Desafios da Formalização de ETIRs em IFEs: Diagnóstico, Conformidade Normativa e Proposta de Gestão.

Emanuel N. Reis[1], **Éder S. Gualberto**[1]

[1]Programa de Pós-Graduação Profissional em Engenharia Elétrica (PPEE)
Universidade de Brasília (UNB)
CEP 70.910-900 – Brasília – DF – Brazil

{emanuel.reis,eder.gualberto}@unb.br

Abstract. *The cybersecurity landscape within Brazilian Federal Educational Institutions (FEIs) is rapidly deteriorating, marked by a 56% surge in attacks between 2023 and 2024. This vulnerability is driven by massive volumes of sensitive data and an expansive attack surface, making the implementation of Computer Security Incident Response Teams (CSIRTs) essential for ensuring service continuity. Supported by GSI/PR Normative Instruction No. 01/2020, this study aims to assess the maturity of CSIRT formalization across FEIs and provide a structured proposal for their regulatory compliance. The methodology involved descriptive and applied research through documentary analysis of 108 FEIs (70 universities and 38 federal institutes). Findings indicate that 39% of these institutions lack a formal CSIRT structure, and only 38% are fully compliant with GSI/PR NC No. 05/2008 standards. To bridge this gap, the paper proposes a centralized formalization model with shared autonomy, structured into five phases: formal institutionalization, team composition/training, operational structuring, government network integration, and continuous monitoring.*
keywords: *Cybersecurity. CSIRT. Federal Educational Institutions. Incident Response. Information Security. Digital Governance.*

Resumo. *O cenário de insegurança cibernética nas Instituições Federais de Ensino (IFEs) brasileiras apresenta rápida deterioração, evidenciada por um aumento de 56% nos ataques registrados entre 2023 e 2024. Essa vulnerabilidade é impulsionada pelo vasto volume de dados sensíveis e pela complexidade das redes acadêmicas, tornando a implementação de Equipes de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) essencial para a continuidade dos serviços. O objetivo deste trabalho é diagnosticar a maturidade da formalização dessas equipes e fornecer uma proposta estruturada de institucionalização em conformidade com as normas do Gabinete de Segurança Institucional (GSI/PR). A metodologia consistiu em uma pesquisa aplicada e descritiva, com análise documental de 108 IFEs (70 universidades e 38 institutos federais). Os resultados revelam que 39% das instituições carecem de qualquer estrutura formal de ETIR e apenas 38% atendem integralmente aos requisitos da NC nº 05/2008 do GSI/PR, possuindo formalização via portaria específica. Para mitigar esses riscos, o artigo propõe um modelo centralizado com autonomia compartilhada, estruturado em cinco passos fundamentais: institucionalização formal, composição e capacitação, estruturação operacional, integração com a rede de governo e monitoramento contínuo.*

Palavras-chave: *Insegurança Cibernética. Formalização de ETIR. Instituições Federais de Ensino. Resposta a Incidentes. Governança Digital.*

1. Introdução.

O cenário de insegurança cibernética enfrentado pelas Instituições Federais de Ensino (IFEs) — incluindo escolas de educação básica, técnica e ensino superior — é crítico e está em rápido deterioramento nos últimos anos. Instituições educacionais em todo o mundo se tornaram um foco de crimes cibernéticos, onde as investidas contra o sistema da Rede nacional de Ensino e Pesquisa aumentaram 56% entre as anos de 2023 e 2024, afirma o artigo da revista de pesquisa Fapesp [REVISTA 2025]. A rede acadêmica Ipê, que conecta aproximadamente 1,8 mil instituições de pesquisa, inovação e ensino superior brasileiras e 4 milhões de usuários, lida com cerca de 20 mil tentativas de ataques por mês. A maioria é bloqueada de forma automática pela Rede Nacional de Ensino e Pesquisa (RNP), organização social vinculada ao Ministério da Ciência, Tecnologia e Inovação (MCTI), que administra a rede. O estudo "Cybersecurity in Education: Protecting Students and Staff"[Frank et al. 2023] ressalta que as instituições de ensino apresentam vulnerabilidades específicas devido ao seu ambiente aberto e colaborativo, no qual muitos usuários acessam redes e sistemas utilizando diferentes dispositivos. Além disso, muitas organizações educacionais possuem limitações orçamentárias, falta de profissionais especializados e infraestrutura de segurança insuficiente, dificultando a implementação de controles robustos.

Nesta perspectiva, a iniciativa observada em "A Framework for Institution to Enhancing Cybersecurity in Higher Education: A Review", o autor Ankit Kumar [Kumar et al. 2024], apresenta um modelo estruturado para fortalecer a postura de cibersegurança em Instituições de Ensino Superior (IES). O estudo justifica a urgência desse *framework* devido ao aumento de ameaças digitais impulsionadas por tecnologias como IA e IoT, que tornam o setor educacional particularmente vulnerável. Contudo, embora nenhuma estratégia ofereça proteção absoluta contra todas as ameaças, a adoção deste framework sistêmico permite que as IES identifiquem lacunas e implementem medidas direcionadas para proteger dados e sistemas sensíveis de forma proativa, a fim de gerenciar, de forma estruturada, incidentes de segurança da informação, visando minimizar danos, erradicar ameaças e restaurar rapidamente os sistemas operacionais, garantindo a continuidade dos serviços educacionais e a proteção de dados.

Diante da obrigatoriedade normativa de resposta a incidentes na Administração Pública Federal, emerge a seguinte problemática: em que medida as Instituições Federais de Ensino (IFEs) brasileiras estão formalmente estruturadas para atender aos requisitos de governança e resposta a incidentes cibernéticos estabelecidos pelo Gabinete de Segurança Institucional? Este estudo busca responder a esta questão através de um diagnóstico da maturidade de formalização de ETIRs nessas instituições, visando compreender se a ausência de amparo normativo atua como um limitador para a resiliência institucional frente aos crescentes ataques cibernéticos. O artigo apresenta um modelo de formalização de ETIR para Instituições Federais de Ensino (IFEs), propondo uma estrutura de ETIR alinhada à IN 01/2020 e NC 05 do GSI/PR, a partir de um diagnóstico da situação de conformidade de 108 instituições federais brasileiras.

Garantir a existência e funcionamento de uma ETIR em IFEs — como Institutos Federais (IFs) e Universidades Federais — envolve a institucionalização formal, capacitação técnica e alinhamento com as normas do Governo Federal. A adequação das equipes de ETIR nas Instituições Federais de Ensino com normas internacionais é fun-

damental para a maturidade cibernética, promovendo agilidade na resposta a ameaças e proteção de dados. A base legal brasileira para essas equipes, alinhada a boas práticas internacionais, está na Instrução Normativa nº 1 de 2020 do GSI/PR [BRASIL 2020], que orienta a gestão da segurança da informação em órgãos da Administração Pública Federal.

O processo de constituição de Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) na Administração Pública Federal (APF) brasileira é um rito estruturado, fundamentado no Gabinete de Segurança Institucional (GSI) e coordenado nacionalmente pelo CTIR Gov, atuando como o ponto focal interno para prevenir, detectar e responder a incidentes. As fases deste processo iniciam pela Instituição e Estrutura (Fase de Preparação), Atuação da ETIR (Fluxo de Trabalho), Comunicação de Incidentes ao CTIR Gov e Pós-Incidente.

A fase de preparação recebe uma maior destaque neste trabalho, tendo em vista que a instituição de uma ETIR deve ser realizada formalmente nos órgãos federais, mediante portaria ou resolução, definindo claramente suas atribuições, escopo de atuação e autoridade. A Norma Complementar nº 05/IN01/DSIC/GSIPR recomenda que a formulação de uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) [BRASIL 2009] seja baseada em sua formalização por meio de um documento aprovado pela alta administração, alinhado à Política de Segurança da Informação do órgão, definindo claramente sua missão, escopo de atuação, comunidade atendida, estrutura organizacional, autonomia, papéis e responsabilidades, bem como os serviços prestados, incluindo recebimento de notificações, análise, tratamento, resposta e coordenação de incidentes. A norma também orienta que seja escolhido um modelo de implementação compatível com a realidade da organização (equipe dedicada, compartilhada, terceirizada ou híbrida), que sejam estabelecidos canais formais de comunicação com usuários, outras ETIRs e o CTIR Gov, e que a equipe atue de forma integrada à governança de segurança da informação, contribuindo para a prevenção de incidentes, a melhoria contínua dos processos de segurança e o fortalecimento da capacidade institucional de resposta a ameaças cibernéticas.

Contudo, Moraes discute na pesquisa ”Desafios à implementação das estratégias de governo digital e o nível de maturidade nas Instituições Federais de Ensino Superior”[de Góes Moraes and Luft 2024], que a formalização de ETIR em IFEs enfrenta desafios complexos devido à natureza aberta e colaborativa dessas organizações, entre os quais se destacam: a dificuldade em contratar e manter profissionais de cibersegurança qualificados, dada a concorrência com o setor privado, além de limitações impostas por concursos públicos, a insuficiência de verba específica para aquisição de ferramentas de segurança, licenciamentos e treinamento contínuo da equipe, a necessidade de autonomia dos laboratórios e departamentos, que gerenciam seus próprios servidores e páginas, engajamento fraco e dificulta a padronização de políticas de segurança, a complexidade em conscientizar a comunidade acadêmica (professores, alunos e técnicos) sobre a importância da segurança, muitas vezes vista como um entrave à pesquisa e ao ensino, além da necessidade de elaborar regimentos internos, definir atribuições claras e integrar a equipe com o CTIR Gov, o que exige maturidade de gestão e da governança digital. Desta forma, o posicionamento dos autores em ”Desafios da segurança cibernética: uma análise da administração pública brasileira”[Silva et al. 2026] corrobora com a afirmativa de que a gestão da segurança da informação no setor público brasileiro enfrenta obstáculos que

vão além da tecnologia, caracterizando-se como um sistema sociotécnico complexo onde o fator humano e a cultura organizacional são determinantes.

