Integração de Requisitos da LGPD em Processos de Resposta a Incidentes de Segurança Cibernética: Um Modelo de Processo para a ETIR da Universidade Federal de Santa Maria

Fabio André Barcelos
Universidade de Brasília (UnB)
Brasília, Distrito Federal, Brasil
fabio.barcelos@ufsm.br

Edna Dias Canedo
Universidade de Brasília (UnB)
Brasília, Distrito Federal, Brasil
ednacanedo@unb.br

Abstract

Contexto: A incidência de ataques cibernéticos e a vigência da Lei Geral de Proteção de Dados Pessoais (LGPD) exigem das instituições públicas brasileiras a integração entre a resposta técnica a incidentes de segurança e as obrigações legais de privacidade. Contudo, evidências empíricas, em especial o Acórdão TCU nº 1.372/2025, revelam que 64,6% das organizações federais não possuem processos padronizados para a comunicação de incidentes à ANPD e aos titulares. Esse cenário indica que o maior desafio atual não é a ausência de normas, mas a deficiência de mecanismos capazes de traduzi-las em fluxos operacionais concretos. **Objetivo:** Propor um modelo de processo em notação BPMN 2.0 que integre os requisitos da LGPD e da Resolução CD/ANPD nº 15/2024 ao ciclo de resposta a incidentes da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos da Universidade Federal de Santa Maria (ETIR/UFSM). **Método:** Por meio da *Design Science Research* (DSR) combinada com Estudo de Caso, o modelo foi desenvolvido a partir de análise documental sistemática dos instrumentos normativos aplicáveis e da literatura sobre gestão de incidentes. A validação qualitativa ocorreu mediante entrevistas semiestruturadas com três especialistas da UFSM. **Resultados:** A validação atestou a adequação normativa do artefato e motivou adaptações ligadas à realidade institucional, destacando-se ajustes nos fluxos de notificação à ANPD, definições de autonomia na comunicação aos titulares e a exigência de abertura de processo administrativo interno. O modelo final estrutura as cinco fases do ciclo de resposta, segregando as atribuições das equipes técnica, jurídica e de gestão. **Conclusões:** O modelo finaliza-se como um artefato TO-BE normativamente aderente e validado de forma empírica, aplicável ao contexto da UFSM e de outras instituições públicas de ensino superior. O estudo demonstra que a modelagem em BPMN embasada em análise documental sistemática atende ao *implementation roadmap gap* apontado na literatura, pois conecta obrigações legais a atividades e decisões auditáveis. Na prática, o artefato atua como instrumento para a governança, a capacitação e a automação da resposta a incidentes nas ETIRs federais.

Palavras-chave: Segurança da informação. Gestão de incidentes. LGPD. BPMN. ETIR. Privacidade.

Keywords

Segurança da Informação; Gestão de Incidentes; LGPD; PPSI 2.0; ETIR; BPMN; Setor Público; resposta a incidentes; proteção de dados; Privacidade de Dados; universidades federais.

1 Introdução

A dependência das organizações em relação às tecnologias digitais tem aumentado significativamente nos últimos anos. Esse movimento traz ganhos evidentes em eficiência e inovação, mas também aumenta a exposição a riscos cibernéticos. Incidentes como vazamentos de dados, ataques de ransomware e exploração de vulnerabilidades têm ocorrido com maior frequência e, em muitos casos, com impactos relevantes [13], [11]. No setor público, essa preocupação é ainda maior pelo volume e sensibilidade das informações tratadas, que envolvem dados de cidadãos [21], [14]. Diante desse cenário, a gestão de incidentes de segurança da informação (GIC) tornou-se uma atividade primordial nas organizações.

Frameworks e normas internacionais, como a ISO/IEC 27035 [12] e o NIST SP 800-61 [15], oferecem uma base estruturada para lidar com esse tipo de situação ao organizar a resposta em etapas bem definidas. No entanto, na prática, é comum ver a aplicação desses modelos com foco predominante em aspectos técnicos, o que nem sempre inclui outras dimensões relevantes, especialmente aquelas relacionadas à proteção de dados pessoais [27], [25]. No contexto brasileiro, a Lei Geral de Proteção de Dados (LGPD)[5] trouxe mudanças importantes ao estabelecer obrigações específicas sobre o tratamento de dados e, em particular, sobre a resposta a incidentes de segurança. A necessidade de comunicar ocorrências à Agência Nacional de Proteção de Dados (ANPD)[2] e, em certos casos, aos próprios titulares transforma a resposta a incidentes em algo que envolve aspectos legais, organizacionais e estratégicos, além de ser apenas uma questão técnica. Isso requer uma articulação maior entre diferentes áreas, o que nem sempre acontece nas instituições de ensino.

