A IMPORTÂNCIA DE UMA TAXONOMIA NACIONAL DE INCIDENTES CIBERNÉTICOS NO CONTEXTO DA REDE FEDERAL DE GESTÃO DE INCIDES CIBERNÉTICOS (ReGIC)

Edesio Cesar Farias dos Santos
242200314@aluno.unb.br

Prof. Dr. Daniel Chaves Café
dcafe@unb.br

Resumo

O aumento constante das ameaças cibernéticas tem evidenciado a necessidade de estruturas capazes de executar o compartilhamento de informações sobre atores e agentes de ameaça. Essas redes de cooperação possibilitam a antecipação de riscos e a disseminação de dados essenciais sobre estratégias de proteção e mitigação de incidentes. A forma com que os eventos de cibersegurança são descritos nas notificações e nos relatórios de incidentes constitui elemento crítico para a comunicação eficaz com os órgãos de coordenação e resposta. Dessa forma, torna-se imprescindível a padronização das terminologias e o registro claro e estruturado dos tipos de eventos que compões esses relatórios. Assim, o emprego de uma taxonomia de incidentes cibernéticos aderente às principais normas e frameworks internacionais, com descrições precisas e adequadas à língua portuguesa, voltada à utilização pelos órgãos participantes da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC), contribuirá para a interpolaridade entre as instituições, o fortalecimento da capacidade de resposta a incidentes e o aprimoramento da gestão da cibersegurança.

Palavras-chave: Taxonomia; Incidentes Cibernéticos; Segurança da Informação; Compartilhamento de Dados; ReGIC.

Abstract

The constant increase in cyber threats has highlighted the need for structures capable of enabling the sharing of information about threat actors and agents. These cooperation networks make it possible to anticipate risks and disseminate essential data on protection strategies and incident-mitigation measures. The way cybersecurity events are described in notifications and incident reports is a critical element for effective communication with coordination and response bodies. Therefore, standardizing terminology and ensuring the clear and structured recording of the types of events that make up these reports becomes essential. In this context, the adoption of a cyber-incident taxonomy aligned with major international standards and frameworks, with accurate descriptions properly adapted to the Portuguese language and intended for use by the entities participating in the Federal Cyber

Incident Management Network (ReGIC), will contribute to interoperability among institutions, strengthen incident-response capabilities, and enhance cybersecurity management.
Keywords: *Taxonomy; Cyber Incidents; Information Security; Data Sharing; ReGIC.*

1. INTRODUÇÃO

A crescente digitalização dos serviços públicos e a dependência de sistemas informatizados pela Administração Pública Federal (APF) têm ampliado significativamente a exposição a incidentes cibernéticos, tornando essencial a adoção de práticas eficientes de gestão e resposta a esses eventos. Nesse contexto, a Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC) assume papel estratégico na coordenação das ações de prevenção, detecção e mitigação de incidentes, garantindo a segurança da informação e a continuidade dos serviços públicos.

Contudo, como observa Alves (2022, p.13), “o espaço cibernético não é um ambiente visível, não havendo nele distinção de fronteiras, do individual, de modo que se torna difícil localizar um ator, assim como as ameaças constantes”, evidenciando a complexidade do ambiente digital e a dificuldade de controle das ameaças. Complementando essa perspectiva, Sheldon (2019) destaca que o espaço cibernético apresenta disponibilidade de atuação por diversos atores, baixo custo e amplas oportunidades estratégicas, caracterizando-se como um ambiente dinâmico, no qual “em sua grande parte, nada é final no espaço cibernético” (Sheldon, 2019, p. 297). Essas características, somadas à velocidade de propagação das informações e à possibilidade de alterações constantes, reforçam a necessidade de instrumentos dinâmicos que facilitem a identificação, classificação e tratamento dos incidentes de forma estruturada e padronizada.

Além disso, com o crescimento do uso de tecnologias digitais e o aumento da complexidade das infraestruturas de informação, os incidentes cibernéticos tornaram-se uma ameaça constante e significativa para organizações públicas e privadas. “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). Nesse contexto, torna-se fundamental o fortalecimento de políticas e práticas voltadas à melhoria da segurança cibernética, por meio da adoção de padrões internacionais de proteção de dados, investimentos em capacitação técnica e desenvolvimento de estratégias integradas

de prevenção, detecção e resposta a incidentes. Tais medidas contribuem para aumentar a resiliência digital dos órgãos e promover um ambiente tecnológico mais seguro e confiável.

Nesse cenário, a inexistência de uma taxonomia nacional padronizada de incidentes cibernéticos dificulta a comunicação entre os órgãos, compromete a interoperabilidade e limita a análise comparativa de informações. Diante disso, este trabalho tem como objetivo analisar a importância de uma taxonomia de incidentes cibernéticos para os órgãos da ReGIC, destacando seu papel na harmonização de terminologias, na padronização de processos e relatórios, e no alinhamento com boas práticas internacionais, contribuindo para a consolidação da governança cibernética e para o fortalecimento da resiliência digital no âmbito da APF.

Ainda sobre a APF, a ReGIC desempenha um papel fundamental na coordenação e resposta aos incidentes cibernéticos, promovendo ações integradas entre os órgãos do governo, órgãos convidados e outras entidades, com o objetivo de garantir a proteção das informações sensíveis e a continuidade dos serviços prestados à sociedade. De acordo com o Decreto nº 10.748, de 16 de julho de 2021, “a Rede Federal de Gestão de Incidentes Cibernéticos tem por finalidade aprimorar e manter a coordenação entre órgãos e entidades da administração pública federal direta, autárquica e fundacional para prevenção, tratamento e resposta a incidentes cibernéticos, de modo a elevar o nível de resiliência em segurança cibernética de seus ativos de informação” (Brasil, 2021).

Nesse contexto, torna-se imprescindível adotar mecanismos que promovam a padronização da linguagem e da classificação dos incidentes, com o objetivo de facilitar a comunicação entre os diversos atores envolvidos na ReGIC e maximizar a eficiência das ações de resposta a ataques cibernéticos. É nesse ponto que uma taxonomia nacional de incidentes cibernéticos se apresenta como um elemento estratégico, capaz de contribuir para a melhoria dos processos de notificação, tratamento de incidentes e elaboração de relatórios técnicos. Segundo a Organização Nacional de Padrões de Informação (*National Information Standards Organization*, 2005), uma taxonomia é um tipo de vocabulário composto por termos preferenciais, ou ainda uma coleção de termos de vocabulário controlado organizados em uma estrutura hierárquica. Cada termo em uma taxonomia está em uma ou mais relações do tipo pai/filho (geral/específico) com outros termos da mesma estrutura.

Assim, a utilização de uma taxonomia estruturada possibilita categorizar diferentes tipos de incidentes, identificar padrões de comportamento malicioso e permitir uma

comunicação precisa entre profissionais da área de segurança, favorecendo o desenvolvimento de estratégias de defesa mais eficazes. A importância dessa uniformização conceitual pode ser ilustrada pelo caso do satélite Mars Climate Orbiter, da *National Aeronautics and Space Administration* (NASA), perdido em 1999 devido a uma falha de comunicação entre duas equipes que utilizavam sistemas de medidas diferentes, o imperial e o métrico. Essa discrepância, aparentemente simples, levou a cálculos incorretos e à destruição da sonda, demonstrando como a falta de padronização terminológica e técnica pode gerar consequências catastróficas. Além disso, ao estabelecer uma linguagem comum entre especialistas, a padronização contribui para a construção de estatísticas confiáveis e comparáveis, que auxiliam na formulação de políticas públicas e ações preventivas. A capacidade de priorizar incidentes com base em seu impacto e gravidade também garante uma resposta mais direcionada e eficiente, especialmente em um ambiente colaborativo, como o da ReGIC

1.2 OBJETIVOS

Objetivo Geral

Analisar a importância da adoção de uma taxonomia nacional de incidentes cibernéticos no contexto da ReGIC, considerando sua contribuição para o fortalecimento da segurança da informação e a melhoria da resposta coordenada a incidentes na APF.

Objetivos Específicos

a. Contextualizar o papel da ReGIC no sistema de gestão de incidentes cibernéticos no âmbito dos órgãos da Administração Pública Federal, conforme estabelecido pelo Decreto nº 10.748, de 16 de julho de 2021, destacando suas atribuições, estrutura e importância estratégica.

b. Conceituar taxonomias de incidentes cibernéticos, apresentando seus fundamentos teóricos, características e benefícios no processo de categorização, comunicação e resposta a incidentes, destacando as dificuldades linguísticas, técnicas e semânticas para criar uma classificação compreensível por diferentes públicos e instituições.

c. Diagnosticar o cenário de classificação de incidentes na ReGIC, avaliando a ausência de um modelo taxonômico padronizado entre os principais órgãos participantes.

d. Sugerir a construção de uma taxonomia nacional que promova interoperabilidade, agilidade na resposta e padronização de relatórios, baseada no consenso entre os

principais atores nacionais da área de segurança cibernética, elaborando uma proposta de tabela de incidentes cibernéticos, listando os principais tipos de incidentes com suas respectivas definições até o segundo nível de classificação, de forma complementar ao Glossário de Segurança da Informação (Portaria GSI/PR nº 93, de 18 de outubro de 2021).

2. REFERENCIAL TEÓRICO

O assunto central deste trabalho abrange o estudo para a utilização de uma taxonomia nacional de incidentes cibernéticos no contexto da ReGIC. Com esse propósito, tornou-se necessária uma fundamentação teórica que contempla reflexões sobre os seguintes temas: taxonomias aplicadas à cibersegurança, padrões internacionais de classificação de incidentes, com o proposto pela Agência da União Europeia para a Cibersegurança (ENISA) e, por fim, a organização da ReGIC.

2.1 O Espaço Cibernético e suas Características

O conceito de espaço cibernético tem sido amplamente debatido por estudiosos da segurança da informação e das relações internacionais. Sobre o espaço cibernético observa Alves (2022, p. 36), "é uma coleção de vários componentes: políticas, conceitos de segurança, proteções, agendas, documentos, avaliação de riscos, atuação, treinamento, garantias, capacidade humana e tecnologias".

De acordo com a Organização para a Segurança e Cooperação na Europa (OSCE, 2023), "o aumento da conectividade e da interdependência digital intensifica os riscos associados às ameaças cibernéticas, exigindo cooperação internacional e mecanismos de resposta coordenada. Esses elementos demonstram que a cibersegurança extrapola os limites técnicos, assumindo relevância estratégica, econômica e política" .

2.2 Gestão de Incidentes Cibernéticos na Administração Pública Federal

No contexto brasileiro, a ReGIC foi instituída pelo Decreto nº 10.748, de 16 de julho de 2021, com o propósito de aprimorar a coordenação entre os órgãos e entidades da APF na prevenção, tratamento e resposta a incidentes cibernéticos. O decreto estabelece que a ReGIC visa "elevar o nível de resiliência em segurança cibernética de seus ativos de informação" (Brasil, 2021).

A estrutura colaborativa da ReGIC representa um avanço na gestão de incidentes, promovendo integração e compartilhamento de informações entre órgãos públicos. Entretanto,

sua efetividade depende de uma linguagem comum entre os participantes, o que demanda a adoção de uma taxonomia nacional de incidentes cibernéticos capaz de uniformizar conceitos, categorias e procedimentos.

Em consonância com essa necessidade, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) publicou a Portaria nº 93, de 18 de outubro de 2021, que institui o Glossário de Termos de Segurança da Informação para uso oficial no governo federal. O documento visa unificar a linguagem de segurança da informação, abordando conceitos fundamentais como autenticidade, confidencialidade, integridade e disponibilidade (Brasil, 2021).

A criação do glossário representou um passo importante rumo à padronização terminológica nacional, servindo de base conceitual para utilização de uma taxonomia nacional de incidentes cibernéticos, alinhada às práticas internacionais e adaptada à realidade da ReGIC e a APF.

2.3 Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC)

A ReGIC foi instituída pelo Decreto nº 10.748/2021, com o objetivo de criar uma rede colaborativa voltada à segurança cibernética entre o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) e os órgãos e entidades da administração direta, autárquica e fundacional da Administração Pública Federal, com foco na gestão de incidentes cibernéticos (Brasil, 2021).

De acordo com o artigo 3º do referido decreto:

> Art. 3º São objetivos da Rede Federal de Gestão de Incidentes Cibernéticos:
> I – divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos;
> II – compartilhar alertas sobre ameaças e vulnerabilidades cibernéticas;
> III – divulgar informações sobre ataques cibernéticos;
> IV – promover a cooperação entre os participantes da Rede; e
> V – promover a celeridade na resposta a incidentes cibernéticos. (Brasil, 2021, p. 2).

A ReGIC estabelece diretrizes para sua composição, funcionamento e articulação institucional. Conforme o artigo 4º, a rede baseia-se na atuação integrada de três tipos principais de equipes:

- Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (EPT-RIC);
- Equipes de Coordenação Setorial;
- Equipes Principais, voltadas à proteção de ativos de informação críticos.

O artigo 5º do decreto define que a ReGIC será coordenada pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR), por meio do CTIR Gov, órgão responsável por centralizar as ações de resposta a incidentes e promover a articulação entre os diferentes membros da rede.

A ReGIC desempenha papel estratégico no enfrentamento das ameaças cibernéticas ao permitir a centralização da resposta a incidentes e o compartilhamento de informações sensíveis entre os órgãos da Administração Pública Federal. Entre seus principais benefícios, destacam-se:

- A existência de equipes principais e de coordenação setorial, que permitem uma resposta eficaz a incidentes de alta severidade que possam comprometer serviços essenciais, como saúde, defesa, transportes e comunicações;
- A obrigatoriedade da criação de ETIRs (Equipes de Tratamento e Resposta a Incidentes de Segurança Cibernética) nos órgãos federais (Art. 12), assegurando que cada entidade possua capacidade mínima para identificar e responder a ameaças, promovendo maior autonomia e resiliência;
- A articulação com estruturas internacionais (Art. 11, IV), que favorece o intercâmbio de informações estratégicas e boas práticas globais em segurança da informação;
- A capacitação constante das equipes técnicas (Art. 12, VII), essencial para enfrentar ameaças sofisticadas e em constante evolução.

