VIII ENCONTRO INTERNACIONAL DE GESTÃO, DESENVOLVIMENTO E INOVAÇÃO
NOVOS CONTEXTOS PARA O AGRONEGÓCIO
ISSN: 2594-8083
VIII EIGEDIN
25 a 27 de Maio de 2026
Totalmente Online e Gratuito

( ) Graduação (X) Pós-Graduação
(X) Artigo completo ( ) Relato de prática ( ) Resumo expandido

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO DAS UNIVERSIDADES FEDERAIS: Análise das Diretrizes de Gestão de Incidentes em Segurança da Informação

Luiz Fernando Torres Alves
Universidade Federal de Mato Grosso do Sul
torres.alves@ufms.br

Jeovan de Carvalho Figueiredo
Universidade Federal de Mato Grosso do Sul
jeovan.figueiredo@ufms.br

RESUMO

A segurança da informação é um pilar estratégico na era digital, e no setor público brasileiro, a sua relevância é central. Este estudo teve como objetivo identificar a conformidade das Políticas de Segurança da Informação (PSI) das universidades federais brasileiras com as diretrizes da Norma Complementar 05/IN/GSI/PR, focando especificamente na existência e na estrutura das Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR). Para tanto, foi realizada uma análise documental qualitativa de 57 PSI das universidades federais. Os resultados revelam que, embora a maioria das instituições tenha formalizado a existência de uma ETIR, a adesão é frequentemente superficial, sendo que pontos como o "modelo de implementação" e a "estrutura organizacional" foram os menos especificados, com poucas universidades detalhando a composição das equipes e as qualificações. Conclui-se que a simples formalização de uma PSI não garante a eficácia na gestão de incidentes, e a falta de clareza sobre procedimentos detalhados das equipes indica a necessidade de avaliar o estágio de amadurecimento na adoção dos procedimentos de segurança da informação. O trabalho destaca a importância da transparência e a necessidade das universidades federais avançarem em suas políticas para torná-las aptas a responderem a eventuais incidentes de segurança da informação.

Palavras-chave: Segurança da informação (SI); Política Nacional de Segurança da Informação (PNSI); Instituições Federais de Ensino Superior (IFES).

ISSN: 2594-8083

1 INTRODUÇÃO

A segurança da informação é um pilar essencial na era digital, pois desde o início da computação, a proteção dos dados e dos sistemas já começa a ser pensada, ainda que em um contexto de menor interconexão. Pensadores como (Parker, 1981; Spafford, 1992) foram cruciais nesse cenário inicial, desvendando os desafios emergentes da segurança computacional e promovendo as bases para o que se tornaria a Política de Segurança da Informação (PSI).

Em pouco tempo, a segurança da informação deixou de ser meramente técnica para se tornar um fator estratégico, determinando a maneira pela qual, organizações e governos defendem seu ativo mais valioso: a informação. A medida que a sociedade se torna cada vez mais dependente de sistemas digitais, a defesa contra ameaças como ataques cibernéticos, fraudes e vazamentos de dados emerge como uma prioridade inegociável, conforme destaca (Anderson, 2008) em sua análise sobre engenharia de segurança, ao enfatizar a necessidade de projetar sistemas seguros desde sua concepção.

No Brasil, a segurança da informação tem ganhado destaque crescente, especialmente no setor público. A promulgação da Lei Geral de Proteção de Dados (LGPD) (Brasil, 2018), por exemplo, trouxe um novo patamar de exigência para o tratamento de dados pessoais, conforme afirma (Schneier, 2015) ao discutir sobre privacidade e vigilância. No contexto da administração pública federal, a relevância da segurança da informação é formalizada por diretrizes governamentais.

O Decreto n. 12.572, de 4 de agosto de 2025, que institui a Política Nacional de Segurança da Informação (PNSI) (Brasil, 2025), e a Instrução Normativa GSI/PR Nº 1/2020,(Brasil, 2020) que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal, são marcos legais que estabelecem as bases para a gestão da segurança e privacidade dos dados em todos os órgãos e entidades da esfera federal, incluindo as instituições de ensino. Essas normativas refletem a necessidade de padronização e fortalecimento das defesas cibernéticas.

Dada a expansão acelerada das redes locais de computadores nas instituições públicas, embora essencial para suportar o fluxo crescente de dados e o desempenho funcional, impõe um desafio crítico à segurança da informação diante de um cenário de ameaças cibernéticas em constante evolução. Nesse contexto, a Norma Complementar 05/IN/GSI/PR (NC 05) (Brasil, 2009) estabelece que a eficácia da estratégia de segurança depende de uma abordagem em camadas, sendo a criação de Equipes de Tratamento e Resposta a Incidentes (ETIR) uma peça

central e obrigatória para a resiliência institucional. A problemática reside portanto, no fato de que, sem essa institucionalização clara e o detalhamento das competências exigidas pelo Gabinete de Segurança Institucional (GSI), a criação de ETIRs torna-se meramente figurativa, falhando em prover a camada de proteção necessária para salvaguardar o ambiente interconectado da Administração Pública contra paralisias sistêmicas.

