# DESAFIOS NO COMPARTILHAMENTO INTERNACIONAL DE INFORMAÇÕES SOBRE ATAQUES CIBERNÉTICOS: UMA ANÁLISE COMPARATIVA ENTRE BRASIL, ESTADOS UNIDOS E EUROPA

Mauri Sudário Ferreira Dantas[1], Éder Souza Gualberto[1], Georges Daniel Amvame Nze[1], Fábio Lúcio Lopes de Mendonça[1] e Daniel Alves da Silva[1,2]
*[1]Programa de Mestrado Profissional em Engenharia Elétrica (PPEE), Universidade de Brasília (UnB), Brasília 70910-900, Brasil*
*[2]Hamm-Lippstadt University of Applied Sciences (HSHL), 59063 Hamm, Alemanha*

**RESUMO**

Com a crescente dependência digital, a cibersegurança torna-se mais importante do que nunca. Este artigo examina os "Desafios no Compartilhamento Internacional de Ciberataques," com foco no Brasil, nos Estados Unidos e na Europa. Os governos enfrentam dificuldades para equilibrar a proteção e a conectividade global em meio ao aumento das ameaças. A cooperação internacional e a troca de informações são cruciais, embora seja necessário um melhor entendimento dessas trocas. O artigo analisa as estratégias no Brasil, nos EUA e na UE, destacando os desafios únicos de cibersegurança que cada um enfrenta e a importância da cooperação e das normas emergentes.

**PALAVRAS-CHAVE**

Cibersegurança, Cooperação Internacional, Normas Emergentes, Brasil, Europa, Estados Unidos

## 1. INTRODUÇÃO

No mundo contemporâneo, caracterizado por uma crescente dependência de tecnologias digitais e por níveis cada vez mais elevados de interconexão, a cibersegurança tornou-se uma preocupação central para governos e organizações. Essa preocupação reflete não apenas os riscos associados às ameaças cibernéticas, mas também a complexidade de se estabelecer mecanismos eficazes de proteção e cooperação global (OSCE, 2023).

Este artigo investiga os "Desafios no Compartilhamento Internacional de Informações sobre Ataques Cibernéticos", com foco em uma análise comparativa das práticas adotadas no Brasil, nos Estados Unidos e na Europa. O objetivo central é identificar barreiras e propor soluções que promovam a troca eficiente e segura de informações entre essas regiões, considerando as diferenças regulatórias, culturais e tecnológicas.

A crescente dependência das tecnologias digitais permeia todos os setores, tornando a cibersegurança essencial para a estabilidade econômica e social das comunidades. No entanto, o aumento exponencial das ameaças e desafios cibernéticos apresenta dificuldades significativas para os governos, mesmo aqueles mais avançados em cibersegurança, à medida que se esforçam para equilibrar a proteção eficaz com a manutenção da conectividade global (Hitchens, T., 2017).

Nesse contexto, a cooperação internacional surge como uma alternativa realista e viável para aprimorar a cibersegurança. O compartilhamento de informações entre nações é um pilar central desse esforço colaborativo. Apesar da crescente importância atribuída a essa prática, há uma falta de compreensão detalhada sobre os mecanismos e a extensão desse intercâmbio (Hitchens, T., 2017). À medida que alguns processos se concluem e outros se intensificam, as normas cibernéticas enfrentam desafios e oportunidades em uma encruzilhada (Ruhl, C. et al., 2020).

Para alcançar esse objetivo, foi utilizada uma abordagem qualitativa e comparativa, com a coleta de dados baseada em análise documental de políticas públicas, regulamentações, relatórios técnicos e literatura acadêmica relevantes ao tema. As fontes foram selecionadas por sua relevância e credibilidade, priorizando documentos de órgãos oficiais, como o NIST nos Estados Unidos e as diretrizes da União Europeia, além de

análises nacionais do Brasil. Os dados foram examinados de forma sistemática para identificar padrões, diferenças e pontos de convergência, com o intuito de embasar a proposta de um modelo que promova a cooperação internacional em cibersegurança. Essa metodologia foi escolhida por sua adequação à análise de contextos distintos e interdependentes.