Embora a ReGIC represente um avanço expressivo na governança da cibersegurança nacional, sua plena efetividade depende da superação de desafios como:

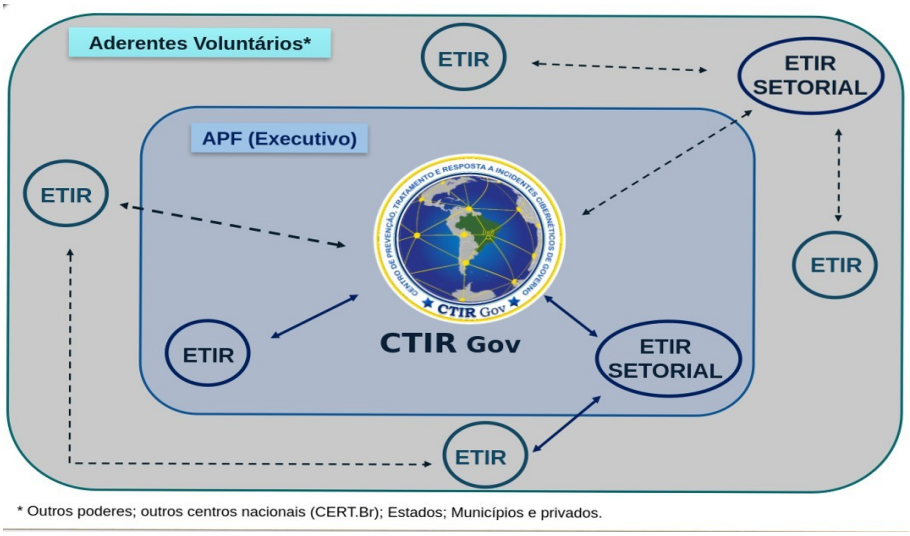
- capacitação e retenção de profissionais especializados;
- atualização contínua da infraestrutura tecnológica;
- cooperação entre diferentes níveis de governo; e
- conformidade com a Lei Geral de Proteção de Dados (LGPD).

O decreto também define prazos específicos para a implementação das ações (Art. 16 e 17), demonstrando a seriedade do compromisso governamental com o fortalecimento da segurança digital no país.

Atualmente, a ReGIC conta em sua *constituency* de aproximadamente 150 organizações participantes, incluindo órgãos convidados de outros Poderes da República,

como o Supremo Tribunal Federal (STF) e o Conselho Nacional de Justiça (CNJ) — este último atuando como órgão setorial da rede e responsável pela coordenação da segurança cibernética no âmbito do Poder Judiciário por meio do Protocolo de Prevenção a Incidentes Cibernéticos do Poder Judiciário (PPICiber/PJ). O esquema de adesão das organizações à ReGIC é apresentado na Figura 1, destacando os diferentes níveis de participação, classificados como obrigatório, voluntário e convidado. O diagrama também evidencia o órgão setorial responsável por receber as notificações de incidentes cibernéticos e encaminhá-las ao CTIR Gov, garantindo o fluxo organizado de informações e o alinhamento das ações de resposta dentro da rede.

Figura 1 - Arquitetura da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC)



Fonte - CTIR Gov (Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo).

O CTIR Gov, enquanto CSIRT de coordenação nacional, disponibiliza diversos produtos e alertas de segurança cibernética, obtidos por meio de instrumentos de cooperação internacional com entidades como a *Cybersecurity and Infrastructure Security Agency* (CISA), o *Forum of Incident Response and Security Teams* (FIRST) e o *National Cybersecurity Network System* (NCNS), entre outros.

O arcabouço normativo reforçado pela ReGIC contribuiu para a melhoria do nível de maturidade do Brasil no *Global Cybersecurity Index* (GCI), elaborado pela *International Telecommunication Union* (ITU), que avalia o compromisso dos países com a cibersegurança com base em cinco pilares: medidas legais, medidas técnicas, medidas organizacionais, desenvolvimento de capacidades e cooperação internacional (ITU, 2024).

As ações voltadas ao compartilhamento de informações sobre ameaças cibernéticas estão alinhadas com as recomendações da Organização das Nações Unidas (ONU). O Relatório do Grupo de Peritos Governamentais sobre os Avanços nas TIC no Contexto da Segurança Internacional destaca que:

> Os Estados devem incentivar a comunicação responsável de vulnerabilidades nas TIC e partilhar informações associadas sobre soluções disponíveis para tais vulnerabilidades, a fim de limitar e possivelmente eliminar potenciais ameaças às TIC e à infraestrutura dependente das TICs (Nações Unidas, 2021, p. 23).

O pilar legal refere-se às leis e regulamentos relacionados à cibersegurança, fundamentais para criar um ambiente seguro no ciberespaço. Envolve a elaboração e aplicação de normas específicas sobre crimes cibernéticos, proteção de dados e privacidade, que possibilitam o processamento de atividades ilícitas on-line e promovem a confiança digital.

Vale destacar que, de acordo com a quinta edição do Global Cybersecurity Index (GCI), elaborado pela International Telecommunication Union (ITU), o Brasil foi classificado no Grupo 1 considerado como modelo e figura como o segundo país mais avançado em maturidade de cibersegurança na América Latina, ficando atrás apenas dos Estados Unidos da América.

Assim, a ReGIC configura-se como instrumento fundamental da Estratégia Nacional de Segurança Cibernética, representando um avanço significativo para a maturidade digital da Administração Pública Federal e para a preservação da soberania e da segurança nacionais.

2.4 Conceito de Taxonomia e sua Aplicação na Cibersegurança

De acordo com a National Information Standards Organization (NISO, 2005), uma taxonomia é um tipo de vocabulário controlado, composto por termos preferenciais organizados de forma hierárquica, de modo a representar relações de generalidade e especificidade entre conceitos. Essa estrutura favorece a padronização terminológica e a consistência na categorização de informações, aspectos fundamentais para a correta interpretação, registro e comunicação de dados em diferentes domínios do conhecimento.

No contexto da cibersegurança, a adoção de uma taxonomia bem definida permite classificar incidentes, identificar padrões de comportamento malicioso e estabelecer indicadores confiáveis que apoiem o planejamento e a execução de estratégias de defesa. Ao proporcionar uma linguagem comum, as taxonomias contribuem para melhorar a

comunicação entre equipes técnicas, instituições e centros de resposta a incidentes, fortalecendo a cooperação e a eficiência operacional no tratamento de ameaças cibernéticas.

Entretanto, a aplicação prática dessas taxonomias enfrenta desafios linguísticos e conceituais, especialmente no que se refere à tradução de termos técnicos do inglês para o português. Essas dificuldades podem gerar ambiguidade terminológica e comprometer a clareza das comunicações, afetando a precisão dos relatórios técnicos e a tomada de decisão em situações críticas. Nesse sentido, torna-se essencial que as iniciativas de padronização considerem aspectos culturais e linguísticos, de modo a garantir que a taxonomia adotada seja consistente, compreensível e aplicável ao contexto nacional.

O termo taxonomia refere-se ao processo sistemático de classificação e organização de elementos com base em características compartilhadas, permitindo estabelecer relações hierárquicas entre conceitos gerais e específicos. Segundo Sant'Ana (2018, p.36), "a definição de uma taxonomia é algo desafiador, uma vez que requer um entendimento detalhado da essência daquilo que se busca definir, ao mesmo tempo em que procura garantir a compreensão universal de um termo, independentemente da audiência à qual ele é exposto".

Em cibersegurança, a aplicação de uma taxonomia tem como objetivo padronizar a terminologia e os critérios de classificação dos incidentes, possibilitando maior consistência e clareza na comunicação entre equipes de resposta, órgãos reguladores e organizações afetadas. Essa estrutura é essencial para reduzir ambiguidades, uniformizar registros e facilitar a análise e o tratamento de incidentes.

A criação de uma taxonomia adequada exige não apenas conhecimento técnico, mas também compreensão semântica e contextual dos eventos de segurança. Isso é particularmente relevante diante da dificuldade de tradução de termos técnicos do inglês para o português, como *phishing*, *spoofing* e *ransomware*, que não possuem equivalentes diretos e podem gerar interpretações ambíguas. Assim, a taxonomia atua como um instrumento de unificação linguística e conceitual, contribuindo para a precisão das comunicações e para o fortalecimento da gestão de incidentes cibernéticos.

2.5 Desafios Linguísticos e Técnicos na Classificação de Incidentes

A tradução de termos técnicos do inglês para o português constitui outro desafio relevante na construção de uma taxonomia nacional. Termos como *phishing*, *spoofing*, *ransomware* e *zero-day* são amplamente utilizados no domínio da segurança cibernética, mas nem sempre possuem equivalentes precisos em português. A falta de uniformização pode

gerar ambiguidades, comprometendo a precisão conceitual e a comunicação entre profissionais.

De acordo com Kaspersky (2022), mesmo profissionais de níveis executivos em empresas brasileiras apresentam dificuldades de compreensão de terminologias comuns da área de segurança cibernética, o que revela uma lacuna linguística e conceitual significativa. A ausência de padronização na tradução pode levar a interpretações equivocadas e afetar a eficácia da resposta a incidentes.

Segundo o CERT.PT, o processo de padronização da classificação de incidentes cibernéticos em Portugal, representou um passo fundamental para a maturidade e a eficácia da resposta nacional a incidentes de cibersegurança. Ao adotar uma taxonomia comum, desenvolvida em conjunto com a Rede Nacional de CSIRT (RNCSIRT), Portugal assegura uma linguagem uniforme entre as diferentes equipes de resposta a incidentes, tanto no contexto nacional como internacional.

Um dos aspetos mais relevantes deste trabalho é a tradução das definições e adaptação dos termos técnicos do inglês para o português, garantindo uma correspondência fiel aos conceitos originais, mas adequada à realidade e ao enquadramento linguístico nacional. Essa harmonização terminológica facilita a compreensão e a utilização da taxonomia por todas as entidades envolvidas, promovendo uma comunicação mais clara e consistente.

2.6 A Situação da Taxonomia de Incidentes Cibernéticos no Brasil

Sobre a taxonomia de incidentes cibernéticos no Brasil, podemos afirmar que:

> No Brasil, inexiste uma taxonomia padrão para a classificação de incidentes cibernéticos compartilhada por múltiplos centros de resposta a incidentes. O CERT.br disponibiliza em seu site estatísticas de incidentes reportados, e por meio destas é possível identificar a forma de classificação de incidentes utilizada pela instituição. Já o CAIS (Centro de Atendimento a Incidentes de Segurança) possui em seu site um grupo de gráficos com bem menos informações, apresentando apenas os quantitativos absolutos de incidentes, conforme imagem a seguir (...). O Centro de Tratamento de Incidentes do governo também possui um rol de classes de ataques bem extensos, possuindo, dentre os três atores comparados, a maior quantidade de classes de incidentes, com 20 classes de ataques em suas estatísticas, que são disponibilizadas em seu site. [...] (Sant’ana, 2018, p. 8)

Além disso, conforme destaca o autor, “a grande variedade de termos pode dificultar a compreensão da exposição do país e das ameaças às quais estamos sujeitos de forma mais cristalina” (Sant’ana, 2018, p. 6). Isso acaba justificando a adoção de um modelo estruturado e nacionalmente reconhecido.

No contexto latino-americano, o Centro de Competência Cibernética da América Latina e Caribe (LAC4), implementado pela EUCyberNet, tem desempenhado papel relevante na adaptação de modelos internacionais às especificidades regionais, promovendo capacitação, intercâmbio de informações e alinhamento terminológico entre países da região. No Brasil, observa-se um movimento crescente de institucionalização da gestão de incidentes. O Decreto nº 10.748/2021 institui a Rede de Gestão de Incidentes Cibernéticos (ReGIC), coordenada pelo GSI/PR, que tem como um de seus objetivos promover integração, comunicação e padronização entre os CSIRTs nacionais.

De forma complementar, a Portaria GSI/PR nº 93/2021 estabeleceu o Glossário de Segurança da Informação, que define terminologias e conceitos fundamentais para a área. O Conselho Nacional de Justiça (CNJ), além de exercer papel fundamental na coordenação das ações de segurança cibernética no âmbito do Poder Judiciário, integra a ReGIC como órgão setorial, conforme estabelecido pelo Decreto nº 10.748/2021. No exercício dessa função, o CNJ elaborou o Protocolo de Prevenção a Incidentes Cibernéticos do Poder Judiciário (PPICiber/PJ), documento que define padrões mínimos de segurança, protocolos de resposta e terminologia unificada para os tribunais e demais órgãos do Judiciário, contribuindo para a harmonização da resposta a incidentes no contexto nacional.

Essas iniciativas demonstram que a padronização terminológica e classificatória é cada vez mais reconhecida como elemento estratégico da governança de cibersegurança. Fazendo-se essencial para a troca eficiente de informações e a coordenação de respostas em âmbito nacional e regional.

2.7 Importância Estratégica da Padronização e da Cooperação

Uma taxonomia estruturada e amplamente adotada permitiria classificar de forma consistente os incidentes cibernéticos, facilitando a identificação de tendências, a priorização de respostas e o desenvolvimento de políticas públicas mais eficazes. Além disso, a padronização da linguagem entre os membros da ReGIC favorece a integração operacional, a interoperabilidade de sistemas e a comunicação entre especialistas.

A implementação de uma taxonomia nacional contribuiria, ainda, para o alinhamento do Brasil com padrões internacionais de cibersegurança, fortalecendo a resiliência institucional e a capacidade de resposta a ameaças digitais complexas. A padronização da classificação de incidentes é uma preocupação de alcance global, e diversas instituições vêm

desenvolvendo estruturas e guias voltados à uniformização das práticas de resposta a incidentes.

O National Institute of Standards and Technology (NIST), dos Estados Unidos, é uma das principais referências internacionais. Seu *Cybersecurity Framework* fornece diretrizes para o gerenciamento de riscos cibernéticos, contemplando categorias e funções padronizadas que auxiliam organizações a identificar, proteger, detectar, responder e recuperar-se de incidentes. Complementarmente, a publicação NIST Special Publication 800-61 Revision 2 – Computer Security Incident Handling Guide propõe uma taxonomia de incidentes que inclui categorias como tentativas de acesso não autorizado, ataques de negação de serviço (DoS/DDoS), malware e violação de políticas de segurança, além de orientar as fases de identificação, contenção, erradicação e recuperação.

A Organização Internacional de Padronização (ISO), por meio da série ISO/IEC 27000, também fornece boas práticas para a gestão da segurança da informação, incluindo métodos para classificação e tratamento de incidentes. Essas normas são amplamente utilizadas por instituições públicas e privadas e constituem referência essencial para certificações e auditorias de segurança.

