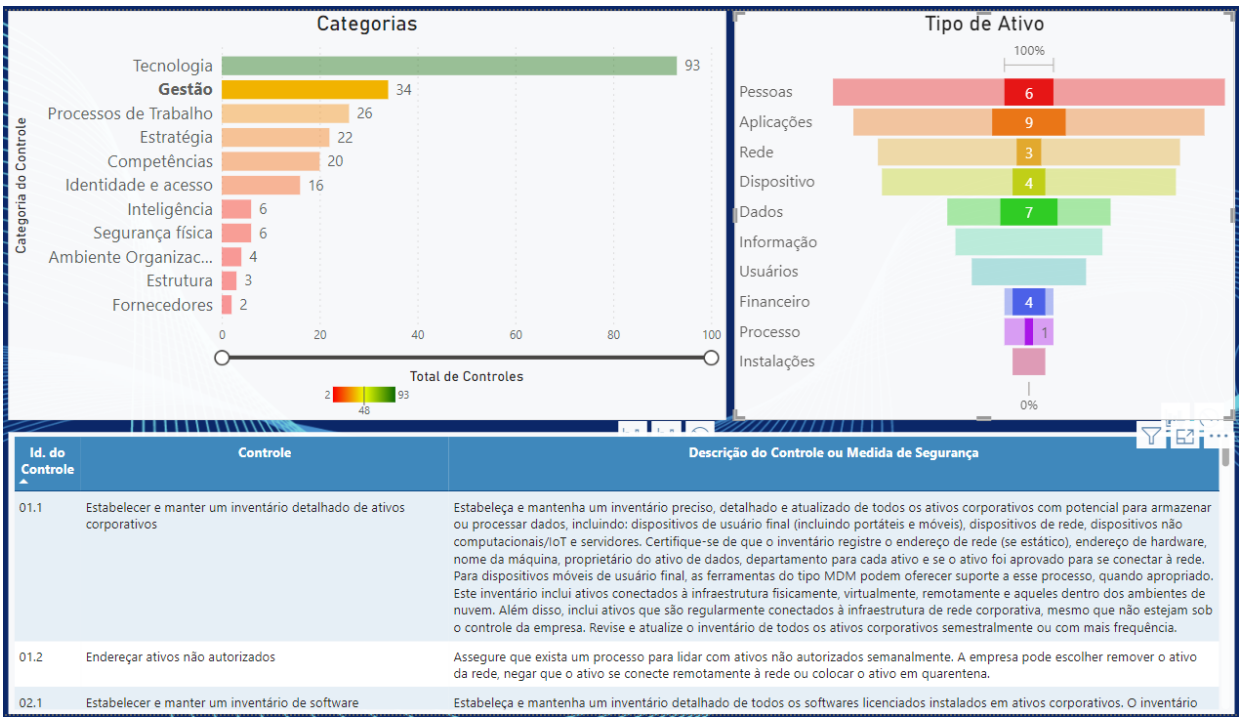
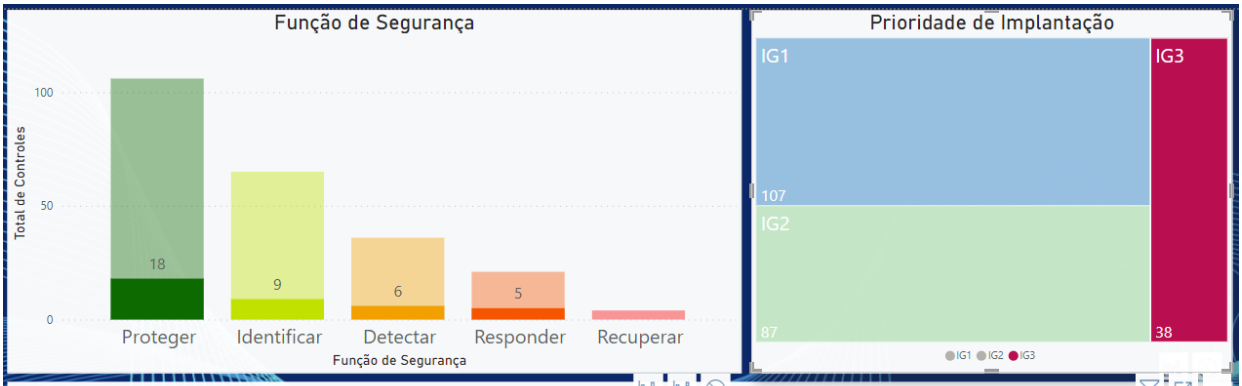


