A GESTÃO DE RISCOS CIBERNÉTICOS NO FUTURO DOS INVESTIMENTOS PÚBLICOS

Cícero Araujo Lisboa
Universidade Federal do Rio Grande do Sul (UFRGS), Brasil
nbkall@gmail.com
Mauro de Almeida
Universidade do Vale do Rio dos Sinos (Unisinos), Brasil
marinho.info@gmail.com

Resumo
A crescente digitalização dos serviços públicos e a consequente exposição a ameaças cibernéticas demandam uma abordagem robusta e adaptada à realidade dos órgãos públicos brasileiros. A dependência de consultorias privadas, incluindo empresas estrangeiras, para a gestão de riscos cibernéticos, pode onerar os cofres públicos e, por vezes, apresentar soluções desalinhadas com as especificidades do contexto nacional. Diante desse cenário, este artigo propõe a criação de um *framework* de gestão de riscos cibernéticos concebido especificamente para órgãos públicos no Brasil. O objetivo central é oferecer uma estrutura metodológica que considere a legislação local, as particularidades operacionais e a criticidade dos ativos de informação dessas entidades. A pesquisa explorará modelos de gestão de riscos existentes, adaptando as melhores práticas de mercado ao setor público brasileiro e incorporando elementos que fortaleçam a autonomia e a capacidade interna das organizações na identificação, avaliação, tratamento e monitoramento de riscos cibernéticos. A metodologia envolverá uma revisão bibliográfica abrangente sobre gestão de riscos, segurança da informação e as especificidades do setor público, complementada por uma análise de *frameworks* de análise de risco relevantes, disponíveis no mercado. A proposta do *framework* será estruturada em etapas claras, desde a definição de políticas e responsabilidades até a implementação de controles. Espera-se que este trabalho auxilie na governança e conformidade da gestão de ativos, para um alinhamento adequado com as boas práticas do setor privado, dando um direcionamento assertivo nos investimentos necessários em tecnologias, e também auxiliando na busca de investimentos externos, através de programas internacionais de financiamento público. Dessa forma, o trabalho contribuirá para o avanço da gestão pública, oferecendo um modelo prático e eficiente para mitigar vulnerabilidades e proteger os ativos digitais dos órgãos públicos brasileiros, promovendo maior segurança e resiliência em seus serviços essenciais.

Palavras-chave: gestão de riscos; risco cibernético; framework.

1 Introdução

O presente artigo tem como objetivo principal discutir o risco cibernético envolvido em investimentos públicos, em especial o desenvolvimento de um *framework* para análise de riscos na administração pública. Nos últimos anos, a humanidade tem se transformado profundamente com uma revolução digital impulsionada pelo crescimento no acesso à internet e pela ampla adoção de novas tecnologias, como a Inteligência Artificial (IA). Segundo o *World Economic Forum*, a IA tem o potencial de transformar a economia global, com uma contribuição estimada de até 15 trilhões de dólares até 2030 (Gerrard *et al.*, 2019).

Neste cenário, as inovações também estão acontecendo no setor público no chamado Governo Digital. Este é um conceito transformador que se apoia em dois pilares essenciais: a adoção de novas tecnologias e uma mudança de mentalidade na administração pública (Cristina; Viana, 2021). Diferente do governo eletrônico, que focava na automação e redução de custos, o Governo Digital utiliza tecnologias disruptivas como Big Data, IoT, inteligência artificial e computação em nuvem para digitalizar processos de ponta a ponta (Cristina; Viana, 2021). Isso permite acesso flexível a recursos e fomenta a co-criação de serviços com cidadãos e empresas, colocando o usuário no centro e transformando-o em cocriador. Trata-se de uma abordagem holística que vai além da eficiência, buscando construir valor público e exigindo alinhamento de instituições, pessoas, tecnologia e dados para uma verdadeira transformação do setor público (Cristina; Viana, 2021).

O Brasil tem demonstrado um compromisso crescente com a transformação digital de sua administração pública, evidenciado por investimentos públicos significativos em tecnologia. Desde 2023, o Ministério da Ciência, Tecnologia e Inovação (MCTI) direcionou mais de R$ 26,3 bilhões do Fundo Nacional de Desenvolvimento Científico e Tecnológico (FNDCT), um valor que supera consideravelmente os anos anteriores e reflete a priorização da digitalização em programas como a Nova Indústria Brasil (NIB) e o Novo PAC (Brasil, 2024b). Além disso, a NIB prevê um investimento total de R$ 186,6 bilhões para a transformação digital da indústria, com R$ 42,2 bilhões já alocados pelo setor público (Brasil, 2024a). Essas alocações estratégicas de recursos visam não apenas a modernização administrativa, mas também o crescimento econômico e a inclusão social, consolidando a tecnologia como um facilitador transversal para o desenvolvimento nacional (Brasil, 2024b).

Esses investimentos são operacionalizados por diversos atores, como o Serpro e a Dataprev, que desempenham papéis estratégicos na infraestrutura e execução da transformação digital. O Serpro, por exemplo, investiu R$ 710 milhões na "Nuvem de Governo", um pilar crucial para a soberania das informações nacionais, com planos de incorporar inteligência artificial treinada com a cultura e linguagem brasileiras (Serpro, 2024). A Estratégia Nacional de Governo Digital (ENGD) e a Estratégia Federal de Governo Digital (EFGD) guiam esses esforços, buscando modernizar a gestão pública, aumentar a eficiência dos serviços e promover um Brasil mais inclusivo, garantindo acesso equitativo a serviços digitais para todos os cidadãos (Brasil, 2025).

Enquanto a Estratégia Nacional de Governo Digital (ENGD) e a Estratégia Federal de Governo Digital (EFGD) orientam os esforços em nível nacional, diversos estados brasileiros também têm desenvolvido iniciativas próprias para promover a transformação digital e aprimorar a gestão pública. O Rio Grande do Sul, por exemplo, apoia municípios através do programa RS Digital e unifica serviços no portal rs.gov.br, além de estimular negócios com o "Empreender RS" (Rio Grande do Sul, 2025). Minas Gerais possui uma Estratégia Estadual de Governo Digital focada em sistemas integrados e canais de atendimento eletrônico (Minas Gerais, 2024). São Paulo, por sua vez, tanto na capital quanto no estado, busca aproximar a gestão do cidadão e melhorar processos por meio de suas Estratégias de Transformação e Governo Digital (São Paulo, 2023). O Ceará, com o "Ceará Mais Digital", seleciona startups para desenvolver soluções inovadoras para a gestão pública e integração municipal, utilizando tecnologias emergentes (Ceará, 2025).

Apesar dos notáveis avanços e investimentos na transformação digital da gestão pública, o cenário cibernético brasileiro entre 2020 e 2025 foi marcado por uma crescente intensificação das ameaças, afetando tanto o setor privado quanto o público. No setor privado, observou-se um aumento expressivo na procura por seguros de Riscos Cibernéticos, que cresceu 880% em cinco anos, e quase seis em cada dez empresas brasileiras sofreram ataques ou incidentes em 2023 (CNSEG, 2025). O Brasil registrou 103 bilhões de tentativas de ataques em 2022, o que representa aproximadamente 30% de todos os casos reportados na América Latina e Caribe

(Jornal Da USP, 2023). De acordo com o Instituto Brasileiro de Resposta a Incidentes Cibernéticos, as projeções para 2025 indicam 509 bilhões de tentativas de ataques cibernéticos em todo o território nacional (IBRINC, 2025).

No setor público, o período foi caracterizado por incidentes notáveis, como a "Operação *Timeout*" da Polícia Federal em 2025, que visou instituições públicas com ataques DDoS, e o comprometimento de sistemas do Ministério da Saúde em 2021 devido a credenciais vulneráveis (Agência Gov, 2025). A Caixa Econômica Federal também sofreu uma invasão em 2020 que resultou em fraudes financeiras em contas de municípios (Bracco, 2024), e o Superior Tribunal de Justiça (STJ) foi alvo de ataques em 2020 e 2025, explorando vulnerabilidades em sistemas legados (Falcão, 2025; Shalders, 2020). Além disso, órgãos federais em geral registraram quase 58.000 incidentes cibernéticos ou alertas de vulnerabilidade, com um aumento de 21 vezes nos vazamentos de dados desde o ano de 2020 (CTIR.Gov, 2020; Caniato, 2025).

Nesse contexto, o cenário atual para companhias de tecnologia, especialmente aquelas inseridas no setor público brasileiro, é marcado por uma complexidade crescente e uma velocidade de mudança sem precedentes. A digitalização acelerada, a emergência de novas tecnologias como a Inteligência Artificial e um ambiente regulatório em constante evolução exigem uma abordagem proativa e integrada à gestão de riscos. Não se trata mais de uma função isolada, mas de um componente intrínseco à estratégia de negócio e à cultura organizacional. Com perdas estimadas em R$ 2,3 trilhões em 2024 devido a ciberataques, e o custo médio de uma violação de dados atingindo R$ 6,75 milhões, torna-se imperativo não apenas investir em soluções, mas também gerenciar de forma eficiente a crescente demanda por serviços de cibersegurança, incluindo consultorias especializadas (Ismerim, 2025; Vultus Cybersecurity, 2025). A persistente lacuna de talentos internos no Brasil, aliada à sofisticação das ameaças e à complexidade regulatória, tem impulsionado a dependência de conhecimento externo, o que levanta questões cruciais sobre a otimização desses investimentos e a construção de capacidades sustentáveis a longo prazo para o Estado.