Além de identificar barreiras regulatórias e técnicas, o artigo também explora como diferenças culturais e políticas impactam a colaboração internacional em cibersegurança. Embora a transparência e a troca de informações sejam amplamente reconhecidas como fundamentais, questões como confiança, soberania nacional e prioridades políticas podem dificultar a implementação de práticas colaborativas. A discussão se aprofunda ao conectar os achados com os desafios específicos de cada região, propondo estratégias para superar essas barreiras e fortalecer a resiliência cibernética global. Dessa forma, o artigo não apenas apresenta resultados, mas oferece uma interpretação crítica e fundamentada que visa contribuir para a literatura e para as práticas do setor.

# 2. ESTATÍSTICAS GLOBAIS DE CIBERATAQUES

Como afirmou de maneira perspicaz o matemático e empreendedor britânico Clive Humby, "Dados são o novo petróleo", uma metáfora eficaz para descrever a abordagem da era digital em relação aos seus recursos mais preciosos. Décadas atrás, grandes corporações focavam seus esforços na aquisição de materiais brutos tangíveis e valiosos, enquanto hoje, a informação dos clientes é considerada o ativo mais valioso de uma empresa (Humby, C., 2006).

A empresa americana Verizon oferece uma perspectiva mais ampla em seu "Verizon Data Breach Investigations Report (DBIR)", que é baseado em dados de 2.013 incidentes de violação de dados fornecidos por 73 fontes diferentes, tanto públicas quanto privadas, em 86 países ao redor do mundo. O DBIR também fornece informações sobre o número de fontes de dados e incidentes, mas não especifica o volume de dados ou os tipos de informação envolvidos nas violações (Neto, N., et al., 2021).

Outro estudo, lançado em novembro de 2019 pela Risk Based Security, relatou que, nos primeiros nove meses de 2019, ocorreram 5.183 violações que expuseram 7,9 bilhões de registros. O número de incidentes de violação de dados compilado pela Risk Based Security em apenas nove meses quase dobra o número relatado pela Verizon em um ano completo de 2019 (Risk Based Security, 2019).

É evidente que os sistemas computacionais estão entre os alvos mais atraentes para indivíduos não autorizados, pois as informações contidas nesses sistemas são extremamente valiosas para tais agentes (Aljanabi, M., et al., 2023). Esses ataques podem ser realizados por um indivíduo ou por um grupo, motivados por incentivos financeiros, objetivos políticos ou até considerações pessoais. (Fleck, A., 2022; Mijwil, M., et al., 2023).

Notavelmente, economias maiores, como China, Brasil, Estados Unidos, Índia, México, França, Austrália e Emirados Árabes Unidos, enfrentam perdas bilionárias para os consumidores devido ao cibercrime (Cybercrime Magazine, 2023). Em 2017, os consumidores chineses sofreram perdas financeiras no valor de 66,3 bilhões de dólares americanos atribuídas ao cibercrime (Statista Research Department, 2023).

## 2.1 O Panorama da Cibersegurança na União Europeia

Em 2 de julho de 2013, a Comissão Europeia estabeleceu a Estratégia de Cibersegurança da União Europeia. Esta estratégia foi desenvolvida para esclarecer o papel da UE (em oposição aos Estados-membros que colaboram por meio do Conselho da UE) na proteção do domínio cibernético e definiu uma série de "ações" a serem implementadas pela UE (Transnational Threats Department OSCE, 2023).

Em julho de 2016, o Conselho da UE assinou e o Parlamento ratificou a "Diretiva sobre a Segurança das Redes e Sistemas de Informação (Diretiva NIS)", que delineia as responsabilidades dos países membros e estabelece mecanismos de cooperação (Zygierewicz, A., 2020). De acordo com essa diretiva, todos os países membros devem criar uma Equipe de Resposta a Incidentes de Segurança Cibernética (CSIRT) e habilitá-las a colaborar por meio de uma Rede de CSIRTs. A diretiva também estabelece um Grupo de Cooperação para gerenciar essa colaboração e incentiva os membros a trabalharem por meio da Agência da União Europeia para a Cibersegurança (ENISA), criada em 2004 na Grécia como um centro de excelência para apoiar os membros da UE no fortalecimento da cibersegurança (Malatras, A., et al., 2023).