Figura 4: Painel geral para filtragem e seleção de controles por meio da associação entre categoria do controle, ativo envolvido, função de segurança e prioridade de implantação.
Fonte: do Autor



Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança
01.1	Estabelecer e manter um inventário detalhado de ativos corporativos	Estabeleça e mantenha um inventário preciso, detalhado e atualizado de todos os ativos corporativos com potencial para armazenar ou processar dados, incluindo: dispositivos de usuário final (incluindo portáteis e móveis), dispositivos de rede, dispositivos não computacionais/IoT e servidores. Certifique-se de que o inventário registre o endereço de rede (se estático), endereço de hardware, nome da máquina, proprietário do ativo de dados, departamento para cada ativo e se o ativo foi aprovado para se conectar à rede. Para dispositivos móveis de usuário final, as ferramentas do tipo MDM podem oferecer suporte a esse processo, quando apropriado. Este inventário inclui ativos conectados à infraestrutura fisicamente, virtualmente, remotamente e aqueles dentro dos ambientes de nuvem. Além disso, inclui ativos que são regularmente conectados à infraestrutura de rede corporativa, mesmo que não estejam sob o controle da empresa. Revise e atualize o inventário de todos os ativos corporativos semestralmente ou com mais frequência.
01.2	Endereçar ativos não autorizados	Assegure que exista um processo para lidar com ativos não autorizados semanalmente. A empresa pode escolher remover o ativo da rede, negar que o ativo se conecte remotamente à rede ou colocar o ativo em quarentena.
02.1	Estabelecer e manter um inventário de software	Estabeleça e mantenha um inventário detalhado de todos os softwares licenciados instalados em ativos corporativos. O inventário

Figura 5: Relações entre categorias dos controles e tipos de ativos.
Fonte: do Autor



Id. do Controle	Controle	Descrição do Controle ou Medida de Segurança
01.5	Usar uma ferramenta de descoberta passiva	Use uma ferramenta de descoberta passiva para identificar ativos conectados à rede corporativa. Revise e use varreduras para atualizar o inventário de ativos corporativos pelo menos semanalmente ou com mais frequência.
02.7	Lista de permissões de Scripts autorizados	Use controles técnicos, como assinaturas digitais e controle de versão, para garantir que apenas scripts autorizados, como arquivos .ps1, .py, etc. específicos, tenham permissão para executar. Bloqueie a execução de scripts não autorizados. Reavalie semestralmente ou com mais frequência.
03.13	Implantar uma solução de prevenção contra perda de dados	Implementar uma ferramenta automatizada, como uma ferramenta de prevenção de perda de dados (DLP) baseada em host para identificar todos os dados sensíveis armazenados, processados ou transmitidos por meio de ativos corporativos, incluindo aqueles localizados no site local ou em um provedor de serviços remoto, e atualizar o inventário de dados sensíveis da empresa.
03.14	Registrar o acesso a dados sensíveis	Registre o acesso a dados sensíveis, incluindo modificação e descarte.
04.12	Separar os Espaços de Trabalho Corporativos nos dispositivos móveis	Certifique-se de que a separação de espaços de trabalho corporativos seja usada nos dispositivos móveis de usuário final, onde houver suporte. Exemplos de implementações incluem o uso de um Apple® Configuration Profile ou Android ™ Work Profile para separar aplicações e dados corporativos de aplicações e dados pessoais.