A justificativa deste artigo repousa na necessidade de avaliar a capacidade das instituições de ensino superior na gestão de incidentes. Como argumentam (Gomide e Pires, 2014), a capacidade de implementação de políticas públicas no Brasil depende da presença de burocracias profissionalizadas e infraestruturas técnicas robustas. A ausência de detalhes sobre a ETIR nas políticas institucionais não é apenas uma omissão técnica, é um risco e vulnerabiliza a infraestrutura de educação. Conforme reforça (Doneda, 2021), a proteção de dados no setor público é um dever que exige prontidão técnica para assegurar os dados que as instituições públicas detêm. Portanto, investigar o alinhamento das Instituições Federais de Ensino Superior (IFES) com os eixos da NC 05 é fundamental para identificar gargalos e propor caminhos que alcancem a segurança da informação.

As instituições federais de ensino superior se pautam nas normativas federais e a Políticas de Segurança da Informação (PSI) se torna, nesse contexto, de suma importância, dada a vastidão e a sensibilidade dos dados que gerenciam, desde informações acadêmicas e financeiras até dados de pesquisa e dados pessoais de alunos e servidores. Assim, objetivo central é identificar a conformidade das PSI das universidades federais brasileiras com as diretrizes da NC 05 (Brasil, 2009), focando especificamente na existência e na estrutura das ETIRs.

Este trabalho está estruturado nas seguintes seções, após esta introdução, a segunda seção dedica-se à revisão da literatura, fundamentando teoricamente os conceitos de segurança da informação e as normativas federais, a terceira seção detalha os procedimentos metodológicos adotados na pesquisa. Em seguida a discussão e análise de dados, onde se examina o alinhamento das IFES com NC 05 e seus 6 conceitos, posteriormente apresenta-se a conclusão, que sintetiza as principais análises e limitações deste trabalho, por fim, as referências bibliográficas e os apêndices que complementam o estudo.

ISSN: 2594-8083

2 REVISÃO DA LITERATURA

A segurança da informação (SI) transcendeu a mera preocupação tecnológica para se consolidar como um pilar estratégico na gestão de qualquer organização. Historicamente, a atenção à segurança da informação começou com um foco técnico, mas rapidamente evoluiu (Parker, 1981) foi um dos pioneiros a reconhecer a gestão da segurança computacional como um problema administrativo, não apenas tecnológico, lançando as bases para uma abordagem mais abrangente.

A perspectiva gerencial é amplamente desenvolvida por autores como (Whitman; Mattord, 2016), que detalham os aspectos de planejamento, desenvolvimento de políticas e gestão de riscos sob uma ótica organizacional. Eles enfatizam que a segurança da informação é um processo contínuo que exige o envolvimento da alta direção e a integração com os objetivos do negócio.

Corroborando essa visão, (Tipton; Nozaki, 2010) oferecem um panorama abrangente das diversas facetas da gestão da SI, desde a formulação de políticas até a resposta a incidentes, reforçando a ideia de que a SI eficaz depende de uma gestão sólida. A robustez técnica, abordada em profundidade por (Anderson, 2020), embora focada em design e implementação de sistemas seguros, fornece o embasamento para entender os porquês dos controles e as ameaças que as políticas visam mitigar.

Abordando o contexto das Instituições de Ensino Superior (IES) o trabalho de (Alraja *et al.,* 2023) apresenta a necessidade das IES estabelecerem e manterem uma PSI sólida é corroborada de um modelo unificado de conformidade de politicas de segurança da informação. Os autores argumentam que a adesão dos colaboradores às diretrizes de segurança em um ambiente globalizado depende de uma integração multifacetada entre a percepção de risco e o suporte organizacional.

De forma tangível, o problema é agravado pelas novas dinâmicas tecnológicas do das instituições de ensino. Conforme (Baleid; Abdullah, 2026), a vulnerabilidade das IES é amplificada pela transição a ambientes de nuvem e pela natureza aberta da cultura acadêmica. Os autores destacam que, embora o armazenamento de dados sensíveis em nuvem seja uma realidade crescente, a responsabilidade compartilhada frequentemente resulta em falhas de configuração. O trabalho apresenta ainda a necessidade de promover uma conscientização eficaz de cibersegurança para capacitar os membros dos círculos acadêmicos e adotar práticas de segurança mais ativas, mitigando assim possíveis ataques.

A complexidade da gestão de cibersegurança em IES pelo mundo, é corroborada pela revisão sistemática de (Afolalu; Tsoeu, 2025), que identifica a natureza aberta e descentralizada das instituições como um fator crítico de vulnerabilidade perante ameaças. Os autores ressaltam que, embora existam progressos na implementação de medidas técnicas, muitas instituições ainda carecem de planos abrangentes que integrem soluções a uma cultura robusta de conscientização. Essa análise reforça a necessidade de alinhar a governança e as políticas institucionais para mitigar ameaças.

No Brasil, essa necessidade de mitigação transcende e assume um caráter de obrigatoriedade legal, e a segurança da informação tornou-se uma agenda estratégica e obrigatória para o setor público brasileiro, regulamentada por uma vasta gama de dispositivos legais, como decretos e instruções normativas. A observância dessas diretrizes é compulsória para os órgãos federais, que são adicionalmente fiscalizados por importantes órgãos de controle, como a Controladoria Geral da União (CGU) e o Tribunal de Contas da União (TCU) (Souza, 2017).

Além do arcabouço legal, a segurança da informação é definida por normas práticas, que oferecem modelos de referência para a implementação de sistemas de gestão robustos e a adoção de controles eficazes. Esses padrões são cruciais para que as organizações, incluindo universidades federais, alcancem um nível de segurança reconhecido.