Sendo assim, o aumento dos ataques cibernéticos e das exigências regulatórias tem levado as instituições de ensino a adotarem uma postura mais proativa em segurança da informação. Nesse contexto, a implementação de Equipes de Tratamento e Resposta a Incidentes de Segurança Cibernética fortalece a proteção de dados, aumenta a confiança nos ambientes de ensino e inovação e contribui para a formação de profissionais qualificados em segurança da informação.

2. Referencial Teórico.

2.1. Incidente Cibernético.

Um incidente cibernético (ou incidente de segurança cibernética/informação) pode ser resumido como um evento adverso, confirmado ou sob suspeita, que resulta no efeito real ou potencial sobre a confidencialidade, integridade ou disponibilidade de um sistema de informações, rede ou dados confidenciais de uma organização. Em [Nelson et al. 2025], NIST (National Institute of Standards and Technology), através do glossário do CSRC (Computer Security Resource Center) define ”Cyber Incident”como uma ação realizada por meio do uso de sistema/rede de informações que resulta em efeito adverso, real ou potencial, sobre tal sistema/rede. A norma internacional ISO/IEC 27035, de 2016 [ISO/IEC 2016], em Gestão de incidentes de segurança da informação, classifica um incidente de segurança da informação como um único ou uma série de eventos indesejados ou inesperados de segurança da informação, que têm uma probabilidade significativa de comprometer as operações de negócios e ameaçar a segurança da informação.

Como alguns exemplos de incidentes cibernéticos em IFEs, podemos citar o ataques de Ransomware (sequestro de dados), o vazamento de dados pessoais ou confidenciais, o acesso não autorizado a sistemas (invasão) e o ataques de negação de serviço (DoS/DDoS). O estudo de caso ”Cyberattack on the Université Paris-Saclay: case study (2024)”divulgado pelo projeto SOCCER (Cybersecurity for Academic Sector) [SOCCER Project 2024], analisa um ataque de ransomware contra uma universidade francesa, destacando vulnerabilidades em instituições de ensino superior, impactos sobre serviços acadêmicos e a necessidade de fortalecer investimentos em segurança cibernética.

2.2. Instituições Federais de Ensino (IFEs).

No entendimento da Lei de Diretrizes e Bases da Educação Nacional [BRASIL 1996], juntamente com a definição da lei de criação das IFs no Brasil [BRASIL 2008], As Instituições Federais de Ensino (IFEs), no contexto brasileiro, são entidades públicas criadas, mantidas e geridas pelo Governo Federal, vinculadas ao Ministério da Educação (MEC). Elas constituem o pilar da educação superior e técnica pública, com autonomia didático-científica, administrativa e de gestão financeira e patrimonial. Elas englobam as Universidades Federais, os Institutos Federais de Educação, Ciência e Tecnologia (IFs), as Escolas Técnicas vinculadas a universidades federais e o Colégio Pedro II. Possuem como características principais a gratuidade do ensino, o acesso via Sistema de Seleção Unificada (SiSU) ou concursos específicos e função social com foco no desenvolvimento socioeconômico local, regional e nacional.

2.2.1. Institutos Federais de Ensino (IFs).

A Lei nº 11.892/2008 [BRASIL 2008] instituiu a Rede Federal de Educação Profissional, Científica e Tecnológica e criou os Institutos Federais (IFs) de Educação, Ciência e Tecnologia. Transformou CEFETs e escolas técnicas em autarquias com autonomia didática e financeira, focadas no ensino profissional, desde cursos técnicos até pós-graduação, com foco no desenvolvimento regional e verticalização do ensino.

2.2.2. Universidades Federais de Ensino (UFs).

As universidades públicas federais no Brasil surgiram da unificação de faculdades isoladas, com marcos iniciais na década de 1910, a exemplo da UFPR em 1912, e consolidação a partir da década de 1920/1930, como a Universidade do Rio de Janeiro (1920) e Universidade do Brasil (1937), visando organizar o ensino superior e formar elites intelectuais/técnicas. A Universidade do Rio de Janeiro, fundada em 1920, é apontada como a primeira de fato Federal, atualmente UFRJ. No governo Getúlio Vargas houve institucionação do ensino superior com a reforma de 1931, criando a Universidade do Brasil (1937) como modelo. A partir da década de 1950 ocorre a federalização de diversas faculdades estaduais e privadas, onde a rede expandiu drasticamente após 2003, especialmente com o programa REUNI (2010), interiorizando o ensino e criando dezenas de novas universidades. Atualmente, a criação de novas universidades públicas segue um processo rigoroso de iniciativa do Poder Executivo, como detalhado no Decreto Federal nº 2.207.

2.3. Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

O Gabinete de Segurança Institucional da Presidência da República (GSI), através do Departamento de Segurança Institucional e Comunicação (DSIC), elabora a Norma Complementar nº5 [BRASIL 2009] e define a Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) como um grupo especializado, geralmente formado por agentes públicos (no contexto da administração pública brasileira), responsável por prevenir, detectar, analisar, responder e tratar incidentes de segurança da informação em redes de computadores. Ela atua para minimizar o impacto de ataques cibernéticos, como malware, phishing ou indisponibilidade de sistemas, garantindo a integridade, confidencialidade e disponibilidade dos dados. Suas funções concentram esforços proativamente na análise de vulnerabilidades e reativamente na resposta a incidentes. No âmbito do Governo Federal brasileiro, integram uma rede coordenada pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov).

As ETIRs atuam como estruturas fundamentais para a prevenção, detecção, análise, resposta e recuperação de incidentes cibernéticos. Este processo especifica ações como receber, analisar, classificar incidentes, notificar autoridades (CTIR Gov) e gerenciar patches de segurança. O seu papel estratégico, em organizações públicas, é observado em ”The Role of Computer Security Incident Response Teams (CSIRTs) in Enhancing Cybersecurity Resilience”[Bada et al. 2014], onde se destaca a necessidade de proteger serviços essenciais, dados governamentais e infraestruturas críticas contra ameaças cada vez mais sofisticadas.

2.4. Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov).

O CTIR Gov integra o Departamento de Segurança da Informação do Gabinete de Segurança Institucional (GSI) da Presidência da República. É a equipe do Governo Federal brasileiro responsável por coordenar a resposta a incidentes de segurança cibernética dentro da Administração Pública Federal (APF). Sua missão é aumentar a segurança e a resiliência das redes de computadores da Administração Pública Federal (APF) [BRASIL 2025]. O público-alvo atende órgãos e entidades da APF. Sua linha de atuação previne, trata e coordena a resposta a incidentes cibernéticos, como ataques de negação de serviço (DoS), vazamento de informações, fraudes, abuso de sítios, e varreduras (scans), tendo como finalidade principal a de proteger a infraestrutura e os dados da Administração Pública contra ameaças digitais, emitindo alertas e recomendações de segurança.

Segundo o Decreto nº 10.748, de 2021 [Brasil 2021], que instituiu a Rede Federal de Gestão de Incidentes Cibernéticos (REGIC) com o objetivo de fortalecer a coordenação entre os órgãos e entidades da Administração Pública Federal para prevenção, tratamento e resposta a incidentes cibernéticos, estabelece que o CTIR Gov atua como órgão coordenador da REGIC, sendo responsável por promover a integração entre as ETIRs, disseminar alertas e orientações técnicas, consolidar informações sobre ameaças cibernéticas e apoiar os órgãos participantes na adoção de boas práticas de segurança. Entretanto, a responsabilidade pela prevenção, tratamento e resposta aos incidentes permanece com a ETIR de cada órgão ou entidade, que é a responsável pela gestão operacional dos eventos de segurança em seu ambiente institucional.

2.5. Frameworks de Cibersegurança.

O artigo "Integrating Cybersecurity Frameworks into IT Security: A Comprehensive Analysis of Threat Mitigation Strategies and Adaptive Technologies" [Lokare et al. 2025] discute como frameworks de cibersegurança auxiliam organizações na estruturação de processos de proteção contra ameaças digitais e analisa frameworks amplamente utilizados, como o NIST Cybersecurity Framework (NIST CSF), ISO/IEC 27001 e abordagens como Zero Trust Architecture, destacando seu papel na gestão de riscos, padronização de controles de segurança e melhoria da capacidade de resposta a incidentes.

Os frameworks de resposta a incidentes cibernéticos são conjuntos estruturados de melhores práticas, diretrizes e procedimentos que ajudam as organizações a detectar, conter, erradicar e recuperar-se de ataques cibernéticos. Com a crescente complexidade das ameaças, a Inteligência Artificial (IA) tem sido integrada a esses frameworks para automatizar a análise e a resposta a incidentes, frequentemente operando em conjunto com plataformas SOAR (Security Orchestration, Automation and Response). Dentre eles se destacam:

- **NIST Cybersecurity Framework (NIST CSF):** O NIST CSF é um framework de boas práticas para gerenciamento de riscos de cibersegurança, organizado em seis funções — Govern, Identify, Protect, Detect, Respond e Recover — que ajudam as organizações a prevenir, detectar, responder e se recuperar de incidentes de segurança de forma estruturada e contínua [National Institute of Standards and Technology 2024].

- **ISO/IEC 27035:2016 (Information technology):** Framework internacional detalhado para a gestão de incidentes de segurança, alinhado à ISO 27001. Abrange desde a detecção até a análise pós-incidente, visando minimizar interrupções operacionais [ISO/IEC 2016].
- **MITRE ATT&CK®:** Framework de táticas e técnicas baseado em observações do mundo real. Utilizado para analisar ameaças e entender como os atacantes operam, facilitando a resposta [The MITRE Corporation 2024].
- **CIS Controls®:** Apresenta um conjunto de 18 controles críticos que incluem práticas específicas para resposta a incidentes e gerenciamento de segurança [Center for Internet Security, Inc. (CIS) 2021].
- **CERT.br - Guia de Gestão de Incidentes:** Guia prático brasileiro para a criação de equipes de resposta a incidentes (CSIRTs) [CERT.br 2012].