Em fevereiro de 2016, a União Europeia assinou um Acordo Técnico com a OTAN para melhorar a prevenção, detecção e resposta a incidentes cibernéticos para ambas as organizações. Os esforços de coordenação em cibersegurança entre a UE e a OTAN começaram em 2010, incluindo reuniões anuais de alto nível. A UE também participa como observadora nos exercícios anuais de cibersegurança da OTAN, conhecidos como Cyber Coalition. No entanto, de acordo com autoridades familiarizadas com a situação, a cooperação ainda é inconsistente e em grande parte indefinida (European Union External Action Service, 2016).

A ENISA publica anualmente o relatório ENISA Threat Landscape (2021), que inclui vários aspectos da cibersegurança em formato gráfico, como impactos financeiros em diferentes setores da União Europeia. A União Europeia também disponibiliza conjuntos de dados com informações abertas de entidades governamentais e do mercado. Esses conjuntos de dados incluem uma variedade de informações sobre cibersegurança, embora alguns dados exijam autorização para acesso. Esses dados abrangem desde violações de dados, detalhes de contato vazados de organizações, até a Taxonomia de Ameaças da ENISA, disponíveis no site data.europa (2023).

## 2.2 O Panorama da Cibersegurança nos Estados Unidos

Os Estados Unidos desempenharam um papel significativo na história da internet, com o grande desenvolvimento da rede a partir da década de 1970, através de projetos relacionados à segurança. Na década de 1990, diversas tecnologias foram desenvolvidas, aumentando o número de usuários na rede. No entanto, foi por volta de 2004, com o advento da Web 2.0, que interfaces mais amigáveis começaram a atrair usuários em todo o mundo (Cezarinho, F., 2018).

Um desenvolvimento notável em 2023 foi a adoção, pela SEC (Securities and Exchange Commission), órgão regulador do mercado de valores mobiliários dos EUA, de regras sobre a divulgação de incidentes cibernéticos para empresas americanas e emissores privados estrangeiros. Essas regras abrangem desde a gestão de riscos de segurança cibernética até a governança. Elas estipulam que qualquer incidente cibernético significativo deve incluir uma descrição de sua natureza, escopo, cronologia e impacto material, e deve ser relatado dentro de quatro dias após ser considerado significativo. O NIST (National Institute of Standards and Technology) desenvolveu o Cybersecurity Framework (CSF), amplamente utilizado por várias organizações governamentais e privadas para relatar vulnerabilidades de segurança cibernética, conforme ilustrado na Tabela 1. O CSF do NIST é composto por um conjunto de atividades agrupadas em subcategorias, que por sua vez são organizadas em categorias divididas em cinco áreas: Identificar, Proteger, Detectar, Responder e Recuperar, seguindo uma abordagem cíclica similar ao ciclo PDCA (NIST, 2023).

Em 2009, o governo dos EUA lançou o data.gov, uma plataforma de transparência e dados abertos que oferece metadados e informações sobre o acesso a conjuntos de dados. Esses dados abrangem 78 agências federais, 40 estados americanos, 46 cidades e condados, e 52 países (Almuhammadi e Alsaleh, 2017). A plataforma inclui diversos conjuntos de dados relacionados à cibersegurança, como o uso dos frameworks NIST CSF e NIST SP 800-53 pela cidade de Tempe para avaliar suas iniciativas de cibersegurança (City of Tempe, 2023).

Outro caso relacionado ao data.gov (2023a) envolve relatórios de violação de dados, como o vazamento de dados de cidadãos do estado de Washington. Esse caso incluiu informações sobre as organizações afetadas, as datas de início e término dos ataques, o número de pessoas afetadas, o tipo de ataque e a indústria impactada. Como mencionado no caso da SEC, essas divulgações são cruciais para a tomada de decisão de investidores em relação às organizações que sofreram violações de dados, promovendo um senso de transparência.