O Decreto n. 12.572, de 4 de agosto de 2025, que institui a Política Nacional de Segurança da Informação (PNSI), estabelece as diretrizes estratégicas para a segurança da informação em toda a administração pública federal, visando proteger ativos de informação críticos e promover uma cultura de segurança. A PNSI é, portanto, a diretriz de alto nível que as universidades federais devem seguir ao formular suas próprias políticas de segurança.

Para operacionalizar a PNSI, a Instrução Normativa GSI/PR Nº 1, de 2020 (IN 01), emitida pelo Gabinete de Segurança Institucional da Presidência da República, detalha os procedimentos e requisitos para a gestão da segurança da informação e comunicações na administração pública federal. Esta Instrução Normativa define a estrutura de governança, os papéis e responsabilidades e os processos que as instituições devem adotar para garantir a segurança de suas informações.

Em seguida, a Instrução Normativa GSI/PR Nº 1/2020 detalha ainda que a aplicação da PNSI, institui a Estrutura de Gestão da Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Essa instrução normativa é fundamental, pois estabelece a necessidade de um Sistema de Gestão da Segurança da Informação e a obrigatoriedade de

criação de Comitês de Segurança da Informação e Privacidade.

Nesse sentido, Norma Complementar 05/IN/GSI/PR (Brasil, 2009) atua como uma diretriz específica e operacional, que se desdobra do arcabouço legal e dedica exclusivamente à gestão de incidentes de segurança cibernética, fornecendo um modelo detalhado para a constituição e operação das ETIRs. A NC 05, portanto, é a normativa que traduz os princípios mais amplos da PNSI e da IN 01 em ações concretas e padronizadas, sendo o principal referencial para a análise deste estudo.

A NC 05, propõe então a criação das ETIRs que tem como objetivo disciplinar e fortalecer a segurança da informação nos órgãos da Administração Pública Federal. O documento orienta que, para instituir uma ETIR, é necessário definir sua missão, estabelecer o público-alvo, escolher o modelo de implementação mais adequado, estruturar a equipe com profissionais capacitados, determinar o nível de autonomia e formalizar os serviços a serem prestados. Dessa forma, garante-se clareza nas responsabilidades e eficiência na prevenção e resposta a incidentes de segurança.

A lacuna estrutural na gestão de incidentes nas IES brasileiras é evidenciada no estudo de (Filho; Afonseca, 2025) ao analisarem os modelos de resposta a incidentes de universidades federais, os autores constataram que, embora existam processos documentados, estes frequentemente falham em atender de forma integral às exigências da família ISO/IEC 27000 e da legislação nacional, como a LGPD. O estudo aponta que os processos acadêmicos tendem a focar em soluções técnicas isoladas, negligenciando a integração com instâncias administrativas e a previsão de canais formais de comunicação com autoridades reguladoras, como a Autoridade Nacional de Proteção de Dados (ANPD), em casos de vazamentos.

Essa constatação empírica na literatura nacional dialoga diretamente com a desconformidade generalizada frente a norma NC 05/IN/GSI/PR, reforçando o argumento de que a mera elaboração e publicação de uma PSI não garante a maturidade operacional e a eficácia das ETIRs.

3 PROCEDIMENTOS METODOLÓGICOS

O presente estudo caracteriza-se como uma pesquisa de abordagem qualitativa, com natureza exploratória, centrada na análise de documentos, onde a metodologia foi selecionada por sua adequação ao objetivo proposto.

De acordo com (RIOS *et al.*, 2017) para alcançar os objetivos institucionais sejam com

integridade, é indispensável a adoção de uma Politica de Segurança da Informação e Comunicação (PoSIC) robusta. Um documento que, estrutura os controles necessários para proteger a informação por meio de um ciclo contínuo de implementação, monitoramento e fiscalização, garantindo assim a conformidade e a resiliência do processo.

Portanto, dada a necessidade de verificar tais controles, o objeto de estudo desta pesquisa consiste na análise dos documentos das Políticas de Segurança da Informação(PSI) ou Políticas de Segurança da Informação e Comunicações (PoSIC) das universidades federais brasileiras onde, essas políticas têm a "finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação no País"(Brasil, 2025). Foram analisados 57 documentos, sendo este o número de universidades que possuem tais políticas formalizadas em documentos acessíveis para consulta pública, entretanto, das 69 universidades federais, 12 delas não possuem ou não estavam disponíveis para acesso.

Apoiado na análise anterior e sob o entendimento da (ABNT, 2020) a gestão de incidentes dentro do ambiente de Gestão da Tecnologia da Informação é um procedimento que tem como objetivo a restauração de serviços com celeridade e atendendo aos níveis de serviço acordados. Nesse sentido, torna-se imperativo que as IES estabeleçam equipes formais de gestão de incidentes, capazes de operacionalizar tais diretrizes e garantir a resiliência dos ativos críticos de informação.

Dada a relevância estratégica dessas equipes, faz-se necessário investigar como as universidades brasileiras têm formalizado tais estruturas em seus documentos oficiais, garantindo que o respaldo normativo sustente sua aplicação efetiva.

Este trabalho portanto, baseia na estratégia metodológica utilizada por (Souza, 2017), que formula questões de pesquisa a partir de conceitos teóricos sólidos, logo propõe-se a seguinte pergunta de pesquisa: Quais elementos da estrutura de gestão de incidentes em segurança da informação de uma universidade federal, conforme estabelecida em sua política de segurança da informação, estão alinhados às diretrizes da Norma Complementar 05/IN/GSI/PR?