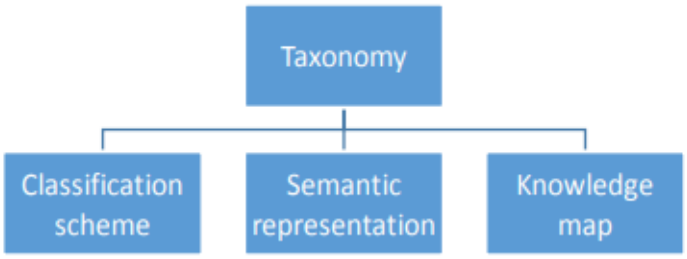
No contexto europeu, a ENISA desenvolveu uma taxonomia detalhada de incidentes de cibersegurança, voltada para a padronização dos relatórios de incidentes entre os Estados-Membros da União Europeia. Essa proposta considera quatro dimensões principais:

- Tipo de incidente (ex.: negação de serviço, acesso não autorizado);
- Origem da ameaça (ex.: humana, natural, técnica);
- Impacto (ex.: vazamento de dados, indisponibilidade de serviço); e
- Setor afetado (ex.: energia, transporte, saúde).

Na Figura 2, observa-se que a estrutura de uma taxonomia é composta por três componentes fundamentais e complementares: o esquema de classificação, a representação semântica e o mapa de conhecimento. O esquema de classificação constitui a base organizacional da taxonomia, sendo responsável por estruturar os conceitos de forma hierárquica e estabelecer relações de generalização e especialização entre eles. Essa organização possibilita a categorização sistemática dos elementos, facilitando a identificação e o agrupamento coerente das informações.

A representação semântica, por sua vez, tem como finalidade definir os significados, atributos e relações entre os termos, assegurando a uniformidade terminológica e a compreensão compartilhada entre os diferentes atores e sistemas que utilizam a taxonomia. Por fim, o mapa de conhecimento atua como um instrumento integrador, responsável por visualizar e correlacionar os conceitos definidos, proporcionando uma visão abrangente das interdependências existentes e favorecendo o compartilhamento e a recuperação de informações. Em conjunto, esses três elementos conferem à taxonomia coerência conceitual, consistência linguística e efetividade prática, características essenciais para sua aplicação na classificação e na gestão de incidentes cibernéticos.

Figura 2 - Representação gráfica de taxonomia – ENISA, 2015



Outras iniciativas relevantes incluem o MITRE ATT&CK, um *framework* amplamente utilizado para mapear o comportamento dos agentes maliciosos com base em táticas e técnicas observáveis. Suas matrizes representam as fases ao longo da linha do tempo tais como *initial access*, *execution*, *persistence* e *exfiltration*, possibilitando a análise e a correlação de campanhas cibercriminosas. Embora o ATT&CK não seja uma taxonomia no sentido estrito, ele serve de base para a categorização técnica e a investigação de incidentes.

O Forum of Incident Response and Security Teams (FIRST), em colaboração com a ENISA e a FS-ISAC, desenvolveu ainda uma taxonomia padronizada de incidentes com foco em interoperabilidade e compartilhamento de relatórios técnicos entre CSIRTs de diferentes países. Essas iniciativas contribuem significativamente para a harmonização internacional das práticas de classificação e resposta a incidentes.

A adoção de uma taxonomia estruturada para incidentes cibernéticos proporciona diversos benefícios. Entre os principais, destacam-se:

- Melhoria da comunicação entre equipes técnicas e gestores;
- Aumento da eficiência na triagem e resposta a incidentes;

- Aprimoramento da colaboração internacional na mitigação de ameaças;
- Criação de bases de dados comparáveis, que facilitam a análise de tendências; e
- Subsídio à formulação de políticas públicas e regulatórias de segurança.

Conforme observa Souza (2023 p. 36), “a taxonomia de incidentes é uma ferramenta crítica para garantir a eficiência e a efetividade da resposta organizacional, permitindo priorizar e tratar incidentes de forma consistente e baseada em evidências”.

Apesar dessas vantagens, ainda existem desafios significativos. A multiplicidade de terminologias técnicas, muitas delas oriundas da língua inglesa, e a falta de equivalentes diretos em português dificultam a tradução e interpretação precisa dos conceitos. Essa realidade pode comprometer a clareza das comunicações e a interoperabilidade entre instituições. Além disso, a rapidez da evolução tecnológica e o surgimento constante de novos tipos de ataques exigem atualização contínua das taxonomias, de modo que elas acompanhem as transformações do cenário cibernético.

Assim, a padronização da linguagem e a adoção de taxonomias compatíveis com os padrões internacionais, como os da ENISA, NIST, MITRE ATT&CK e CERT.PT, constituem etapas fundamentais para o fortalecimento da resiliência cibernética nacional e para o desenvolvimento de uma resposta coordenada, eficiente e sustentável frente às ameaças digitais emergentes.

2.8 Definição do problema – Situação Atual

A ausência de padronização na classificação de incidentes cibernéticos entre as ETIRs e o CSIRT de coordenação, bem como a inexistência de uma taxonomia nacional compartilhada por múltiplos centros de resposta a incidentes, compromete a clareza, a interoperabilidade e a eficiência na comunicação de incidentes. A grande variedade de termos e categorias utilizadas pode dificultar a compreensão das ameaças enfrentadas pelo país e reduzir a efetividade da resposta a incidentes.

Segundo Sant’Ana (2018), a formulação de uma taxonomia puramente brasileira passa pelo entendimento acerca do cenário nacional e de seus atores no tocante às ameaças comuns enfrentadas, devendo ser produto de um consenso entre a comunidade e seus principais representantes. De acordo com Souza (2023), sem uma taxonomia clara, os incidentes podem ser reportados de maneira inconsistente ou com falta de informações importantes, o que pode

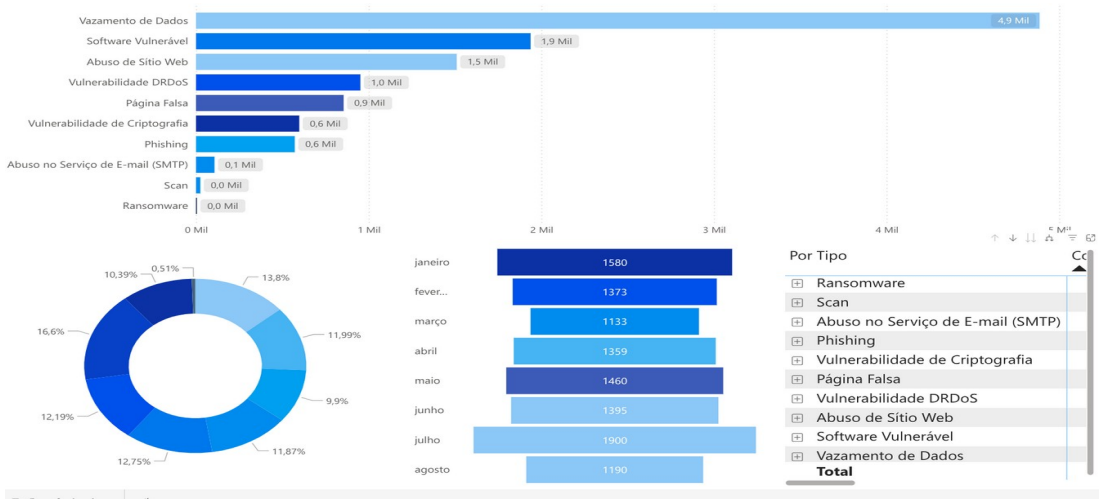
resultar em uma resposta ineficaz ou até mesmo na perda de oportunidades para melhorar a segurança.

Portanto, a falta de uma taxonomia de classificação de incidentes de segurança constitui um problema relevante, pois dificulta a comunicação eficiente entre as equipes, a priorização de incidentes, a alocação adequada de recursos e a melhoria contínua dos processos de segurança da informação.

Complementarmente à análise de artigos relacionados ao assunto, foi aplicado um formulário de avaliação sobre a utilização de taxonomias, respondido por analistas de centros de resposta nacionais, incluindo representantes do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Pesquisa (CAIS/RNP) e Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), compondo uma amostra representativa da diversidade institucional da ReGIC. O instrumento foi estruturado em torno de eixos temáticos que contemplam aspectos técnicos, operacionais e conceituais do tratamento de incidentes.

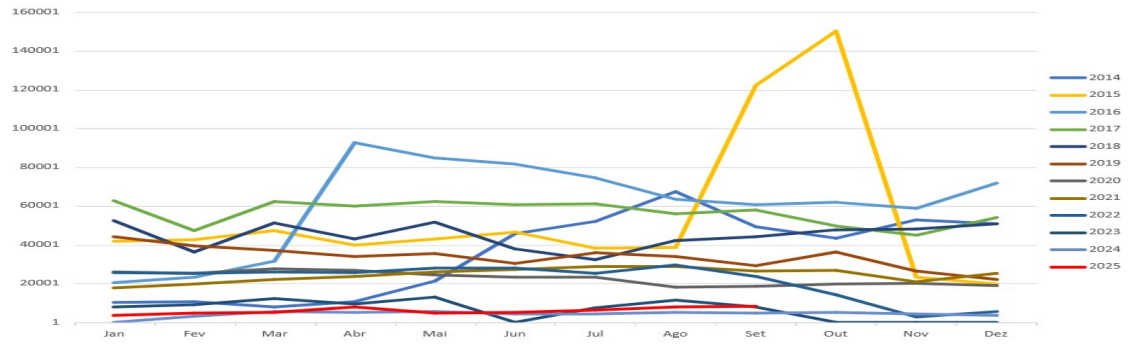
Além disso, foram examinados os relatórios estatísticos publicados pelo CTIR Gov, CAIS/RNP e CERT.br, abaixo apresentados nas Figuras 3, 4 e 5 ,com o objetivo de identificar tendências, categorias de incidentes e práticas de classificação adotadas por cada centro. Observou-se que as formas de apresentação dos dados variam entre as instituições: enquanto o CERT.br divulga séries históricas detalhadas em gráficos e tabelas que permitem a análise comparativa por tipo de incidente e período, o CAIS/RNP enfatiza relatórios anuais com painéis descritivos e indicadores agregados de segurança em redes acadêmicas. Já o CTIR Gov apresenta seus dados em relatórios analíticos, frequentemente acompanhados de avaliações qualitativas e correlações com ameaças emergentes no âmbito governamental.

Figura 3 – Representação das estatísticas de incidentes cibernéticos reportados ao CTIR Gov em 2024.



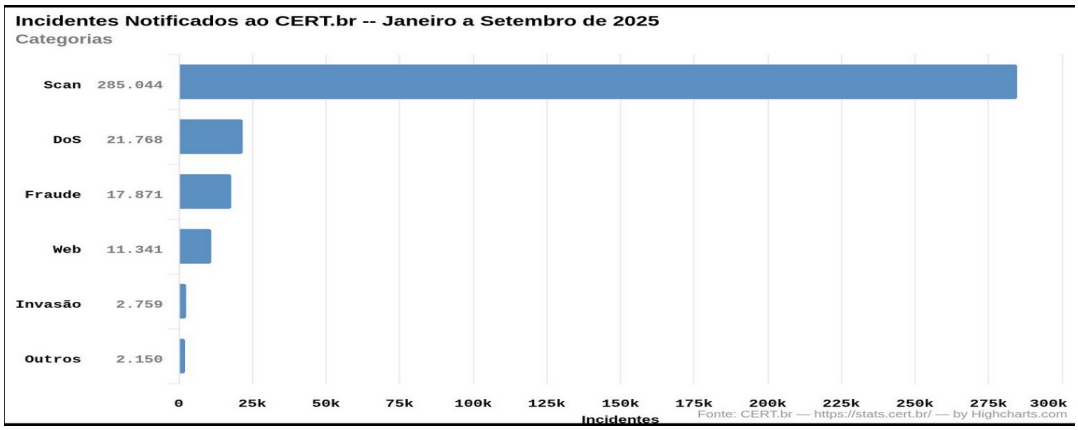
Fonte: CTIR Gov. Disponível em: https://www.ctir.gov.br/.

Figura 4 – Incidentes de segurança reportados ao CAIS/RNP, em 2024



Fonte - CAIS/RNP Disponível em: https://www.rnp.br/cais/.

Figura 5 – Estatísticas de incidentes de segurança reportados ao CERT.br em 2024.



Fonte – CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: https://www.cert.br/.

Essa diversidade de formatos evidencia diferenças nas metodologias de coleta, categorização e divulgação das informações, refletindo as especificidades do público atendido por cada centro e a ausência de um modelo padronizado de reporte de incidentes no contexto nacional. Como observado por Sant'Ana (2018):

> A inexistência de uma taxonomia padrão no Brasil, compartilhada entre múltiplos centros de resposta a incidentes, reflete a fragmentação das abordagens de classificação. Enquanto o CERT.br e o CAIS apresentam categorias e métricas

> distintas, os órgãos governamentais possuem classificações ainda mais amplas e heterogêneas, o que dificulta a comparação de estatísticas e a consolidação de informações em nível nacional. Esse cenário reforça a necessidade de um modelo unificado de categorização de incidentes, que sirva como referência comum para todos os atores envolvidos (Sant'ana, 2018, p. 4).

Dessa forma, a revisão bibliográfica e documental fornece a base teórica e contextual necessária para interpretar os resultados obtidos na pesquisa empírica. Ao reunir informações sobre a estrutura, os referenciais técnicos e as práticas de classificação utilizadas por CERT.br, CTIR Gov e CAIS/RNP, torna-se possível compreender o cenário em que se insere a utilização de taxonomias no tratamento de incidentes. A próxima seção apresenta os resultados do questionário de avaliação da utilização da taxonomia, detalhando as percepções dos analistas participantes e evidenciando como essas práticas se refletem na rotina operacional dos centros de resposta nacionais.

Comparação com redes CSIRT nacionais

A análise comparativa entre os centros de resposta evidencia diferenças significativas na estrutura, abrangência e modelo de atuação, conforme apresentado no Quadro 1 abaixo. O CTIR Gov, vinculado ao Gabinete de Segurança Institucional da Presidência da República, tem foco na coordenação e resposta a incidentes no âmbito da Administração Pública Federal brasileira, atuando como ponto central para notificação, tratamento e disseminação de alertas. Já o CCN-CERT, integrado ao Centro Criptológico Nacional da Espanha, apresenta um modelo mais centralizado e com elevado grau de maturidade, sendo responsável por proteger infraestruturas críticas governamentais e promover a integração com redes europeias de cibersegurança, além de adotar mecanismos avançados de inteligência de ameaças e cooperação internacional. Em contraste, a Rede Nacional de CSIRTs (RNCSIRT) de Portugal, coordenada pelo Centro Nacional de Cibersegurança (CNCS), adota um modelo colaborativo e descentralizado, reunindo múltiplas equipes de resposta de diferentes setores públicos e privados para promover a partilha de informações e boas práticas. Essas distinções refletem as particularidades institucionais e regulatórias de cada país, bem como diferentes níveis de integração, especialização técnica e estratégia de governança na gestão de incidentes cibernéticos.