Nesse cenário de inovação digital e diante da grande quantidade de ataques cibernéticos direcionados ao ambiente público brasileiro, emerge a seguinte questão: seria possível que iniciativas de análise de risco cibernético desenvolvidas pelas próprias instituições públicas pudessem avaliar o risco inerente de seus ambientes, reduzindo seu próprio risco, bem como o custo e a dependência de consultorias externas? A hipótese deste trabalho discute a criação de um *framework* de risco cibernético para órgãos públicos, capaz de analisar suas ações em cibersegurança e orientar a adoção de novas atividades, como a criação de políticas, a aquisição de ferramentas e as atividades de *compliance*. Em relação aos objetivos, o trabalho tem como propósito geral promover a discussão sobre a avaliação do risco cibernético nos investimentos públicos, principalmente aqueles direcionados às ferramentas digitais e iniciativas de Governo Digital. Para tanto, os objetivos específicos compreendem apresentar uma proposta de análise de riscos baseada em ameaças, detalhando o percurso de avaliação das políticas e ferramentas de cibersegurança existentes nas organizações públicas, mensurando seus impactos e probabilidades, e analisando o tratamento do risco e possíveis investimentos em mitigações para aprimorar a segurança cibernética nesses ambientes.

Com o propósito de abordar os objetivos propostos, este trabalho está estruturado nas seguintes seções: após esta introdução e as considerações finais, a próxima seção detalha os aspectos metodológicos que guiaram a pesquisa. Em seguida, serão apresentados os resultados e discussões, descrevendo a construção do framework de análise de risco cibernético proposto, bem como os testes realizados e os resultados obtidos em sua aplicação.

2. Metodologia

A metodologia para a criação deste *framework* de riscos baseia-se no estudo de ataques cibernéticos e das vulnerabilidades que permitem esses incidentes, com a análise de *frameworks* existentes como a ISO 27002 e OWASP, além da análise de incidentes ocorridos no mercado. O principal objetivo é fornecer uma definição metodológica abrangente para riscos cibernéticos, alinhando-o com *frameworks* reconhecidos globalmente, como NIST CSF, NIST SP 800-30 e ISO 27005, além de considerar modelos estratégicos como o OCTAVE. Além disso, esta ferramenta busca integrar controles legais brasileiros, como a Lei Geral de Proteção de Dados, bem como controles normativos comuns do mercado. O propósito é transformar essa ferramenta em um instrumento prático de gestão de riscos sólido e defensável.

A relevância da metodologia reside no foco explícito em uma análise de riscos baseada em ameaças priorizando os ataques mais prevalentes no cenário brasileiro nos últimos cinco anos (2020-2024). Essa abordagem pragmática garante que a avaliação de riscos esteja diretamente vinculada às atividades adversárias mais prováveis e impactantes. Para organizações que desenvolvem soluções de TI, compreender e mitigar esses riscos é crucial para a continuidade operacional, a proteção de dados, a conformidade regulatória e a reputação. Ao priorizar táticas e técnicas de adversários antecipadas, a metodologia permite direcionar recursos de cibersegurança de forma mais eficiente, enfrentando os riscos de maior impacto de maneira proativa e preditiva, alinhando-se às melhores práticas modernas de cibersegurança.

2.1 Abordagem Baseada em Ameaças e Cenário Brasileiro

A análise de riscos do framework proposto prioriza os tipos de ciberataques mais prevalentes no Brasil nos últimos cinco anos (2020-2024): Phishing, Ransomware, DDoS e Exploração de Vulnerabilidades. Essa escolha estratégica garante que a avaliação seja focada nas ameaças com maior impacto no contexto operacional nacional. Para isso, foram analisados relatórios de empresas de cibersegurança como Trend Micro (2025), Crowdstrike (2025), Check Point (2025) e Fortinet (2025), bem como estatísticas de ataques do Cert.br e do CTIR Gov, a fim de definir as maiores ameaças do período.

O Phishing[1] se trata de um vetor de ataque persistente e eficaz no Brasil, explorando a vulnerabilidade humana. Entre 2020 e 2024, houve um aumento significativo na sofisticação e no volume desses ataques, com o Brasil sendo um dos principais alvos globais. Em 2020, o país registrou 241,2 milhões de detecções de ameaças por e-mail (Trend Micro, 2020), e em 2021, mais de 150 milhões de pessoas foram vítimas de phishing (Cert.Br, 2025). Em 2023, as tentativas de golpe de phishing aumentaram 617%, com 286 milhões de bloqueios, e em 2024, o phishing foi o vetor inicial mais comum para PMEs brasileiras, com custo médio de R$ 7,75 milhões por violação (Nogueira, 2025). A IBM X-Force observou um aumento de 84% na entrega de *infostealers*[2] via e-mails de phishing em 2024 (IBM, 2025). O *phishing*, ao roubar credenciais válidas, serve como precursor para ataques mais complexos como ransomware e violações de dados, evidenciando a fragilidade da sociedade em termos de conhecimento em cibersegurança e o baixo custo para os criminosos. Isso ressalta a necessidade de a metodologia do *framework* considerar fatores humanos, por meio de treinamento e conscientização contínuos.

[1] Phishing é uma técnica de fraude digital em que golpistas se passam por instituições confiáveis, como bancos ou empresas conhecidas, para enganar usuários e obter informações sensíveis - como senhas, dados bancários ou números de cartão de crédito - por meio de e-mails, mensagens ou sites falsos que parecem legítimos.

[2] Tipo de malware projetado para roubar informações confidenciais do sistema da vítima, como credenciais de login, dados financeiros, históricos de navegação e outros arquivos pessoais.

O Ransomware[3] consolidou-se como uma ameaça cibernética significativa no Brasil, com sua evolução marcada pelo crescimento, sofisticação e pela proliferação do modelo Ransomware-as-a-Service (RaaS). Grupos criminosos, cada vez mais organizados, não apenas criptografam dados, mas também ameaçam vazar informações sensíveis, aumentando a pressão sobre as vítimas. O Brasil e o México são alvos prioritários, e a popularidade do RaaS na Dark Web tem democratizado o acesso a ferramentas para criminosos menos experientes (Fortinet, 2025).

A velocidade de ação dos invasores é alarmante, comprometendo sistemas em menos de 24 horas, e em 2022, 82% dos cibercrimes financeiramente motivados envolveram ransomware (Crowdstrike, 2025). Os incidentes de ransomware no Brasil mostram uma escalada preocupante. Em 2021, as Lojas Renner foram alvo de um ataque ransomware que paralisou seus sistemas (Guimarães, 2021), e em 2023, 96% das empresas na América Latina consideraram o ransomware a ameaça mais significativa, com 30% delas sofrendo pelo menos um incidente de ransomware (ESET, 2024). Em 2024, 73% das empresas brasileiras foram vítimas de ransomware, com 105 organizações atacadas, um aumento expressivo em relação aos anos anteriores (Sousa, 2025). O setor da saúde, devido à criticidade de seus dados e sistemas legados, tornou-se um alvo prioritário, saltando para o quarto lugar entre os mais atacados por ransomware (Crowdstrike, 2025).

Os ataques de Negação de Serviço Distribuída (DDoS[4]) no Brasil têm mostrado um aumento notável em volume e sofisticação, visando sobrecarregar sistemas e torná-los indisponíveis. Em 2019, o CERT.br registrou mais de 301 mil notificações de participação em ataques DDoS, um aumento de 90% em relação a 2018, com destaque para ataques do tipo UDP flood gerados por botnets IoT como Mirai (Cert.Br, 2025). Neste cenário, em 2021, o Brasil foi um dos alvos principais em um dos maiores ataques DDoS da história contra o serviço da Azure da Microsoft (Microsoft, 2022). Em 2024, dados parciais e projeções indicam um crescimento alarmante de 1.801% ano a ano nos ataques DDoS na América Latina, com o Brasil sendo o país mais afetado, registrando mais de 372 mil ataques (FORTINET, 2025).

Em relação a *Exploração de Vulnerabilidades*[5], dado o ritmo acelerado de descobertas (uma nova a cada 17 minutos) e o fato de que metade das vulnerabilidades recentes surgiu nos últimos cinco anos. A combinação da rápida emergência de vulnerabilidades técnicas e o aprimoramento das capacidades adversárias pela IA exige que a metodologia do framework seja dinâmica, incorporando a integração contínua de inteligência de ameaças e reavaliações de risco frequentes para manter a relevância e eficácia.