Para alcançar este objetivo, foi realizada uma análise documental qualitativa de 57 PSI das 69 universidades federais brasileiras. O plano de ação consistiu em avaliar a presença e o detalhamento de seis pontos-chave, conforme orientações do documento de constituição da ETIR, da Norma Complementar 05/IN/GSI/PR. Estes pontos são: Missão, Comunidade ou Público-Alvo, Modelo de Implementação, Estrutura Organizacional, Autonomia da ETIR e Serviços (Brasil, 2009).

ISSN: 2594-8083

Com relação a pesquisa, foi conduzida exclusivamente pelo método documental, o que implicou a coleta e análise sistemática de informações contidas nos documentos selecionados. O universo da pesquisa delimitou-se aos documentos acessíveis publicamente, caracterizando uma pesquisa de cunho exploratório no que tange à compreensão do estado da arte e das práticas adotadas.

A escolha pela pesquisa documental se justifica pela natureza do objeto de estudo, que reside em normativas e diretrizes formais, e pela intenção de investigar como essas políticas são concebidas e formalizadas pelas instituições. A pesquisa exploratória, por sua vez, busca familiarizar o pesquisador com um problema, tornando-o mais claro e permitindo a formulação de hipóteses. Seu principal objetivo é aprimorar ideias e obter novas percepções sobre o tema e para isso, o planejamento é flexível e pode incluir levantamento bibliográfico (Gil, 2002).

Para análise de cada PSI orientou-se por meio de uma verificação sistemática da presença e do detalhamento dos seguintes pontos-chave descritos em (Brasil, 2009):

• Missão: Avalia a clareza e o propósito declarado da ETIR dentro da universidade.

• Comunidade ou Público-Alvo: Identifica a abrangência de atuação da equipe, definindo quem são os usuários e sistemas que estão sob sua proteção.

• Modelo de Implementação: Descreve a forma como a ETIR foi estabelecida e como opera, seja de maneira centralizada ou distribuída.

• Estrutura Organizacional: Analisa a hierarquia, as funções e as responsabilidades dos membros da equipe.

• Autonomia da ETIR: Verifica o nível de autoridade e a capacidade de decisão da equipe para atuar em incidentes.

• Serviços: Detalha os tipos de serviços oferecidos pela equipe, como resposta a incidentes, análise forense ou monitoramento de segurança.

As PSIs foram retiradas dos sites das universidades públicas federal onde a busca se deu a partir do acesso ao site de cada uma delas, e após isso, foi procedida a busca no mecanismo voltado para esse fim no website, utilizando as palavras-chave “Política de Segurança da Informação” e/ou “Política” (nas situações nas quais a primeira palavra-chave não foi localizada).

A busca foi orientada pelo entendimento de que esses documentos, por sua natureza jurídica, são geralmente emitidos como Resoluções pelo Conselho Universitário de cada instituição de ensino. Portanto, a estratégia de coleta incluiu a busca por essa instância superior, o que se mostrou crucial para assegurar a localização e a validade dos documentos oficiais.

ISSN: 2594-8083

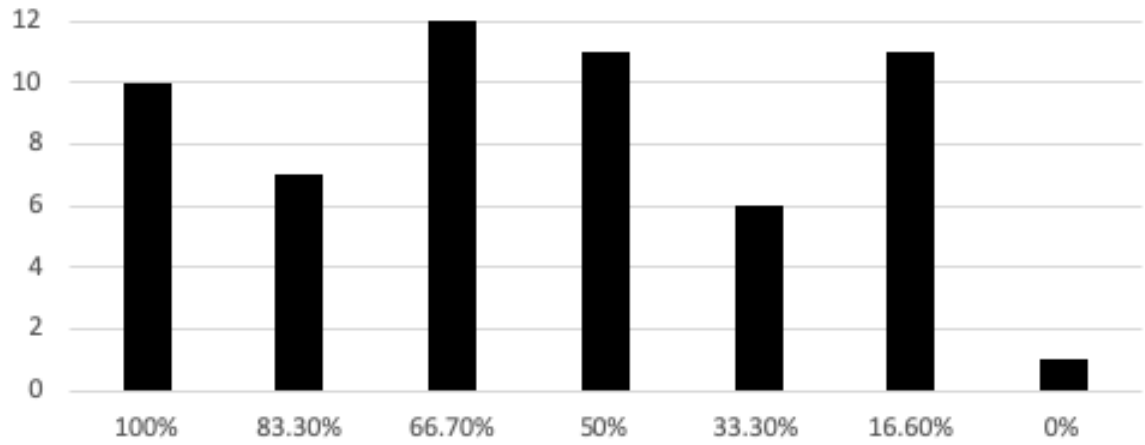
Conforme o Apêndice B deste trabalho, foram identificados e analisados documentos referentes à PSI em 57 dos sites pesquisados. Um pequeno grupo, descrito no Apêndice A, correspondente a 12 universidades, não teve seus dados analisados, dada a inacessibilidade, inexistência de documentos a elas referentes ou documentos incompletos. Os hiperlinks para acesso as PSIs das universidades federais estão disponíveis no Apêndice C, cujas buscas foram realizadas no período de junho de 2025 a setembro de 2025, sendo o dia 11 de setembro de 2025 a data do último acesso a todos os links.

Uma vez reunido o grupo a ser analisado, procedeu-se a análise dos documentos para que pudesse ser verificada a existência ou não dos elementos previamente selecionados para análise, cujos resultados são apresentados na seção a seguir.