Quadro 1 - Comparação entre os CSIRTs nacionais do Brasil (CTIR Gov), Espanha (CCN-CERT) e Portugal (RNCSIRT/CNCS)

Item	CTIR Gov(Brasil)	CCN-CERT (Espanha)	RNCSIRT (Portugal)
Missão / papel principal	Centro de prevenção, tratamento e resposta a incidentes cibernéticos no	CSIRT nacional para Administração Pública espanhola, coordenação de	Rede de CSIRTs com entidades públicas e privadas para partilha,

	âmbito da APF.	resposta, inteligência de ameaças, colaboração público-privada.	coordenação e estatísticas de incidentes.
Abrangência (constituency)	Órgãos e entidades da APF no Brasil.	Governo central, administrações autônomas e locais, entidades críticas estratégicas espanholas.	Mais de 40 entidades de diferentes setores, inclui públicas e privadas, fórum de compartilhamento.
Estrutura / organização	Inserido no Gabinete de Segurança Institucional (GSI) da Presidência da República, vinculado ao Departamento de Segurança de Cibernética.	Parte do Centro Criptológico Nacional (CNI) espanhol; reconhecido como entidade acreditada no sistema europeu de CSIRTs.	Rede de CSIRTs coordenada sob o CNCS (Centro Nacional de Cibersegurança) em Portugal; funciona como fórum de excelência para partilha.
Serviços / atividades principais	Notificação de incidentes, triagem/análise/resposta, estatísticas, alertas, cooperação.	Prevenção, detecção, resposta a incidentes, investigação de táticas de ameaça, apoio técnico e operacional à Administração.	Coordenação de incidentes, fóruns técnicos, partilha de boas práticas, produção de indicadores estatísticos nacionais.
Estatísticas / divulgação de dados	Disponibiliza estatísticas de detecção, triagem, análise e resposta por meio do “CTIR Gov em Números”	Participa em redes europeias de CSIRTs	Disponibiliza registro estatístico dos incidentes cibernéticos dos CERT. PT.
Modelo de rede / cooperação	Atua como “CSIRT de coordenação nacional” para a APF, integrando rede de ETIRs e mecanismos de reporte.	Além do CSIRT central, existe rede nacional de SOCs (centros de operações de segurança) integrados sob CCN-CERT.	É uma rede (fórum) de CSIRTs – não é um único centro, mas agrupamento de múltiplas entidades que cooperam.
Taxonomia de Incidentes Cibernéticos	Não possui taxonomia nacional publicamente descrita com classes/tipos detalhados.	Alinhada com a taxonomia da ENISA. Com versão espanhola adaptada no contexto do setor público.	Disponível uma taxonomia nacional em português para classificação de incidentes cibernéticos.

Fonte - Elaborado pelo autor (2025).

3. METODOLOGIA

A utilização de uma Taxonomia Nacional de Incidentes Cibernéticos, no contexto da ReGIC, baseou-se em uma abordagem qualitativa, descritiva e exploratória, com foco na comparação de modelos internacionais e no alinhamento terminológico com as realidades nacionais e regionais, considerando os termos definidos no Glossário de Segurança da Informação (Portaria GSI/PR Nº 93, de 18 de outubro de 2021).

Inicialmente, foram analisadas as principais taxonomias internacionais de referência, incluindo os modelos desenvolvidos pela ENISA, NIST (National Institute of Standards and Technology) e Kaspersky. Essas estruturas foram examinadas quanto à categorização de incidentes, terminologia utilizada, nível de detalhamento e aplicabilidade em diferentes contextos organizacionais.

Além disso, foi considerada a experiência no âmbito do Grupo Agenda Digital do Mercosul (GAD/Mercosul), que discute iniciativas regionais de integração em tecnologia e segurança digital. No contexto das discussões técnicas promovidas pelo grupo, foi sugerida a criação de um mecanismo conjunto para coordenação de atividades de detecção, prevenção, gestão e resposta a incidentes de segurança digital. Essa proposta regional reforça a importância da harmonização terminológica entre os países-membros, contribuindo para a construção de uma taxonomia comum que permita a comunicação eficiente e o intercâmbio de informações estratégicas sobre ameaças.

No plano nacional, foram incorporadas as definições contidas no Glossário de Segurança da Informação, aprovado pela Portaria GSI/PR nº 93/2021, com o objetivo de alinhar os termos propostos aos já reconhecidos oficialmente pelo Governo Federal. Esse alinhamento buscou preservar a consistência conceitual, melhorar as descrições existentes e ampliar a compreensão por parte dos profissionais que atuam na área.

Complementarmente, foram realizadas análises da taxonomia de incidentes cibernéticos adotada por Portugal, considerando a proximidade linguística com o português do Brasil, o que favorece a adaptação e a compreensão dos conceitos técnicos por profissionais locais. Nesse contexto, destaca-se o uso da Taxonomia Comum da Rede Nacional de CSIRT – Versão 3.0, elaborada pelo Grupo de Trabalho - Taxonomia, com apoio da ENISA e do TF-CSIRT RSTI WG (“Task Force for Computer Security Incident Response Teams”)(2020), que apresenta uma estrutura organizada e compatível com os princípios de categorização de incidentes amplamente aceitos internacionalmente. A adoção dessa taxonomia por Portugal reforça sua relevância como referência para países lusófonos em busca de padronização terminológica e operacional no tratamento de incidentes de segurança digital.

A estruturação da proposta também levou em conta a realidade prática das equipes da ReGIC, considerando não só as características operacionais como também os seus níveis de maturidade em cibersegurança. Foi aplicado um formulário de consulta aos CSIRTs participantes da rede, cujas informações foram fornecidas pelos chefes das equipes de analistas. O objetivo foi obter relatos de experiência sobre a importância da adoção de uma taxonomia nacional de incidentes cibernéticos, com ênfase na padronização da classificação e da notificaçãode incidentes no setor público federal.

O formulário foi respondido por analistas de centros de resposta nacionais, incluindo representantes do CAIS/RNP e CTIR Gov, permitindo a coleta de relatos de experiência e percepções desses centros e refletindo a diversidade institucional da ReGIC O instrumento foi composto por questões estruturadas que abordaram: (i) o uso atual de taxonomias padronizadas (como ENISA, NIST ou versões próprias); (ii) os guias e referenciais utilizados pelas equipes; (iii) a existência de distinção entre o tipo de incidente e sua causa-raiz técnica; (iv) a frequência de revisão dos critérios de classificação; (v) a capacidade de mapeamento de incidentes às técnicas do MITRE ATT&CK; (vi) o nível de dificuldade na adequação às taxonomias dos centros de coordenação; (vii) barreiras linguísticas enfrentadas com os termos técnicos em inglês; (viii) o uso de ferramentas que integrem frameworks de classificação; (ix) o grau de granularidade utilizado nas subcategorias de incidentes; e (x) a percepção sobre o nível de padronização entre os diferentes CSIRTs da administração pública federal. Por fim, o formulário incluiu um campo aberto para sugestões de melhorias. As respostas foram tratadas de forma restrita, respeitando os princípios da Lei Geral de Proteção de Dados (LGPD), e analisadas qualitativamente, subsidiando o aprimoramento da proposta de taxonomia quanto à clareza terminológica, aderência às práticas atuais e viabilidade de implementação em nível nacional.

Esse conjunto metodológico permitiu consolidar uma base sólida técnica, normativa e contextual para adoção de taxonomia nacional aderente às necessidades reais das equipes de resposta e aos princípios orientadores da segurança cibernética no setor público brasileiro, em particular pelos órgãos participantes da ReGIC.

4. RESULTADOS

4.1 Instrumento de coleta de dados

O instrumento de pesquisa foi desenvolvido na plataforma Google Forms e direcionado aos analistas dos CSIRTs nacionais, considerando que esses profissionais são os responsáveis por receber, analisar e coordenar as atividades de apoio aos órgãos notificantes, a partir do trabalho executado pelas ETIRs desses órgãos.

O questionário foi composto por dez questões objetivas e uma questão subjetiva (de resposta aberta), elaboradas a partir de pontos-chave relacionados à adoção, utilização e adaptação de taxonomias de incidentes cibernéticos. Os temas abordados incluíram o uso de taxonomias padronizadas (ENISA, NIST, MITRE ATT&CK, entre outras), os referenciais técnicos adotados, a frequência de revisão das classificações, a integração de ferramentas de

apoio, o grau de dificuldade na adequação às taxonomias de centros de coordenação, e a percepção sobre o nível de padronização entre os diferentes CSIRTs da administração pública federal.

4.2 Perfil dos respondentes

O formulário foi encaminhado a profissionais atuantes em centros de resposta que integram a REGIC, contando com a participação de analistas do CTIR Gov, CAIS/RNP e CERT.br. Essa amostra representa a diversidade institucional do ecossistema brasileiro de resposta a incidentes, abrangendo os setores governamental, acadêmico e de coordenação nacional.

A escolha desse público buscou garantir que as respostas refletissem a realidade operacional dos principais atores responsáveis pela classificação e tratamento de incidentes cibernéticos no país, oferecendo um panorama confiável sobre as práticas vigentes.

4.3 Apresentação dos resultados

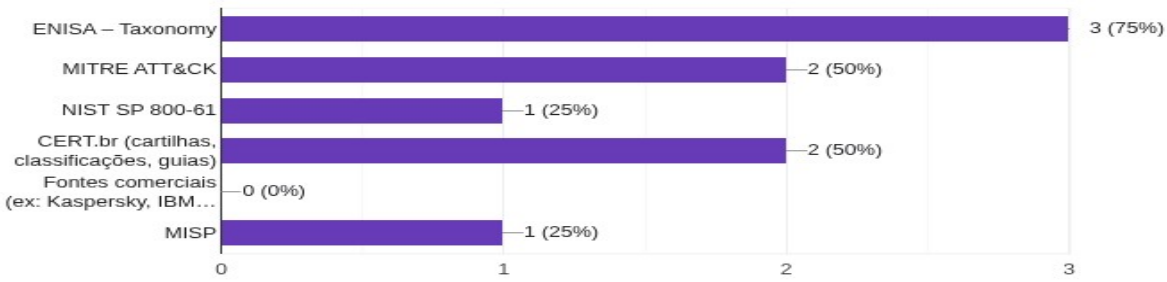
Os resultados do questionário aplicado aos analistas dos centros de resposta nacionais, incluindo representantes do CERT.br, CTIR Gov e CAIS/RNP, permitem compreender o grau de adesão e as práticas relacionadas ao uso de taxonomias e frameworks de classificação de incidentes cibernéticos no contexto da ReGIC.

De maneira geral, as respostas evidenciam um cenário de adoção parcial e adaptativa de taxonomias internacionais, com diferentes níveis de formalização, padronização e integração entre os centros. Essa diversidade de práticas reflete tanto esforços de alinhamento com padrões internacionais quanto ajustes locais voltados à realidade e às necessidades operacionais de cada instituição.

4.4 Resultados do questionário de avaliação da utilização da taxonomia

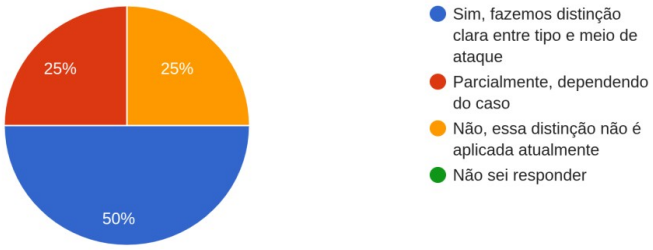
No que se refere à utilização de taxonomias padronizadas, sendo a primeira pergunta do formulário, todos (100%) afirmaram empregar versões adaptadas de taxonomias internacionais, o que demonstra a preocupação em alinhar-se a referenciais globais, embora com ajustes locais para atender às especificidades de cada domínio institucional. Nenhum dos respondentes indicou utilizar uma taxonomia própria ou deixar de empregar um modelo formal, sinalizando uma tendência de harmonização conceitual, ainda que com adaptações contextuais.

Figura 6 - Guias e referencias para classificação e tratamento de incidentes



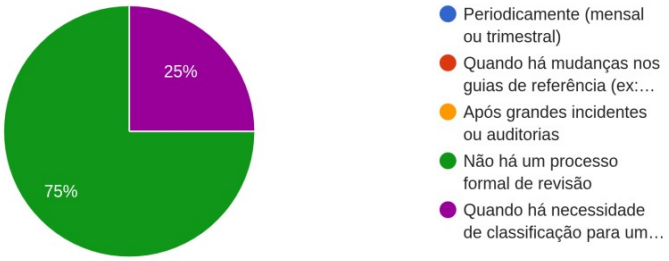
Quanto aos guias e referenciais utilizados para classificação e tratamento de incidentes, Figura 6, os resultados apontam predominância de múltiplas fontes complementares. As mais citadas foram a taxonomia da ENISA (75%) e o MITRE ATT&CK (50%), seguidas pelas cartilhas e classificações do CERT.br (50%) e o NIST SP 800-61 (25%). Apenas um dos respondentes (25%) mencionou o uso do MISP, enquanto fontes comerciais não foram referenciadas. Essa combinação indica que as equipes buscam integrar padrões amplamente reconhecidos a materiais nacionais e operacionais, reforçando o caráter híbrido das práticas de categorização.

Figura 7 - Diferenciação entre vetor de ataque e incidente



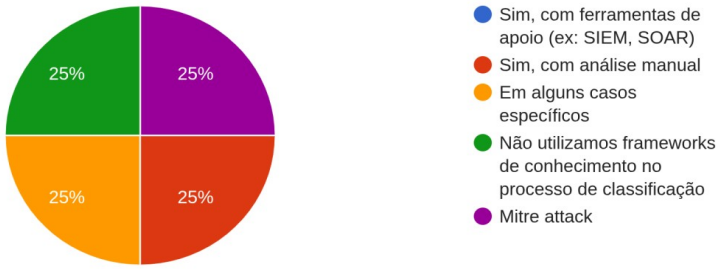
Em relação à diferenciação entre tipo de incidente e vetor de ataque, Fig 7, metade dos participantes (50%) afirmou adotar uma distinção clara entre essas dimensões, enquanto 25% a aplicam parcialmente e outros 25% declararam não utilizar essa diferenciação. Essa variação sugere que, embora o conceito esteja difundido, sua aplicação prática ainda não é uniforme entre os centros.