Figura 6: Relações entre funções de segurança e prioridades de implantação.
Fonte: do Autor

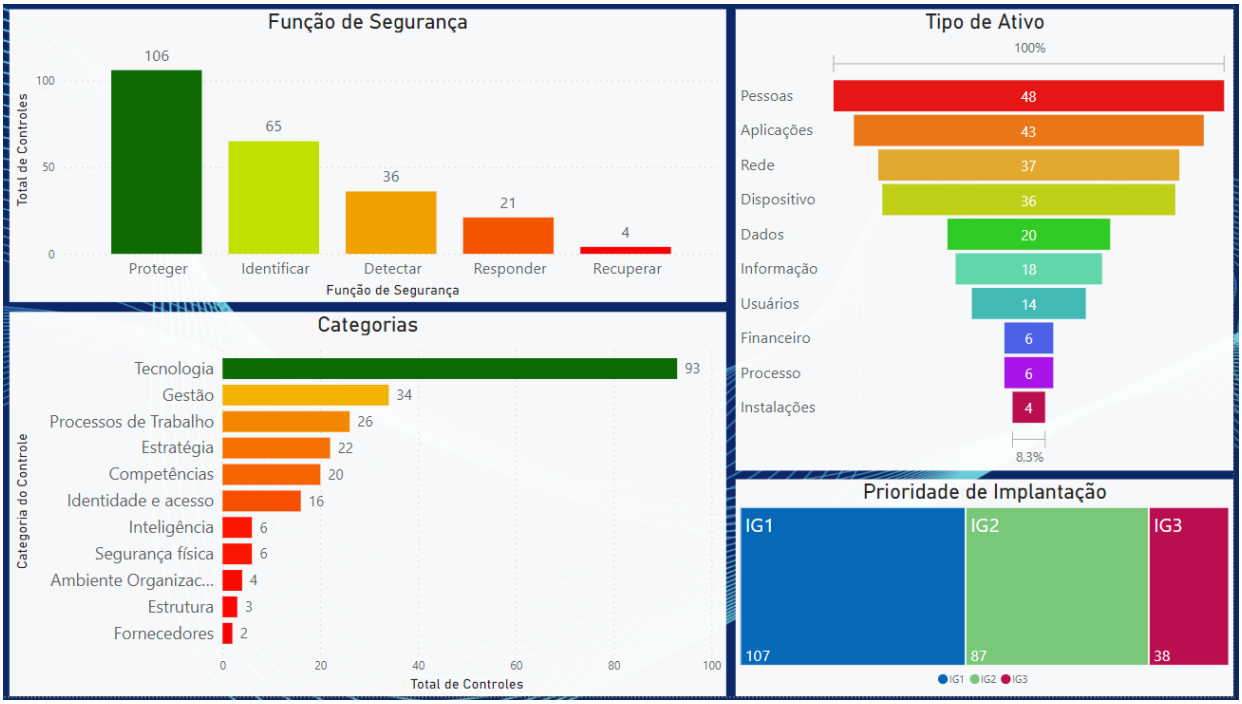


Figura 7: Painel geral de interações entre as classificações dos controles.
Fonte: do Autor