Eles são fundamentais para a atuação da Equipe de Tratamento e Resposta a Incidentes Cibernéticos, pois fornecem uma estrutura metodológica, padronizada e proativa para a gestão de crises. No contexto do Governo Federal Brasileiro, as ETIRs utilizam essas referências para alinhamento com o CTIR Gov.

Tabela 1. Comparativo entre as Funções dos Frameworks

Framework	Foco Principal	Função no Tratamento de Incidentes
NIST CSF	Estratégia/Gestão	Estrutura de alto nível (Detectar, Responder, Recuperar).
ISO 27035	Processo/Procedimento	Ciclo de vida completo do incidente (Prep - Lições Aprendidas).
MITRE	Inteligência/Tática	Entendimento do comportamento do atacante e gaps de detecção.
CIS Controls	Ações Técnicas	Implementação prática de controles de segurança (Hardening/Monitoramento).
CERT.BR	Operacional/Nacional	Orientação técnica, parceria e CSIRT.

Em um cenário prático, uma organização utiliza o **NIST** para governança, o **ISO 27035** para estruturar o processo, o **CIS Controls** para configurar os alertas, o **MITRE** para entender a técnica do invasor e o **CERT.BR** para apoio e inteligência de ameaças locais.

3. Impactos da Implementação do modelo de ETIR nas IFEs.

O framework descrito na pesquisa ”A Context-Aware Cybersecurity Readiness Assessment Framework for Organisations in Developing and Emerging Environments”, os autores Raymond Agyemang, Steven Furnell e Tim Muller [Agyemang et al. 2026], propõem uma solução inovadora para avaliar a prontidão em cibersegurança, especificamente adaptado para organizações que operam em ambientes em desenvolvimento e emergentes em arquitetura de dois níveis, sendo o primeiro capaz de avaliar o quanto a organização conhece e se engaja com obrigações regulatórias nacionais, estratégias governamentais de cibersegurança e mecanismos de suporte institucional, como equipes de resposta a incidentes (ETIR). O segundo foca nas capacidades internas da empresa, abrangendo governança e liderança, controles técnicos e operacionais, conscientização e cultura, e

colaboração externa. O estudo fundamenta-se na premissa de que a cibersegurança é um problema sociotécnico, ou seja, uma dimensão humana de prontidão integrada à governança e à cultura da organização. Os resultados da aplicação do framework revelaram padrões consistentes entre as organizações: Força em Controles Técnicos, Fraqueza em Cultura e Colaboração e Diagnóstico da Incerteza.

A implementação de uma estrutura organizada e coordenada para atuar nas Instituições Federais de Ensino fortalece a segurança da informação, protegendo dados sensíveis de alunos, servidores e pesquisas.

3.1. Benefícios da Utilização de ETIR.

São inúmeros os benéficios atraibuídos a utilização de ETIR nas IFEs, dentre eles se destacam a rápida detecção de ameaças, mitigação de riscos, redução de paralisações operacionais e maior conformidade com normas federais de segurança cibernética. O estudo apresentado por [Brito and Ferreira 2017] defende que a implementação do modelo de ETIR produz benefícios organizacionais, como a formalização dos processos de resposta a incidentes, o fortalecimento da governança de segurança da informação e o aumento da capacidade institucional de prevenção e resposta a incidentes cibernéticos. Esses resultados dialogam diretamente com os objetivos de programas de governança, como o PPSI, que buscam elevar a maturidade em privacidade e segurança da informação na Administração Pública Federal.

3.1.1. Resposta Rápida a Incidentes.

Agir de forma eficiente na detecção e mitigação de ataques cibernéticos, minimizando o impacto de incidentes e restabelecendo a normalidade dos serviços de TI. A ETIR atua na detecção, análise e contenção de ataques cibernéticos, diminuindo o tempo de inatividade dos sistemas acadêmicos. Ignaim, em seu estudo ”Improving Incident Management Processes with Feature Models”[Ignain and Fernandes 2024] aborda a necessidade de reduzir o tempo de resposta a incidentes cibernéticos por meio da melhoria dos processos de gerenciamento de incidentes. Ele apresenta um modelo baseado em feature models para aprimorar processos de gestão de incidentes, demonstrando que uma estrutura organizada pode aumentar a eficiência das equipes responsáveis pela resposta e diminuir o tempo necessário para restaurar serviços afetados, utilizando métodos através de classificação e priorização dos incidentes, padronização das etapas de tratamento, redução do tempo entre detecção, contenção e recuperação e melhoria da documentação e comunicação entre equipes de resposta.

3.1.2. Gestão de Vulnerabilidades.

A gestão de vulnerabilidades é uma atividade preventiva essencial para reduzir a probabilidade de incidentes cibernéticos. Em uma estrutura de resposta coordenada, como a REGIC, as ETIRs locais podem utilizar processos maduros de gestão de vulnerabilidades para: identificar fragilidades antes da exploração por atacantes, priorizar correções conforme criticidade dos ativos, compartilhar indicadores e riscos relevantes com equipes coordenadoras e reduzir o tempo de exposição dos sistemas vulneráveis. Neste viés,

há várias pesquisa de otimização que utilizam uma equipe de tratamento e um processo baseado em Process Mining (mineração de processos) para aprimorar a gestão de vulnerabilidades, analisando como os processos reais de identificação, avaliação, priorização e correção de vulnerabilidades ocorrem nas organizações. Meyer, no artigo "Improving Vulnerability Management Through Process Mining"[Meyer et al. 2024], destaca que a gestão eficiente não depende apenas de ferramentas de varredura, mas também da capacidade de compreender e otimizar o fluxo operacional de tratamento das vulnerabilidades.

A ETIR realiza varreduras proativas em redes e servidores, corrigindo falhas antes que sejam exploradas. Essas equipes, muitas vezes coordenadas pelo CTIR Gov na administração pública, utilizam softwares especializados para mapear ativos, identificar riscos e automatizar correções, alinhando-se com a Política de Segurança da Informação.

3.1.3. Proteção de Dados e Imagem.

É essencial a proteção dos sistemas, dados acadêmicos e administrativos, além da infraestrutura de rede contra artefatos maliciosos. A equipe foca os esforços para minimizar o risco de vazamento de dados pessoais de estudantes e colaboradores, preservando a reputação da instituição. Uma boa governança de segurança da informação contribui não apenas para a proteção dos dados, mas também para a manutenção da credibilidade institucional. Isso é o resultado da pesquisa de Benaroch "Cyber Failures and Information Technology Capability Reputation: Examining Ex Ante and Ex Post Interplay Effects"[Benaroch 2024], que investiga como falhas de segurança cibernética afetam a reputação (imagem) das organizações e demonstra que empresas com elevada capacidade de gestão de TI sofrem menor impacto reputacional após incidentes.

3.1.4. Conformidade Normativa.

A conformidade normativa na Administração Pública Federal exige uma gestão estruturada de Segurança da Informação. Nesse contexto, a ETIR é fundamental para que as IFEs cumpram as diretrizes federais, alinhando-se à Política de Segurança da Informação (PNSI), às normas complementares do MGI e aos requisitos da LGPD.

3.2. Riscos associados.

A gestão de riscos associada ao tema foca na prevenção, detecção e resposta a ataques cibernéticos. Ela envolve o tratamento de vulnerabilidades, monitoramento de infraestrutura, conscientização acadêmica, e o estabelecimento de planos de contingência, visando minimizar interrupções nas atividades educacionais e administrativas. Conforme apontam Rios, Teixeira Filho e Rios (2017) [Rios et al. 2017], fragilidades na governança e na gestão da segurança da informação em instituições federais de ensino podem comprometer a efetividade dos controles de proteção, tornando necessária a adoção de processos estruturados de gestão de riscos e resposta a incidentes.

Durante a formulação e implementação de uma equipe de tratamento e resposta a incidentes ciberneticos em instituições de ensinos federais, ocorrem diversos riscos que, caso não sejam mitigados, podem afetar fortemente o sucesso das ações previstas na regulamentação do GSI. A ausência de uma Equipe de Prevenção, Tratamento e Resposta

a Incidentes Cibernéticos em uma Instituição Federal de Ensino expõe a organização a riscos graves, tanto operacionais quanto jurídicos e institucionais.

3.2.1. Riscos Operacionais e de Segurança.

- **Ataques de Ransomware e Perda de Dados:** Sem uma equipe focada, a instituição fica vulnerável ao sequestro de dados e invasões, paralisando atividades acadêmicas e administrativas.
- **Indisponibilidade de Sistemas (DDoS):** Ataques de negação de serviço podem derrubar sites, sistemas acadêmicos (como SIGAA) e ambientes virtuais de aprendizagem, impedindo aulas e matrículas.
- **Vazamento de Informações Sensíveis:** Exposição de dados pessoais de alunos, servidores e pesquisas, gerando danos de imagem.

3.2.2. Riscos Jurídicos e Normativos.

- **Descumprimento da LGPD:** A LGPD exige, em seu artigo 50, que a instituição tenha governança e planos de resposta a incidentes (que a ETIR operacionaliza). A falta dela torna a instituição vulnerável a sanções.
- **Violação de Normas do GSI:** A não implementação da ETIR desobedece a instruções normativas do Gabinete de Segurança Institucional (GSI) da Presidência da República, que exige a gestão de segurança da informação em toda a administração pública federal.
- **Responsabilidade dos Gestores:** A ausência de uma estrutura formal de resposta pode levar a responsabilização pessoal dos gestores de TI e da reitoria em casos de incidentes graves por negligência.

3.2.3. Riscos Institucionais.

- **Perda de Credibilidade:** Vazamentos de pesquisas ou sistemas inoperantes destroem a confiança na instituição por parte da comunidade acadêmica e sociedade.
- **Danos à Reputação:** Incidentes cibernéticos noticiados podem impactar a busca por novos alunos e parcerias de pesquisa.
- **Prejuízo Financeiro:** Custos com a recuperação de sistemas, consultorias de emergência e potenciais multas da ANPD (Autoridade Nacional de Proteção de Dados).