## 2.3 O Panorama da Cibersegurança no Brasil

A cibersegurança tornou-se uma preocupação nacional no Brasil, impulsionada pelas profundas transformações resultantes da digitalização da infraestrutura, sociedade, economia e política. Entre 2008 e 2017, a taxa de penetração digital no país aumentou significativamente de 18% para 61%. Instituições financeiras adotaram completamente uma abordagem digital, com mais de 604 fintechs surgindo no país. Além disso, as redes sociais passaram a desempenhar um papel central na formação e mediação da opinião pública, com mais de 120 milhões de usuários no Brasil. Relatórios do Centro de Tratamento e Resposta a Incidentes Cibernéticos (CTIR) indicam um aumento no número de incidentes registrados, subindo de 3.107 em 1999 para 833.775 em 2017,

com um pico de mais de um milhão de incidentes reportados em 2014. Esses incidentes incluem diversos tipos de ataques, como Negação de Serviço Distribuída (DDoS), invasões de computadores, varreduras, worms, fraudes e ataques a websites (Hurel, L. e Lobato, L., 2021).

Dada sua posição geopolítica proeminente e o avanço de sua economia digital, o Brasil tem sido frequentemente alvo de agentes maliciosos, evidenciando a urgência em melhorar suas defesas cibernéticas. Sua dimensão e relevância econômica significativa também o tornam um alvo atrativo para esses ataques. Com uma infraestrutura digital em constante expansão e uma grande base de usuários de internet, o país está se tornando gradualmente mais vulnerável a ameaças cibernéticas, resultando em perdas financeiras substanciais tanto para empresas quanto para entidades governamentais (Devanny, J. et al., 2022; Kshetri, N. e DeFranco, J., 2020).

Os custos associados ao cibercrime no Brasil são particularmente alarmantes, com a McAfee estimando perdas de aproximadamente 10 bilhões de dólares, posicionando o país no centro de uma onda global de cibercrimes (Machado, F., 2018). O Brasil ocupa o segundo lugar nas perdas de consumidores devido ao cibercrime e é o país mais visado da América Latina. Esse cenário é contextualizado pelas inovações no setor bancário brasileiro e pela crescente infraestrutura de comércio eletrônico (Muggah, R. e Thompson, N., 2015; Farahbod, K., Shayo, C. e Varzandeh, J., 2020).

Até meados de 2012, o Brasil não possuía uma legislação específica para crimes cibernéticos, e as leis redigidas décadas antes não conseguiam abranger as complexidades introduzidas pela informática, incluindo vulnerabilidades em sistemas de informação (Costa, R. e Pacheco, G., 2018). Em 2023, completam-se dez anos da promulgação da Lei 12.737/2012, conhecida como Lei Carolina Dieckmann, que surgiu após o roubo de 36 fotos íntimas do computador da vítima, levando a uma tentativa de extorsão (Araújo, J., 2023).

Em 13 de abril de 2014, foi sancionada a Lei 12.965/2014, conhecida como Marco Civil da Internet, que inclui disposições sobre a interação na internet, assegurando princípios de liberdade de expressão, privacidade e direitos humanos em ambientes virtuais. A lei também aborda penalidades para atores que violam dados privados e garante que os termos de coleta e uso de dados estejam claramente disponíveis (Arnaudo, D., 2017).

Seguindo esses avanços nacionais, o Brasil promulgou a Lei Geral de Proteção de Dados (LGPD), que foca na proteção de dados, trazendo diversas atualizações, incluindo a responsabilização de agentes pelo tratamento, conservação e processamento de dados, definindo dados pessoais e dados pessoais sensíveis, e delegando à Autoridade Nacional de Proteção de Dados (ANPD) a função de fiscalização (Lugati, L. e Almeida, J., 2022).

Simultaneamente, foram desenvolvidos padrões para a notificação de incidentes cibernéticos ao CTIR Gov. Esses padrões são essenciais para garantir uma resposta eficaz e coordenada às ameaças cibernéticas. De acordo com a Instrução Normativa nº 4/2020 do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), todas as entidades governamentais devem notificar incidentes cibernéticos ao CTIR Gov no máximo duas horas após a identificação do incidente. Esse padrão visa garantir que o CTIR Gov possa rapidamente avaliar e fornecer orientações apropriadas para mitigar os impactos dos incidentes. Além disso, a regulamentação estipula que as notificações devem incluir informações detalhadas sobre a natureza do incidente, os sistemas afetados, o impacto inicial e as medidas de contenção adotadas. Essas diretrizes são fundamentais para manter a segurança cibernética nacional, permitindo uma resposta unificada e coordenada às ameaças emergentes (Gabinete de Segurança Institucional, 2019).