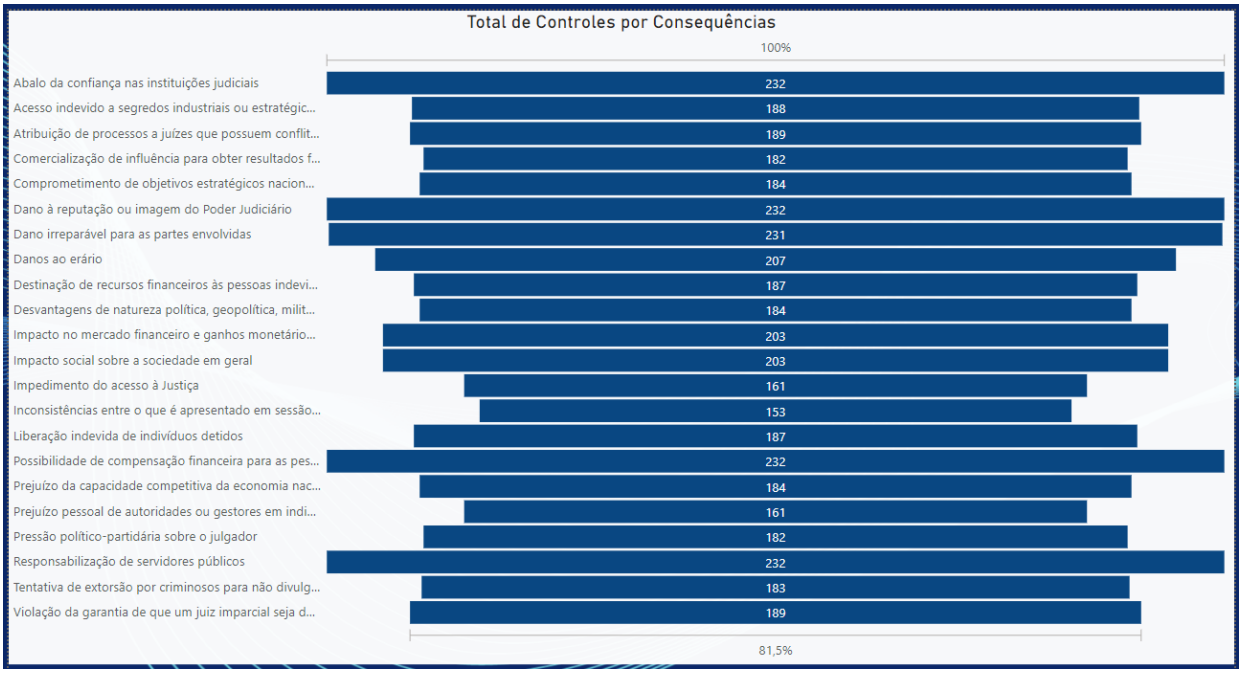


Figura 8: Quantidade de controles relacionados com cada consequência dos riscos de negócio.
Fonte: do Autor

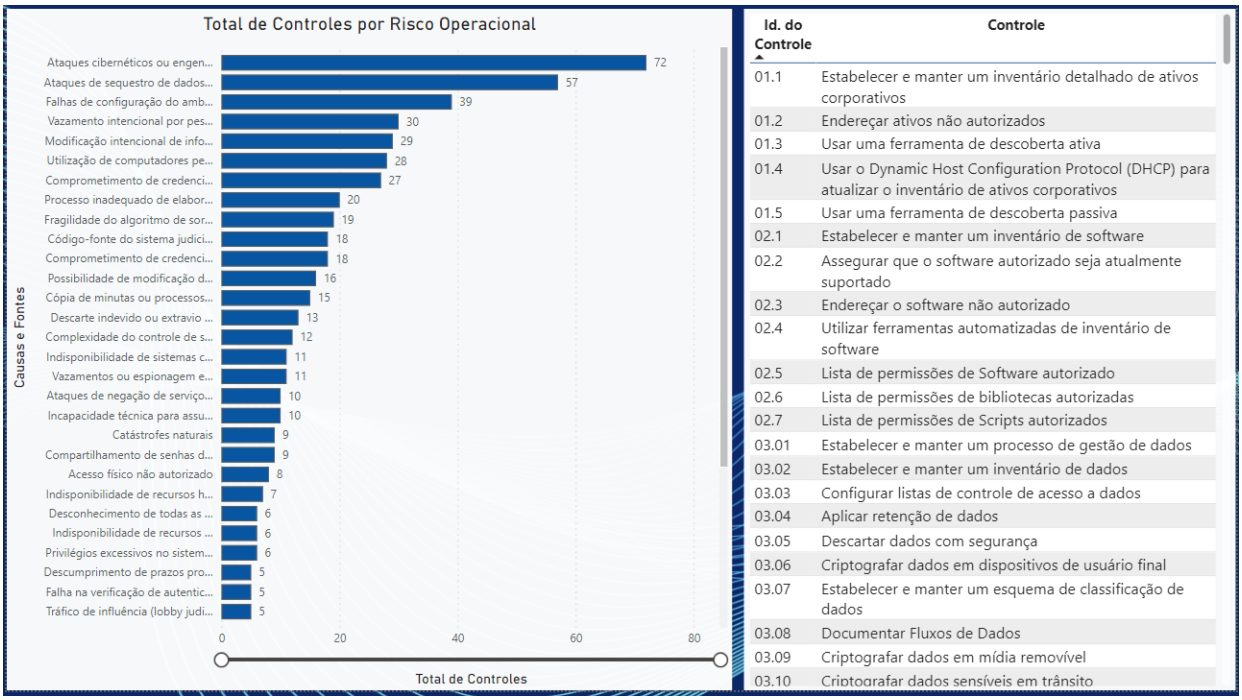


Figura 9: Quantidade de controles por cada risco operacional.
Fonte: do Autor