No setor público federal, já existem iniciativas que buscam essa integração. O Programa de Privacidade e Segurança da Informação (PPSI), na versão mais recente (PPSI 2.0)[7], estruturado pela Portaria SGD/MGI nº 9.511/2025, o qual cria um framework integrado de controles de segurança da informação e privacidade. O foco está na conformidade legal, na maturidade organizacional e na implementação prática de medidas de proteção de dados. Esse framework organiza controles que vão da governança até aspectos operacionais, incluindo a gestão de incidentes e a proteção de dados durante todo o seu ciclo de vida. Além disso, o Plano de Gestão de Incidentes Cibernéticos (Plangic) estabelece diretrizes específicas para a coordenação da resposta a incidentes nos órgãos da administração pública federal. Esse plano define papéis, fluxos e responsabilidades entre as equipes envolvidas [9]. Contudo, a implementação efetiva desses processos ainda enfrenta desafios. Uma auditoria recente do Tribunal de Contas da União revelou que uma parte significativa

dos órgãos públicos federais ainda está nos estágios iniciais de maturidade em relação à conformidade com a LGPD. Os fluxos são pouco definidos e a integração entre equipes técnicas e áreas de conformidade é baixa [20].

Universidades federais podem ser consideradas um caso particularmente sensível nesse contexto. A Universidade Federal de Santa Maria (UFSM), com aproximadamente 30 mil estudantes e 5 mil servidores, trata cotidianamente um volume expressivo e diversificado de dados pessoais [24], distribuídos em sistemas acadêmicos, administrativos e de saúde. A Equipe de Tratamento e Resposta a Incidentes (ETIR) é a principal linha de atuação diante de ocorrências de segurança que afetam esses dados. Ela também é prevista como parte integrante da governança de segurança da informação dentro do PPSI 2.0 [7]. No entanto, a lacuna entre o que as normas estabelecem e o que é efetivamente realizado no dia a dia dessas equipes ainda não foi bem explorada na literatura, especialmente em relação a modelos operacionais aplicáveis a instituições públicas de ensino superior [27], [25].

Esse cenário destaca um problema que vai além da existência de normas ou diretrizes. A questão parece estar na forma como esses elementos são traduzidos em processos estruturados e aplicáveis. Em outras palavras, há conhecimento disponível, mas ele nem sempre se converte em fluxos operacionais que integrem, de maneira coordenada, a dimensão técnica da resposta e as obrigações legais da LGPD. É nesse contexto que este trabalho se insere. Assim, a pergunta de pesquisa é: como integrar, de maneira prática e estruturada, os requisitos da LGPD aos processos de gestão de incidentes de segurança da informação, considerando as particularidades do setor público? Para responder a essa pergunta, foi desenvolvido um modelo de processo em notação BPMN. Este modelo incorpora os requisitos da LGPD em todas as fases de resposta a incidentes. A estrutura adota o framework do PPSI 2.0 como referência para a gestão e governança.

As contribuições deste trabalho são de duas naturezas. Do ponto de vista teórico, busca-se identificar e descrever os requisitos da LGPD que devem ser incorporados a cada etapa do ciclo de resposta a incidentes em instituições públicas de ensino superior. Isso ajudará na construção de modelos operacionais que integrem conformidade legal e resposta técnica, uma dimensão que ainda carece de estudos específicos na literatura nacional [27], [25]. Do ponto de vista prático, é proposto um modelo processual que diminua a diferença entre o que é previsto pelas normas e o que é executado na prática, servindo como referência para a ETIR/UFSM e para outras instituições públicas que enfrentam desafios semelhantes.

2 Fundamentação Teórica e Trabalhos Relacionados

Nesta seção, apresentam-se os conceitos fundamentais que sustentam a integração entre a gestão de incidentes e a proteção de dados no setor público brasileiro.