4 DISCUSSÃO E ANÁLISE DOS DADOS

Os critérios selecionados a partir da Norma Complementar 05 (Brasil, 2009), que estabelece diretrizes para a criação de ETIR, foram coletados nas instituições públicas federais e são apresentados no Apêndice B deste trabalho. Os resultados dos elementos especificados nas PSI das 57 universidades federais analisadas são apresentados na figura 1.

Figura 1: Percentual dos elementos previstos na NC 05 nas PSI das universidades federais.



Fonte: Elaborado pelos autores.

As PSI analisadas revelaram que apenas um grupo de 10 universidades contemplou no documento todos os seis elementos previstos na NC 05 (comunidade ou público-alvo; missão; serviços; autonomia da ETIR; modelo de implementação; estrutura organizacional). Ou seja, 100% das informações previstas constavam no documento.

Por sua vez, sete universidades federais fizeram constar no documento um total de 83,3% do conteúdo previsto na NC 05 (cinco das seis dimensões). Outras 12 universidades fizeram constar quatro dos seis elementos (66,7%), 11 delas fizeram constar apenas a metade dos seis elementos (50%), seis universidades fizeram constar apenas dois (33,3%) e 11 universidades fizeram constar apenas um dos seis elementos que deveriam ser especificados (16,6% do total).

Na figura 2, são apresentados os elementos que foram especificados nas PSI, da maior para a menor frequência no grupo analisado.

Figura 2: Elementos especificados nas PSI das universidades federais.

Fonte: Elaborado pelos autores.

A partir das informações apresentadas na figura 2, duas constatações parecem ganhar contorno: a primeira é que a maior parte das universidades analisadas especificam claramente em suas políticas de segurança da informação as definições de comunidade e público-alvo, a missão das ETIR, seus serviços e as condições de sua autonomia. A segunda constatação é que as PSIs parecem não especificar em igual proporção o modelo de implementação das ETIR e a sua localização na estrutura organizacional.

A análise dos resultados sugere que a adesão das universidades federais pode ser, em muitos casos, superficial e não atender à especificidade e à clareza que a normativa exige. Embora a maior parte das universidades abordem os pontos orientados pela NC 05, as informações contidas em seus documentos são genéricas e carecem dos detalhes necessários

para uma implementação eficaz. Portanto, para que as universidades federais atinjam a maturidade esperada na gestão de segurança da informação, é fundamental que elas não se contentem com a simples formalização de uma PSI (RIOS *et al.*, 2017).

Tal simplicidade é um problema recorrente, observando o ponto "Modelo de Implementação", por exemplo, a NC 05 não apenas solicita que a universidade defina um modelo para sua Equipe de Tratamento e Resposta a Incidentes (ETIR), mas também pede que ela aponte a designação formal dos membros ou funções que compõem a estrutura operacional da ETIR. A análise revelou que, em muitos casos, as políticas apenas afirmam a existência de uma equipe, sem a devida especificação dos que a compõem, o que diverge com as exigências da norma.

Sob uma perspectiva similar, (Quintino *et al*, 2020) argumentam que a PoSIC deve atuar como o alicerce da segurança organizacional, normatizando o acesso e o manuseio dos dados. É essencial que tal documento estabeleça não apenas diretrizes genéricas, mas a governança específica dos controles de proteção, garantindo que a instituição alcance seus objetivos com a devida segurança e integridade.

Outro ponto crítico é que, embora muitas políticas listem serviços como análise e resposta a incidentes, poucas detalham a forma como esses serviços são executados. A norma exige, por exemplo, que a equipe mantenha articulação com o CTIR Gov e elabore planos de contingência, porém, a maioria das universidades não especifica esses procedimentos de forma clara, o que pode levar a incertezas sobre as responsabilidades em caso de incidentes graves.

Como detalha a norma (ABNT, 2020), a maioria das PSI não especifica detalhes, logo essa falta de clareza sobre quem compõe a equipe e quais são as suas qualificações contraria a especificidade exigida pela normativa o que pode impactar diretamente em garantir a resiliência dos ativos críticos de informação.

Ainda que a criação formal de uma ETIR é um passo importante e alinhado com a NC 05, a discussão sobre a implementação prática das políticas revela que a simples menção de uma equipe não garante a eficácia da gestão de incidentes. A ausência de procedimentos detalhados e específicos são indicativos de que a gestão de incidentes ainda está em um estágio de amadurecimento nas universidades federais. Para que as ETIRs sejam verdadeiramente eficientes, é crucial que as universidades revisem suas políticas, tornando-as mais específicas e operacionais, conforme a essência e o detalhamento propostos pela NC 05.

ISSN: 2594-8083

5 CONCLUSÕES

A análise das Políticas de Segurança da Informação das universidades federais brasileiras, à luz da Norma Complementar 05/IN/GSI/PR, revelou um cenário em que a adesão formal não se traduziu, necessariamente, em uma implementação robusta e detalhada. O estudo demonstra que, embora a maioria das instituições tenha formalizado a criação de equipes de resposta a incidentes (ETIR), a falta de clareza e de especificidade em pontos importantes pode comprometer a eficácia dessas estruturas.

É preciso então ir além, detalhando as atribuições de forma clara e objetiva, conferindo a autonomia necessária às equipes e garantindo que a implementação prática reflita a seriedade e a especificidade exigidas pela Norma Complementar 05/IN/GSI/PR.