Um relatório da Anatel (Agência Nacional de Telecomunicações) informou que o Brasil co-liderou um relatório de cibersegurança aprovado em Genebra. O relatório destaca pontos importantes a serem adotados no país, como o princípio de que diferentes níveis de criticidade requerem diferentes níveis de segurança, um atributo do framework NIST. O documento também lista o uso do framework e suas atualizações como padrões para a cibersegurança (Malatras, A., et al., 2023).

## 3. DESAFIOS NO COMPARTILHAMENTO INTERNACIONAL

No que se refere à troca de informações entre agências governamentais, países e entidades em diversos setores do mercado, muitas nações possuem um Centro de Resposta a Incidentes de Segurança Cibernética (CERT), frequentemente integrado ao Fórum de Equipes de Resposta a Incidentes e Segurança (FIRST). Esta organização internacional é composta por equipes confiáveis de resposta a incidentes cibernéticos dedicadas à prevenção de ataques de segurança cibernética. Os membros do FIRST colaboram compartilhando informações

sobre novas vulnerabilidades e enfrentando uma ampla gama de ameaças à segurança computacional (Neto, N., et al., 2021).

A colaboração internacional para aprimorar a cibersegurança apresenta-se como um caminho mais pragmático e viável. Embora o compartilhamento de informações seja frequentemente defendido como a principal forma de cooperação internacional, há uma lacuna substancial na compreensão dos tipos de informações relacionadas à cibersegurança que estão sendo compartilhadas, com quem, para quais finalidades e sob quais condições (Hitchens, T., 2017).

Apesar do consenso político entre os Estados sobre a necessidade imperativa de cooperação para proteger o ciberespaço, os detalhes são cruciais. Especialistas, como Hitchens, T., (2017), catalogaram uma variedade de razões pelas quais os Estados podem decidir compartilhar ou reter informações sobre ameaças e incidentes cibernéticos, como mostrado na Tabela 1.

Tabela 1. Razões para compartilhar ou abster-se de compartilhar informações

| **Razões para partilhar informações (bilateral ou globalmente)** | **Razões para se abster de partilhar informações: (de carácter nacional ou de convénio)** |
|---|---|
| Vantagem recíproca na partilha de informações, uma vez que todos seriam prejudicados na eventualidade de um incidente cibernético | Necessidade de tempo para corrigir a vulnerabilidade antes que outros tomem conhecimento dela própria |
| Uma resposta mais ágil | Defesa das fontes e dos métodos |
| Prevenção (informações sobre vulnerabilidades, soluções, atores de ameaças) | Falta de confiança no outro país (podem usá-lo contra outra pessoa ou não o empregar corretamente) |
| Identificação (atribuição, motivações, métodos) | Utilização ofensiva (informações/fontes e métodos, Ciberataque) |
| Reforço das capacidades para preparar o futuro | Falta de incentivo: falta de compreensão do valor da partilha |
| Cultivo de parcerias (confiança, segurança no ciberespaço, como meio para outras ligações - militares, económicas, políticas) | Falta de capacidade (a nível interno, para proteger os "bens" e não dar a conhecer aos outros as atividades questionáveis que está a realizar), ou a nível internacional (falta de ponto de contacto, metodologia) |
| Identificação de ameaças e tendências emergentes | Alavancar a vantagem competitiva (manter as vulnerabilidades em segredo - para vender um produto ou não perder clientes, proteger a reputação, velocidade de correção em relação ao concorrente) |
| Reafirmação (autocontrolo, eliminação inequívoca da culpa) | Reter informações como alavanca, moeda de troca contra outro país ou deixá-lo sofrer as consequências |

Uma das ferramentas fundamentais para colaboração e compartilhamento de informações sobre vulnerabilidades cibernéticas é o Common Vulnerabilities and Exposures (CVE). O CVE é uma lista de informações publicamente divulgadas sobre vulnerabilidades de segurança em software e hardware. Cada vulnerabilidade identificada recebe um identificador único de CVE, facilitando a troca de informações e a coordenação dos esforços de resposta entre diferentes organizações e países. Esse sistema é mantido pela MITRE Corporation, em colaboração com várias agências e parceiros globais (Robert, M., Christey, S. e Baker, D., 2002).