2.1 Gestão de Incidentes de Segurança da Informação

A crescente sofisticação das ameaças cibernéticas e a ampliação da superfície de ataque nas organizações tornaram a gestão de incidentes de segurança da informação uma disciplina central dentro das estratégias de segurança corporativa e governamental. A gestão de incidentes transcende procedimentos reativos. Quando bem estruturada, é um processo contínuo de preparação e análise retrospectiva. Seu objetivo é reduzir impactos e aprimorar a capacidade de resposta organizacional[12], [15].

2.1.1 Conceito de Incidente de Segurança. A norma ISO/IEC 27035-1:2023 define incidente de segurança da informação como um ou mais eventos indesejados ou inesperados que apresentam probabilidade significativa de comprometer as operações de negócio e ameaçar a segurança da informação. Essa definição abrange tanto eventos de origem técnica, como exploração de vulnerabilidades e ataques de negação de serviço, quanto ocorrências de natureza humana e organizacional, como erros de configuração e acessos indevidos [12].

O guia NIST SP 800-61r3 complementa essa visão ao posicionar o incidente como a manifestação concreta de riscos cibernéticos no ambiente organizacional, integrando a resposta a incidentes diretamente às funções do NIST Cybersecurity Framework (CSF) 2.0 (Governar, Identificar, Proteger, Detectar, Responder e Recuperar). Nessa perspectiva, a eficácia da resposta depende não apenas de capacidades técnicas, mas de uma função central de governança, exigindo planejamento organizacional, definição de responsabilidades e maturidade institucional em uma abordagem formal e coordenada [15].

No contexto da administração pública federal brasileira, o Programa de Privacidade e Segurança da Informação (PPSI 2.0) estabelece, por meio do Controle 17, os requisitos operacionais para a gestão de incidentes. A normativa exige a definição de critérios formais para a distinção clara entre evento e incidente (Medida 17.9) [7]. Classificada no Grupo de Implementação 3 (GI3), essa exigência técnica representa um nível avançado de maturidade, ainda não amplamente alcançado pelas organizações públicas, conforme evidenciado por auditorias recentes do Tribunal de Contas da União (Acórdão nº 1.372/2025)[20]. Quando o incidente envolve dados pessoais, sua natureza se amplia, passando a configurar também uma possível violação de direitos fundamentais dos titulares. Nesses casos, a resposta deixa de ser técnica e passa a envolver obrigações legais, conforme estabelecido pela Lei Geral de Proteção de Dados (LGPD), aspecto que será aprofundado na Seção 2.2.

2.1.2 Fases do Ciclo de Resposta a Incidentes. A estruturação da resposta a incidentes em fases sequenciais é um elemento central dos principais frameworks da área. A ISO/IEC 27035-1:2023 organiza esse ciclo em cinco fases: planejamento e preparação; detecção e geração de relatórios; avaliação e decisão; respostas; e lições aprendidas. Por sua vez, a revisão mais recente do guia norte-americano NIST SP 800-61r3 abandonou o seu modelo clássico de quatro etapas para integrar o ciclo de resposta diretamente às funções do NIST Cybersecurity Framework (CSF) 2.0, categorizando as atividades em Preparação (Govern, Identify, Protect), Resposta Ativa (Detect, Respond, Recover) e Melhoria Contínua (Improvement) [12, 15].

No contexto da administração pública brasileira, a estruturação dessas fases é ditada pelo Plano de Gestão de Incidentes Cibernéticos (PLANGIC) do GSI/PR, exigido como complemento ao PPSI 2.0.

O Quadro 1 apresenta a correspondência entre as fases desses referenciais, ele demonstra a convergência conceitual entre os modelos internacionais e sua adaptação obrigatória para as ETIRs brasileiras.

A fase de preparação/prevenção que torna a resposta eficaz, definindo políticas, responsabilidades e fluxos de comunicação internos. Como afirmam Woods e Böhme [25], sem um planejamento adequado, a resposta a incidentes torna-se ineficaz. No entanto, muitas organizações, na prática, não a priorizam, focando predominantemente na reação tecnológica.

A fase de detecção, avaliação e tratamento envolve a identificação de indicadores de comprometimento, a triagem de eventos e a classificação do incidente quanto à sua severidade. No âmbito legal, esta etapa configura um momento crítico: é a partir da confirmação (validação) de que o incidente afetou dados pessoais que se inicia a contagem do prazo de três dias úteis para a comunicação oficial à Agência Nacional de Proteção de Dados (ANPD) e aos titulares, conforme o Art. 6º da Resolução CD/ANPD nº 15/2024 [2].