Figura 8 - Frequência de revisões de classificação



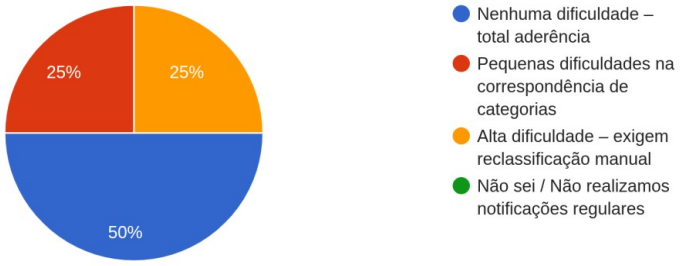
Sobre a frequência de revisão dos critérios de classificação, Fig. 8, três das quatro equipes (75%) relataram não possuir um processo formal de atualização, realizando revisões apenas quando necessário ou diante de novos tipos de incidentes. Esse resultado revela uma baixa institucionalização dos ciclos de manutenção e melhoria contínua das taxonomias utilizadas, o que pode impactar a padronização e a atualização frente às ameaças emergentes.

Figura 9 - Uso de frameworks para mapear TTPs



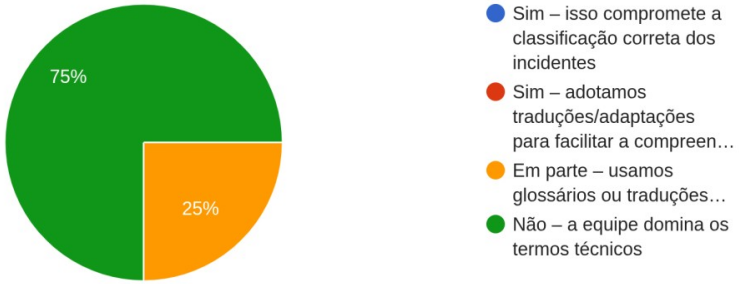
Em relação ao uso de frameworks para mapear técnicas, táticas e procedimentos (TTPs), Figura 9, as respostas foram equilibradas: 25% afirmaram realizar o processo manualmente, 25% aplicá-lo em casos específicos, 25% não utilizar frameworks de conhecimento e 25% mencionaram explicitamente o MITRE ATT&CK como referência. Esses resultados demonstram que, embora o conceito de TTPs seja reconhecido, sua incorporação sistemática ainda não é homogênea.

Figura 10 - Adequação às taxonomias dos centros de coodenação.



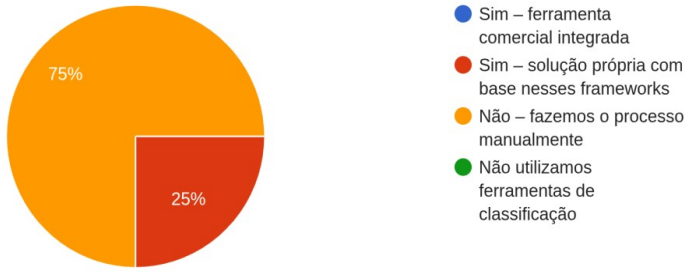
Quanto à adequação às taxonomias dos centros de coordenação (CSIRTs centrais), Figura 10, metade dos respondentes (50%) relatou não encontrar dificuldades significativas, demonstrando aderência às classificações de referência. No entanto, 25% apontaram pequenas dificuldades na correspondência de categorias, e outros 25% relataram alta dificuldade, exigindo reclassificações manuais o que evidencia desafios de interoperabilidade entre taxonomias institucionais.

Figura 11- Barreira linguistica na classificação de incidentes



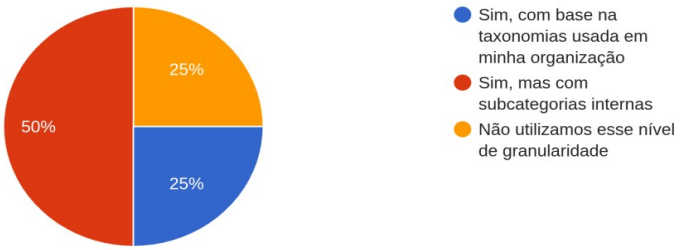
Sobre as barreiras linguísticas, Figura 11, 75% dos participantes afirmaram não enfrentar dificuldades com termos técnicos em inglês, indicando domínio da terminologia especializada. Apenas 25% mencionou recorrer a glossários ou traduções internas para padronizar a compreensão, o que reforça que a língua inglesa não constitui um entrave significativo para a maioria das equipes.

Figura 12 - Ferramentas de integração com taxonomias ou frameworks consolidados



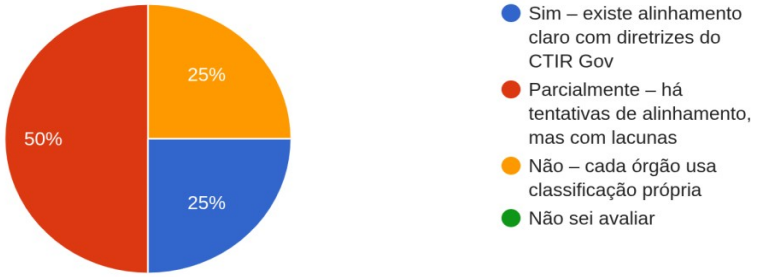
Em relação ao uso de ferramentas que integrem taxonomias ou frameworks consolidados, Figura 12, 75% dos respondentes declararam realizar o processo manualmente, enquanto 25% afirmaram utilizar uma solução própria baseada nesses referenciais. Nenhum participante relatou uso de ferramentas comerciais integradas, o que sugere baixo grau de automação nos processos de classificação.

Figura 13 - Granularidade das classificações



No que diz respeito ao nível de granularidade das classificações, Figura 13, metade das equipes (50%) indicou empregar subcategorias internas próprias, enquanto 25% seguem as subcategorias da taxonomia oficial e outros 25% não utilizam esse nível de detalhamento. Essa diversidade demonstra que há uma tendência à customização interna das categorias, mas sem consenso quanto à profundidade desejada.

Figura 14 - Alinhamento com as diretrizes do CTIR Gov



Quanto à padronização entre os diferentes ETIRs e CSIRTs da administração pública federal, Figura 14, as respostas refletiram uma percepção de alinhamento parcial: a maioria indicou que há tentativas de harmonização com as diretrizes do CTIR Gov, mas ainda com lacunas e inconsistências entre os órgãos. Nenhum participante afirmou haver divergência total, o que reforça a existência de um esforço coletivo em direção à padronização, embora ainda em estágio de consolidação.

Sobre a ultima pergunta, que permitiu respostas abertas sobre sugestões de melhorias para a padronização e o apoio à classificação de incidentes na ReGIC reforçam essa percepção e oferecem subsídios práticos para o aprimoramento do modelo atual. Entre as principais propostas, destaca-se a necessidade de fortalecer o trabalho colaborativo entre as equipes ETIRs e CSIRTs, com ênfase na integração comunicacional e no compartilhamento de informações. Também foi sugerida a criação de uma taxonomia própria e aplicável ao contexto da administração pública federal, alinhada às práticas do CTIR Gov, que viabilize a padronização e o aprimoramento contínuo das trocas entre órgãos e setores.

A análise dos resultados evidencia um cenário compatível com as constatações da literatura revisada, que aponta para uma adoção gradual e não uniforme de taxonomias padronizadas no contexto nacional. Assim como observado nos relatórios públicos do CERT.br, CTIR Gov e CAIS/RNP, as equipes demonstram comprometimento com boas práticas internacionais, mas ainda dependem de adaptações locais e processos manuais para adequar as classificações à sua realidade operacional. A predominância de taxonomias adaptadas reforça a necessidade de um modelo comum de referência, capaz de equilibrar padronização e flexibilidade institucional. Além disso, a ausência de revisões formais e a baixa automação dos processos de categorização indicam maturidade intermediária na gestão da taxonomia, o que pode limitar a integração e a troca de informações entre os CSIRTs. Por

outro lado, a familiaridade com frameworks como o MITRE ATT&CK e o domínio da terminologia técnica demonstram capacidade técnica consolidada nas equipes.

Outro ponto relevante nas respostas é a compreensão dinâmica da categorização de incidentes. Os participantes ressaltaram que a classificação é um processo interativo, sujeito a revisões conforme novas informações são obtidas durante a análise e resposta, em consonância com as fases de contenção, erradicação e recuperação descritas no NIST SP 800-61. Essa perspectiva destaca a importância da flexibilidade e da revisão contínua das categorias, evitando taxonomias excessivamente detalhadas que possam gerar retrabalho ou perda de eficiência operacional.

Por fim, também foram apontadas duas medidas de caráter mais estratégico: (i) a adoção de uma taxonomia consolidada por setor de negócio, com destaque para a ENISA Taxonomy como referência adequada; e (ii) a publicação de um normativo específico para a ReGIC, que defina critérios, responsabilidades e diretrizes para a padronização nacional da classificação de incidentes cibernéticos.

De forma geral, essas recomendações reforçam a convergência entre os achados empíricos e a literatura: a padronização efetiva no contexto da ReGIC não depende apenas da escolha de uma taxonomia, mas da institucionalização de um processo colaborativo e evolutivo de gestão de incidentes, sustentado por mecanismos normativos, interoperabilidade técnica e cultura de cooperação entre os centros de respostas.

5. Lacunas e hipóteses para o presente trabalho

Considerando os diversos estudos que destacam a relevância da definição de uma taxonomia voltada à classificação de incidentes cibernéticos, observa-se que a padronização terminológica e conceitual constitui um elemento essencial para o fortalecimento das práticas de gestão da segurança da informação. Segundo a Agência da União Europeia para a Cibersegurança (ENISA, 2018), uma taxonomia eficaz permite organizar e classificar sistematicamente as ameaças, favorecendo a compreensão dos riscos, a comunicação eficiente entre equipes técnicas, a alocação adequada de recursos e a melhoria contínua dos processos de segurança.

No contexto da ReGIC e dos Centros de Tratamento e Resposta a Incidentes de Segurança Cibernética (CSIRTs) nacionais, conforme verificado a partir dos resultados da pesquisa conduzida por meio do formulário apresentado anteriormente, identificam-se desafios persistentes relacionados à padronização dos termos empregados no processo de

notificação de incidentes cibernéticos. Essa necessidade mostra-se particularmente relevante entre as ETIRs integrantes da rede, considerando que os principais instrumentos de referência atualmente utilizados são a taxonomia da ENISA e o Glossário de Segurança da Informação.

Além disso, destaca-se a importância de aprimorar a compreensão dos termos que não possuem tradução literal para o português, uma vez que tal limitação pode gerar ambiguidades e dificultar os processos de notificação, tratamento e apresentação dos dados. Assim, a adoção de um vocabulário comum, claro e tecnicamente preciso revela-se fundamental para promover a consistência terminológica, a eficiência comunicativa e a confiabilidade dos registros de incidentes cibernéticos no âmbito da ReGIC.

5.1 Estrutura da Taxonomia Proposta

Considerando o cenário identificado a partir da pesquisa realizada e a necessidade de apresentar uma proposta de solução que reduza as dificuldades nos processos de notificação de incidentes cibernéticos, aprimore a compreensão de expressões em inglês e promova a padronização na apresentação dos dados referentes a eventos de segurança, elaborou-se uma proposta de taxonomia nacional de incidentes cibernéticos.

Ao final deste trabalho, no Apêndice 2, são apresentadas as tabelas de taxonomia desenvolvidas com base nas diretrizes da ENISA e ajustadas conforme o Glossário de Segurança da Informação. Essa proposta ainda requer avaliação e validação para futura implementação pelos órgãos integrantes da ReGIC, de modo a possibilitar a descrição detalhada de cada termo até o segundo nível hierárquico (Quadro 2).

No início das tabelas, a seção “Conceitos Gerais” apresenta os termos fundamentais da segurança da informação e da segurança cibernética, servindo como base conceitual para as demais tabelas. Essa etapa busca garantir uniformidade terminológica e coerência semântica, alinhando os conceitos ao vocabulário oficial do Governo Federal. Ao oferecer uma visão sistemática e organizada, os conceitos gerais auxiliam na compreensão das interconexões entre os diferentes componentes da taxonomia.

As tabelas estão organizadas em três categorias principais, incidentes, vulnerabilidades e testes, com o objetivo de oferecer um modelo uniforme, compreensível e aplicável ao contexto institucional da Administração Pública Federal. A divisão da taxonomia proposta baseia-se na distinção conceitual entre eventos controlados, potenciais e reais no contexto da

segurança cibernética. Essa estrutura permite organizar de forma lógica o ciclo de gestão de incidentes, desde a identificação preventiva de falhas até a resposta a eventos efetivos.

Além disso, a separação das categorias facilita a comunicação entre as ETIRs, promove a interoperabilidade com frameworks internacionais, como a ENISA *Taxonomy* e a NIST SP 800-61, e contribui para a consistência terminológica e semântica entre os órgãos integrantes da ReGIC.

A estrutura da taxonomia foi concebida para abranger os principais elementos da gestão de incidentes cibernéticos, proporcionando uma visão integrada e sistemática da segurança digital. Essa organização visa não apenas padronizar a comunicação entre as ETIRs, mas também facilitar a análise de riscos, a identificação de lacunas de segurança e a implementação de estratégias preventivas que reforcem a resiliência cibernética das instituições públicas.

Por fim, a seção “Taxonomia de Incidentes” reúne as principais modalidades de incidentes cibernéticos reconhecidas internacionalmente, incorporando também categorias emergentes que refletem as tendências atuais do setor. Essa classificação possibilita maior precisão na identificação e categorização de incidentes, promovendo agilidade na resposta, consistência nos relatórios e interoperabilidade entre os CSIRTs.

Quadro 2 - Extrato Taxonomia de Incidente Cibernéticos

Classificação de incidente	Categoria	Descrição
Conteúdo Abusivo	Criança/Sexual/Violência/	Pornografia Infantil, glorificação da violência etc.
	Discurso Nocivo	Descrédito ou discriminação de alguém (por exemplo, perseguição cibernética, racismo e ameaças contra um ou mais indivíduos).
	Doxxing	Refere-se à coleta de informações privadas de uma pessoa, realizada por um indivíduo não autorizado, através de múltiplas plataformas, incluindo mídias sociais. Essas informações são então analisadas e publicadas com a intenção de prejudicar a vítima de alguma forma.