O uso de padrões como o CVE é essencial para garantir que todas as partes envolvidas compreendam claramente a natureza das vulnerabilidades e possam agir de forma eficaz. Além disso, o CVE facilita a criação de relatórios padronizados, cruciais para a análise e mitigação de riscos. A adoção de tais padrões contribui para maior transparência e confiabilidade na comunicação de vulnerabilidades, permitindo que organizações em diferentes partes do mundo respondam rapidamente a ameaças emergentes.

Mesmo com ferramentas como o CVE, desafios no compartilhamento de informações sobre ataques cibernéticos internacionais persistem. A diversidade de regulamentações e políticas entre os países pode dificultar a criação de um protocolo unificado para notificação e resposta a incidentes cibernéticos. Por exemplo, enquanto os Estados Unidos possuem um conjunto robusto de diretrizes por meio de plataformas como o data.gov, que inclui informações detalhadas sobre incidentes cibernéticos, a União Europeia adota uma abordagem mais macro através da ENISA, focando em áreas afetadas, em vez de entidades específicas.

Além disso, a recente legislação brasileira sobre notificação de incidentes cibernéticos ao CTIR Gov destaca a importância de um sistema de notificação ágil e detalhado. De acordo com a Instrução Normativa nº 4/2020 do GSI/PR, entidades governamentais brasileiras devem notificar o CTIR Gov de incidentes

cibernéticos no prazo máximo de duas horas após a identificação do incidente. Essas notificações devem incluir informações detalhadas sobre a natureza do incidente, sistemas afetados, impacto inicial e medidas de contenção adotadas (Gabinete de Segurança Institucional, 2020). Esse nível de detalhe é crucial para uma resposta eficaz, mas também requer alto grau de coordenação e confiança entre as partes envolvidas.

Em conclusão, embora padrões de vulnerabilidade como o CVE forneçam uma base sólida para comunicação e mitigação de riscos, a implementação eficaz do compartilhamento de informações sobre ataques cibernéticos ainda enfrenta desafios significativos. A harmonização das práticas regulatórias e a construção de confiança entre as nações são passos essenciais para melhorar a cooperação internacional em segurança cibernética.

# 4. PROPOSTAS DE SOLUÇÃO

Apesar de suas diferenças, essas três potências possuem regulamentações independentes. Embora a Lei Geral de Proteção de Dados (LGPD) do Brasil seja fortemente inspirada pelo Regulamento Geral de Proteção de Dados (GDPR) europeu, as melhores práticas de cada região para transparência e provisão de informações têm suas particularidades. Cada região trata incidentes cibernéticos à sua maneira. Por exemplo, os Estados Unidos fornecem relatórios e disponibilizam diversos conjuntos de dados públicos em sua plataforma data.gov. Esses conjuntos de dados incluem informações detalhadas sobre violações de dados em organizações públicas e empresas privadas, incluindo empresas estrangeiras. As informações são altamente detalhadas, listando o período do ataque, tipo de incidente, empresa, cidadãos afetados, mercado impactado e outros detalhes. Esses conjuntos de dados são relatados por cidade, estado ou empresa.

Em contraste, a União Europeia, por meio da ENISA, disponibiliza um relatório com métricas sobre ataques cibernéticos de maneira mais macro, sem especificar empresas, mas sim áreas afetadas. Além disso, embora a ENISA também tenha um site de dados para transparência, nem todos os dados estão disponíveis para consulta pública por outros países.

Com base nos casos acima e na recente participação do Brasil no relatório de segurança cibernética aprovado em Genebra em 2023 (DATA.GOV, 2023b), fica claro que esse tema já está sendo abordado. Embora ambas as regiões utilizem o NIST framework para suas iniciativas de gestão de risco, o Brasil carece de uma iniciativa transparente para o compartilhamento de informações sobre incidentes cibernéticos. Segundo a análise das regiões, a visão geral a seguir é apresentada na Tabela 2.

Tabela 2. Comparação de políticas e legislação de dados de vulnerabilidade

| | Brasil | Estados Unidos | União Europeia |
|---|---|---|---|
| Conjuntos de dados públicos de vulnerabilidades nacionais | Não | data.gov | data.europe, apenas para membros da UE |
| Relatório detalhando os danos aos setores | Não | data.gov | ENISA |
| NIST | Sim | data.gov | Sim |
| Legislação | LGPG | CCPA, NY SHIELD, DDPA | GDPR |

Depois de realizar uma ampla exploração ao longo deste estudo, propomos a seguinte estrutura para padronizar a comunicação de riscos e vulnerabilidades, conforme descrito na Tabela 3.