Para complementar a abordagem baseada nas ameaças cibernéticas mais prevalentes, o *framework* de análise de riscos também incorpora a análise de Ameaças Geopolíticas no Contexto Cibernético. Essa inclusão, alinhada com o Fórum Econômico Mundial - *World Economic Forum* - (WEF), é crucial porque as tensões geopolíticas globais, como guerras comerciais, a rápida e muitas vezes acrítica adoção de IA (incluindo vieses e desafios com

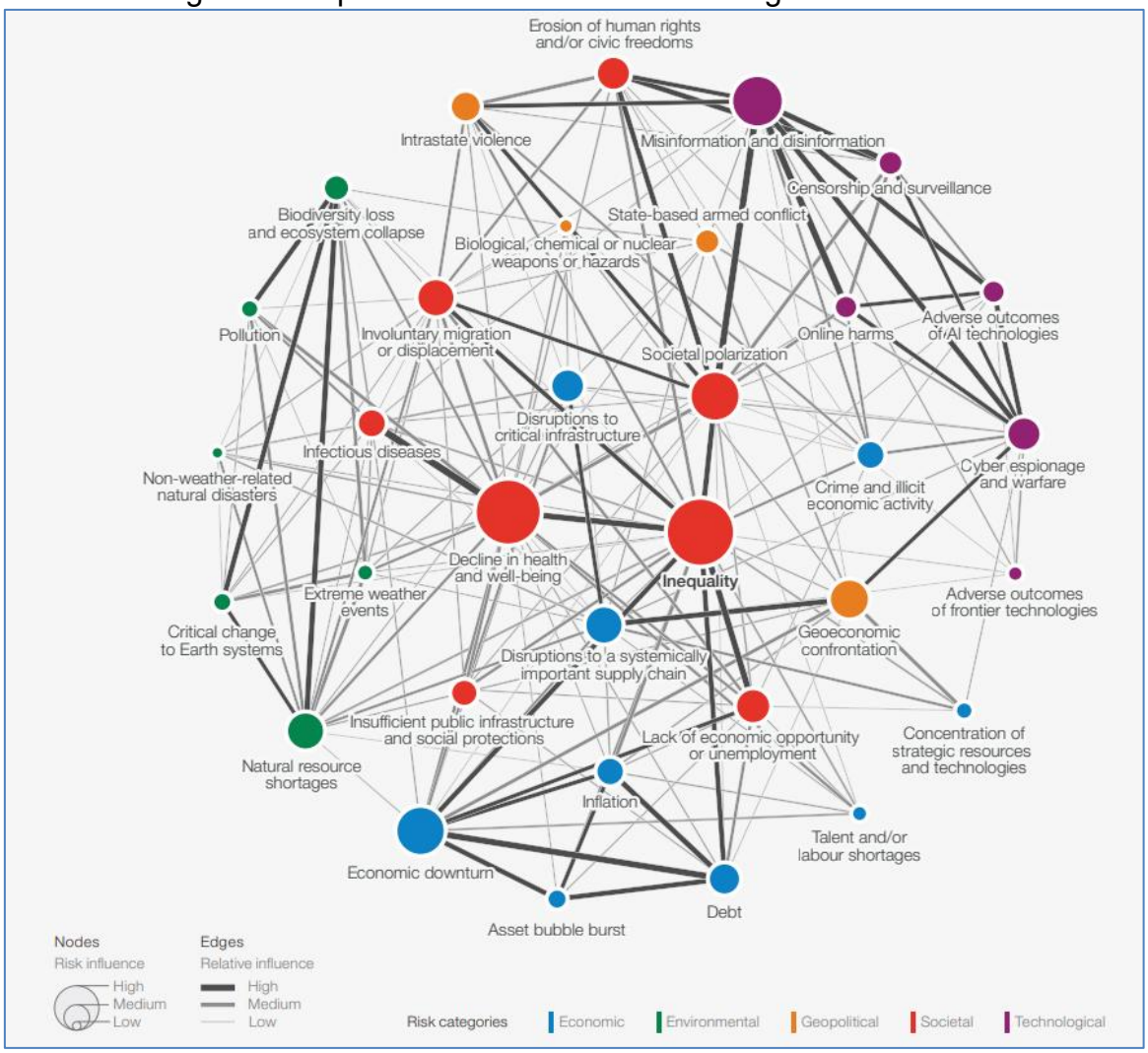
[3] Ransomware é um tipo de malware que sequestra dados digitais ao criptografá-los e exigir o pagamento de um resgate para liberá-los. Em muitos casos, os criminosos ameaçam expor as informações roubadas, tornando a extorsão ainda mais grave. O ransomware é frequentemente disseminado por meio de golpes de phishing e outras vulnerabilidades exploradas em sistemas desatualizados.

[4] DDoS é um tipo de ataque cibernético que visa tornar um sistema, servidor ou rede indisponível por meio de uma sobrecarga de acessos simultâneos. Para isso, os criminosos utilizam múltiplos dispositivos - muitas vezes infectados com malware - que, coordenadamente, enviam uma quantidade excessiva de requisições ao alvo, sobrecarregando sua capacidade de resposta. Esse tipo de ataque pode interromper serviços online, prejudicar operações empresariais e causar danos à reputação das organizações afetadas.

[5] Exploração de vulnerabilidades é uma técnica utilizada por cibercriminosos para tirar proveito de falhas ou brechas presentes em sistemas, softwares ou dispositivos. Ao identificar essas vulnerabilidades - muitas vezes causadas por falta de atualizações, configurações inadequadas ou erros de código - os atacantes podem invadir, executar comandos maliciosos ou comprometer a segurança dos dados. Esse tipo de exploração é frequentemente o ponto de partida para ataques mais complexos, como instalação de malware, roubo de informações ou sequestro de sistemas.

tecnologias de fronteira) e conflitos armados, impactam diretamente a cibersegurança das organizações.

Figura 1: Mapa de interconexões de riscos globais do WEF



Fonte: (JURGENS; DAL CIN, 2025)

Esses fatores externos podem gerar interrupções na cadeia de suprimentos, introduzir vulnerabilidades em softwares e hardwares, comprometer a integridade de sistemas governados por IA e aumentar a atividade de guerra cibernética, com espionagem e ataques a infraestruturas críticas. Para as empresas públicas, a integração proativa desses riscos geopolíticos na avaliação de cibersegurança é fundamental, pois eventos macro se traduzem em ameaças cibernéticas tangíveis e localizadas, exigindo uma abordagem preditiva e baseada em inteligência para proteger ativos digitais e operações.

2.2 Correlação entre Ataques, Ameaças e Vulnerabilidades

Para assegurar uma análise de risco abrangente e eficaz, o *framework* proposto integra uma correlação sistemática entre ataques, ameaças e vulnerabilidades. Essa funcionalidade é crucial, pois reconhece que os riscos cibernéticos não são eventos isolados, mas sim o resultado de uma sequência lógica: um ator de ameaça emprega um vetor de ataque (ex: Phishing) para explorar uma vulnerabilidade (ex: erro humano ou software desatualizado), resultando em um

evento de ameaça (ex: violação de dados ou comprometimento de sistema) e, consequentemente, um impacto negativo.

Essa correlação se alinha com metodologias de avaliação de riscos de *frameworks* renomados, como NIST SP 800-30, ISO 27005 e OCTAVE, que enfatizam a interdependência entre fontes de ameaça, vulnerabilidades e ativos (NIST, 2012). Desta forma, se estabelece uma espinha dorsal metodológica, justificando como ataques específicos levam a eventos de ameaça ao explorar vulnerabilidades particulares. Ao mapear explicitamente "ataques" (ações observáveis dos adversários) para "ameaças" (eventos adversos potenciais) e "vulnerabilidades" (fraquezas exploradas), a guia oferece a granularidade necessária para uma mitigação eficaz. Por exemplo, compreender que um ataque de Phishing explora o "Erro Humano" para roubar credenciais permite a identificação de controles altamente direcionados, como treinamento de conscientização e autenticação multifator. Essa visão interconectada é fundamental para um tratamento de risco eficaz, pois esclarece o que está sendo explorado e como, conduzindo a recomendações de controle mais precisas e impactantes. O Quadro 1 descreve a correlação entre alguns elementos de ataque, ameaças e vulnerabilidades utilizados para a construção do *framework* proposto, bem como o impacto potencial em caso de concretização do respectivo ataque.

Quadro 1: Correlação entre ataques, ameaças e vulnerabilidades exploradas

Tipo de Ataque	Evento de Ameaça Associado	Vulnerabilidade Explorada	Categoria de Impacto Potencial
Phishing	Roubo de Credenciais	Erro Humano / Falta de Conscientização, Controles de E-mail Ineficazes	Violação de Dados, Acesso Não Autorizado, Perda Financeira
Ransomware	Indisponibilidade de dados	Software Desatualizado, Configuração Inadequada, Falta de Backup	Interrupção Operacional, Perda de Dados, Perda Financeira, Dano à Reputação
DDoS	Negação de Serviço	Largura de Banda Insuficiente, Configuração de Rede Vulnerável, Proteção DDoS Inadequada	Interrupção Operacional, Perda de Receita, Dano à Reputação
Exploração de Vulnerabilidades	Acesso não autorizado, Elevação de privilégios	Software Desatualizado, Vulnerabilidades de Dia Zero, Configurações Inseguras	Violação de Dados, Acesso Não Autorizado, Interrupção Operacional

Fonte: Elaborado pelos autores

O Quadro 1, ao detalhar a correlação entre tipos de ataque, eventos de ameaça e vulnerabilidades, é um elemento de grande valor para a metodologia do *framework* proposto. Em primeiro lugar, ele representa visualmente o fluxo lógico central e as premissas subjacentes da avaliação de riscos, tornando o processo mais compreensível, transparente e defensável para todas as partes interessadas. Essa clareza é primordial para fomentar a confiança e o apoio organizacional. Em segundo lugar, a tabela oferece uma estrutura consistente e repetível para identificar e analisar riscos de forma uniforme, permitindo que os usuários sigam as correlações estabelecidas, reduzam a subjetividade e garantam a consideração de todos os aspectos

relevantes de um cenário de risco. Por fim, ao vincular claramente vulnerabilidades específicas aos ataques e eventos de ameaça que elas possibilitam, a matriz direciona naturalmente à identificação e seleção de controles de segurança apropriados e eficazes. Por exemplo, se o "Erro Humano" é uma vulnerabilidade chave para o "Phishing", o treinamento de conscientização em segurança se torna um controle óbvio e justificável, otimizando a alocação de recursos. Finalmente, a estrutura desta matriz reflete inerentemente os princípios centrais de identificação de riscos encontrados em frameworks líderes como NIST SP 800-30, ISO 27005 e OCTAVE, demonstrando a solidez metodológica e o alinhamento com as melhores práticas estabelecidas.