Durante as etapas de resposta (contenção, erradicação e recuperação), a equipe técnica atua para minimizar os impactos e restaurar a operação. Embora o PLANGIC exija ações rápidas de mitigação, estabelece que as medidas de contenção devem ser aplicadas evitando-se a destruição de evidências que possam subsidiar processos administrativos ou judiciais [15]. O registro dessas ações (accountability) é essencial para demonstrar conformidade com o Art. 46 da LGPD [5].

Por fim, a fase de lições aprendidas (pós-incidente) é responsável por retroalimentar o processo. Mais do que uma boa prática técnica para evitar a recorrência de ataques, essa etapa atende a uma exigência regulatória de privacidade: a Resolução CD/ANPD nº 15/2024 (Art. 10) determina que a instituição mantenha um registro formal e detalhado do incidente, das medidas corretivas adotadas e das análises de riscos por, no mínimo, cinco anos [2].

2.1.3 ETIRs e CSIRTs: Papel e Estrutura. A operacionalização da resposta a incidentes depende de equipes especializadas, reconhecidas internacionalmente como *Computer Security Incident Response Teams* (CSIRTs). Na Administração Pública Federal brasileira, essas estruturas são oficialmente denominadas Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIRs). Conforme o Plano de Gestão de Incidentes Cibernéticos (PLANGIC), as ETIRs atuam como o ponto focal técnico de cada órgão e integram a Rede Federal de Gestão de Incidentes Cibernéticos (Regic), sob a coordenação nacional do CTIR Gov. Este atua como o elemento central da governança reativa de segurança do Estado [9].

No âmbito normativo, o PPSI 2.0 exige a formalização dessas equipes pela alta administração logo em seu segmento de governança (Medida 0.8). Em complemento, o Controle 17 do framework (Medidas 17.1 e 17.2) exige a designação de um agente responsável por gerenciar a equipe, além de definir suas responsabilidades e mecanismos de comunicação institucional[7]. Contudo, evidências empíricas demonstram que a efetividade das ETIRs ainda é limitada. O Acórdão nº 1.372/2025 do Tribunal de Contas da União (TCU) revelou que apenas cerca de um terço das organizações possuem planos de resposta formalizados para lidar com violações [20]. Mais criticamente, 64,6% das instituições não possuem processos padronizados de comunicação à Agência Nacional de Proteção de Dados (ANPD) e aos titulares. Isso evidencia uma desconexão estrutural entre a remediação técnica (TI) e as obrigações legais de privacidade [20].

No contexto específico da Universidade Federal de Santa Maria (UFSM), a atuação da ETIR é formalizada pela Política de Segurança da Informação (PoSIN), instituída pela Resolução UFSM nº 121/2023. O normativo adota um modelo de implementação misto (Equipe Central e Descentralizada) e define como missão institucional a análise, o tratamento e a resposta a incidentes, além da promoção de uma cultura de cibersegurança na comunidade acadêmica [23]. Essa estruturação, contudo, reforça a necessidade de operacionalizar tais diretrizes por meio de fluxos verificáveis que integrem, de forma sistemática, a resposta técnica às obrigações legais da LGPD.

No ecossistema das Instituições de Ensino Superior (IES), esses obstáculos operacionais assumem contornos ainda mais críticos. Redes universitárias são construídas de forma orgânica e descentralizada. Esta característica gera um choque cultural entre a tradição de abertura acadêmica e as exigências de cibersegurança [21]. Adicionalmente, a diversidade de plataformas, a adoção de dispositivos pessoais (*Bring Your Own Device* - BYOD), o intenso fluxo de dados pessoais e a custódia de propriedade intelectual tornam essas instituições alvos prioritários. Elas são frequentemente visadas tanto por cibercriminosos, motivados por extorsão financeira (como ransomware), quanto por operações de espionagem patrocinadas por Estados [13].