Tabela 3. Framework proposto

| Vertical | Categoria | Classificação de segurança cibernética |
|---|---|---|
| Identificação | Governança | NIST SP 800-53 PM - 2, 3, 7, 9, 10 e 11 |
| | Estratégia de gerenciamento de riscos | NIST SP 800-53 PM - 9 |
| Proteção | Identificação | NIST SP 800-53 AC - 1, 2, 3, 5, 6, 14 |
| | Gerenciamento | |
| | Autenticação e Controle de Acesso | |
| Detecção | Monitoramento Continuo | NIST SP 800-53 AU - 12, CA - 7 |
| Resposta | Transparência | NIST SP 800-53 PT - 1, 2, 4 e 5 |
| | Mitigação | NIST SP 800-53 IR - 4 |
| Recuperação | Melhoria Continua | NIST SP 800-53 CP - 2 |

# 5. CONCLUSÃO

Esta pesquisa revelou as práticas únicas de regulamentação e divulgação de riscos cibernéticos em diferentes regiões, destacando os desafios e oportunidades específicos de cada abordagem. Nosso objetivo foi não apenas mapear essas particularidades, mas também identificar um caminho viável para a harmonização global, fundamentado em melhores práticas.

Com base no estudo das diferenças regulatórias e modelos regionais, desenvolvemos uma proposta ancorada no NIST SP 800-53, estruturada em subcategorias alinhadas às principais verticais do setor. Este modelo fornece uma base sólida para a padronização do compartilhamento de informações, promovendo transparência e privacidade em um nível granular.

Reconhecemos que a cooperação internacional depende de esforços diplomáticos significativos, mas acreditamos firmemente que a transparência é uma alavanca essencial para fomentar confiança, incentivar investimentos em segurança e minimizar os danos reputacionais. Nosso modelo visa criar um ambiente em que organizações e mercados possam interagir de forma mais segura e informada, permitindo a avaliação precisa de riscos e, ao mesmo tempo, incentivando a resiliência cibernética em escala global.

# REFERÊNCIAS


Aljanabi, M., et al., (2023). ChatGPT: open possibilities. *Iraqi Journal for Computer Science and Mathematics*, 4, pp. 62-64.

Almuhammadi, S. and Alsaleh, M., (2017). Information security maturity model for NIST Cybersecurity Framework. *Computer Science & Information Technology (CS & IT)*, 7, pp. 51-62.

Araújo, J., (2023). *Dez anos de vigência da Lei Carolina Dieckmann: a primeira a punir crimes cibernéticos*. [Online]. Available at: https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos [Accessed: 12 Nov. 2023].

Arnaudo, D., (2017). O Brasil e o Marco Civil da Internet. *O estado da governança digital brasileira: Instituto Igarapé, a think tank*.

Cezarinho, F., (2018). História e fontes da internet: uma reflexão metodológica. *Temporalidades*, 10, pp. 320-338.

City of Tempe, (2023). *Data table for the Cybersecurity (detail) performance measure*. TempeData, Tempe, AZ, USA. [Online]. Available at: https://data.tempe.gov/maps/tempegov::5-12-cybersecurity-detail.

Costa, R. and Pacheco, G., (2018). Crimes virtuais e a legislação penal brasileira. *Revista Eletrônica de Ciências Jurídicas*, 1.

Cybercrime Magazine, (2023). *Cybercrime to cost the world $10.5 trillion annually by 2025*. [Online]. Available at: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ [Accessed: 5 Nov. 2023].

DATA.EUROPA, (2023). *The official portal for European data*. [Online]. Available at: https://data.europa.eu/en [Accessed: 19 Oct. 2023].

DATA.GOV, (2023a). *Aprovado relatório de cibersegurança, em questão de estudo co-liderada pelo Brasil, em Genebra*. [Online]. Available at: https://agenciagov.ebc.com.br/noticias/202311/aprovado-relatorio-de-ciberseguranca-em-questao-de-estudo-co-liderada-pelo-brasil-em-genebra [Accessed: 24 Nov. 2023].