3.2.4. Riscos de Incapacidade de Notificação.

A incapacidade de notificar tempestivamente vulnerabilidades ou incidentes compromete a coordenação entre os participantes da rede e aumenta a exposição ao risco. Essa preocupação é observada em ”Tell Them They Are a Responsible Entity, Not a Customer”, onde os autores [Ethembabaoglu et al. 2026] investigam os desafios enfrentados por profissionais de CSIRTs setoriais e identifica um problema diretamente relacionado

ao risco de incapacidade de notificação: alertas e notificações críticas nem sempre chegam aos destinatários devido a falhas nos processos de encaminhamento e comunicação. A pesquisa revela que existem lacunas sistêmicas no encaminhamento das notificações e que organizações atendidas frequentemente deixam de receber alertas importantes, reduzindo diretamente a efetividade da resposta a incidentes.

4. Desafios da Implementação do Modelo.

As instituições de ensino federais enfrentam desafios como resistência cultural à mudança, limitação orçamentária, necessidade de capacitação contínua de pessoal e a fragilidade na gestão documental e a defasagem tecnológica da infraestrutura da organização.

4.1. Restrição Orçamentária Específica.

No artigo "The Use of Public Data and Free Tools in National CSIRTs' Operational Practices: A Systematic Literature Review"[Mohd Kassim et al. 2023], os autores evidenciam que muitas equipes de resposta dependem de soluções de baixo custo ou abertas para complementar suas capacidades operacionais, indicando que restrições financeiras influenciam escolhas tecnológicas e processos de trabalho.

No serviço público federal, a criação e operacionalização de ETIR enfrenta limitações orçamentárias decorrentes de contingenciamentos e da ausência de reajustes compatíveis com a inflação, dificultando a aquisição de ferramentas de segurança, a contratação de profissionais especializados e a atualização da infraestrutura. Essas restrições comprometem a implementação de políticas de segurança da informação e aumentam a exposição da instituição a incidentes cibernéticos, sendo considerado essencial a reserva de investimento dedicado a novas tecnologias de segurança, treinamentos e, possivelmente, contratação de serviços terceirizados, estrutura organizacional definida para atender as exigencias de segurança da informação presentes na legislação vigente.

4.2. Regulamentação Interna.

A elaboração de uma Política de Segurança da Informação (PSI) em Institutos Federais de Educação (IFEs) enfrenta desafios complexos centrados na conciliação entre a abertura acadêmica necessária para pesquisa e ensino e a rigidez exigida pela proteção de dados. Os principais obstáculos incluem a necessidade de adequação imediata à LGPD em um ambiente com vasto volume de dados sensíveis e diversos usuários (alunos, servidores, terceiros), a carência de recursos técnicos especializados, e a dificuldade em disseminar uma cultura de segurança da informação em uma estrutura descentralizada. Além disso, a PSI deve superar a resistência cultural a mudanças de comportamento, integrar sistemas legados e estabelecer diretrizes claras que não impeçam o fluxo de informações, ao mesmo tempo em que mitigam ameaças cibernéticas frequentes no ambiente acadêmico.

4.3. Resistência Organizacional e Cultural.

O artigo de Ioannou, Stavrou e Bada (2019) [Ioannou et al. 2019] destaca que a criação e o funcionamento efetivo de um CSIRT dependem não apenas de recursos tecnológicos, mas também de fatores humanos e organizacionais. Os autores apontam que a resistência à mudança, a comunicação deficiente entre setores, a falta de apoio da alta gestão e uma cultura de segurança imatura podem dificultar a implantação e a atuação dessas equipes.

Nesse contexto, a institucionalização de um CSIRT/ETIR exige o desenvolvimento de uma cultura organizacional voltada à segurança da informação, com definição clara de responsabilidades, cooperação entre áreas e incentivo ao compartilhamento de informações sobre incidentes. Esses aspectos são especialmente relevantes para instituições públicas de ensino, nas quais a diversidade de usuários e setores torna a mudança cultural um fator crítico para o sucesso da equipe de resposta a incidentes.

A resistência à criação de ETIR decorre principalmente de uma cultura organizacional avessa a mudanças, limitada conscientização sobre riscos digitais e escassez de recursos humanos e financeiros. A estrutura descentralizada, a falta de padronização nos procedimentos de segurança e a percepção da Tecnologia da Informação apenas como suporte, e não estratégica, dificultam a implementação dessas equipes, gerando relutância em adotar novas políticas normativas e de segurança da informação exigidas pelos órgãos federais. A mudança de processos e a necessidade de relatar incidentes (cultura de transparência) podem encontrar resistência interna, dificultando a adesão da comunidade acadêmica e de servidores da equipe de Tecnologia da informação e comunicações.

4.4. Escassez de Pessoal Qualificado.

Falta de servidores capacitados em cibersegurança e TI para compor a equipe de ETIR, além da dificuldade em manter equipes técnicas atualizadas em concorrência com a velocidade de inovações no mercado de cibercrimes. Essa carência é agravada pela dificuldade na retenção de talentos no setor público, limitações orçamentárias e a necessidade de formação contínua, o que dificulta o monitoramento eficaz, a conformidade com diretrizes da administração federal e a resposta ágil a incidentes cibernéticos. A tabela 2 correlaciona os benefícios de possuir uma ETIR atuante na organização e os riscos de não possuir essa estrutura no ambiente corporativo. Em seguida aponta os principais desafios em relação a implementação de equipes de tratamento e resposta a incidentes cibernéticos para as IFEs na administração pública federal.

Tabela 2. Relação de Impacto e Desafios de Constituição de ETIR em IFEs.

Benefícios	**Riscos**	**Desafios**
5.1.1 - Resposta rápida a Incidentes.	5.2.4 - Riscos de Incapacidade de Notificação.	6.3 - Resistência Organizacional e Cultural.
5.1.2 - Gestão de Vulnerabilidades.	5.2.1 - Riscos Operacionais de Segurança.	6.4 - Escassez de Pessoal Qualificado.
5.1.3 - Proteção de Dados e Imagem.	5.2.3 - Riscos Institucionais.	6.1 - Restrição Orçamentária Específica.
5.1.4 - Conformidade Normativa.	5.2.2 - Riscos Jurídicos e Normativos.	6.2 - Regulamentação Interna.

4.5. Programa de Privacidade e Segurança da Informação (PPSI).

O documento oficial do PPSI [MGI-PR 2023] estabelece que o programa tem como objetivo elevar a maturidade e a resiliência dos órgãos e entidades da Administração Pública Federal, por meio da implementação de práticas estruturadas de privacidade e segurança da informação. Isso inclui universidades e institutos federais integrantes do SISP. Atualmente se encontra no primeiro ciclo da versão 2.0.

Essencialmente, o programa atua como um roteiro padronizado que obriga os institutos e universidades a mudarem a forma como tratam a segurança digital e a privacidade de ponta a ponta, fornecendo implicações profundas e estruturais:

- **Adequação Legal e LGPD:** As IFEs lidam diariamente com um volume massivo de dados sensíveis de milhares de alunos, servidores e terceiros. O PPSI consolida a base de governança necessária para garantir a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD).
- **Adoção do Framework Oficial:** As IFEs são obrigadas a adotar e implementar o Framework de Privacidade e Segurança da Informação do Governo Federal. Isso exige que as instituições passem por ciclos contínuos de autodiagnóstico, mapeamento de vulnerabilidades e correção de lacunas de segurança.
- **Revisão de Processos e Cultura Organizacional:** A implantação exige que as instituições reformulem e padronizem suas políticas internas. Isso inclui desde a limitação de acesso a sistemas críticos até a conscientização e treinamento de professores, técnicos e estudantes sobre boas práticas no uso da tecnologia.
- **Resiliência a Incidentes:** As IFEs devem estar estruturadas para prevenir, detectar e responder rapidamente a possíveis ataques cibernéticos ou vazamentos de dados, aumentando a sua resiliência e a confiabilidade dos serviços públicos digitais prestados à comunidade.

As implicações da adesão ao PPSI nas instituições envolvem:

- **Governança e Cultura:** Exige a criação de comitês internos, revisão de processos e o treinamento constante de servidores e alunos.
- **Implementação de Frameworks:** Obriga a instituição a adotar um framework rigoroso com controles técnicos para identificar falhas e prevenir vazamentos de dados.
- **Adequação Orçamentária:** Demanda investimentos em tecnologia (criptografia, firewalls, backups) e em ferramentas de apoio para mitigar riscos de ataques cibernéticos.
- **Gestão de Incidentes:** Estabelece protocolos padronizados de resposta rápida caso ocorram violações de segurança ou sequestro de dados.

A implementação do PPSI nas Instituições Federais de Ensino eleva a maturidade institucional na proteção de dados. Seus benefícios incluem a conformidade com a LGPD, prevenção de ataques cibernéticos, resiliência contra incidentes, otimização de recursos e a disseminação de uma cultura sólida de segurança e privacidade. Dentro dessa estrutura, a ETIR atua como um forte aliado operacional e técnico responsável por executar as políticas de segurança. Enquanto o programa define os processos de adequação, a equipe lida com o monitoramento contínuo, tratamento de ataques e mitigação de vulnerabilidades para garantir a resiliência institucional.

4.6. Regulamentação e Conformidade.

A relação entre as Instruções Normativas (IN) do Gabinete de Segurança Institucional (GSI) e suas Normas Complementares (NC) estabelece a espinha dorsal da governança de segurança cibernética na Administração Pública Federal (APF) brasileira, com foco na criação das Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) e na padronização de ações.

4.6.1. Instruções Normativas (GSI/PR)

- **IN 01 (IN01/DSIC/GSIPR):** Estabelece requisitos metodológicos para a gestão de segurança da informação nos órgãos da APF, servindo de base para a criação da ETIR e normatização de procedimentos [BRASIL 2020].
- **IN 03 (IN03/DSIC/GSIPR):** Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal. [Brasil. Gabinete de Segurança Institucional da Presidência da República 2021].