2.3 Ameaças Geopolíticas no Contexto Cibernético das Empresa Públicas

Além da correlação entre ataques, ameaças e vulnerabilidades técnicas e normativas, o *framework* de análise de riscos proposto integra a inclusão de riscos geopolíticos, uma abordagem avançada extraída do Fórum Econômico Mundial (WEF). Essa decisão é crucial, pois o cenário global, cada vez mais fragmentado, apresenta desafios geopolíticos, ambientais, sociais e tecnológicos que moldam a estratégia de cibersegurança de quase 60% das organizações, intensificando a complexidade do cenário cibernético (Jurgens; Dal Cin, 2025). Os riscos geopolíticos, com suas implicações cibernéticas, incluem, por exemplo:

Quadro 2: Descrição de alguns riscos geopolíticos utilizados no *framework*

Risco Geopolítico	Descrição/Detalhamento	Dinâmica de Negócios/Órgãos Públicos Afetada
Riscos Geoeconômicos	Guerras comerciais, sanções ou instabilidade econômica podem impactar cadeias de suprimentos globais, levando à introdução de vulnerabilidades ou dificuldades na aquisição de componentes essenciais.	Resiliência da cadeia de suprimentos, continuidade operacional, custos de conformidade, acesso a mercados.
Vieses de IA / Adoção Rápida de IA	A implementação acelerada da Inteligência Artificial, muitas vezes sem as devidas salvaguardas, introduz novas vulnerabilidades. A IA Generativa, em particular, capacita cibercriminosos a desenvolver ataques de engenharia social e phishing mais sofisticados, podendo comprometer a integridade de sistemas em operações públicas.	Tomada de decisão, confiança nos sistemas de TI, conformidade regulatória (privacidade de dados), reputação.
Problemas com Tecnologia de Fronteira	Tecnologias emergentes além da IA, como computação quântica e IoT avançada, podem criar novas superfícies de ataque, introduzir vulnerabilidades inéditas ou tornar obsoletos os controles criptográficos existentes, representando riscos cibernéticos significativos a longo prazo.	Inovação, competitividade, segurança de longo prazo, capacidade de adaptação tecnológica.
Conflitos Armados	Conflitos geopolíticos correlacionam-se diretamente com o aumento de atividades de guerra cibernética, incluindo espionagem, roubo de propriedade intelectual e ataques disruptivos a infraestruturas críticas, muitas vezes envolvendo atores de estado-nação.	Continuidade operacional, confidencialidade de dados, integridade de sistemas, reputação, conformidade legal.

Fonte: Elaborada pelos autores

Esses riscos geopolíticos têm implicações profundas para as empresas públicas, podendo gerar interrupções na cadeia de suprimentos, comprometer a confidencialidade e integridade dos dados, introduzir vulnerabilidades complexas e resultar em perdas financeiras e danos à reputação. A integração proativa desses riscos globais na avaliação de risco cibernético no Brasil é fundamental, pois mudanças geopolíticas se traduzem diretamente em ameaças

cibernéticas tangíveis e localizadas. Isso exige uma abordagem preditiva e baseada em inteligência, que antecipe os efeitos desses fatores sobre os ativos digitais e operações da organização, movendo a avaliação de riscos de uma visão puramente interna e técnica para uma consideração estratégica em nível macro.

Ao detalhar os riscos geopolíticos e seus potenciais impactos cibernéticos, o *framework* proposto revela-se um instrumento valioso. Desta forma, preenche a lacuna entre riscos geopolíticos globais e suas implicações cibernéticas concretas para as organizações, tornando a consideração desses fatores mais compreensível e gerenciável. Além disso, ao delinear os impactos cibernéticos de diversos cenários geopolíticos, auxilia na antecipação de ameaças futuras que a inteligência de ameaças puramente técnica poderia não identificar, promovendo uma postura proativa e essencial para a resiliência a longo prazo. Além disso, demonstra como a gestão de riscos de cibersegurança é parte integrante da Gestão de Riscos Corporativos (GRC) mais ampla, evidenciando à liderança executiva que riscos externos podem se transformar em consequências cibernéticas significativas, exigindo uma estratégia de risco holística. Por fim, a compreensão dessas conexões intrincadas justifica investimentos em áreas como segurança da cadeia de suprimentos, *frameworks* de segurança de IA e inteligência de ameaças avançada, garantindo a alocação de recursos para riscos emergentes e de alto impacto.

2.4 Definição e Justificativa dos Controles

Após a análise das ameaças e vetores de ataque no cenário cibernético atual, especialmente no contexto do setor público brasileiro conforme detalhado nas seções anteriores, torna-se imperativa a discussão sobre os controles de segurança cibernética. Estes representam o conjunto de salvaguardas e contramedidas implementadas por uma organização para proteger seus ativos de informação, mitigar os riscos identificados e garantir a continuidade dos serviços essenciais. A eficácia desses controles reside em sua natureza multifacetada, abrangendo aspectos normativos, tecnológicos e processuais, e alinhando-se a diretrizes e padrões internacionais de segurança amplamente reconhecidos, como o *NIST Cybersecurity Framework* e as normas ISO 27001, 27002, 27005 e 27032.

A estrutura de controles que fundamenta o *framework* risco cibernético proposto pode ser compreendido através de três pilares principais, em consonância com as melhores práticas de gestão de segurança da informação e com o objetivo de abordar as ameaças prevalentes no Brasil (Phishing, Ransomware, DDoS, Exploração de Vulnerabilidades) e os riscos geopolíticos discutidos no relatório de riscos globais do Fórum Econômico Mundial (JURGENS; DAL CIN, 2025).

2.4.1 Controles Normativos: A Base da Governança e Conformidade

Os controles normativos formam a espinha dorsal de um programa de segurança da informação, estabelecendo a direção estratégica e as regras que guiam o comportamento e as operações da organização. Neste trabalho eles se subdividem em: políticas internas, legislação nacional, regulamentações setoriais e normas técnicas de referência. Os controles normativos representam o conjunto de atividades, procedimentos e rotinas que asseguram a implementação contínua e eficaz das políticas de segurança, bem como o uso apropriado das tecnologias. Essenciais para a operacionalização da segurança cibernética, eles transformam diretrizes e ferramentas em defesas ativas e responsivas (NIST, 2012). Em última análise, são vitais para a resiliência de um sistema contra-ataques de todos os tipos, garantindo que a segurança não seja apenas uma camada técnica, mas uma prática organizacional contínua. O Quadro 3 descreve alguns desses controles normativos usados como controle e suas aplicações para o ambiente de organizações públicas.

Quadro 3: Exemplos de controles normativos do *framework* proposto

Item de controle	Descrição/Detalhamento
Política de Segurança da Informação	Documento fundamental que define o compromisso da alta direção, o escopo da segurança e as responsabilidades gerais, servindo como base para todas as outras políticas.
Política de Gestão de Senhas e de Acessos	Fundamentais contra phishing e exploração de vulnerabilidades. Definem requisitos de complexidade, rotação e, idealmente, a obrigatoriedade de autenticação multifator (MFA), além de garantir o princípio do menor privilégio e a segregação de funções.
Políticas de Soberania de Dados e Due Diligence de Fornecedores	Ganham particular relevância frente a riscos geopolíticos, definindo as regras para armazenamento e processamento de dados transfronteiriços e exigindo a avaliação da postura de segurança e exposição geopolítica de parceiros da cadeia de suprimentos.

Fonte: Elaborado pelos autores

2.4.2 Controles Cibernéticos/Tecnológicos: A Barreira Tática

Ferramentas e sistemas de segurança cibernética constituem a defesa técnica e automatizada essencial para combater ameaças digitais (Goodrich; Tamassia, 2010). A implementação estratégica desses recursos não é apenas uma opção, mas uma medida crítica para a proteção proativa de ativos digitais, como dados, sistemas e infraestrutura. A sua relevância reside na capacidade de agir diretamente contra os tipos de ataques mais prevalentes e conhecidos, oferecendo uma camada robusta de proteção que opera de forma contínua e eficiente (Pfleeger, 1997). Em um cenário de ameaças em constante evolução, a integração dessas tecnologias é a base para a criação de um ambiente seguro e resiliente. O Quadro 4 exibe alguns exemplos de controles técnicos desenvolvidos para o *framework* proposto.

Quadro 4: Exemplos de controles técnicos para segurança cibernética

Item de controle	Descrição/Detalhamento
Firewall, WAF e IPS/IDS	são a primeira linha de defesa contra acessos não autorizados e exploração de vulnerabilidades, controlando o tráfego de rede, protegendo aplicações web, detectando e prevenindo intrusões em tempo real. São essenciais também na mitigação de ataques DDoS.
Anti-DDoS e CDN	Serviços especializados para proteger a disponibilidade dos sistemas, absorvendo e mitigando grandes volumes de tráfego malicioso de DDoS antes que atinjam a infraestrutura da organização. CDNs também ajudam na distribuição de carga e resiliência.
Cofre de Senhas/PAM e Autenticação Multifator	Combatem o roubo de credenciais via phishing e limitam a exploração de vulnerabilidades por acesso privilegiado, gerenciando e protegendo as contas mais críticas.