Contudo, é importante ressaltar as limitações deste estudo. Das 69 universidades federais analisadas, 12 não tiveram suas Políticas de Segurança da Informação (PSI) localizadas, e, portanto, não foram incluídas na pesquisa. No entanto, a dificuldade em encontrar esses documentos não significa, necessariamente, que eles não existam, isso mostra também que a dificuldade de acesso é uma questão relevante para documentos de interesse público.

Sob o outro enfoque, para as universidades que, de fato, não possuem uma PSI formalmente publicada, foi possível verificar, por meio de notícias em portais institucionais, que já existem iniciativas e esforços para a elaboração desses documentos. Esse fato reforça a relevância da pauta e sugere um movimento de conscientização e adequação às normativas de segurança da informação no setor público.

Este trabalho contribui para o debate acadêmico ao avaliar a conformidade das políticas de segurança das universidades federais brasileiras com normativas do setor público. Embora o estudo tenha se restringido à análise documental, a análise enfrentou obstáculos como a falta de acesso a determinadas PSIs e a escassez de detalhamento técnico em outros documentos analisados, essa contatação levanta questões importantes sobre a transparência e a eficácia da gestão de incidentes de segurança nas instituições.

É sugerido que pesquisas futuras possam complementar este estudo com entrevistas, questionários ou a análise de dados empíricos diretos para uma compreensão mais aprofundada da maturidade em segurança da informação nas universidades. Isso permitirá não apenas verificar a existência das PSI, mas também a sua efetiva aplicação na prática, garantindo a proteção dos ativos e a continuidade das operações em um ambiente digital cada vez mais

complexo.

AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) - Código de Financiamento 001 e da Fundação Universidade Federal de Mato Grosso do Sul (UFMS).

REFERÊNCIAS

AFOLALU, Oladele; TSOEU, Mohohlo Samuel. **Cybersecurity in Higher Education Institutions: A Systematic Review of Emerging Trends, Challenges and Solutions. Information**, [S. l.], v. 15, n. 1, p. 575, jan. 2025. DOI https://doi.org/10.3390/fi17120575. Disponível em: https://www.mdpi.com/1999-5903/17/12/575. Acesso em: 3 abr. 2026.

ALRAJA, Mansour Naser; BUTT, Usman Javed; ABBOD, Maysam. **Information security policies compliance in a global setting: An employee's perspective.** Computers & Security, [s. l.], v. 129, p. 103208, 2023. DOI https://doi.org/10.1016/j.cose.2023.103208. Acesso em: 29 mar. 2026.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 20000-1: Tecnologia da informação — Gestão de serviço — Parte 1: Requisitos do sistema de gestão de serviço. Rio de Janeiro: ABNT, 2020.

ANDERSON, R. J. **Security Engineering**. 2. ed. Indianapolis: Wiley, 2008.

BALEID, Hanan Mahmood; ABDULLAH, Mohammed Fadhl. Cybersecurity in Higher Education: **A systematic review of threats, challenges, and mitigation strategies**. Journal of Science and Technology, [S. l.], v. 28, n. 1, p. 1-19, 2023. DOI https://doi.org/10.53392/jst.v28i1.3563. Disponível em: https://journals.ust.edu/index.php/JST/article/view/3563 .

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União: seção 1, Brasília, DF, 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 22 jun. 2025.

BRASIL. Decreto n. 12.572, de 4 de agosto de 2025. **Institui a Política Nacional de Segurança da Informação**. Diário Oficial da União: seção 1, Brasília, DF, 5 ago. 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2025/Decreto/D12572.htm#art12. Acesso em: 2 set. 2025.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Instrução Normativa GSI/PR Nº 1, de 27 de maio de 2020**. Brasília, DF: GSI/PR, 2020. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-

cibernetica/legislacao/copy_of_IN01_consolidada.pdf. Acesso em: 22 jun. 2025.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009. Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR.** Brasília, 2009. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/legislacao/NC05.pdf. Acesso em: 4 set. 2025.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental.** [S. l.]: Doneda, [s.d.]. Disponível em: https://doneda.net/a-protecao-dos-dados-pessoais-como-um-direito-fundamental/. Acesso em: 29 mar. 2026.

FONTES, Edison Luiz Gonçalves. **Segurança da informação: o usuário faz a diferença**. Rio de Janeiro: Brasport, 2010.

FILHO, Marcelo dos Santos Silva; AFONSECA, Ulisses Rodrigues. **Um modelo integrado para a gestão de incidentes em segurança da informação**. Revista Foco, [s. l.], v. 18, n. 4, p. e8378, 2025. DOI: https://doi.org/10.54751/revistafoco.v18n4-154. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/8378/5930. Acesso em: 3 abr. 2026.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002. Disponível em: <https://files.cercomp.ufg.br/weby/up/150/o/Anexo_C1_como_elaborar_projeto_de_pesquisa_-_antonio_carlos_gil.pdf>. Acesso em: 8 set. 2025.

GOMIDE, Alexandre de Ávila; PIRES, Roberto Rocha C. (org.). **Capacidades estatais e democracia: a abordagem dos arranjos institucionais para análise de políticas públicas.** Brasília: Ipea, 2014. Disponível em: https://portalantigo.ipea.gov.br/agencia/images/stories/PDFs/livros/capacidades_estatais_e_democracia_web.pdf. Acesso em: 29 mar. 2026.

NIST. NIST Special Publication 800-53, Revision 4. **Security and Privacy Controls for Federal Information Systems and Organizations**. Gaithersburg, MD: National Institute of Standards and Technology, 2013.