4.6.2. Normas Complementares (NC) - Estrutura e Atuação da ETIR

- **NC 05 (NC05/IN01/DSIC/GSIPR):** Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal [BRASIL 2009].
- **NC 08 (NC08/IN01/DSIC/GSIPR):** Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal [BRASIL 2010].
- **NC 21 (NC21/IN01/DSIC/GSIPR)** Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta [BRASIL 2014].

Tabela 3. Relação entre a Norma e seu Foco Principal com a ETIR/Incidente

Norma	Foco Principal	Relação com a ETIR/Incidente
IN 01	Gestão de Segurança da Informação	Fornece a base normativa que torna obrigatória a existência das ETIRs na APF.
NC 05	Criação da ETIR	Disciplina a criação de ETIR nos órgãos e entidades da APF.
NC 08	Tratamento de Incidentes	Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da APF.
NC 21	Comunicação/Segurança	Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da APF.

Portanto, os orgão e entidades da administração pública federal devem seguir a NC 05 para que a ETIR seja instituída, a NC 08 para agir durante um ataque e a NC 21 para se comunicar oficialmente.

5. Metodologia.

O procedimento metodológico divide-se em três fases distintas:

5.1. Fase de Diagnóstico (Quantitativa).

Realizada em maio de 2026, consistiu em uma análise documental estruturada nos sítios eletrônicos oficiais de 108 IFEs (composta por 38 Institutos Federais e 70 Universidades Federais). A pesquisa analisou as home page das instuições individualmente e em uma única visita pelo autor no momento do levantamento de dados, a fim de identificar quais possuem ETIR constituídas. As informações revelaram que uma certa quantidade ainda não possui uma equipe formalizada para atuar no tratamento de incidentes ciberneticos. Outra parte utiliza a politica de segurança da informação (PSI) para informar que possui uma ETIR, mas não especifica suas caracteristicas principais. Desta forma, a despadronização demonstra certa inconformidade das instuições com a norma complementar nº 5 [BRASIL 2009], o qual recomenda a formalização das equipes através de portaria específica, destacado em um menor grupo de instituições de ensino.

O critério de avaliação baseou-se na identificação de evidências documentais (portarias, resoluções ou normas internas) que formalizam a existência e o grau de autonomia das ETIRs, confrontando esses dados empíricos com as exigências da Norma Complementar nº 05/2008 do GSI/PR [BRASIL 2009], organizados em 3 categorais:

- **Não Possuem ETIR:** Não foi identificado evidências de constituição de ETIR em documentação emitida e publicada ou informação em seções do site institucional;
- **Possuem ETIR sem Portaria:** Possui pelo menos uma seção no site da instituições contendo informações sobre a ETIR, ou discriminado na Política de Segurança da Informação (PSI), ou em Regimento interno da instituição;
- **Possuem ETIR com Portaria:** Possui portaria específica formalização de acordo com as orientações normativas da IN01/2020 e NC05/2008.

5.2. Fundamentação Normativa e Comparativa.

A análise dos dados foi balizada pelo arcabouço regulatório do Gabinete de Segurança Institucional (GSI/PR) e por frameworks internacionais de cibersegurança (NIST, ISO/IEC 27035 e MITRE ATTCK). Foram consideradas as seguintes normativas brasileiras essenciais:

- **IN nº 01/2020:** Estabelece requisitos metodológicos para a gestão de segurança da informação nos órgãos da APF, servindo de base para a criação da ETIR e normatização de procedimentos [BRASIL 2020].
- **NC nº 05/2008:** Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal [BRASIL 2009].
- **NC nº 08/2010:** Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal [BRASIL 2010].
- **NC nº 21/2014:** Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta [BRASIL 2014].

5.3. Fase Propositiva e Construção do Artefato (Qualitativa).

A partir do ”gap”de conformidade identificado no diagnóstico (onde apenas 38% das IFEs atendiam integralmente às normas), a pesquisa utilizou uma abordagem sociotécnica para elaborar a proposta final. O modelo de formalização foi construído sob um modelo centralizado com autonomia compartilhada, estruturado em um rito de cinco passos: institucionalização formal, composição/capacitação, estruturação operacional, integração com a rede de governo e monitoramento contínuo.

A metodologia assegura a triangulação entre a ”norma ideal”(legislação) e a ”realidade operacional”das instituições, permitindo que o modelo proposto não seja apenas um trâmite burocrático, mas uma ferramenta de governança resiliente e adaptada ao contexto de restrições orçamentárias e escassez de pessoal qualificado do setor público brasileiro.

6. Cenário atual de adesão ao modelo de Criação de ETIR em Instituições Federais de Ensino (IFEs).

6.1. Institutos Federais de Ensino (IFs).

A pesquisa levantou informações de 38 instituições de ensino técnico profissionalizantes, distribuídos em 5 regiões geográficas (Norte, Nordeste, Contro-Oeste, Sudeste e Sul), conforme a tabela 4.

Tabela 4. Organização Geográfica da Rede de Institutos Federais (IFs).

Região	**UF**	**Instituições**	**Possuem ETIR**	**Constituiu Portaria**
Centro-Oeste	MT, GO, DF e MS.	IFB, IFMT, IFMS, MFG e IFGOIANO.	IFB, IFMS e IFGOIANO	IFB e IFMS
Nordeste	MA, PI, CE, RN, PB, PE, AL, SE e BA.	IFAL, IFBA, IFBAIANO, IFCE, IFMA, IFPB, IFPE, IFSertãoPE, IFPI, IFRN e IFS.	IFBAIANO, IFCE, IFMA, IFPB, IFSertãoPE, IFPI, IFRN e IFS	IFPB, IFSertãoPE, IFPI, IFRN e IFS
Norte	RR, AM, AC, RO, AP, PA e TO.	IFAC, IFAP, IFAM, IFPA, IFRO, IFTO e IFRR.	IFAP, IFAM e IFRR	IFRR.
Sudeste	MG, ES, RJ e SP.	IFES, IFRJ, IFF, IFMG, IFNMG, IFSudesteDeMinas, IFSulDeMinas, IFTM e IFSP.	IFRJ, IFF, IFMG, IFSudesteDeMinas, IFSulDeMinas, IFTM e IFSP.	IFRJ, IFF, IFMG, IFSulDeMinas e IFSP.
Sul	PR, SC e RS.	IFRS, IFFarroupilha, IFSUL, IFPR, IFSC e IFC.	IFC	IFC

6.2. Universidades Federais de Ensino.

O estudo verificou a documentação e os dado públicos referentes a formalização e existência de ETIR em 70 universidades federais, distribuídos em 5 regiões geográficas (Norte, Nordeste, Contro-Oeste, Sudeste e Sul). Os números evidenciam um gap de organização em cibersegurança enfrentado pelas organizações federais de ensino público superior, observado na tabela 5.

Tabela 5. Organização Geográfica da Rede de Universidades Federais (UFs).

Região	**UF**	**Instituições**	**Possuem ETIR**	**Possuem Portaria**
Centro-Oeste	MT, GO, DF e MS.	UFMT, UFR, UFG, UFCat, UFJ, UnB, UFMS e UFGD.	UFMT, UFG, UFCat, UFJ, UnB, UFMS e UFGD.	UFJ, UnB, UFMS e UFGD.
Nordeste	MA, PI, CE, RN, PB, PE, AL, SE e BA.	UUFMA, UFPI, UFDPar, Univasf, UFCE, UFCA, Unilab, UFRN, Ufersa, UFPB, UFCG, UFPE, UFRPE, Ufape, UFAL, UFS, UFBA, UFRB e UFSB.	UFCE, UFCA, Unilab, Ufersa, UFAL e UFSB.	UFCE, UFCA, Unilab, Ufersa, UFAL e UFSB.
Norte	RR, AM, AC, RO, AP, PA e TO.	UFRR, UFAM, UFAC, UNIR, UNIFAP, UFPA, Unifesspa, Ufopa, Ufra, UFT e UFNT.	UFAM, UFPA, Unifesspa, Ufopa, UFT e UFNT.	UFAM, Unifesspa, UFT e UFNT.
Sudeste	MG, ES, RJ e SP.	UFMG, Ufop, UFU, UFVJM, UFTM, UFSJ, UFV, Ufla, UFJF, Unifal-MG, Unifei, UFES, UFRJ, UNIRIO, UFF, UFRRJ, Unifesp, UFSCar e UFABC.	UFMG, Ufop, UFVJM, UFSJ, UFV, Ufla, UFJF, Unifal-MG, UFES, UFRJ, UNIRIO, UFF, Unifesp, UFSCar e UFABC.	UFSJ, Ufla, Unifal-MG, UFRJ e Unifesp.
Sul	PR, SC e RS.	UFPR, UTFPR, Unila, UFFS, UFSC, UFFS, UFRGS, UFPel, Furg, UFCSPA, Unipampa, UFSM e UFFS.	UFPR, UTFPR, Unila, UFFS, UFSC, UFFS, UFPel, Furg, UFSM e UFFS.	UFPR, UTFPR, Unila, UFFS, UFFS, UFPel, Furg, UFSM e UFFS.

7. Resultados.

A análise dos resultados demonstrou uma heterogeneidade significativa na maturidade de governança cibernética entre as instituições. Dos 108 órgãos pesquisados, observou-se que 39% carecem de estrutura formal de ETIR. Dentre os 61% que evidenciam a existência dessas equipes, nota-se uma fragilidade na conformidade formal, visto que apenas uma parcela atende integralmente à exigência de portaria específica prevista na NC nº 05/2008.

7.1. Análise Quantitativa da Presença de ETIR nos Institutos Federais (IFs).

O resultado encontrado organizou os 38 institutos federais em 5 regiões geogáficas e classificou os dados em 3 categorais: (1) Não possui ETIR; (2) Possui ETIR sem Portaria e (3) Possui ETIR com Portaria, conforme tabela 6.

Tabela 6. Distribuição Regional Quantitativa de Institutos Federais(IFs) e Constituição de ETIR.

Região	A	B	C	Total
Norte	4	2	1	7
Nordeste	3	3	5	11
Centro-Oeste	2	1	2	5
Sudeste	2	2	5	9
Sul	5	0	1	6
Total	16	8	14	**38**

Legenda: A: Não possui ETIR. **B:** Possui ETIR sem Portaria. **C:** Possui ETIR com Portaria.
Fonte: Elaborado pelo autor (2026).