Essa complexidade resulta em um descompasso entre as diretrizes regulatórias que orientam a atuação das ETIRs e sua capacidade operacional efetiva. A principal dificuldade reside em alinhar a contenção técnica dos incidentes às exigências legais da Lei Geral de Proteção de Dados (LGPD) [14]. Nesse contexto, a modelagem proposta nesta pesquisa apresenta-se como uma abordagem estruturada para mitigar essa lacuna.

2.2 A Lei Geral de Proteção de Dados e a Resposta a Incidentes

A Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018)[5], em vigor desde setembro de 2020, constitui o principal marco regulatório brasileiro no campo da proteção de dados. Inspirada no Regulamento Geral de Proteção de Dados da União Europeia (*General Data Protection Regulation* – GDPR), a lei estabelece um conjunto abrangente de princípios, bases legais, direitos dos titulares e obrigações aos agentes de tratamento, aplicável tanto ao setor privado quanto à administração pública.

No contexto da segurança da informação, o impacto da LGPD é significativo. A lei impõe obrigações formais sobre a prevenção e a resposta a incidentes com dados pessoais. Essas atividades saem do campo técnico e entram no campo da responsabilidade jurídica, sujeita a sanções administrativas[5].

2.2.1 Princípios e Bases Legais Relevantes para a Gestão de Incidentes. A Lei Geral de Proteção de Dados Pessoais (LGPD) estrutura o tratamento de dados a partir de dez princípios fundamentais (Art. 6º), dos quais três impactam diretamente a gestão de incidentes. O princípio da segurança exige a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e contra situações acidentais ou ilícitas de destruição, perda, alteração ou vazamento [14].

Table 1: Correspondência entre fases de resposta a incidentes

ISO/IEC 27035-1:2023	NIST SP 800-61r3 (CSF 2.0)	PLANGIC (GSI/PR)	Descrição Geral
Planejamento e preparação	Govern, Identify, Protect	Prevenção	Estrutura organizacional, definição de papéis, inventários e prontidão preventiva.
Detecção e geração de relatórios	Detect	Detecção	Monitoramento contínuo, identificação e notificação de eventos anômalos.
Avaliação e decisão	Detect/Respond	Tratamento (Triagem e Análise)	Validação do evento, classificação, correlação de evidências e priorização de impacto.
Respostas	Respond/Recover	Resposta (Contenção, Erradicação e Recuperação)	Mitigação de danos, eliminação da ameaça raiz e restauração dos sistemas.
Lições aprendidas	Improvement	Pós-incidente	Revisão, documentação de evidências para conformidade legal e melhoria contínua.

Fonte: Elaborado pelo autor com base na ISO/IEC 27035-1:2023, NIST SP 800-61r3 e PLANGIC/GSI.

O princípio da prevenção exige ações para evitar danos aos titulares. Isso inclui capacidades proativas de detecção e resposta, antes que os prejuízos se materializem. O princípio da responsabilização impõe ao controlador o dever de demonstrar a eficácia de suas medidas. A documentação do processo de resposta deixa de ser operacional e passa a ser um elemento jurídico[5].

No que se refere às bases legais, o tratamento de dados pelo Poder Público fundamenta-se predominantemente no cumprimento de obrigação legal ou regulatória e na execução de políticas públicas, nos termos dos Arts. 7º e 23 da LGPD [5]. Essa premissa é essencial para as ETIRs em instituições públicas, pois legitima o fundamento jurídico sob o qual os dados podem ser acessados e processados durante a investigação de incidentes, inclusive quando envolvem dados sensíveis [14].

2.2.2 Obrigações Específicas em Caso de Incidente: Arts. 46 e 48. O Art. 46 da LGPD institui o dever geral de segurança. Os agentes de tratamento devem adotar medidas técnicas e administrativas para proteger dados pessoais contra acessos não autorizados e situações ilícitas. A norma exige capacidades operacionais reais de prevenção, detecção e resposta — não apenas políticas declaratórias. O descumprimento configura tratamento irregular, conforme o Art. 44[5].

O Art. 48 torna obrigatória a comunicação de incidentes à ANPD e aos titulares. A obrigação se ativa quando o incidente pode causar risco ou dano relevante. A notificação deve ocorrer em prazo razoável e conter, no mínimo: natureza dos dados afetados, perfil dos titulares, riscos envolvidos, medidas de segurança adotadas e ações de mitigação.[5].