Fonte: Elaborado pelos autores

2.4.3 Controles de Processos/Operacionais: A Dinâmica da Segurança

Os controles de gestão e processos são fundamentais para uma estratégia de segurança cibernética robusta. Eles transformam políticas e tecnologias em ações concretas, garantindo que a segurança seja uma prática contínua e gerenciada, não apenas um conjunto de ferramentas (ABNT, 2023). Esses controles são a base para uma defesa proativa e resiliente, assegurando que a organização esteja preparada para responder a incidentes, mitigar riscos e

manter a continuidade das operações. O Quadro 5 a seguir, apresenta alguns exemplos de controles de gestão e processos utilizados no *framework* proposto.

Quadro 5: Exemplos de processos e operações do *framework* proposto

Item de controle	Descrição/Detalhamento
Gestão de Incidentes (Plano de Resposta a Incidentes)	Um processo vital para detectar, conter, erradicar e recuperar-se de qualquer tipo de ataque (DDoS, ransomware, phishing, exploração). Define as responsabilidades e os passos a serem seguidos durante uma crise.
Simulações de Ataques (Phishing, Ransomware, Cenários Geopolíticos)	Exercícios práticos (como simulações de phishing para funcionários ou tabletop exercises para a diretoria) são essenciais para testar a eficácia dos controles, a capacidade de resposta das equipes e a conscientização dos colaboradores frente a diversas ameaças.
Mapeamento da Cadeia de Suprimentos e Análise de Controles de Terceiros	Procedimentos essenciais para gerenciar riscos geopolíticos e de terceiros, garantindo que a segurança dos fornecedores esteja alinhada com as expectativas da organização.

Fonte: Elaborado pelos autores

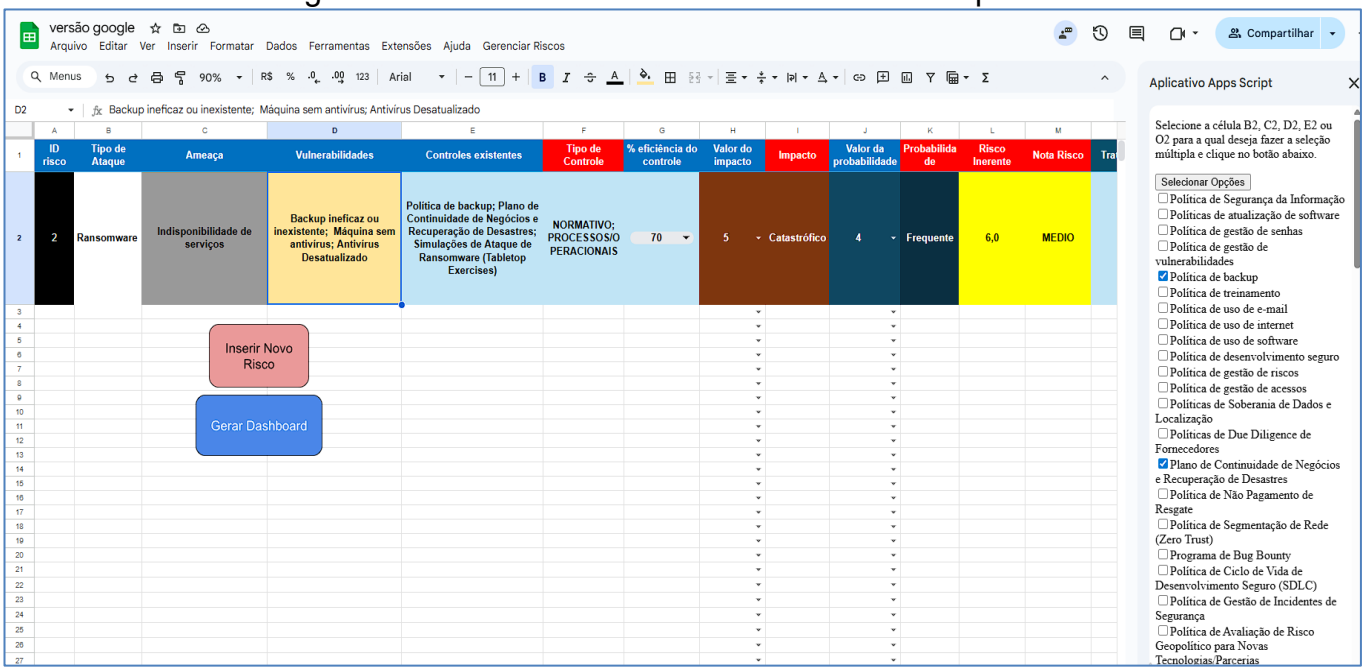
A implementação e a gestão contínua desses controles normativos, tecnológicos e processuais são essenciais para construir uma postura de segurança cibernética robusta e adaptável. Em um cenário de ameaças em constante evolução, onde ataques como DDoS, ransomware, exploração de vulnerabilidades e phishing são cada vez mais sofisticados e onde os riscos geopolíticos adicionam uma camada complexa de desafios, a sinergia entre esses controles é o que permite às organizações não apenas se proteger, mas também detectar, responder e se recuperar eficazmente, garantindo a continuidade e a resiliência de seus negócios no ambiente digital.

3. Resultados e Discussão

Esta seção detalha a aplicação prática do framework de gestão de riscos cibernéticos, utilizando um conjunto de planilhas criadas em Microsoft Excel e Google Sheets como ferramentas de teste. A elaboração e o preenchimento dessas planilhas foram executados pela equipe do projeto com o objetivo de simular e validar a metodologia de análise de riscos proposta. Além disso, é realizada uma discussão comparativa com outros frameworks de mercado para avaliar a funcionalidade do *framework* proposto. O processo de teste foi estruturado para demonstrar a operacionalidade do framework, com foco nos seguintes pontos: 1. Análise e Cálculo de Riscos; 2. Teste e Validação da Metodologia.

1. Análise e Cálculo de Riscos: As planilhas foram concebidas para registrar e avaliar os riscos com base em um cálculo automatizado. A equipe do projeto desenvolveu e aplicou fórmulas para determinar o risco inerente (o risco com os controles existentes (ou não) na organização) e o risco residual (o risco remanescente após as mitigações propostas). *Risco Inerente*: Calculado a partir da *Matriz de Risco* (presente na aba com o mesmo nome), que cruza o *Impacto* e a *Probabilidade do ataque*. A aba *Ferramentas da Planilha* forneceu a base para essa avaliação qualitativa. *Controles Propostos*: A equipe avaliou os controles existentes e, em caso de mitigação, valeu-se da aba *Controles* para incorporar os novos controles ao cálculo. *Risco Residual*: A planilha foi configurada para que o cálculo do risco residual refletisse a eficácia dos controles propostos. No caso de o tratamento de risco ser ACEITAR (não haverá correção ou mitigação), neste caso, o valor do risco residual receberia o mesmo valor do risco inerente.

Figura 2: Preenchimento dos dados de riscos na planilha



Fonte: Elaborado pelos autores

2. *Teste e Validação da Metodologia*: Para os testes, o cenário hipotético foi delineado para representar uma empresa pública com algumas políticas de segurança da informação estabelecidas, mas com uma infraestrutura de ferramentas técnicas ainda limitada. Adicionalmente, considerou-se a localização da empresa em uma região suscetível a ameaças climáticas e que está desenvolvimento de um novo produto que incorpora inteligência artificial para otimizar os resultados de busca dos clientes. Essa configuração permite avaliar a capacidade do *framework* proposto em identificar e gerenciar riscos cibernéticos em um ambiente complexo e multifacetado, com vulnerabilidades tanto internas quanto externas, e que abrange tecnologias emergentes. A Figura 3 exibe os dados preenchidos na planilha, resultado do processo de análise e avaliação de riscos.