DATA.GOV, (2023b). *Data breach notifications affecting Washington residents*. [Online]. Available at: https://catalog.data.gov/dataset/data-breach-notifications-affecting-washington-residents [Accessed: 19 Oct. 2023].

Devanny, J., et al., (2022). The rise of cyber power in Brazil. *Revista Brasileira de Política Internacional*, 65.

European Union External Action Service, 2016. *EU and NATO cyber defence cooperation*. [Online]. Available at: https://www.eeas.europa.eu/node/3667_en/ [Accessed: 19 Oct. 2023].

Farahbod, K., et al., (2020). Cybersecurity indices and cybercrime annual loss and economic impacts. *Journal of Business and Behavioral Sciences*, 32, pp. 63-71.

Fleck, A., (2022). *Cybercrime expected to skyrocket in coming years*.

Gabinete de Segurança Institucional, (2019). *Padrões para notificação de incidentes cibernéticos ao CTIR Gov*. In Atos do Poder Executivo.

Gabinete de Segurança Institucional, (2020). *Regulamento de segurança cibernética aplicada ao setor de telecomunicações*. In Atos do Poder Executivo.

Hitchens, T., (2017). *International Cybersecurity Information Sharing Agreements*.

Humby, C., (2006). *Data is the new oil. Proceedings of ANA Sr. Marketer's Summit*, Evanston, IL, USA, pp. 1.

Hurel, L. and Lobato, L., (2021). Cyber security governance in Brazil: Keeping silos or building bridges? In *Routledge Companion to Global Cyber-Security Strategy*, pp. 504-518.

Kshetri, N. and DeFranco, J., (2020). The economics of cyberattacks on Brazil. *Computer*, 53, pp. 85-90.

Lugati, L. and Almeida, J., (2022). A LGPD e a construção de uma cultura de proteção de dados. *Revista de Direito*, 14, pp. 01-20.

Machado, F., (2018). *Brasil perde US$ 10 bilhões por ano com cibercrime, diz McAfee*. [Online]. Available at: https://veja.abril.com.br/economia/brasil-perde-us-10-bilhoes-por-ano-com-cibercrime-diz-mcafee [Accessed: 28 Oct. 2023].

Malatras, A., et al., (2023). *ENISA threat landscape: Transport sector* (January 2021 to October 2022).

Mijwil, M., et al., (2023). Exploring the top five evolving threats in cybersecurity: An in-depth overview. *Mesopotamian Journal of Cybersecurity*, 2023, pp. 57-63.

Muggah, R. and Thompson, N., (2015). *Brazil's cybercrime problem. Council on Foreign Relations*. [Online]. Available at: https://www.foreignaffairs.com/articles/south-america/2015-09-17/brazils-cybercrime-problem [Accessed: 28 Nov. 2023].

Neto, N., et al., (2021). Developing a global data breach database and the challenges encountered. *Journal of Data and Information Quality (JDIQ)*, 13, pp. 1-33.

NIST, (2023). *NIST Cybersecurity Framework (CSF) 2.0 reference tool*. [Online]. Available at: https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters [Accessed: 19 Oct. 2023].

Risk Based Security, (2019). 2019 *Year end data breach quickview report*. [Online]. Available at: https://pages.riskbasedsecurity.com/2019-year-end-data-breach-quickview-report [Accessed: 19 Oct. 2023].

Robert, M., Christey, S. and Baker, D., (2002). The Common Vulnerabilities and Exposures (CVE) Initiative. *MITRE* Corporation.

Ruhl, C. et al., (2020). *Cyberspace and geopolitics: Assessing global cybersecurity norm processes at a crossroads. Carnegie Endowment for International Peace*.

Statista Research Department, (2023). *Consumer loss through cyber crime worldwide in 2017, by victim country*. [Online]. Available at: https://www.statista.com/statistics/799875/countries-with-the-largest-losses-through-cybercrime/ [Accessed: 19 Nov. 2023].

Transnational Threats Department OSCE, (2023). *Emerging Practices in Cybersecurity-Related Public-Private Partnerships and Collaboration in OSCE participating States*. Vienna, Austria.

Zygierewicz, A., (2020). *Directive on security of network and information systems (NIS Directive)*. EPRS: European Parliamentary Research Service.