A efetividade prática dessa exigência foi consolidada pela Resolução CD/ANPD nº 15/2024, que fixou o prazo de três dias úteis para a comunicação oficial. Além disso, a norma definiu critérios objetivos para a caracterização de risco ou dano relevante, bem como o escopo documental exigido no relatório de incidente, aspectos operacionais que serão aprofundados na subseção seguinte [2].

2.2.3 Resolução CD/ANPD nº 15/2024: Prazos, Critérios e Notificação. A Resolução CD/ANPD nº 15/2024 constitui o principal instrumento regulatório para a operacionalização das obrigações de comunicação de incidentes previstas na LGPD. O normativo materializa os dispositivos legais ao introduzir contribuições de impacto direto sobre os processos das ETIRs [2].

A primeira contribuição são os critérios objetivos de avaliação do risco ou dano relevante. O Art. 5º determina que o controlador avalie se o incidente afeta interesses fundamentais dos titulares. A análise considera a natureza do evento e o volume de dados — inclusive casos de tratamento em larga escala. A norma elenca fatores agravantes: dados sensíveis, financeiros, credenciais de autenticação ou dados de titulares em condição de vulnerabilidade. Essa avaliação é etapa obrigatória e deve ser documentada. [2].

A segunda contribuição versa sobre os limites temporais. A resolução fixa que a comunicação preliminar à Agência Nacional de Proteção de Dados (ANPD) e aos titulares deve ocorrer em até três dias úteis, contados a partir da ciência, pelo controlador, de que o incidente afetou dados pessoais. Informações complementares podem ser apresentadas no prazo de até vinte dias úteis. Esse gatilho temporal evidencia a necessidade de integração entre as etapas técnicas de detecção e contenção e os procedimentos legais de notificação [2].

A terceira contribuição estabelece o conteúdo mínimo da comunicação e a obrigação de guarda documental. A notificação deve incluir a descrição das categorias de dados afetados, o número estimado de titulares e registros envolvidos, as medidas de mitigação adotadas e a identificação do encarregado pelo tratamento de dados pessoais. Ademais, o Art. 10 determina a manutenção de registro completo do incidente pelo prazo mínimo de cinco anos, a norma exige processos padronizados e alinhados ao princípio da responsabilização e prestação de contas [2].

2.2.4 Responsabilidades do Controlador e do Operador. A LGPD (Art. 5º) distingue dois papéis centrais na cadeia de tratamento: o controlador, responsável pelas decisões referentes ao tratamento de dados pessoais, e o operador, que realiza o tratamento em nome

do controlador [5]. No contexto das instituições públicas de ensino, a universidade atua como controladora dos dados de estudantes e servidores, enquanto fornecedores de serviços de tecnologia assumem o papel de operadores.

Essa distinção possui implicações diretas na resposta a incidentes. O Art. 48 da LGPD atribui ao controlador a responsabilidade pela comunicação do incidente à ANPD e aos titulares, independentemente de a origem do incidente estar associada a sistemas operados por terceiros. Dessa forma, a ETIR institucional deve não apenas conduzir a resposta técnica, mas também acionar os fluxos de comunicação legal dentro dos prazos estabelecidos [5].

O Art. 46 da LGPD e o Controle 22 do PPSI 2.0 exigem cláusulas contratuais que formalizem as obrigações de segurança dos operadores [7]. O TCU confirma o risco: organizações sem responsabilidades definidas junto a terceiros expõem a Administração Pública a falhas graves (Acórdão nº 1.372/2025) [20]. As ETIRs devem, portanto, ir além da dimensão técnica e incorporar mecanismos formais de interação com operadores e obtenção de evidências.

2.3 Segurança da Informação no Setor Público Federal

A segurança da informação na administração pública federal evoluiu na última década. O arcabouço normativo atual responde ao avanço das ameaças cibernéticas e ao amadurecimento da proteção de dados. Suas obrigações vão além do técnico: abrangem governança, conformidade legal e capacidade operacional [7, 9].

No centro desse ecossistema regulatório, o Programa de Privacidade e Segurança da Informação (PPSI) consolidou-se como o principal instrumento de orientação e avaliação da maturidade em segurança da informação e privacidade para os órgãos do Poder Executivo federal [7].