A análise gráfica demonstra que as regiões Nordeste e Sudeste possuem maior quantitativo de institutos e a melhor conformidade normativa, em detrimento as regiões Norte e Sul, que possuem o maior gap de conformidade normativa, ao paço que a região Centro-Oeste apresenta equilíbrio normativo, conforme observado no gráfico da figura 1.

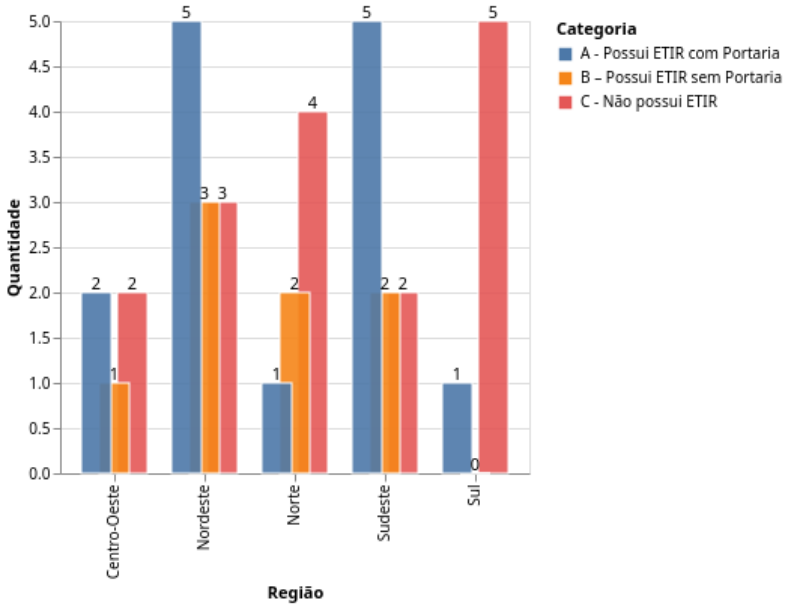

Figura 1. Gráfico de presença de ETIR em Institutos Federais (IF).

7.2. Análise Quantitativa da Presença de ETIR nas Universidades Federais (UFs).

O levantamento quantitativo organizou as 70 universidades federais em 5 regiões geogáficas, e utilizou a classifição dos dados em 3 categorais: (1) Não possui ETIR; (2) Possui ETIR sem Portaria e (3) Possui ETIR com Portaria, conforme tabela 6

Tabela 7. Distribuição Regional Quantitativa de Universidades Federais(UFs) e Constituição de ETIR.

Região	A	B	C	Total
Norte	5	2	4	11
Nordeste	13	0	6	19
Centro-Oeste	1	3	4	8
Sudeste	4	10	5	19
Sul	3	1	9	13
Total	26	16	28	**70**

Legenda: A: Não possui ETIR. **B:** Possui ETIR sem Portaria. **C:** Possui ETIR com Portaria.
Fonte: Elaborado pelo autor (2026).

A análise gráfica demonstra que as regiões Centro-Oeste e Sul possuem a melhor conformidade normativa, em detrimento as regiões Norte e Nordeste, que possuem o maior gap de formalização, ao paço que a região Sudeste, apesar de possuir um elevado número de ETIR sem portaria formalizada, demonstra equilíbrio normativo e apenas 4 universidades sem a evidencia de presença de ETIR. Além disso, a região Nordeste se destaca pela elevada quantidades de instituições em desalinhamento com a conformidade legal de formalização das ETIR, conforme observado no gráfico da figura 2.

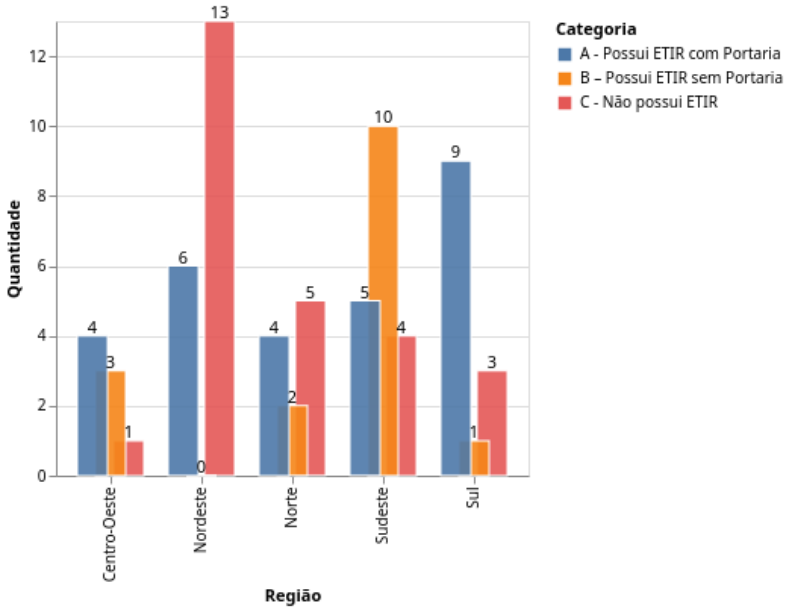

Figura 2. Gráfico de presença de ETIR em Universidades Federais.

Em um panorama geral da presença formalizada de ETIR em IFEs, observou-se que em 100% pesquisadas (108), 39% não apresentação ETIR em suas estruturas (42), dado que indica uma possível sobrecarga da equipe de infraestrutura de tecnologia da informação acumulando atividades diárias da área de TIC e atuando de maneira reativa para os casos de incidentes cibernéticos tempestivos. Em uma segunda análise, 39% possuem a formalização em portaria específica (42), indicando que ainda persiste um gap de 22% das IFEs (24) que atuam com equipes de resposta a incidentes cibernéticos em desconformidade com a Instrução Normativa 01 (IN01/DSIC/GSIPR) e Norma Complementar 05 (NC n° 05/IN01/DSIC/GSIPR), conforme observado no gráfico da figura 3.

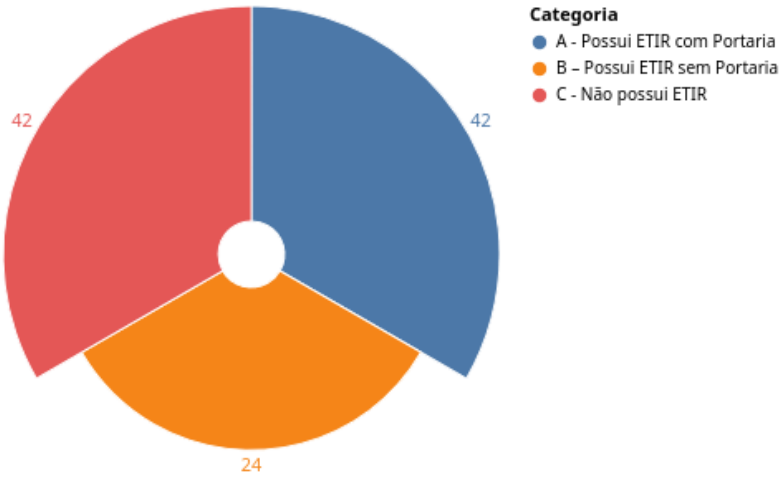

Figura 3. Gráfico de presença de ETIR em IFEs.

A análise visual dos gráficos apresenta semelhança na quantidade de presença de ETIR e destaca que pelo menos 39% das intituições federais de ensino possuem mais chance de vulnerabilidades em atendimento de incidentes cibernéticos em suas equipes de infraestrutura de tecnologia da informação. Deste Percentual, os Institutos federais (IF) possuem um gap de aproximadamente 42% (16/38) em comparação aos 37% (26/70) apresentados pelas Universidades federais (UF), conforme observado no gráfico da figura 4. Apesar da ausência de formalização de ETIR encontra-se em equilíbrio com o quantitativo de conformidade normativa, observada-se nas Univeridades federais uma pequena vantagem relativa em comparação aos institutos federais.

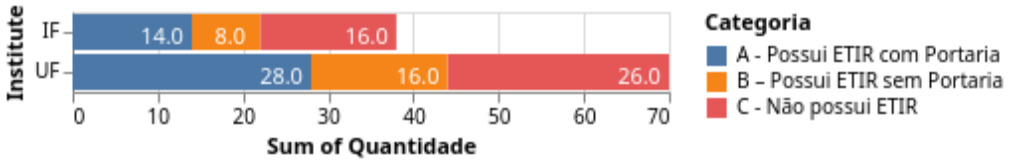

Figura 4. Gráfico de presença de ETIR em Regiões.

8. Implementação do modelo.

A norma complementar nº 05 [BRASIL 2009] deixa claro que cada órgão ou entidade deverá estabelecer, dentre os modelos descritos, aquele que melhor se adequar às suas necessidades e limitações, ressalvado que, independentemente do modelo escolhido, deverão ser observadas as diretrizes da Norma Complementar, e deverá ser designado formalmente o Agente Responsável (Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a incidentes em Redes Computacionais), que terá, dentre outras atribuições, a de ser a interface com o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV, sendo ele o responsável por criar os procedimentos internos, gerenciar as atividades e distribuir tarefas para a Equipe ou Equipes que compõem a ETIR. A norma propõe quatro tipo de modelos:

- **Modelo 1:** Utilizando a equipe de Tecnologia da Informação.
- **Modelo 2:** Centralizado.
- **Modelo 3:** Descentralizado.
- **Modelo 4:** Combinado ou Misto.

A implementação do modelo será o Modelo 2 (Centralizado), onde a equipe será composta por pessoal com dedicação exclusiva às atividades de tratamento e resposta aos incidentes em redes computacionais.