Figura 3: Dados de risco do ambiente de teste

ID risco	Tipo de Ataque	Ameaça	Vulnerabilidades	Controles existentes	Tipo de Controle	% eficiência do controle	Valor do impacto	Impacto	Valor da probabilidade	Probabilidade	Risco Inerente	Nota Risco	Tratamento do Risco	Mitigações	Tipo de Controle	% Possibilidade de Mitigação	Valor Risco Residual	Nota Risco Residual
1	Phishing	Roubo de credenciais	Falta de Treinamento (para identificar phishing)	Política de Segurança da Informação	NORMATIVO	20	4	Grande	4	Provável	10,2	MEDIO	MITIGAR	Treinamentos, palestras, cultura de segurança	PROCESSOS/OPERACIONAIS	60	4,1	BAIXO
2	Phishing	Instalação de software malicioso	Antivírus Desatualizado	Antivírus/EDR	CIBERNÉTICO/ TECNOLÓGICO	80	4	Grande	4	Provável	2,6	BAIXO	MITIGAR	Políticas de atualização de software	NORMATIVO	30	1,8	BAIXO
3	Ransomware	Indisponibilidade de dados	Inexistência de política de segurança (de backup)	Política de Segurança da Informação	NORMATIVO	10	5	Catastrófico	4	Provável	18,0	ALTO	MITIGAR	Política de backup	NORMATIVO	40	10,8	MEDIO
4	Ransomware	Indisponibilidade de dados	Backup ineficaz ou inexistente	Backup Imutável/Air-Gapped	CIBERNÉTICO/ TECNOLÓGICO	70	5	Catastrófico	5	Frequente	7,5	MEDIO	MITIGAR	Testes de backup/Recuperação de Desastres	PROCESSOS/OPERACIONAIS	70	2,3	BAIXO
5	Ransomware	Indisponibilidade de dados	Antivírus Desatualizado	Antivírus/EDR	CIBERNÉTICO/ TECNOLÓGICO	70	5	Catastrófico	4	Provável	6,0	MEDIO	MITIGAR	XDR (Extended Detection and Response)	CIBERNÉTICO/TECNOLÓGICO	80	1,2	BAIXO
6	Ransomware	Indisponibilidade de serviços	Ausência de planos de continuidade de negócios			0	5	Catastrófico	5	Frequente	25,0	ALTO	MITIGAR	Plano de Continuidade de Negócios e Recuperação de Desastres	NORMATIVO	80	5,0	MEDIO
7	Ransomware	Indisponibilidade de serviços	Monitoramento de segurança cibernética ineficiente	Detecção de Anomalias de Comportamento	CIBERNÉTICO/ TECNOLÓGICO	40	5	Catastrófico	4	Provável	12,0	MEDIO	MITIGAR	Gestão de incidentes	PROCESSOS/OPERACIONAIS	80	2,4	BAIXO
8	DDoS	Indisponibilidade de serviços	Balanceamento de carga ineficiente ou inexistente	Anti-DDoS	CIBERNÉTICO/ TECNOLÓGICO	90	4	Grande	4	Provável	1,3	BAIXO	ACEITAR			0	1,3	BAIXO

Fonte: Elaborado pelos autores

3.1. Testes e Resultados da Aplicação do *Framework*

Para validar a aplicabilidade e a eficácia do framework proposto, os dados foram inseridos com todos os tipos de ataques disponíveis (phishing, ransomware, DDos, exploração de vulnerabilidades, geopolítico e ataques contra aplicações), priorizando os controles normativos. Dessa forma, a ideia é demonstrar que além do risco inerente, o framework é capaz de demonstrar as necessidades técnicas, normativas e de gestão desta organização fictícia. Desta forma, visando uma abordagem moderna de análise, as planilhas foram conectadas ao Gemini e ao Copilot para que as consultas fossem respondidas por uma IA, capazes de responder por meio de prompt, gerando gráficos e relatórios de risco cibernético deste ambiente hipotético. A Figura 4 apresenta o Gerador de Dashboard criado a partir da conexão da planilha criada no Google Sheets com o Gemini.

Figura 4: Ambiente web criado para interagir com a planilha por meio de IA

Fonte: Elaborado pelos autores por meio do Gemini Google

Além disso, o Gemini foi capaz de analisar os dados e realizar um relatório deste ambiente hipotético. A análise dos riscos cibernéticos revela que ataques geopolíticos e ransomware são os mais frequentes, causando principalmente indisponibilidade de dados e serviços. As vulnerabilidades mais comuns incluem a dependência excessiva de tecnologias de países em desacordo político, a ausência de planos de continuidade de negócios e antivírus desatualizados. Controles como Anti-DDoS e Backup Imutável mostram alta eficiência, enquanto a Política de Segurança da Informação e planos de continuidade de negócios apresentam baixa eficácia. A matriz de risco indica que a maioria dos riscos possui alto impacto e alta probabilidade. Os dados do relatório estão na Figura 5.

As mitigações mais eficazes incluem Cofre de senhas/PAM, ferramentas de scan de vulnerabilidades e WAF, com mais de 90% de sucesso. Em contraste, políticas de atualização de software e de backup têm menor eficácia, necessitando de aprimoramento. Embora as estratégias de mitigação demonstrem ser eficazes na redução do risco inerente para um nível residual geralmente baixo, ainda há um caso de risco residual alto que merece atenção especial.

Para uma proteção cibernética robusta, as recomendações prioritárias incluem fortalecer a resiliência contra ransomware com backups imutáveis e planos de continuidade de negócios aprimorados, além de investir em soluções Anti-DDoS e XDR. É crucial abordar vulnerabilidades comuns, como a atualização de antivírus/EDR e o gerenciamento de acesso privilegiado (PAM). Adicionalmente, revisar e reforçar a Política de Segurança da Informação, investir em treinamento e conscientização em cibersegurança, e fortalecer o monitoramento e resposta a incidentes com um SOC e gestão de incidentes são passos essenciais para construir uma postura de segurança mais resiliente. A Figura 6 exibe os dados de recomendação gerados pelo Gemini para aprimorar a segurança cibernética deste ambiente.

Figura 5: Relatório gerado pelo Gemini sobre os riscos cibernéticos

Principais Conclusões

1. **Tipos de Ataque e Ameaças Mais Comuns:**
   - **Geopolítico** e **Ransomware** são os tipos de ataque mais frequentes.
   - As ameaças mais comuns são a **Indisponibilidade de dados** e a **Indisponibilidade de serviços**, seguidas por **Acesso não autorizado**.
   - O Ransomware está diretamente ligado à indisponibilidade de dados e serviços, o que indica a necessidade de foco nessas áreas.
2. **Vulnerabilidades Prevalentes:**
   - As vulnerabilidades mais recorrentes são a **Dependência excessiva de tecnologias, fornecedores ou mercados específicos de países em desacordo político** e a **Ausência de planos de continuidade de negócios**.
   - **Antivírus Desatualizado** também aparece como uma vulnerabilidade significativa.
3. **Eficiência dos Controles Existentes:**
   - Controles como **Anti-DDoS** (90%) e **Backup Imutável/Air-Gapped** (70%) mostram alta eficiência.
   - Controles como **Política de Segurança da Informação** (12%) e **Plano de Continuidade de Negócios e Recuperação de Desastres** (20%) têm baixa eficiência média, indicando que precisam de revisão e melhoria.
4. **Matriz de Risco:**
   - A maioria dos riscos se concentra em `Valor do impacto` 4 e 5, com `Probabilidade` "Provável" e "Frequente", indicando que a organização enfrenta riscos com alto impacto potencial e alta probabilidade de ocorrência.
5. **Eficácia das Mitigações:**
   - Mitigações com alta possibilidade de sucesso incluem **Cofre de senhas/PAM (Privileged Access Management)** (95%), **Ferramenta de Scan de vulnerabilidades** (90%) e **WAF (Web Application Firewall)** (90%).
   - Mitigações como **Políticas de atualização de software** (30%) e **Política de backup** (40%) apresentam menor possibilidade de mitigação, sugerindo que podem ser menos eficazes ou que sua implementação precisa ser aprimorada.
6. **Risco Inerente vs. Risco Residual:**
   - Há uma redução notável nos níveis de risco após a aplicação das mitigações.
   - A `Nota Risco` "MEDIO" é a mais comum no risco inerente, enquanto a `Nota Risco Residual` "BAIXO" é a mais comum, o que demonstra que as estratégias de mitigação estão, em geral, sendo eficazes para reduzir o risco.
   - No entanto, ainda há um risco residual "ALTO" em um caso (`Valor Risco Residual` de 15), o que merece atenção especial.

Fonte: Elaborado pelos autores com dados gerados pelo Gemini

Figura 6: Relatório de recomendações para melhoria do ambiente

Melhor Ação para Proteção Cibernética

Com base na análise, a melhor ação para proteção cibernética deve ser uma abordagem multifacetada, focando nos riscos mais críticos e nas mitigações mais eficazes, ao mesmo tempo em que se aprimoram os controles existentes com baixa eficiência.

Recomendações Prioritárias:

1. **Fortalecer a Resiliência contra Ransomware e Indisponibilidade de Dados/Serviços:**
   - **Implementar e Testar Backups Imutáveis/Air-Gapped:** Dado que o Ransomware é um tipo de ataque frequente e a indisponibilidade de dados/serviços é uma ameaça comum, e que o "Backup Imutável/Air-Gapped" já tem alta eficiência (70%), é crucial garantir que essa prática seja robusta e testada regularmente. A baixa eficiência da "Política de backup" (40%) indica que a política precisa ser revista e reforçada.
   - **Melhorar Planos de Continuidade de Negócios e Recuperação de Desastres:** A "Ausência de planos de continuidade de negócios" é uma vulnerabilidade chave e o "Plano de Continuidade de Negócios e Recuperação de Desastres" tem baixa eficiência (20%). É vital desenvolver, testar e atualizar esses planos para garantir a rápida recuperação em caso de ataques.
   - **Investir em Soluções Anti-DDoS e XDR:** O Anti-DDoS já tem alta eficiência (90%). Além disso, o XDR (Extended Detection and Response) tem uma alta possibilidade de mitigação (80%) e é fundamental para detectar e responder a ameaças avançadas como o Ransomware.
2. **Abordar Vulnerabilidades Comuns:**
   - **Atualização e Gerenciamento de Antivírus/EDR:** O "Antivírus Desatualizado" é uma vulnerabilidade comum. Embora o "Antivírus/EDR" tenha uma eficiência média de 63.33%, é crucial garantir que todas as soluções de endpoint estejam sempre atualizadas e configuradas para máxima proteção.
   - **Gerenciamento de Acesso Privilegiado (PAM):** A mitigação "Cofre de senhas/PAM" tem uma altíssima possibilidade de mitigação (95%). A "Perda/Roubo/Vazamento de Credenciais" é uma ameaça, e o PAM é essencial para proteger acessos privilegiados, reduzindo o risco de acesso não autorizado e elevação de privilégios.
3. **Aprimorar Controles e Políticas Existentes:**
   - **Revisar e Reforçar a Política de Segurança da Informação:** Com apenas 12% de eficiência, a "Política de Segurança da Informação" precisa de uma revisão completa para garantir que seja abrangente, atualizada e efetivamente comunicada e aplicada.
   - **Treinamento e Conscientização em Cibersegurança:** A "Falta de Treinamento (para identificar phishing)" é uma vulnerabilidade. "Treinamentos, palestras, cultura de segurança" têm uma possibilidade de mitigação de 60%, mas são fundamentais para fortalecer a primeira linha de defesa contra ataques de engenharia social.
4. **Monitoramento e Resposta a Incidentes:**
   - **Implementar ou Fortalecer um SOC (Security Operations Center) e Gestão de Incidentes:** A "Ausência de um Centro de Operações de Segurança (SOC)" é uma vulnerabilidade crítica. O SOC e a "Gestão de incidentes" (80% de possibilidade de mitigação) são cruciais para a detecção proativa e resposta rápida a incidentes cibernéticos.