PARKER, D. B. **Computer Security Management. Reston**, VA: Reston Publishing Company, 1981.

QUINTINO, Eliana Maria et al. **Um estudo sobre gestão de segurança da informação em instituições do ensino superior públicas.** Educação & Linguagem, [S. l.], ano 7, n. Especial 1, p. 23-30, fev. 2020. Disponível em: https://www.fvj.br/revista/wp-content/uploads/2020/02/3_REdLi_2020.ESPECIAL_1.pdf. Acesso em: 29 mar. 2026.

RIOS, Olga Klyssma Lira; TEIXEIRA FILHO, José Gilberto de Andrade; RIOS, Victor Paulo Silva. **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, Florianópolis, v. 7, n. 2, p. 49-65, abr./jun. 2017. Disponível em: https://navus.sc.senac.br/navus/article/view/482/pdf. Acesso em: 29 mar. 2026.

SCHNEIER, B. **Data and Goliath: The Hidden Battles to Collect Your Data and Control**

Your World. New York: W. W. Norton & Company, 2015.

SOUZA, J. G. S. **Análise de tratamento da segurança da informação na gestão de riscos da governança de tecnologia da informação de uma instituição de ensino público federal**. 2017. Dissertação (Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos) – Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2017. Disponível em: <http://www.pos.cps.sp.gov.br/files/dissertacoes/file/73/b55e568c03373ffe558008fa6e0ad2fa.pdf>. Acesso em: 17 jan. 2021.

SPAFFORD, E. H. **Are computer experts professional? Communications of the ACM**, v. 35, n. 6, p. 28-35, June 1992.

TIPTON, H. F.; NOZAKI, M. K. (Ed.). **Information Security Management Handbook**. 6. ed. Boca Raton, FL: CRC Press, 2010.

WHITMAN, Michael E.; MATTORD, Herbert J. **Management of information security.** 5. ed. Boston: Cengage Learning, 2017.

ISSN: 2594-8083

APÊNDICE A: Documentos ausentes ou indisponíveis

UNIVASF	Não possui PSI
UFJ	Não possui PSI
UFR	Não possui PSI
UFJF	Não possui PSI
UFRA	Não possui PSI
UFAPE	Não possui PSI
UNIR	Não possui PSI
UFTM	Não possui PSI
UFVJM	Não possui PSI mas possui um documento somente para a ETIR
UFSJ	Não possui PSI mas possui um documento somente para a ETIR
UNIFESP	Não possui PSI mas possui um documento somente para a ETIR
UFLA	Sem acesso

Fonte: Elaborado pelos autores.

ISSN: 2594-8083

APÊNDICE B: Análise dos documentos disponíveis

Universidade	Estrutura Organizacional	Modelo de Implementação	Autonomia da ETIR	Serviços	Missão	Comunidade ou Público-Alvo
UFMG	Sim	Sim	Sim	Sim	Sim	Sim
UFMS	Sim	Sim	Sim	Sim	Sim	Sim
UFMT	Sim	Sim	Sim	Sim	Sim	Sim
UFRGS	Sim	Sim	Sim	Sim	Sim	Sim
UFCSPA	Sim	Sim	Sim	Sim	Sim	Sim
UFS	Sim	Sim	Sim	Sim	Sim	Sim
UFSM	Sim	Sim	Sim	Sim	Sim	Sim
UFU	Sim	Sim	Sim	Sim	Sim	Sim
UNB	Sim	Sim	Sim	Sim	Sim	Sim
UTFPR	Sim	Sim	Sim	Sim	Sim	Sim
UFGD	Não	Sim	Sim	Sim	Sim	Sim
UFMA	Não	Sim	Sim	Sim	Sim	Sim
UFRR	Não	Sim	Sim	Sim	Sim	Sim
UNIFESSPA	Não	Sim	Sim	Sim	Sim	Sim
UFABC	Sim	Não	Sim	Sim	Sim	Sim
UFCA	Sim	Não	Sim	Sim	Sim	Sim
UFPE	Sim	Não	Sim	Sim	Sim	Sim
FURG	Não	Não	Sim	Sim	Sim	Sim
UFAM	Não	Não	Sim	Sim	Sim	Sim
UFBA	Não	Não	Sim	Sim	Sim	Sim
UFCG	Não	Não	Sim	Sim	Sim	Sim
UFFS	Não	Não	Sim	Sim	Sim	Sim
UFG	Não	Não	Sim	Sim	Sim	Sim
UFNT	Não	Não	Sim	Sim	Sim	Sim
UFOP	Não	Não	Sim	Sim	Sim	Sim
UFPel	Não	Não	Sim	Sim	Sim	Sim
UNIFEI	Não	Não	Sim	Sim	Sim	Sim
UNILA	Não	Não	Sim	Sim	Sim	Sim