2.3.1 O PPSI 2.0: Estrutura, Controles e Governança. O Programa de Privacidade e Segurança da Informação, em sua versão mais recente (PPSI 2.0), foi instituído pela Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025, e detalhado no Guia do Framework de Privacidade e Segurança da Informação (versão 1.2, de janeiro de 2026) [7]. O PPSI 2.0 representa uma evolução ao adotar uma abordagem baseada em frameworks internacionais consolidados, como o CIS Controls v8.1, e ao integrar, em um único instrumento, controles técnicos de segurança da informação e controles de privacidade orientados à conformidade com a LGPD.

O framework organiza suas diretrizes em três segmentos complementares. O segmento base compreende controles estruturantes voltados à governança e ao estabelecimento de instrumentos institucionais fundamentais, como a formalização de políticas e a designação de responsáveis críticos (alta administração, Gestor de Segurança da Informação e Encarregado de Dados - DPO). Esses elementos constituem pré-requisitos para a implementação efetiva dos demais controles [7].

O segmento de segurança da informação abrange os Controles 1 a 18, organizados conforme áreas de risco técnico. Cada controle desdobra-se em medidas específicas e verificáveis, classificadas em três Grupos de Implementação (GI), que refletem níveis progressivos de maturidade: o GI1 corresponde à higiene cibernética; o GI2 contempla organizações com infraestrutura gerenciada e risco moderado; e o GI3 abrange organizações com maior exposição e capacidade técnica avançada. Essa estrutura é particularmente relevante para este estudo, pois permite avaliar o nível de maturidade esperado para uma ETIR em instituições públicas [7].

O segmento de privacidade, por sua vez, compreende os Controles 19 a 25, voltados às obrigações decorrentes da LGPD e das resoluções da ANPD. Esses controles incluem o registro das operações de tratamento, a aplicação dos princípios legais, a gestão do encarregado de dados, a relação com operadores e a realização de análises de impacto. A existência desse segmento evidencia a integração entre segurança da informação e privacidade no framework nacional [7].

A Secretaria de Governo Digital publicou guias operacionais alinhados à Resolução CD/ANPD nº 15/2024 [8]. Eles operacionalizam o Controle 17 (gestão de incidentes), o Controle 20 (incidentes com dados pessoais) e o Controle 22 (contratos com provedores), com fluxos de avaliação, contenção e comunicação à ANPD. Esses documentos formam a base normativa do modelo proposto.

O PGI-DP, publicado pelo MGI em julho de 2025, é o exemplo mais direto de integração entre resposta a incidentes e LGPD [6]. O plano adota as fases do NIST SP 800-61r3 e incorpora os requisitos de notificação da ANPD. Sua existência prova a viabilidade da abordagem integrada proposta neste trabalho.

Por fim, o Plano de Gestão de Incidentes Cibernéticos (PLANGIC), coordenado pelo GSI/PR, estabelece o modelo operacional das ETIRs na Administração Pública Federal [9]. O plano organiza o ciclo de resposta em fases de prevenção, detecção, tratamento, resposta e pós-incidente. Contudo, quando há envolvimento de dados pessoais, essa abordagem técnica deve ser integrada aos requisitos do PPSI 2.0 e da Resolução CD/ANPD nº 15/2024. A integração entre esses instrumentos, ainda não plenamente operacionalizada, constitui a lacuna que este trabalho busca abordar por meio da modelagem em BPMN.

2.3.2 O Controle 17 do PPSI 2.0 e as ETIRs como Elemento Estruturante. O Controle 17 do PPSI 2.0 posiciona a ETIR como agente central da resposta a incidentes. A Medida 17.1 exige a designação formal do coordenador da equipe, restrita a servidores efetivos ou militares de carreira. A liderança é, portanto, estratégica e indelegável [7].

A Medida 17.2 determina que a ETIR se comunique, no mínimo, com o CTIR Gov e o CISC Gov.br. Essa exigência insere a equipe local em uma rede nacional de resposta coordenada [7]. Essa arquitetura institucional evidencia que o PPSI 2.0 trata a gestão de incidentes como um processo organizacional integrado, com interfaces claras entre as dimensões técnica, jurídica e de comunicação. Nesse contexto, o modelo BPMN proposto nesta pesquisa operacionaliza essa integração por meio de fluxos estruturados e aplicáveis ao cotidiano das ETIRs em instituições públicas.