Fonte: Elaborado pelos autores com dados gerados pelo Gemini

3.2. Comparação dos Elementos do *Framework* com Outros *Frameworks* de Mercado

O *framework* proposto, embora adaptado ao contexto público brasileiro e focado em ameaças prevalentes, estabelece um forte alinhamento com os princípios e estruturas de *frameworks* de segurança cibernética e gestão de riscos reconhecidos globalmente. A tabela a seguir compara os elementos-chave da nossa proposta com as abordagens do NIST CSF, NIST SP 800-30, ISO 27005 e OCTAVE, destacando pontos de convergência e diferenciação.

Quadro 6: Comparação com frameworks de mercado

Elementos do Framework Proposto	NIST Cybersecurity Framework (CSF)	NIST SP 800-30	ISO 27005	OCTAVE
Abordagem Baseada em Ameaças (Foco em Phishing, Ransomware, DDoS, Exploração de Vulnerabilidades)	Alinha-se às funções "Detectar" e "Proteger", onde a inteligência de ameaças é crucial para identificar e defender-se contra vetores de ataque comuns. Não possui foco explícito nos tipos de ataques específicos prevalentes no Brasil.	Foca diretamente na "Identificação de Ameaças" (Threat Identification) como ponto de partida para a análise de riscos. Abrange a identificação de ameaças gerais.	Prevê a "Identificação de Ameaças" (Threat Identification) como fase inicial da gestão de riscos. Abrange a identificação de ameaças gerais.	O processo começa com a identificação de "Práticas de Informação Críticas" e, em seguida, as "Ameaças" a elas. Abrange a identificação de ameaças gerais.
Inclusão de Ameaças Geopolíticas no Contexto Cibernético	Recomenda considerar o ambiente de risco amplo, que pode incluir fatores geopolíticos, mas não como foco explícito ou função dedicada.	Não possui foco explícito na análise de ameaças geopolíticas no texto fornecido, embora uma avaliação de riscos abrangente possa considerá-las implicitamente.	Não possui foco explícito na análise de ameaças geopolíticas no texto fornecido, embora a gestão de riscos possa ser adaptada para incluí-las.	Não possui foco explícito na análise de ameaças geopolíticas no texto fornecido, concentrando-se mais em ameaças a ativos organizacionais específicos.
Correlação entre Ataques, Ameaças e Vulnerabilidades	Implícita nas funções "Identificar" e "Proteger", mas não apresenta uma "guia fonte" sistemática e explícita para essa correlação como o framework proposto.	Enfatiza a interdependência entre fontes de ameaça, vulnerabilidades e ativos.	Enfatiza a interdependência entre fontes de ameaça, vulnerabilidades e ativos.	Enfatiza a interdependência entre fontes de ameaça, vulnerabilidades e ativos.
Tipos de Controles Abrangidos (Normativos, Tecnológicos, Operacionais/Proces-sos)	Organiza os controles em cinco funções essenciais (Identificar, Proteger, Detectar, Responder e Recuperar), abrangendo implicitamente esses tipos de controles de forma holística.	Foca no processo de avaliação de riscos e, por consequência, na necessidade de controles, mas não os categoriza explicitamente da mesma forma tripartida.	A ISO 27001/27002 detalha objetivos de controle e controles que se enquadram nessas categorias, mas a 27005 é focada na gestão de riscos e não na lista detalhada de controles.	Leva à implementação de controles para mitigar riscos identificados, mas a categorização explícita em normativos, tecnológicos e operacionais pode variar na sua apresentação.
Especificidade para Órgãos Públicos Brasileiros / Legislação Local	Framework geral e adaptável, não específico para o contexto regulatório brasileiro.	Framework geral e adaptável, não específico para o contexto regulatório brasileiro.	Framework geral e adaptável, não específico para o contexto regulatório brasileiro.	Framework geral e adaptável, não específico para o contexto regulatório brasileiro.
Foco na Autonomia e Capacidade Interna	Embora promova boas práticas que podem levar a uma maior capacidade interna, não tem como objetivo central explícito a redução da dependência de consultorias externas.	Foca na metodologia de avaliação de riscos, não na forma de aquisição de capacidades internas ou externas.	Foca nas diretrizes para gestão de riscos, não no modelo de fortalecimento de capacidades internas versus consultoria externa.	Concentra-se na identificação de riscos e na proteção de ativos, mas não no fortalecimento da autonomia interna como um pilar explícito.

Fonte: Elaborado pelos autores

4. Considerações Finais

Diante da crescente digitalização dos serviços públicos e da intensificação das ameaças cibernéticas no Brasil, este trabalho buscou responder à questão de pesquisa sobre a possibilidade de as próprias instituições públicas avaliarem o risco inerente de seus ambientes, reduzindo custos e a dependência de consultorias externas. Para tal, propôs-se e desenvolveu-se um framework de gestão de riscos cibernéticos especificamente adaptado ao contexto dos órgãos públicos brasileiros.

O framework foi estruturado com base na análise dos ataques mais prevalentes no cenário nacional (Phishing, Ransomware, DDoS e Exploração de Vulnerabilidades), incorporando também a análise de ameaças geopolíticas, um diferencial que alinha a abordagem à complexidade do cenário global, conforme preconizado pelo Fórum Econômico Mundial. A metodologia enfatizou a correlação sistemática entre ataques, ameaças e vulnerabilidades, o que permite uma identificação de riscos mais precisa e direcionada. Além disso, a proposta de controles foi categorizada em normativos, tecnológicos e operacionais/de processos, fornecendo uma visão abrangente das salvaguardas necessárias.

As potencialidades do framework residem na sua capacidade de oferecer uma estrutura metodológica para a identificação, avaliação, tratamento e monitoramento de riscos cibernéticos, considerando a legislação local e as particularidades operacionais do setor público. Isso permite uma governança e conformidade mais assertivas, orientando investimentos em tecnologias e práticas de cibersegurança de forma autônoma e eficiente.

Os resultados práticos do teste do framework, utilizando planilhas em Microsoft Excel e Google Sheets, demonstraram sua aplicabilidade e eficácia. A conexão dessas planilhas com inteligências artificiais como Gemini e Copilot representou um avanço significativo, possibilitando a análise automatizada dos dados de risco, a geração de gráficos e relatórios detalhados, e até mesmo a produção de recomendações de mitigação por meio de prompts. Essa integração com a IA validou a capacidade do framework em fornecer uma análise moderna e eficiente, revelando não apenas o risco inerente, mas também as necessidades técnicas, normativas e de gestão da organização fictícia. Em suma, o trabalho comprova que iniciativas internas de análise de risco, embasadas por um framework robusto e impulsionadas por ferramentas de IA, podem de fato empoderar as instituições públicas, otimizando investimentos e fortalecendo sua resiliência cibernética.

Referências

JORNAL DA USP. **Brasil sofreu mais de 100 bilhões de tentativas de ataques cibernéticos no último ano**. [*S. l.*], 2023. Disponível em: https://jornal.usp.br/radio-usp/brasil-sofreu-mais-de-100-bilhoes-de-tentativas-de-ataques-ciberneticos-no-ultimo-ano/. Acesso em: 30 jul. 2025.

AGÊNCIA GOV. **Operação Timeout combate ataques cibernéticos a instituições públicas e privadas**. [*S. l.*], 2025. Disponível em: https://agenciagov.ebc.com.br/noticias/202506/pf-deflagra-a-operacao-timeout-contra-ataques-ciberneticos-a-instituicoes-publicas. Acesso em: 30 jul. 2025.

ABNT. **ABNT NBR ISO/IEC 27032. Tecnologia da Informação - Técnicas de segurança - Diretrizes para segurança cibernética**. [*S. l.*]: ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2023-.

BRACCO, Matheus. **Polícia Federal abre operação contra ciberataque e fraude na Caixa - Security Leaders**. [*S. l.*], 2024. Disponível em: https://securityleaders.com.br/policia-federal-abre-operacao-contra-ataque-hacker-e-fraude-na-caixa-economica/. Acesso em: 30 jul. 2025.