A autonomia da ETIR descreve o escopo de atuação e o nível de responsabilidade que a Equipe tem sobre as suas próprias ações e sobre as atividades de resposta e tratamento dos incidentes na rede de computadores, definindo o nível de controle da Equipe no relacionamento com os componentes da sua organização e deverá ser definida, explicitamente, no documento de constituição da Equipe. A NC05 orienta três especificações:

- **Autonomia Completa.**
- **Autonomia Compartilhada.**

- **Sem Autonomia.**

O modelo proposto recomendará a utilização da Autonomia Compartilhada, ou seja, a ETIR participará no resultado da decisão, sendo, no entanto, apenas um membro no processo decisório. Neste caso, a Equipe poderá recomendar os procedimentos a serem executados ou as medidas de recuperação durante um ataque e discutirá as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas) com os outros membros da organização.

O processo de elaboração envolve cinco passos:

- **(1) Institucionalização formal.**
- **(2) Composição e Capacitação da Equipe.**
- **(3) Estruturação Operacional.**
- **(4) Integração com a Rede Governo.**
- **(5) Monitoramento e Auditoria.**

Com base na Instrução Normativa nº 1/2020 do GSI/PR [BRASIL 2020] e práticas adotadas em IFEs, aqui estão os passos fundamentais para garantir a presença e eficácia da ETIR.

8.1. Institucionalização Formal (Base Legal):

- **Emissão de Portaria:** A ETIR deve ser criada por meio de uma portaria oficial emitida pelo reitor ou autoridade máxima da instituição.
- **Documento de Constituição:** Elaborar e publicar um documento que formalize o ”Documento de Constituição da ETIR”, definindo suas atribuições, escopo de atuação (quais sistemas e unidades cobre), e responsabilidades.
- **Vínculo com o CGSIC:** A ETIR deve estar alinhada ao Comitê Gestor de Segurança da Informação e das Comunicações (CGSIC) da IFE.

8.2. Composição e Capacitação da Equipe:

- **Equipe de Servidores Efetivos:** A composição deve ser preferencialmente por servidores públicos civis efetivos ou militares de carreira com capacitação técnica compatível.
- **Equipe Multidisciplinar:** Embora a base seja de TI, é recomendado incluir membros de áreas jurídico-legais, auditoria, gestão de riscos e comunicação para lidar com incidentes complexos.
- **Treinamento Contínuo:** Garantir que a equipe passe por capacitações constantes em resposta a incidentes, análise de vulnerabilidades e forense computacional.

8.3. Estruturação Operacional:

- **Definição do Modelo de Atuação:** Definir se a ETIR atuará de forma reativa (apenas quando o incidente ocorre) ou proativa (prevenção e análise de vulnerabilidades). O Modelo será centralizado, com pessoal em dedicação exclusiva às atividades da ETIR.
- **Autonomia:** A autonomia será Compartilhada, onde a equipe participará do resultado da decisão, porém, apenas como um membro no processo decisório através de recomendações a procedimentos de recuperação durante um ataque e discutirá as acões a serem tomadas com os demais membros da organização.
- **Canal de Notificação:** Criar um canal oficial e conhecido (ex: etir@if.edu.br) para que usuários da IFE notifiquem incidentes.

8.4. Integração com a Rede Governo:

- **Conexão com CTIR Gov:** A ETIR da IFE deve se integrar à ReGIC (Rede Federal de Gestão de Incidentes Cibernéticos) coordenada pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov).
- **Relatórios de Incidentes:** Estabelecer procedimentos para elaboração de relatórios detalhados sobre incidentes, reportando-os conforme exigido pelas autoridades superiores (Regic/GSI).

8.5. Monitoramento e Auditoria:

- **Revisão Periódica:** O documento de constituição e as normas da ETIR devem ser revisados periodicamente, em intervalos, por exemplo, de até dois anos, para se manterem atualizados contra novas ameaças.
- **Simulados de Incidente:** Realizar exercícios práticos (simulados) de ataque cibernético para testar a prontidão da equipe e os planos de resposta.

A ETIR deverá guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede orientados pelo Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV. Poderá usar as melhores práticas de mercado e frameworks, desde que não conflitem com os dispositivos desta Norma Complementar. Deverá comunicar de imediato a ocorrência de todos os incidentes de segurança ocorridos na sua área de atuação ao CTIR GOV, conforme padrão definido por esse órgão, a fim de permitir a geração de estatísticas e soluções integradas para a Administração Pública Federal. A troca de informações e a forma de comunicação entre as ETIR, e entre estas e o CTIR GOV, serão formalizadas caso a caso, se necessário, por Termo de Cooperação Técnica.

9. Discussão dos resultados.

O cenário atual de ataques cibernéticos em Instituições Federais de Ensino é crítico, caracterizado por um aumento expressivo e sofisticado, com foco dinâmico em tecnologias emergentes de atuação, auxiliadas por técnicas de inteligência artifical. A dependência de TICs e a interconexão das redes acadêmicas tornam essas instituições alvos atraentes, resultando em sequestro de informações, paralisação de serviços essenciais, como datacenters, e necessidade de fortalecimento imediato na segurança da informação. A tendência é de alta nas ameaças, exigindo políticas rigorosas de prevenção, backup e capacitação dos usuários para lidar com a evolução dos crimes virtuais.

Neste contexto, o Ministério da Gestão e da Inovação em Serviços Públicos (MGI), por meio da Secretaria de Governo Digital (SGD), tem intensificado o combate a ciberataques através da reestruturação do Programa de Privacidade e Segurança da Informação (PPSI 2.0), transformando-o em uma política de governança e resiliência digital de Estado com vigência para 2026. As ações incluem a obrigatoriedade de medidas técnicas e de gestão de riscos para mais de 250 órgãos do SISP, como o uso de novos guias de framework e a criação do Centro Integrado de Segurança Cibernética (CISC) para detecção e resposta a incidentes. Além disso, o MGI emite instruções normativas e notas técnicas para aumentar a maturidade cibernética, priorizar o tratamento de riscos críticos e fortalecer a cultura de segurança da informação, alinhando-se à proteção de dados pessoais (LGPD) e à Estratégia Federal de Governo Digital.

Por outro lado, é observado uma baixa adesão de Institutos Federais (IFEs) e Universidades Federais na formalização de Equipes de Tratamento e Resposta a Incidentes de Segurança Cibernética, sendo interpretado como reflexo da escassez de recursos orçamentários, déficit de profissionais qualificados em TI e ausência de cultura institucional focada em segurança da informação. Esse cenário é agravado pela burocracia administrativa e pela complexidade na verticalização das ações de segurança entre os diversos campi, retardando a implementação de políticas preventivas de segurança da informação eficazes recomendadas pelo Governo Federal.

A predominância de ETIRs sem formalização em portaria (o 'gap' de 38% de conformidade plena) sugere que as instituições operam em uma zona de risco jurídico e operacional. Como discutido por [Krueger 2009], a descentralização de TI em universidades frequentemente desenvolvem suas próprias políticas de TI e segurança, o que pode enfraquecer uma política institucional única e consistente. Com isso, a ausência de coordenação faz com que práticas de segurança variem entre departamentos, dependendo da atuação dos profissionais locais, o que leva a uma segurança baseada em esforços voluntários dos técnicos, e não em uma política de Estado. Sem o amparo de um documento de constituição, conforme preconiza a NC nº 05/2008, o Agente Responsável não detém a autoridade delegada necessária para impor políticas de segurança em laboratórios departamentais autônomos, tornando a resiliência da rede dependente da boa vontade institucional e não de um processo de governança resiliente conforme a IN nº 03/2021. Como apontado por [Forum of Incident Response and Security Teams (FIRST) 2024] e [Moyle 2024], a falta de formalização do ETIR reduz sua atuação a funções predominantemente operacionais de infraestrutura, sobrecarregando equipes que não possuem mandato institucional para coordenar a gestão de riscos, definir prioridades e articular a resposta organizacional a incidentes.

Uma proposta simples para implementar a criação e formalização de ETIR, baseada nas normas emitidas pelo MGI, através do SGI é abordada neste artigo, recomendando uma estrutura organizacional onde os membros sejam constituidos por administradores de sistema ou de segurança, administradores de banco de dados, administradores de rede, analistas de suporte ou quaisquer outras pessoas da organização com conhecimento técnico comprovado. A Equipe poderá ser estendida com a inclusão de representantes legais de áreas específicas da organização, advogados, estatísticos, recursos humanos, relações públicas, gestão de riscos, controle interno e grupo de investigação, ou outro que a organização entenda ser adequado, em um número máximo de sete integrantes preferencialmente composta por servidores públicos ocupantes de cargo efetivo ou militares de carreira, conforme o caso, com perfil técnico compatível, lotados nos seus respectivos órgãos. O modelo de implementação é centralizado, composto por pessoal com dedicação exclusiva às atividades de tratamento e resposta aos incidentes em redes computacionais. A autonomia deve ser compartilhada, ou seja, a Equipe poderá recomendar os procedimentos a serem executados ou as medidas de recuperação durante um ataque e discutirá as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas) com os outros membros da organização.

A formalização deve ser emitida em portaria específica através de documento de constituição de ETIR. Em atuação, a equipe poderá usar as melhores práticas de mercado, desde que não conflitem com os dispositivos de norma complementares e deverá guiar-se

por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede orientados pelo Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV. Assim sendo, sempre que possível, o grupo deverá comunicar de imediato a ocorrência de todos os incidentes de segurança ocorridos na sua área de atuação ao CTIR GOV, conforme padrão definido por esse órgão, a fim de permitir a geração de estatísticas e soluções integradas para a Administração Pública Federal, favorecendo a troca de informações e a forma de comunicação entre as ETIR, e entre estas e o CTIR GOV, sejam formalizadas caso a caso, se necessário, por Termo de Cooperação Técnica.

Uma Instituição Federal de Ensino, que possui uma ETIR institucionalizada, usufrui dos principais benefícios a estruturação de uma gestão centralizada de segurança, permitindo a detecção ágil e a resposta coordenada a ataques cibernéticos, o que minimiza danos e garante a continuidade das atividades de ensino, pesquisa e extensão. Além de reduzir riscos e vulnerabilidades através de monitoramento contínuo e ações preventivas, a ETIR fortalece a resiliência institucional, promove a conformidade com as diretrizes de segurança da informação da administração pública federal e protege dados sensíveis da comunidade acadêmica contra vazamentos ou manipulações.