ISSN: 2594-8083

UFRB	Não	Sim	Não	Sim	Sim	Sim
UFAL	Não	Não	Não	Sim	Sim	Sim
UFDPAR	Não	Não	Não	Sim	Sim	Sim
UFF	Não	Não	Não	Sim	Sim	Sim
UFOB	Não	Não	Não	Sim	Sim	Sim
UFRJ	Não	Não	Não	Sim	Sim	Sim
UFRN	Não	Não	Não	Sim	Sim	Sim
UNIPAMPA	Não	Não	Não	Sim	Sim	Sim
UFSCar	Não	Não	Sim	Não	Sim	Sim
UFPI	Não	Não	Não	Não	Sim	Sim
UFPR	Não	Não	Não	Não	Sim	Sim
UFRPE	Não	Não	Não	Não	Sim	Sim
UNIFAP	Não	Não	Não	Não	Sim	Sim
UFC	Não	Não	Sim	Sim	Não	Sim
UFOPA	Não	Não	Sim	Sim	Não	Sim
UFAC	Não	Não	Não	Não	Não	Sim
UFERSA	Não	Não	Não	Não	Não	Sim
UFES	Não	Não	Não	Não	Não	Sim
UFPA	Não	Não	Não	Não	Não	Sim
UFPB	Não	Não	Não	Não	Não	Sim
UFRRJ	Não	Não	Não	Não	Não	Sim
UFSC	Não	Não	Não	Não	Não	Sim
UFT	Não	Não	Não	Não	Não	Sim
UNIFAL	Não	Não	Não	Não	Não	Sim
UNILAB	Não	Não	Não	Não	Não	Sim
UFCAT	Não	Não	Sim	Sim	Sim	Não
UFSB	Não	Não	Não	Sim	Sim	Não
UFV	Não	Não	Não	Sim	Sim	Não
UNIRIO	Não	Não	Não	Não	Não	Não

Fonte: Elaborado pelos autores.

ISSN: 2594-8083

APÊNDICE C: Análise dos documentos disponíveis

Os hiperlinks estão disponíveis na parte azul sublinhada.
(Último acesso aos links: 11 de setembro de 2025)

Nome das Universidades Federais
Universidade de Brasília (UnB)
Universidade do Espírito Santo (UFES)
Universidade Federal da Fronteira Sul (UFFS)
Universidade Federal da Grande Dourados (UFGD)
Universidade Federal da Integração Latino-Americana (Unila)
Universidade Federal da Lusofonia Afro-Brasileira (Unilab)
Universidade Federal da Paraíba (UFPB)
Universidade Federal de Alagoas (UFAL)
Universidade Federal de Alfenas (Unifal-MG)
Universidade Federal de Campina Grande (UFCG)
Universidade Federal de Catalão (UFCat)
Universidade Federal de Ciências da Saúde de Porto Alegre (UFCSPA)
Universidade Federal de Goiás (UFG)
Universidade Federal de Itajubá (Unifei)
Universidade Federal de Jataí (UFJ)
Universidade Federal de Juiz de Fora (UFJF)
Universidade Federal de Lavras (Ufla)
Universidade Federal de Minas Gerais (UFMG)
Universidade Federal de Ouro Preto (Ufop)
Universidade Federal de Pelotas (UFPel)
Universidade Federal de Pernambuco (UFPE)
Universidade Federal de Rondônia (UNIR)
Universidade Federal de Rondonópolis (UFR)
Universidade Federal de Roraima (UFRR)
Universidade Federal de Santa Catarina (UFSC)
Universidade Federal de Santa Maria (UFSM)
Universidade Federal de São Carlos (UFSCar)
Universidade Federal de São João del-Rei (UFSJ)

ISSN: 2594-8083

Universidade Federal de São Paulo (Unifesp)

Universidade Federal de Sergipe (UFS)

Universidade Federal de Uberlândia (UFU)

Universidade Federal de Viçosa (UFV)

Universidade Federal do ABC (UFABC)

Universidade Federal do Acre (UFAC)

Universidade Federal do Agreste de Pernambuco (Ufape)

Universidade Federal do Amapá (UNIFAP)

Universidade Federal do Amazonas (UFAM)

Universidade Federal do Bahia (UFBA)

Universidade Federal do Cariri (UFCA)

Universidade Federal do Ceará (UFC)

Universidade Federal do Delta do Parnaíba (UFDPar)

Universidade Federal do Estado do Rio de Janeiro (UNIRIO)

Universidade Federal do Maranhão (UFMA)

Universidade Federal do Mato Grosso (UFMT)

Universidade Federal do Mato Grosso do Sul (UFMS)

Universidade Federal do Norte do Tocantins (UFNT)

Universidade Federal do Oeste da Bahia (UFOB)

Universidade Federal do Oeste do Pará (Ufopa)

Universidade Federal do Pampa (Unipampa)

Universidade Federal do Pará (UFPA)

Universidade Federal do Paraná (UFPR)

Universidade Federal do Piauí (UFPI)

Universidade Federal do Recôncavo da Bahia (UFRB)

Universidade Federal do Rio de Janeiro (UFRJ)

Universidade Federal do Rio Grande (Furg)

Universidade Federal do Rio Grande do Norte (UFRN)

Universidade Federal do Rio Grande do Sul (UFRGS)

Universidade Federal do Sul da Bahia (UFSB)

Universidade Federal do Tocantins (UFT)

Universidade Federal do Triângulo Mineiro (UFTM)

ISSN: 2594-8083

Universidade Federal do Vale do São Francisco (Univasf)

Universidade Federal dos Vales do Jequitinhonha e Mucuri (UFVJM)

Universidade Federal Fluminense (UFF)

Universidade Federal Rural da Amazônia (Ufra)

Universidade Federal Rural de Pernambuco (UFRPE)

Universidade Federal Rural do Rio de Janeiro (UFRRJ)

Universidade Federal Rural do Semi-Árido (Ufersa)

Universidade Federal Sul e Sudeste do Pará (Unifesspa)

Universidade Tecnológica Federal do Paraná (UTFPR)

Fonte: Elaborado pelos autores.