A “Taxonomia de Vulnerabilidades” apresenta uma abordagem holística, abrangendo vulnerabilidades conhecidas e recém-descobertas. Seu propósito é facilitar a análise de riscos e apoiar a adoção de medidas preventivas, permitindo identificar falhas de segurança e priorizar ações corretivas. Essa estrutura contribui para a resiliência cibernética institucional e para o aprimoramento contínuo da postura de segurança dos órgãos da ReGIC.

Por fim, a “Taxonomia de Testes” contempla os principais conceitos e práticas de verificação de segurança, essenciais para avaliar a robustez de sistemas e infraestruturas tecnológicas. Essa parte da proposta busca organizar e planejar os testes de forma sistemática, proporcionando uma visão abrangente das etapas de avaliação e auxiliando na detecção de vulnerabilidades, mitigação de riscos e aprimoramento da segurança operacional.

De modo geral, a estrutura da taxonomia proposta representa um modelo de padronização conceitual e operacional, capaz de fortalecer a governança cibernética e promover interoperabilidade técnica, clareza terminológica e eficiência na comunicação de incidentes no âmbito da Administração Pública Federal.

6. CONCLUSÃO

6.1 Problema de pesquisa

O problema central deste estudo consiste na ausência de uma taxonomia padronizada de incidentes cibernéticos entre as organizações que integram a ReGIC. Essa falta de uniformidade dificulta a padronização da comunicação e dos relatórios produzidos pelas ETIRs, comprometendo a clareza, a interoperabilidade e o alinhamento com padrões internacionais. A inexistência de um modelo comum também prejudica o compartilhamento eficiente de informações entre os CSIRTs e a compreensão de termos técnicos, especialmente aqueles de origem inglesa. Tais termos frequentemente apresentam dificuldades de entendimento para profissionais que não dominam o idioma, e muitos não possuem equivalentes diretos que preservem seu sentido técnico preciso. Manter os termos em inglês garante consistência internacional e facilita a comunicação entre profissionais de diferentes países, mas reforça a necessidade de adequação terminológica e esclarecimento conceitual para assegurar o entendimento uniforme entre os diferentes órgãos participantes.

6.2 Objetivos da pesquisa

O presente trabalho teve como objetivo analisar o papel da ReGIC no sistema de gestão de incidentes cibernéticos da Administração Pública Federal, conforme o Decreto nº 10.748, de 16 de julho de 2021, destacando sua estrutura, atribuições e importância

estratégica. Além disso, buscou conceituar e discutir as taxonomias de incidentes cibernéticos, abordando seus fundamentos teóricos, benefícios e os desafios linguísticos, técnicos e semânticos envolvidos na padronização da comunicação e da resposta a incidentes. O estudo também procurou diagnosticar o cenário atual de classificação de incidentes no âmbito da ReGIC, evidenciando a ausência de um modelo taxonômico unificado entre os órgãos participantes, e, por fim, propôs a construção de uma taxonomia nacional que promova interoperabilidade, agilidade na resposta e padronização de relatórios, de forma complementar ao Glossário de Segurança da Informação (Portaria GSI/PR nº 93, de 18 de outubro de 2021).

6.3 Proposta de solução

Como solução para os problemas identificados nos processos de notificação e classificação de incidentes cibernéticos no âmbito da ReGIC, o trabalho apresenta uma proposta de taxonomia nacional de incidentes cibernéticos, elaborada com base nas diretrizes da ENISA e ajustada conforme o Glossário de Segurança da Informação (Portaria GSI/PR nº 93/2021). A proposta visa padronizar a apresentação dos dados, facilitar a compreensão de termos técnicos em inglês e uniformizar os relatórios de incidentes. Estruturada em três categorias principais incidentes, vulnerabilidades e testes, a taxonomia foi concebida para oferecer um modelo coerente, compreensível e aplicável no contexto institucional, permanecendo sujeita à avaliação e validação pelos órgãos integrantes da ReGIC antes de sua implementação.

6.4 Metodologia aplicada

A metodologia adotada neste estudo caracteriza-se como pesquisa exploratória e descritiva, de abordagem qualitativa, fundamentada em pesquisa bibliográfica e análise comparativa. O estudo buscou proporcionar maior familiaridade com o problema da ausência de padronização na classificação de incidentes cibernéticos e descrever o contexto organizacional da ReGIC.

Foram analisadas taxonomias internacionais de referência, como as desenvolvidas pela ENISA, NIST e Kaspersky, considerando sua estrutura de categorização, terminologia e aplicabilidade em diferentes contextos institucionais. Também foram incorporadas referências regionais, como as discussões do Grupo Agenda Digital do Mercosul, que reforçam a importância da harmonização terminológica para o intercâmbio de informações sobre ameaças.

No âmbito nacional, o estudo baseou-se nas definições do Glossário de Segurança da Informação, buscando alinhar a proposta de taxonomia aos padrões oficiais do Governo Federal. Além disso, foi examinada as definições dos termos utilizados na Taxonomia Comum da Rede Nacional de CSIRT de Portugal (versão 3.0), em razão da proximidade linguística e da relevância como modelo para países lusófonos.

Por fim, foi aplicado um formulário de opinião junto a analistas dos CSIRTs da ReGIC, com o intuito de coletar percepções sobre a necessidade e os benefícios da adoção de uma taxonomia nacional de incidentes cibernéticos, visando à padronização dos processos de notificação e tratamento de incidentes no setor público federal.

6.5 Avaliação sintética dos resultados

A avaliação dos resultados revelou que a adoção de taxonomias de incidentes cibernéticos no âmbito nacional ocorre de forma gradual e não uniforme, confirmando as constatações da literatura e dos relatórios de entidades como CERT.br, CTIR Gov e CAIS/RNP. Observou-se que as equipes demonstram adesão às boas práticas internacionais, mas ainda dependem de adaptações locais e processos manuais, evidenciando a necessidade de um modelo padronizado de referência que equilibre uniformidade e flexibilidade institucional.

A ausência de revisões formais e a baixa automação dos processos de categorização apontam para uma maturidade intermediária na gestão da taxonomia, limitando a integração entre os CSIRTs. Por outro lado, a familiaridade com frameworks como o MITRE ATT&CK e o domínio da terminologia técnica demonstram capacidade técnica consolidada.

As respostas também destacaram que a categorização é um processo dinâmico e iterativo, sujeito a revisões conforme novas informações são obtidas, em consonância com as diretrizes do NIST SP 800-61. Entre as medidas sugeridas, destacam-se a adoção de uma taxonomia consolidada por setor, tomando a ENISA *Taxonomy* como referência, e a publicação de um normativo específico para a ReGIC, estabelecendo critérios e diretrizes para a padronização nacional.

De modo geral, os resultados indicam que a efetiva padronização depende não apenas da definição de uma taxonomia comum, mas da institucionalização de um processo colaborativo e evolutivo de gestão de incidentes, apoiado por normas, interoperabilidade técnica e cultura de cooperação entre os centros de resposta.

6.6 Considerações finais

A análise dos resultados e a consolidação das discussões permitem afirmar que os objetivos propostos foram integralmente alcançados. O estudo contextualizou o papel da ReGIC no sistema de segurança da Administração Pública Federal, destacando sua estrutura, atribuições e relevância estratégica, conforme o Decreto nº 10.748/2021. Também foi conceituado o uso de taxonomias de incidentes cibernéticos, apresentando seus fundamentos teóricos, benefícios e desafios de padronização linguística e técnica, em consonância com a literatura especializada.

O trabalho diagnosticou o cenário atual de classificação de incidentes na ReGIC, confirmando a inexistência de um modelo taxonômico unificado e a consequente necessidade de harmonização terminológica e processual entre os órgãos participantes. Por fim, foi elaborada e apresentada uma proposta de taxonomia nacional de incidentes cibernéticos, estruturada com base nas diretrizes da ENISA e alinhada ao Glossário de Segurança da Informação (Portaria GSI/PR nº 93/2021), contemplando as categorias de incidentes, vulnerabilidades e testes.

Portanto, o trabalho cumpriu seus objetivos geral e específicos, ao propor uma solução prática e conceitualmente fundamentada para promover padronização, interoperabilidade e clareza na comunicação de incidentes cibernéticos, contribuindo para o aprimoramento da governança de segurança digital no âmbito da Administração Pública Federal.

7. REFERÊNCIAS

AGANETTE, Elisângela Cristina. **Taxonomias corporativas: um estudo sobre definições e etapas de construção fundamentado na literatura publicada.** 2010. 104 f. Dissertação (Mestrado em Ciência da Informação) – Escola de Ciência da Informação, Universidade Federal de Minas Gerais, Belo Horizonte, 2010.

ALVES, Dafne. **Ataques cibernéticos ao Brasil: levantamento sistemático dos últimos dez anos (2010–2020)**. 2022. Trabalho de Conclusão de Curso (Bacharelado em Relações Internacionais) – Faculdade de Ciências Econômicas, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2022.

BRASIL. **Decreto nº 10.748, de 16 de julho de 2021. Institui a Rede de Gestão de Incidentes Cibernéticos (ReGIC)**. Diário Oficial da União: seção 1, Brasília, DF, 19 jul. 2021.

BRASIL. **Portaria GSI/PR nº 93, de 26 de fevereiro de 2021. Aprova o Glossário de Segurança da Informação**. Diário Oficial da União: seção 1, Brasília, DF, 1º mar. 2021.

CENTRO NACIONAL DE CIBERSEGURANÇA. Taxonomia de classificação de incidentes de cibersegurança. Lisboa: CNCS, v. 1.1, 1 ago. 2024. Disponível em: https://www.cncs.gov.pt/pt/certpt/taxonomia/. Acesso em: 23 out. 2025.

CCN - CERT – CENTRO CRIPTOLÓGICO NACIONAL. Disponível em: https://www.ccn-cert.cni.es/en/. Acesso em: 30 out. 2025.

CONSELHO NACIONAL DE JUSTIÇA (Brasil). Protocolo de Prevenção a Incidentes Cibernéticos do Poder Judiciário (PPICiber/PJ). Brasília, DF: CNJ, 2022. Disponível em: https://www.cnj.jus.br/. Acesso em: 23 out. 2025.

DANTAS, Mauri Sudário Ferreira et al. **Desafios no compartilhamento internacional de informações sobre ataques cibernéticos: uma análise comparativa entre Brasil, Estados Unidos e Europa.** Brasília, DF: Universidade de Brasília, Programa de Mestrado Profissional em Engenharia Elétrica, 2023.

ENISA – EUROPEAN UNION AGENCY FOR CYBERSECURITY. Reference incident classification taxonomy. Luxemburgo: ENISA, 26 jan 2018. Disponível em: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy. Acesso em: 3 out 2025.

EUCYBERNET. LAC4 – **Latin America and Caribbean Cyber Competence Centre**. Tallinn: EUCyberNet, 2024. Disponível em: https://eucybernet.eu/lac4/. Acesso em: 23 out 2025.

FERREIRA, Herbert Alcântara. **Sistema de organização do conhecimento para aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD): desenvolvimento de taxonomias para instituições hospitalares.** 2023. Tese (Doutorado em Ciência da Informação) – Programa de Pós-Graduação em Ciência da Informação, Universidade Federal de Santa Catarina, Florianópolis, 2023.

FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS (FIRST). Traffic Light Protocol (TLP) and incident classification guidelines. Cary, NC: FIRST, 2023. Disponível em: https://www.first.org/. Acesso em: 23 out 2025.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GRUPO DE TRABALHO – **TAXONOMIA. Taxonomia comum da Rede Nacional de CSIRT (RNCSIRT)**: versão 3.0 (ENISA / TF-CSIRT RSTI WG v.1002). Lisboa: CNCS, jan 2020. Disponível em: https://www.cncs.gov.pt/content/files/Taxonomia_CSIRT_PT.pdf. Acesso em: 9 out. 2025.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). Global Cybersecurity Index (GCI) 2024. Genebra: ITU, 2024. Disponível em: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. Acesso em: 9 out. 2025.

ISO – INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27000 series – Information security management systems. Genebra: ISO, 2018. Disponível em: https://www.iso.org/isoiec-27001-information-security.html. Acesso em: 23 out. 2025.

KASPERSKY LAB. Incident response taxonomy and threat intelligence framework. Moscou: Kaspersky, 2022. Disponível em: https://www.kaspersky.com/. Acesso em: 23 out 2025.

71**Agenda Digital: mecanismo conjunto para coordenação de atividades de detecção, prevenção, gestão e resposta a incidentes de segurança digital.** Montevidéu: MERCOSUL, 2023. Disponível em: https://www.mercosur.int/pt-br/temas/agenda-digital/. Acesso em: 9 out 2025.

MITRE CORPORATION. MITRE ATT&CK® framework. McLean, VA: MITRE, 2024. Disponível em: https://attack.mitre.org/. Acesso em: 23 out 2025.

NAÇÕES UNIDAS. Relatório do Grupo de Peritos Governamentais sobre os avanços nas TIC no contexto da segurança internacional. A/76/135, 14 jul. 2021. Disponível em: https://undocs.org/A/76/135. Acesso em: 3 out 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Framework for improving critical infrastructure cybersecurity. Gaithersburg, MD: NIST, 2018. Disponível em: https://www.nist.gov/cyberframework. Acesso em: 23 out 2025.

NATIONAL INFORMATION STANDARDS ORGANIZATION (NISO). Guidelines for the construction, format, and management of monolingual controlled vocabularies (ANSI/NISO Z39.19-2005). Bethesda, MD: NISO Press, 2005. Disponível em: https://www.niso.org/standards/z39-19-2005. Acesso em: 23 out 2025.

SANT’ANA, Hélio Cabral. **A importância de uma taxonomia para classes de incidentes cibernéticos**. LinkedIn, 6 jul. 2018. Disponível em: <URL-exato-do-artigo>. Acesso em: 22 out 2025.

SANT’ANA, José Ricardo de Souza. **Taxonomia para classificação de incidentes cibernéticos: proposta para o Brasil**. Brasília, DF: Escola Superior de Guerra, 2018.

SOUZA, Rafael de. T**axonomias de incidentes de segurança: aplicação e importância para resposta organizacional.** Revista Brasileira de Segurança da Informação, São Paulo, v. 5, n. 2, 2023.