BRASIL. **Decreto nº 12.069 de 21 de junho de 2024**. [*S. l.*], 2025. Disponível em: https://legislacao.presidencia.gov.br/atos/?tipo=DEC&numero=12069&ano=2024&ato=d59AzZ61ENZpWTb88. Acesso em: 22 jul. 2025.

BRASIL. **Investimentos de R$ 186,6 bilhões impulsionam transformação digital da indústria brasileira**. [*S. l.*], 2024a. Disponível em: https://agenciagov.ebc.com.br/noticias/202409/investimentos-de-r-186-6-bilhoes-impulsionam-transformacao-digital-da-industria-brasileira. Acesso em: 22 jul. 2025.

BRASIL. **MCTI tem recorde de investimentos em ciência, tecnologia e inclusão digital**. [*S. l.*], 2024b. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2024/12/mcti-tem-recorde-de-investimentos-em-ciencia-tecnologia-e-inclusao-digital. Acesso em: 22 jul. 2025.

CANIATO, Bruno. **Vazamentos de dados no governo crescem mais de 20 vezes em 4 anos**. [*S. l.*], 2025. Disponível em: https://veja.abril.com.br/coluna/maquiavel/vazamentos-de-dados-no-governo-crescem-mais-de-20-vezes-em-4-anos/. Acesso em: 30 jul. 2025.

CEARÁ. **Startups do Ceará podem ganhar até R$ 25 mil com soluções inovadoras para gestão pública - Secretaria da Educação**. [*S. l.*], 2025. Disponível em: https://www.seduc.ce.gov.br/2025/01/22/startups-do-ceara-podem-ganhar-ate-r-25-mil-com-solucoes-inovadoras-para-gestao-publica/.

CERT.BR. **CERT.br - Estatísticas**. [*S. l.*], 2025. Disponível em: https://stats.cert.br/incidentes/. Acesso em: 3 ago. 2025.

CHECK POINT. **Check Point**. [*S. l.*], 2025. Disponível em: https://engage.checkpoint.com/quantum-force-ppc-broad/items/report--cyber-security-report-2025. Acesso em: 3 ago. 2025.

CNSEG. **Seguro Contra Riscos Cibernéticos: Crescimento de 880% em 5 Anos**. [*S. l.*], 2025. Disponível em: https://cnseg.org.br/noticias/protecao-contra-riscos-ciberneticos-cresce-880-em-cinco-anos. Acesso em: 29 jul. 2025.

CRISTINA, Ana; VIANA, Aguilar. Transformação digital na administração pública: do governo eletrônico ao governo digital. **Revista Eurolatinoamericana de Derecho Administrativo**, [*s. l.*], v. 8, n. 1, p. 115–136, 2021.

CROWDSTRIKE. **CrowdStrike 2025 Latin America Threat Landscape Report**. [*S. l.*], 2025. Disponível em: https://www.crowdstrike.com/en-us/resources/reports/latam-threat-landscape-report/. Acesso em: 3 ago. 2025.

CTIR.GOV. **Visão Geral**. [*S. l.*], 2020. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros. Acesso em: 30 jul. 2025.

ESET. **ESET Security Report**. [*S. l.*], 2024. Disponível em: https://web-assets.esetstatic.com/wls/pt/artigos/relatorios/eset-security-report-2024-pt.pdf. Acesso em: 3 ago. 2025.

FALCÃO, Márcio. **Portais do STJ e do CNJ são alvo de tentativas de ataque hacker**. [*S. l.*], 2025. Disponível em: https://g1.globo.com/politica/noticia/2025/03/05/portais-do-cnj-e-do-stj-sao-alvo-de-tentativas-de-ataque-hacker.ghtml. Acesso em: 30 jul. 2025.

FORTINET. **GLOBAL THREAT LANDSCAPE REPORT 2025 A Report by FortiGuard Labs**. [*S. l.: s. n.*], 2025. Disponível em: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-landscape-report-2025.pdf. Acesso em: 3 ago. 2025.

GERRARD, Juliet A *et al.* **By 2030, AI Will Contribute $15 Trillion to the Global Economy**. [*S. l.*], 2019. Disponível em: https://www.weforum.org/agenda/2019/08/by-2030-ai-will-contribute-15-trillion-to-the-global-economy/. Acesso em: 24 maio 2024.

GOODRICH, Michael T; TAMASSIA, Roberto. **Introduction to Computer Security**. [*S. l.*]: Pearson Education, 2010-.

GUIMARÃES, Leonardo. **Site da Renner sai do ar após ataque hacker – entenda o caso**. [*S. l.*], 2021. Disponível em: https://www.cnnbrasil.com.br/economia/macroeconomia/site-da-renner-continua-fora-do-ar-apos-ataque-hacker/. Acesso em: 3 ago. 2025.

IBM. **IBM X-Force 2025 Threat Intelligence Index**. [*S. l.: s. n.*], 2025. Disponível em: https://www.ibm.com/downloads/documents/us-en/1227cc9e83cb97ae. Acesso em: 3 ago. 2025.

IBRINC. **IBRINC - Instituto Brasileiro de Resposta a Incidentes Cibernéticos**. [*S. l.*], 2025. Disponível em: https://www.ibrinc.org.br/. Acesso em: 29 jul. 2025.

ISMERIM, Flávio. **Hackers: empresas do Brasil perderão R$ 2,2 trilhões em 3 anos, diz estudo**. [*S. l.*], 2025. Disponível em: https://www.cnnbrasil.com.br/tecnologia/hackers-empresas-do-brasil-perderao-r-22-trilhoes-em-3-anos-diz-estudo/. Acesso em: 30 jul. 2025.

JURGENS, Jeremy; DAL CIN, Paolo. **Global Cybersecurity Outlook 2025World Economic Forum**. [*S. l.*]: World Economic Forum, 2025. Disponível em: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf. Acesso em: 28 jul. 2025.

MICROSOFT. **Azure DDoS Protection—2021 Q3 and Q4 DDoS attack trends**. [*S. l.*], 2022. Disponível em: https://azure.microsoft.com/en-us/blog/azure-ddos-protection-2021-q3-and-q4-ddos-attack-trends/. Acesso em: 3 ago. 2025.

MINAS GERAIS. **Decreto nº 48.937, de 06/11/2024 - Texto Original - Assembleia Legislativa de Minas Gerais**. [*S. l.*], 2024. Disponível em: https://www.almg.gov.br/legislacao-mineira/texto/DEC/48937/2024/. Acesso em: 28 jul. 2025.

NIST. **NIST Special Publication 800-30**. [*S. l.*], 2012. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf#page=64.11. Acesso em: 4 ago. 2025.

NOGUEIRA, Michele. **O Impacto da Cibersegurança nas Pequenas e Médias Empresas Brasileiras - Horizontes**. [*S. l.*], 2025. Disponível em: https://horizontes.sbc.org.br/index.php/2025/03/o-impacto-da-ciberseguranca-nas-pequenas-e-medias-empresas-brasileiras/. Acesso em: 3 ago. 2025.

PFLEEGER, Charles P. **Security in Computing**. [*S. l.*]: Addison-Wesley Professional, 1997-.

RIO GRANDE DO SUL. **Com foco no empreendedorismo, governo e Invest RS anunciam conjunto de ações e iniciativas do Empreender RS**. [*S. l.*], 2025. Disponível em: https://estado.rs.gov.br/com-foco-no-empreendedorismo-governo-e-invest-rs-anunciam-conjunto-de-acoes-e-iniciativas-do-programa-empreender-rs. Acesso em: 28 jul. 2025.

SÃO PAULO. **Portal da Estratégia de Transformação Digital da Cidade de São Paulo**. [*S. l.*], 2023. Disponível em: https://governodigital.prefeitura.sp.gov.br/. Acesso em: 28 jul. 2025.

SERPRO. **Serpro vai investir mais de 70% do R$ 1 bi previsto para infraestrutura de nuvem do Plano Nacional de Inteligência Artificial**. [*S. l.*], 2024. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2024/nuvem-serpro-inteligencia-artificial-nacional. Acesso em: 22 jul. 2025.

SHALDERS, André. **Alvo de ataque hacker, STJ gastou R$ 13,7 milhões com empresa de informática investigada - BBC News Brasil**. [*S. l.*], 2020. Disponível em: https://www.bbc.com/portuguese/brasil-54847723. Acesso em: 30 jul. 2025.

SOUSA, Pamela. **Brasil: 73% das empresas sofrem com ransomware, mas custo de recuperação cai**. [*S. l.*], 2025. Disponível em: https://itforum.com.br/noticias/ransomware-atinge-73-empresas-br-2024/. Acesso em: 4 ago. 2025.

TREND MICRO. **Brasil figura como um dos países com mais ameaças cibernéticas do mundo em 2020, alerta Trend Micro**. [*S. l.*], 2020. Disponível em: https://www.trendmicro.com/pt_br/about/newsroom/press-releases/2020/2020-12-18.html. Acesso em: 3 ago. 2025.

TREND MICRO. **CYBER RISK REPORT**. [*S. l.: s. n.*], 2025. Disponível em: https://documents.trendmicro.com/images/TEx/articles/Research-Risk-Report-2025.pdf#page=22.09. Acesso em: 3 ago. 2025.

VULTUS CYBERSECURITY. **1º Panorama do Risco Cibernético no Brasil**. [*S. l.*], 2024. Disponível em: https://ecosystem.vultuscyber.com.br/report-panorama-do-risco-cibernetico. Acesso em: 30 jul. 2025.