10. Conclusão.

O cenário atual e dinâmico de insegurança em ambiente cibernético que permeia as instituições de ensino federais, se faz necessário a formulação de equipes de tratamento e resposta a incidentes cibernéticos para atuar de maneira preventiva, a fim de mitigar os riscos de perda de dados institucionais e interrupção de serviços essenciais a comunidade acadêmica. Neste contexto, observa-se a baixa adesão de instituições à criação de ETIR, a qual pode ser justificada pela ausência de um modelo simples e bem estruturado capaz de preencher os requisitos mínimos exigidos pela legislação normativa e promove uma estrutura básica suficiente para a atuação inicial em tratamento e resposta a incidentes cibernéticos e realizar a comunicação necessária aos orgãos competentes da administração pública federal. Entretanto, a pesquisa limitou-se ao levantamento de informações publicadas nos sites oficiais das instituições e não poderá afirmar que a ausência de publicidade nos canais de divulgação oficiais confirme a inexistência da documentação comprobatória de existência de ETIR nos orgãos de visitados.

A proposta de formalização centralizada e com autonomia compartilhada apresentada neste trabalho visa preencher o gap de conformidade identificado no diagnóstico realizado. A adoção desta estrutura permite que as IFEs transitem de um modelo de resposta reativa para uma postura de resiliência digital, cumprindo não apenas as normas do GSI/PR [BRASIL 2020], mas também as exigências da LGPD e as melhores práticas de governança cibernética citadas por [NIST 2025].

Este artigo tem como objetivo principal disponibilizar o conhecimento necessário para a formalização da criação de ETIR em conformidade com as instruções normativas e normas complementares emitidas pelo MGI e SGI. Através desta implementação, os orgãos poderão fazer uso de equipe dedicadas a atuar de forma preventiva desde a análise vulnerabilidades do ambiente e infraestutura de TIC, até os reports adequados em tempo hábil aos orgão de controles e registros, além de garantir junto a alta administração o modelo centralizado de atuação e autonomia compartilhada de tomada de decisões. Com

isso, o orgão estará certamente contribuindo constantemente para a construção de um ambiente cibernético mais seguro e robusto e poderá contar com o suporte de uma rede de instituições integradas organizadas pelo CTIR Gov. Essa iniciativa visa melhorar a adesão das IFEs à criação de ETIR e conscientizar os orgão para a utilização destas equipes como uma ferramenta aliada ao combate e defesa de ataques cibernéticos e possui como trabalho futuro a proposta de implementação de processo de atuação das ETIRs integrado ao Programa de Privacidade e Segurança da Informação (PPSI).

Referências

Agyemang, R., Furnell, S., and Muller, T. (2026). A context-aware cybersecurity readiness assessment framework for organisations in developing and emerging environments. *Future Internet*. Published: 24 March 2026.

Bada, M., Sasse, A., and Nurse, J. R. C. (2014). National csirts and their role in computer security incident response. Technical Report 10, Global Commission on Internet Governance. Accessed: 2026-07-10.

Benaroch, M. (2024). Cyber failures and information technology capability reputation: Examining ex ante and ex post interplay effects. *Journal of Management Information Systems*, 41(3):744–778.

BRASIL (1996). Lei n° 9.394, de 20 de Dezembro de 1996. Presidência da República. Casa Civil. Acesso em: 18 mar. 2026.

BRASIL (2008). Lei n° 11.892, de 29 de Dezembro de 2008. Presidência da República. Casa Civil. Acesso em: 18 mar. 2026.

BRASIL (2009). Norma Complementar n° 05/IN01/DSIC/GSIPR, de 14 de Agosto de 2009. Gabinete de Segurança Institucional da Presidência da República (GSIPR). Departamento de Segurança da Informação e Comunicações. Acesso em: 17 mar. 2026.

BRASIL (2010). Norma Complementar n° 08/IN01/DSIC/GSIPR, de 24 de Agosto de 2010. Gabinete de Segurança Institucional da Presidência da República (GSIPR). Departamento de Segurança da Informação e Comunicações. Acesso em: 17 mar. 2026.

BRASIL (2014). Norma Complementar n° 21/IN01/DSIC/GSIPR, de 8 de Outubro de 2014. Gabinete de Segurança Institucional da Presidência da República (GSIPR). Departamento de Segurança da Informação e Comunicações. Acesso em: 17 mar. 2026.

BRASIL (2020). Instrução normativa nº 1, de 27 de maio de 2020. Dispõe sobre a gestão de segurança da informação.

Brasil (2021). Decreto nº 10.748, de 16 de julho de 2021: Institui a rede federal de gestão de incidentes cibernéticos.

BRASIL (2025). Orientações para notificação de incidentes cibernéticos ao ctir gov. Acessado em: 18 mar. 2026.

Brasil. Gabinete de Segurança Institucional da Presidência da República (2021). Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021: Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal. `https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/legislacao/copy_of_IN03_consolidada.pdf`. Acesso em: 15 jul. 2026.

Brito, I. V. S. and Ferreira, Y. (2017). Estabelecimento de csirts e processo de tratamento de incidentes de segurança em instituições acadêmicas brasileiras: estudo de caso da parceria cais/rnp e ufba. In *Anais da Sétima Conferência de Diretores de Tecnologia da Informação – TICAL 2017: Gestão de TIC para Pesquisa e Colaboração*, pages 1–10, San José, Costa Rica. RedCLARA. Disponível em: http://hdl.handle.net/10786/1290. Acesso em: 9 jul. 2026.

Center for Internet Security, Inc. (CIS) (2021). Cis critical security controls version 8. Acessado em: 18 mar. 2026.

CERT.br (2012). *Tratamento de Incidentes de Segurança*. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, São Paulo. Disponível na série de documentos do CERT.br.

de Góes Moraes, D. C. M. and Luft, M. C. M. S. (2024). Desafios à implementação das estratégias de governo digital e o nível de maturidade nas instituições federais de ensino superior. In *Anais do VII Encontro Internacional de Gestão, Desenvolvimento e Inovação (EIGEDIN)*, volume 7, Campo Grande, MS. Universidade Federal de Mato Grosso do Sul.

Ethembabaoglu, A., Kadenko, N. I., Angelova, Y., Zhauniarovich, Y., van Wegberg, R., Parkin, S., and van Eeten, M. (2026). Tell Them They Are a Responsible Entity, Not a Customer: Understanding practitioner challenges in sector csirts. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26)*, pages 1–23, New York, NY, USA. Association for Computing Machinery (ACM).

Forum of Incident Response and Security Teams (FIRST) (2024). Csirt services framework, version 2.1. Acesso em: 21 jul. 2026.

Frank, E., Olaoye, G., and Emmanuel, O. K. (2023). Cybersecurity in education: Protecting students and staff. *Computer Science and Engineering*. Accessed: 2026-07-10.

Ignain, K. M. and Fernandes, J. M. (2024). Improving incident management processes with feature models. *Journal of Cyber Security and Mobility*, 13(4):701–724.

Ioannou, M., Stavrou, E., and Bada, M. (2019). Cybersecurity culture in computer security incident response teams: Investigating difficulties in communication and coordination. In *Cyber Science 2019*, Oxford, United Kingdom. Acesso em: 9 jul. 2026.

ISO/IEC (2016). Iso/iec 27035:2016 - information technology – security techniques – information security incident management. Standard, International Organization for Standardization, Geneva, Switzerland.

Krueger, D. A. (2009). Decentralized it governance and policy in higher education. Research Bulletin Issue 5, EDUCAUSE Center for Applied Research (ECAR), Boulder, CO.

Kumar, A., Mishra, K., Mahto, R. K., and Mishra, B. K. (2024). A framework for institution to enhancing cybersecurity in higher education: A review. *LatIA*, 2(94).

Lokare, A., Bankar, S., and Mhaske, P. (2025). Integrating cybersecurity frameworks into it security: A comprehensive analysis of threat mitigation strategies and adaptive technologies. *arXiv preprint*. Accessed: 2026-07-10.

Meyer, C., Heininger, R., and Stary, C. (2024). Improving vulnerability management through process mining. *Applied Sciences*, 14(23).

MGI-PR (2023). Programa de privacidade e segurança da informação (ppsi). Acesso em: 9 jul. 2026.

Mohd Kassim, S. R. B., Li, S., and Arief, B. (2023). The use of public data and free tools in national csirts' operational practices: A systematic literature review. *arXiv preprint arXiv:2306.07988*. Acesso em: 9 jul. 2026.

Moyle, E. (2024). How to create a csirt: 10 best practices. Publicado em 17 jan. 2024.

National Institute of Standards and Technology (2024). The nist cybersecurity framework (csf) 2.0. Technical Report NIST CSWP 29, National Institute of Standards and Technology (NIST).

Nelson, A., Rekhi, S., Souppaya, M., and Scarfone, K. (2025). Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile. Special Publication (SP) NIST SP 800-61 Rev. 3, National Institute of Standards and Technology (NIST).

REVISTA (2025). Ataques cibernéticos a universidades e instituições científicas crescem no país. Report, FAPESP, São Paulo, SP.

Rios, O. K. L., Teixeira Filho, J. G. d. A., and Rios, V. P. d. S. (2017). Gestão de segurança da informação: práticas utilizadas pelas instituições federais de ensino superior para implantação de política de segurança da informação. *Navus – Revista de Gestão e Tecnologia*, 7(2):49–65.

Silva, J. P. B. d., Ferreira, L. V. A., and Nunes, R. R. (2026). Desafios da segurança cibernética: uma análise da administração pública brasileira. *Revista Tecnologia e Sociedade*, 23(69):157–178.

SOCCER Project (2024). Cyberattack on the université paris-saclay: Case study. Case study on ransomware attack against a higher education institution.

The MITRE Corporation (2024). Mitre att&ck® - adversarial tactics, techniques, and common knowledge. `https://attack.mitre.org/`. Acessado em: 18 mar. 2026.