Apêndice A – Instrumento de Coleta de Dados: Questionário sobre Taxonomia Nacional de Incidentes Cibernéticos

A IMPORTÂNCIA DE UMA TAXONOMIA NACIONAL DE INCIDENTES CIBERNÉTICOS NO CONTEXTO DA REGIC

Esta pesquisa integra um estudo acadêmico vinculado ao Programa de Pós-Graduação Profissional em Engenharia Elétrica da Universidade de Brasília (UnB).

O objetivo do estudo é coletar informações para avaliar a importância da adoção de uma taxonomia nacional de incidentes cibernéticos, com foco na padronização da classificação e da notificação entre os órgãos da REGIC (Rede Federal de Gestão de Incidentes Cibernéticos), contribuindo para o fortalecimento da segurança da informação e a melhoria da atuação conjunta no setor público federal.

A sua participação consiste no preenchimento de um questionário estruturado, com tempo estimado de menos de 10 minutos. Ao prosseguir com o preenchimento do questionário, você declara estar ciente das informações aqui apresentadas e consente, de forma livre e esclarecida, com a utilização das suas respostas nos termos da LGPD (Lei nº 13.709/2018).

Agradeço pela sua colaboração!

- 1. Sua equipe utiliza alguma taxonomia padronizada para classificar incidentes cibernéticos?

( ) Sim, a taxonomia da ENISA

( ) Sim, uma versão adaptada da ENISA

( ) Sim, uma taxonomia própria

( ) Não utilizamos uma taxonomia formal

( ) Outro (especifique): _____

- 2. Quais guias e referenciais sua equipe utiliza para classificar, categorizar ou tratar incidentes cibernéticos? (Marque todos que se aplicam)

( ) ENISA – Taxonomy

( ) MITRE ATT&CK

( ) NIST SP 800-61

( ) CERT.br (cartilhas, classificações, guias)

( ) Fontes comerciais (ex: Kaspersky, IBM X-Force, etc.)

( ) Outro (especifique): _____

- 3. A taxonomia utilizada contempla a diferenciação entre tipo de incidente e causa raiz (técnica ou tática)?

( ) Sim, fazemos distinção clara entre tipo e causa técnica

( ) Parcialmente, dependendo do caso

( ) Não, essa distinção não é aplicada atualmente

( ) Não sei responder

- 4. Com que frequência a sua equipe revisa e atualiza os critérios de classificação de incidentes?

( ) Regularmente (mensal ou trimestral)

( ) Quando há mudanças nos guias de referência (ex: ENISA, NIST)

( ) Após grandes incidentes ou auditorias

( ) Não há um processo formal de revisão

( ) Outro (especifique): _____

- 5. Sua equipe consegue mapear incidentes reais às técnicas e táticas do MITRE ATT&CK de forma sistemática?

( ) Sim, com ferramentas de apoio (ex: SIEM, SOAR)

( ) Sim, com análise manual

( ) Em alguns casos específicos

( ) Não utilizamos o MITRE ATT&CK no processo de classificação

( ) Outro (especifique): _____

- 6. Durante a notificação de incidentes ao CSIRT, qual o nível de dificuldade encontrado na adequação à taxonomia utilizada pelo centro de coordenação?

( ) Nenhuma dificuldade – total aderência

( ) Pequenas dificuldades na correspondência de categorias

( ) Alta dificuldade – exigem reclassificação manual

( ) Não sei / Não realizamos notificações regulares

- 7. A equipe encontra dificuldades com termos técnicos em inglês presentes nas classificações (ex: Initial Access, Persistence, Exfiltration)?

( ) Não – a equipe domina os termos técnicos

( ) Em parte – usamos glossários ou traduções internas

( ) Sim – isso compromete a classificação correta dos incidentes

( ) Sim – adotamos traduções/adaptações para facilitar a compreensão

- 8. Sua equipe utiliza alguma ferramenta ou sistema que já integra taxonomias ou frameworks (ENISA, MITRE, NIST)?

( ) Sim – ferramenta comercial integrada

( ) Sim – solução própria com base nesses frameworks

( ) Não – fazemos o processo manualmente

( ) Não utilizamos ferramentas de classificação

- 9. Sua equipe utiliza subcategorias específicas conforme a taxonomia (ex: "Malicious Code > Ransomware")?

( ) Sim, com base em taxonomias como ENISA ou CERT.br

( ) Sim, mas com subcategorias internas

( ) Não utilizamos esse nível de granularidade

( ) Outro (especifique): _____

- 10. Existe padronização na forma como os incidentes são classificados e descritos entre as(os) ETIRs, CSIRTs setoriais, CERT.BR e o CTIR Gov?

( ) Sim – existe alinhamento claro com diretrizes do CTIR Gov

( ) Parcialmente – há tentativas de alinhamento, mas com lacunas

( ) Não – cada órgão usa classificação própria

( ) Não sei avaliar

- 11. Sugira melhorias para padronização ou apoio à classificação de incidentes na REGIC e na interação com o CSIRT:

(Resposta aberta)

Apêndice B – Proposta de Tabelas de Taxonomia de Incidentes Cibernéticos

1. Conceitos Gerais

Termo	Descrição
Adware	Software projetado especificamente para apresentar propagandas. Pode ser usado de forma legítima, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro, para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo realizado.
Agente de Ameaça	Responsável por desencadear e atuar como catalisador de uma ameaça. Esse termo engloba tanto atores humanos maliciosos quanto eventos naturais (terremotos, inundações e incêndios). A relação entre agente e ameaça é intrínseca, pois é a ação do primeiro que concretiza o segundo.
Ameaça	Refere-se à possibilidade de um agente de ameaça causar danos a um sistema informatizado. Esse dano pode incluir a perda ou alteração de dados, acesso não autorizado a recursos, interrupção de serviços ou até danos físicos à infraestrutura, entre outros;
Ameaça Persistente Avançada (APT)	Ataque de longo prazo com o objetivo de infiltrar ou exfiltrar dados, sem ser descoberto. Possui ciclo de vida mais longo e mais complexo do que em outros ataques, sendo mais elaborado e necessitando de volume significativo de recursos para sua viabilização, o que exige forte coordenação. Em geral, são realizadas por grupos com intenção de espionagem ou sabotagem.
Antimalware	Software desenvolvido para proteger os sistemas contra diversos tipos de malware, como worms, trojans e vírus. Seu mecanismo de detecção é baseado em análise comportamental, sendo capaz de detectar, remover ou isolar muitas atividades suspeitas. Ao contrário do antivírus, pode ser capaz de identificar ameaças nunca vistas antes.
Antivírus	Software que ajuda na proteção de sistemas, especificamente contra ataques de vírus. Tipicamente utiliza um mecanismo de detecção baseado em assinaturas, limitando-se a identificar apenas ameaças cujas assinaturas sejam conhecidas.
Arma Cibernética	Software, hardware ou firmware projetado e aplicado especificamente para causar dano, por meio do domínio cibernético, podendo ser utilizado individualmente ou em

	conjunto para aumentar os efeitos desejados.
Arma Cibernética Cinética	Arma cibernética projetada ou aplicada especificamente para causar danos físicos, direta ou indiretamente, tanto em pessoas como em equipamentos, somente por meio da exploração de vulnerabilidades dos sistemas e dos processos de informação.
Atividade Maliciosa	Qualquer atividade que infrinja a política de segurança de uma instituição e que atente contra a segurança de um sistema.
Artefato Malicioso	Software ou código criado com o objetivo de causar danos, roubar dados ou comprometer a segurança de sistemas e redes. Esses artefatos podem se infiltrar em dispositivos de diversas maneiras e são projetados para operar de forma oculta, dificultando sua detecção e remoção.
Ataque Cibernético	Trata-se de um ato intencional realizado com a finalidade de causar danos aos sistemas computacionais, visando provocar prejuízos, paralisações, obter acesso indevido ou roubar informações.
Ator de Ameaça	Indivíduo ou grupo que representa um risco à segurança cibernética, intencionalmente causando incidentes. Esse termo abrange não apenas criminosos cibernéticos, mas também um espectro mais amplo de agentes, incluindo hackers, script kiddies, ativistas (hacktivistas), ideólogos, terroristas, insiders e Estados estrangeiros. Todos esses perfis se enquadram no conceito de agente de ameaça
Blockchain	Tecnologia de registro descentralizado que armazena transações em blocos encadeados. A base de dados cresce continuamente com a adição de novos blocos, sem que os registros anteriores sejam excluídos. Cada bloco é protegido criptograficamente, garantindo a integridade e a imutabilidade das informações.
Código Malicioso	Software ou parte de software anexado a outro, projetado para realizar atividades prejudiciais ou indesejadas em um sistema computacional.
Comprometimento	Situação em que ocorre uma violação da segurança da informação, resultante de ação ou omissão, seja intencional ou acidental.
Crime Cibernético	Ato criminoso ou abusivo contra redes ou sistemas de informação, envolvendo o uso de um ou mais computadores, seja como ferramentas para a execução do delito ou como alvo, com o objetivo de causar incidentes, desastres cibernéticos ou obter lucro financeiro.
Firewall	Dispositivo de segurança cibernética cujo objetivo é controlar o tráfego entre redes computacionais distintas, de acordo com um conjunto de regras pré-estabelecidas que delimitam o tráfego de dados de entrada, saída ou de passagem.

Incidente Cibernético	Qualquer evento adverso, relacionado à segurança dos sistemas de computação ou das redes de computadores, confirmado ou sob suspeita de impactar a disponibilidade, integridade, confidencialidade ou a autenticidade de um ativo de informação.
Informações de Segurança e Gerenciamento de Eventos (SIEM — Security Information and Event Management)	Ferramenta que oferece uma visão centralizada do cenário de segurança de uma infraestrutura de TI, monitorando, registrando e analisando eventos de segurança em tempo real. Coleta dados de diversos dispositivos e sistemas, sinaliza anomalias e notifica equipes responsáveis sobre possíveis violações de segurança.
Invasão	Incidente de segurança no qual o ataque foi bem-sucedido, resultando no comprometimento da disponibilidade, integridade, confiabilidade ou autenticidade das informações ou dos ativos de informação de uma organização.
Malware	Software malicioso, projetado para infiltrar um sistema computacional, geralmente com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. É um termo genérico que inclui vírus, *worms*, trojans, entre outros.
Open Source Intelligence (OSINT)	Inteligência produzida pela coleta, avaliação e análise de informações publicamente disponíveis com o objetivo de responder a uma questão específica de inteligência. No contexto de segurança cibernética, OSINT pode ser usado para coletar informações sobre alvos potenciais ou para entender melhor as ameaças emergentes.
Rede Privada Virtual (VPN —Virtual Private Network)	Rede de comunicações privada construída sobre uma rede pública. Ela criptografa o tráfego de internet e oculta sua identidade online, dificultando que terceiros rastreiem suas atividades ou roubem seus dados. A criptografia ocorre em tempo real, garantindo maior segurança durante a navegação.
Script	Um conjunto de instruções escritas que automatizam tarefas em um sistema computacional, fornecendo uma maneira eficiente de realizar operações específicas.
Sniffer	Ferramenta de monitoramento de tráfego de rede que captura e analisa pacotes de dados que são transmitidos. Tipicamente utilizada para identificar problemas, otimizar desempenho e detectar intrusões. Pode ser hardware, software ou ambos, e opera na camada de enlace de dados.
Spam	Mensagens eletrônicas comumente enviadas em grandes quantidades (envios em massa), geralmente não solicitadas pela vítima, contendo anúncios comerciais, mas sendo possível, por vezes, haver conteúdo malicioso.
Vulnerabilidade	Fraqueza ou falha encontrada em um sistema de software ou hardware que pode ser explorada por um agente de ameaça para realizar atividades mal intencionadas, como obter acesso não autorizado, roubar dados, instalar

	malware ou interromper operações.
Zumbi	Computador que foi comprometido por malware que instalou um “bot”, viabilizando o acesso e controle remoto por um agente malicioso, geralmente sem o conhecimento do proprietário do equipamento.

2. Taxonomia

2.1 Taxonomia de Incidentes

Classificação de incidente	Categoria	Descrição
Conteúdo Abusivo	Criança/Sexual/Violência/	Pornografia Infantil, glorificação da violência etc.
	Discurso Nocivo	Descrédito ou discriminação de alguém (por exemplo, perseguição cibernética, racismo e ameaças contra um ou mais indivíduos).
	Doxxing	Refere-se à coleta de informações privadas de uma pessoa, realizada por um indivíduo não autorizado, através de múltiplas plataformas, incluindo mídias sociais. Essas informações são então analisadas e publicadas com a intenção de prejudicar a vítima de alguma forma.
	Backdoor	Mecanismo inserido intencionalmente ou acidentalmente em um sistema, com o objetivo de permitir acesso não documentado ao sistema ou aos seus dados.
	Clickjacking	Técnica maliciosa em que a vítima é induzida a clicar em um elemento na tela sem perceber ou ter a intenção. O clickjacking pode ser realizado de várias maneiras, como sobrepor um conteúdo invisível sobre outro visível, fazendo com que a vítima interaja involuntariamente com o conteúdo oculto.
	Falsificação de Solicitação entre Sites (Cross Site Request Forgery - CSRF)	Solicitação maliciosa que permite ao invasor o uso de identidade e privilégios legítimos da vítima.
	Script entre Sites (Cross Site Scripting - XSS)	Método de ataque que explora vulnerabilidades de scripting para contornar controles de acesso. Ao injetar um script malicioso em uma entrada não protegida ou não validada, o atacante faz com que o script seja executado no navegador. Um ataque bem-sucedido pode permitir que o atacante controle funcionalidades do aplicativo, manipule

Código Malicioso		dados ou adicione códigos maliciosos. Também pode permitir a injeção de scripts em páginas web vistas por outros usuários.
	Cryptojacking	Exploração de vulnerabilidade que permite utilizar os recursos do host vulnerável para minerar criptomoedas, explorando a CPU e GPU para cálculos de hashes.
	Exploit	Ferramentas, técnicas ou códigos maliciosos que exploram vulnerabilidades em sistemas, programas, hardware e ambientes.
	Exploração de Dia Zero	Exploração de vulnerabilidade ainda não corrigida pelo fabricante, desenvolvedor e/ou proprietário.
	Jailbreak	Processo que altera o sistema operacional original de um dispositivo, permitindo a execução de aplicativos não autorizados pelo fabricante. Um dispositivo modificado dessa forma pode instalar aplicativos que não estão disponíveis nos canais oficiais e também pode permitir a instalação de aplicações adquiridas ilegalmente.
	Keylogger	Spyware específico que captura e armazena teclas digitadas pela vítima.
	Malvertising	Uso de publicidade para disseminar malware, redirecionando vítimas para páginas corrompidas ou instalando malware diretamente.
	Ransomware	Malware que criptografa dados do usuário, bloqueando o acesso até que um resgate seja pago.
	Rootkit	Conjunto de programas e técnicas usados para esconder e manter a presença de um ator de ameaça ou de código malicioso em um computador comprometido.
	Screenlogger	Spyware específico que registra a posição do cursor e a tela durante cliques, usado principalmente para capturar entradas em teclados virtuais.
	Spyware	Malware projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.
	Cavalo de Tróia (Trojan)	Malware que se disfarça como um software legítimo, podendo também estar

		oculto em programa legítimo, levando os usuários a instalá-lo sem saber que estão comprometendo sua segurança com um software malicioso.
	Vírus	Código malicioso que se replica ao infectar programas, necessitando de execução do programa hospedeiro para ativar-se.
	Wiper	Malware destrutivo projetado para apagar ou destruir permanentemente dados e programas em dispositivos infectados, causando perda irreversível de informações. Criptografa, sobrescreve arquivos ou ataca o sistema operacional.
	Worm	Malware que se propaga automaticamente pelas redes, explorando vulnerabilidades para se disseminar, sem precisar se anexar a outros códigos ou arquiv
Coleta de Informações	Engenharia Social	Manipulação psicológica de pessoas para obter informações confidenciais ou acesso não autorizado.
	Espionagem Cibernética	Atividade de coleta de dados sensíveis de governos, empresas ou indivíduos, geralmente orquestrados por entidades de inteligência ou concorrentes.
	Scanning	Verificação tipicamente automatizada de sistemas, redes ou aplicativos para identificar e priorizar vulnerabilidades de segurança, permitindo sua correção antes de serem exploradas por invasores.
	Sniffing	Processo de monitoramento e captura de todos os pacotes de dados que trafegam em uma rede. Pode ser utilizado legitimamente para diagnóstico e gestão de redes, mas também maliciosamente para interceptar e roubar informações.
	Nova Assinatura de Ataque	Ataques que se utilizam de vulnerabilidades anteriormente desconhecidos.
	Configurações Inadequadas	

Tentativa de Intrusão		Ameaça que envolve a exploração de vulnerabilidades conhecidas, identificadas por CVEs, ou configurações incorretas em sistemas, com o objetivo de comprometer a segurança, interromper serviços ou obter acesso não autorizado.
	Bot	Software útil para automatização de tarefas computacionais repetitivas. Também pode ser utilizado com finalidades mal intencionadas, como ataques de negação de serviço ou disseminação de phishing, spam e malwares.
	Botnet	Rede formada por diversos computadores zumbis (infectados com bots). Permite potencializar as ações danosas executadas pelos bots e ser usada em ataques de negação de serviço, esquemas de fraude, envio de spam, entre outros.
	Cloud Jacking	Infiltração de sistemas armazenados em ambientes de nuvem, geralmente com o propósito de usar os recursos para atividades maliciosas como mineração de criptomoedas.
	Credential Stuffing	Injeção automatizada de pares de nome de usuário e senha, obtidos de listas roubadas ou geradas, em formulários de login de um site para obter acesso não autorizado às contas dos usuários. Como muitas pessoas reutilizam suas credenciais, os atacantes podem usar essas informações obtidas em vários sites com uma alta probabilidade de sucesso.
	Defacement	Ataque cibernético que visa atingir o conteúdo legítimo de páginas de um site, alterando sua aparência ou modificando o conteúdo original disponibilizado, atacando sua disponibilidade e integridade
	Path Traversal	Ataque que visa acessar arquivos, diretórios e comandos localizados fora do diretório raiz do site ou do diretório raiz CGI. Geralmente, o ataque é realizado manipulando uma URL para que o site divulgue ou execute o conteúdo dos arquivos no servidor.
	Tailgating	Ato de uma pessoa não autorizada burlar controles de acesso físico, frequentemente seguindo alguém autorizado para entrar em um local de acesso restrito.
	Ataque de Negação de Serviço (DoS)	Ataque que tem como objetivo

Disponibilidade		interromper ou perturbar o serviço normal de um sistema ou rede, tornando-o inacessível aos seus usuários.
	Ataque de Negação de Serviço Distribuído (DDoS)	Ataque em que diversos sistemas comprometidos são usados para direcionar um volume massivo de tráfego ou requisições a um único sistema ou serviço, com o objetivo de sobrecarregá-lo e torná-lo indisponível. Devido à distribuição da origem do tráfego, esses ataques são mais complexos de mitigar do que os ataques DoS tradicionais, já que vêm de múltiplas fontes ao mesmo tempo.
	Indisponibilidade Parcial	Interrupção ou indisponibilidade de um serviço ou sistema na qual a operação não é comprometida em sua totalidade, podendo ser causada ou não por meio de ações maliciosas.
	Indisponibilidade Total	Interrupção ou indisponibilidade de um serviço ou sistema na qual a operação é comprometida em sua totalidade, podendo ser causada ou não por meio de ações maliciosas.
	Sabotagem Cibernética	Atividade maliciosa que visa comprometer a integridade, autenticidade ou disponibilidade de sistemas, redes ou dados. Diferentemente dos ataques que visam roubar ou espionar informações, a sabotagem cibernética tem como objetivo principal causar interrupções, danos ou destruição.
Segurança do Conteúdo da Informação	Acesso Indevido	Qualquer ação que viole limites e controles definidos na política de segurança ao obter acesso lógico ou físico sem permissão.
	Modificação Indevida	Qualquer ação que comprometa a integridade lógica ou física sem permissão.
	Vazamento de Dados	Divulgação não autorizada ou não intencional de informações confidenciais. Seja por falhas de segurança, erro humano ou ataques maliciosos, o vazamento pode resultar em perda financeira, danos à reputação ou exposição de informações sensíveis.
	Disfarce	Ataque em que uma entidade assume ilegitimamente a identidade de outra para dela se beneficiar.
	Caça-clique (Clickbait)	Técnica de publicidade online que utiliza

Fraude		títulos sensacionalistas ou enganosos para atrair a atenção e incentivar cliques. Embora muitas vezes seja usado apenas para aumentar as visualizações de páginas, em alguns casos pode levar a sites maliciosos ou conter malware.
	Ataque Sybil	Estratégia direcionada especificamente a redes descentralizadas do tipo P2P, especialmente redes blockchain, consistindo na saturação do serviço partir da utilização de diversos clones (sybils) com a finalidade de manipular o processo de decisão, subvertendo o sistema de reputação do serviço.
	Comprometimento de e-mail Comercial (BEC — Business *e*-mail Compromise)	Ataque cibernético em que o invasor se passa por um executivo ou parceiro de negócios de uma empresa, utilizando um e-mail corporativo comprometido ou falsificado, para enganar funcionários, clientes ou fornecedores a realizar transferências bancárias ou revelar informações confidenciais.
	Deepfeak	Manipulação digital avançada de vídeo, áudio, texto ou imagem, geralmente utilizada com o intuito de criar conteúdos falsificados que parecem autênticos, distorcendo a realidade para enganar ou influenciar a percepção pública.
	Notícias Falsas	Falsificação da forma de notícia que se propaga massivamente através de plataformas digitais. A desinformação pode ser classificada em três tipos: • Disinformation: Informações falsas criadas intencionalmente para causar dano. • Misinformation: Informações erradas divulgadas sem a intenção de causar dano. • Malinformation: Informações verdadeiras, mas divulgadas fora de contexto com o objetivo de causar dano.
	Identidade Sintética	Fraude de identidade na qual os golpistas usam uma mistura de credenciais reais e fabricadas, para criar a ilusão de uma pessoa real. É bastante popular, pois os criminosos podem facilmente criar identidades sintéticas com apenas alguns dados verdadeiros (como nome e número de um documento de identificação), sendo normalmente utilizada com o objetivo de abrir contas fraudulentas e realizar aquisições.
	Phishing	Técnica de engenharia social na qual o atacante se passa por uma entidade

		confiável para obter informações confidenciais de usuários. Isso geralmente é feito por meio de comunicações que parecem autênticas ou direcionando o usuário para um site falso que solicita informações.
	Smishing	Ataque de engenharia social que utiliza mensagens SMS fraudulentas, simulando fontes confiáveis, para induzir o usuário a clicar em links maliciosos ou fornecer informações sensíveis.
	Spear Phishing	Forma direcionada de phishing, onde os criminosos personalizam mensagens fraudulentas para enganar alvos específicos. Essas mensagens muitas vezes parecem legítimas, visando obter informações confidenciais, como senhas ou dados financeiros, por meio da persuasão.
	Software de Segurança Desonesto (Scareware/Rogueware)	Software malicioso disfarçado de solução de segurança legítima que induz o usuário a adquirir a solução, acreditando que o seu dispositivo está comprometido. Além do prejuízo financeiro, tal ação pode acarretar tanto em roubo de dados sensíveis da vítima quanto na instalação de malware no sistema.
	Spamdexing	Técnica de ataque que visa manipular de forma deliberada os índices dos mecanismos de pesquisa para burlar o sistema de indexação. O objetivo é alterar a relevância ou a proeminência dos recursos indexados.
	Spoofing	Ato de falsificação de identidade, quando alguém ou algo se faz passar por outra entidade para obter uma vantagem indevida. Pode envolver a falsificação de vários identificadores, como endereços IP, sites, e-mails, ou outros dados de comunicação.
	Vishing	Técnica de engenharia social que se utiliza de chamadas telefônicas para enganar as pessoas e obter informações confidenciais. Durante essas chamadas, os golpistas podem se passar por representantes de instituições bancárias, agências governamentais ou outras entidades para enganar as vítimas.
	Whaling	Variação de phishing direcionado a indivíduos de alto escalão em organizações, como executivos ou altos funcionários. Similar ao spear phishing, o whaling envolve o envio de mensagens personalizadas e enganosas, buscando obter informações sensíveis ou acesso

		privilegiado, explorando a posição de destaque da vítima na hierarquia corporativa.

2.2 Taxonomia de Vulnerabilidades

Classificação	Exemplo	Descrição
Vulnerabilidades	Autenticação ao Nível do Objeto Quebrada (BOLA)	Vulnerabilidade que, quando explorada, possibilita o acesso direto a um objeto por meio de seu identificador, ocorrendo geralmente pela falta de mecanismos de autorização.
	Common Vulnerabilities and Exposures (CVE)	Banco de dados online que documenta ataques, explorações e comprometimentos de segurança. Ele abrange uma ampla gama de ataques e abusos conhecidos que afetam diversos sistemas e produtos de software.
	Server-Side Request Forgery (SSRF)	Vulnerabilidade de segurança em que um atacante manipula um aplicativo para fazer solicitações não autorizadas em nome do servidor, potencialmente obtendo acesso a recursos internos ou contornando medidas de segurança.
	Server-Side Template Injection (SSTI)	Vulnerabilidade de segurança em que um atacante consegue injetar código malicioso em modelos de servidor, explorando a capacidade do sistema de processar e executar código no lado do servidor. Isso pode levar à execução de código arbitrário, comprometimento do sistema ou exposição de dados sensíveis.
	Shadow API	APIs que não são oficialmente publicadas ou documentadas, muitas vezes ignorando os padrões de segurança exigidos, tornando-as vulneráveis a ataques.
	Vulnerabilidade de Dia Zero	Falha de segurança em um software ou hardware que sua correção ainda é desconhecida pelo respectivo fabricante, desenvolvedor ou mantenedor.
	XML External Entity Injection (XXE)	Exploração de vulnerabilidades no processamento de XML para acessar ou executar recursos externos não autorizados. Isso pode resultar na

		exposição de informações sensíveis ou no vazamento de dados.

2.2 Taxonomia de Testes

Classificação	Exemplo	Descrição
Tipos de Teste	Análise de Vulnerabilidades	Verificação técnica de sistemas e dispositivos em busca de falhas ou lacunas de segurança para identificar e determinar a possibilidade de exploração por atores de ameaças, a fim de corrigir ou mitigar as vulnerabilidades encontradas.
	Análise Dinâmica	Teste que examina o comportamento externo e operacional do software em busca de falhas e vulnerabilidades. Sua principal vantagem é revelar defeitos complexos que a análise estática não detecta. Embora contribua para a segurança, seu foco principal é a identificação e correção de erros.
	Análise Estática	Teste que verifica o código-fonte ou binários de um software, por meio de revisão, análise automatizada ou verificação formal do código-fonte ou dos binários. Uma ferramenta que executa a análise estática de forma automatizada procura, essencialmente, por erros que possam impedir a execução do software (run-time errors), por erros comuns da linguagem alvo e por código potencialmente malicioso.
	Captura de Banner	Técnica utilizada para obter informações sobre sistemas e serviços de computadores em rede sendo executados em portas abertas. Pode ser útil para identificar versões desatualizadas ou vulneráveis de software.
	Deep Packet Inspection (DPI)	Técnica de inspeção de pacotes de dados em trânsito por um ponto de controle de rede. Diferente dos firewalls tradicionais, que apenas verificam os cabeçalhos dos pacotes (como endereços IP e números de porta), o DPI analisa tanto o cabeçalho quanto o conteúdo dos pacotes. Isso permite identificar ameaças ocultas, como tentativas de exfiltração de dados, violações de políticas de conteúdo e malware,

Tipos de Teste		tornando o DPI uma ferramenta mais eficaz para a filtragem e proteção da rede.
	Honeypot	Sistema de computador sacrificial que pretende atrair ataques cibernéticos, como uma emboscada. Ele emula um alvo para os hackers e usa suas tentativas de intrusão para obter informações sobre os criminosos cibernéticos e a maneira como eles estão operando ou para distraí-los de outros alvos.
	Honeynet	Rede simulada que contém vários honeypots. Seu objetivo é atrair atacantes e monitorar seu comportamento, permitindo que os defensores aprendam sobre as táticas, técnicas e procedimentos dos atacantes.
	Sandbox	Ambiente controlado para testar e analisar softwares desconhecidos ou potencialmente maliciosos, isolando-os do sistema principal.
	Teste de Penetração (PENTEST)	Teste de segurança executado por meio de um ataque cibernético simulado, para encontrar vulnerabilidades em um sistema de computadores. Possui diferentes abordagens, tais como o teste de caixa branca, no qual o testador possui acesso integral às informações do sistema; o teste de caixa preta, conduzido sem qualquer conhecimento prévio sobre o sistema; e o teste de caixa cinza, que combina aspectos das abordagens de caixa branca e caixa preta.