2.3.3 O Plano de Gestão de Incidentes Cibernéticos (PLANGIC). Embora o ciclo operacional do Plano de Gestão de Incidentes Cibernéticos (PLANGIC) já tenha sido delineado nas seções anteriores, é importante destacar seu papel na governança interinstitucional. Enquanto o framework do PPSI 2.0 concentra-se na maturidade dos controles internos das organizações, o PLANGIC atua como instrumento de coordenação externa. Ele define papéis e fluxos de comunicação no âmbito da Rede Federal de Gestão de Incidentes Cibernéticos (Regic) [9]. Para as ETIRs federais, o PLANGIC

padroniza a classificação de severidade e os critérios de escalonamento. Incidentes com dados pessoais exigem comunicação ao CTIR Gov. A atuação local aciona, simultaneamente, obrigações legais e resposta coordenada em nível federal

2.3.4 Maturidade e Desafios de Conformidade: Evidências do TCU. A adequação à LGPD na Administração Pública Federal enfrenta deficit operacional grave. O TCU auditou 387 organizações e concluiu: parcela expressiva permanece em estágios iniciais de maturidade (Acórdão nº 1.372/2025) [20]. As falhas são três: resposta a incidentes sem padronização, políticas de segurança sem formalização e DPOs sem designação. TI e conformidade jurídica operam de forma isolada. Esse cenário reflete uma baixa integração entre as áreas técnicas de tecnologia da informação e as instâncias jurídicas de conformidade.

No contexto das Instituições Federais de Ensino Superior, essa defasagem é intensificada por características estruturais, como a autonomia acadêmica, a heterogeneidade de sistemas e a restrição de recursos. Como consequência, a implementação do Controle 17 do PPSI 2.0 tende a ocorrer de forma fragmentada. Esse diagnóstico sustenta a tese de que o principal desafio não reside na ausência de normativos, uma vez que a LGPD, o PPSI 2.0 e o PLANGIC estabelecem diretrizes abrangentes, mas na ausência de mecanismos que traduzam essas diretrizes em fluxos operacionais concretos. Nesse contexto, a operacionalização estruturada e verificável da resposta a incidentes no cotidiano das ETIRs constitui a lacuna que o modelo proposto neste estudo busca endereçar.

2.4 Modelagem de Processos com BPMN

A representação formal de fluxos organizacionais transcende a simples documentação: no contexto da gestão de incidentes, permite identificar lacunas, delimitar responsabilidades com precisão e estabelecer uma base probatória relevante para auditorias de conformidade [25, 27]. Nesse cenário, a *Business Process Model and Notation* (BPMN) consolida-se como a abordagem adequada para a modelagem proposta neste trabalho.

2.4.1 O que é BPMN e por que é adequada para modelar a GIC. Mantida pelo *Object Management Group* (OMG) em sua versão 2.0, a BPMN é um padrão global de modelagem gráfica que reduz ambiguidades inerentes à descrição textual. Ele estabelece uma linguagem comum entre equipes técnicas e não técnicas [16]. Sua aplicação na gestão de incidentes integrada às exigências da LGPD justifica-se por um conjunto de capacidades técnicas:

- **Fluxos condicionais (Gateways):** permitem representar bifurcações decisórias baseadas em critérios variáveis, como a severidade do incidente ou a necessidade de comunicação à ANPD.
- **Delimitação de responsabilidades (Pools e Lanes):** possibilitam a segregação visual dos atores envolvidos que distingue as atribuições da ETIR, do Encarregado de Dados (DPO), da alta administração e de entidades externas.
- **Eventos temporizados:** viabilizam a associação de restrições temporais às atividades que permite o controle de prazos regulatórios, como o limite de três dias úteis para notificação previsto na Resolução CD/ANPD nº 15/2024.
- **Interoperabilidade e sustentabilidade:** por se tratar de um padrão aberto e amplamente suportado, possibilita a manutenção, evolução e eventual automação dos processos modelados ao longo do tempo.

O quadro 2 apresenta um resumo dos principais elementos BPMN utilizados no modelo proposto, com a respectiva função no processo.

2.4.2 BPMN na Modelagem de Processos de Segurança da Informação. A utilização da BPMN para modelar processos de segurança da informação tem se consolidado como uma abordagem relevante para a formalização de fluxos de resposta e a integração de requisitos de conformidade. Silva Filho e Afonseca (2025) [18] propuseram um modelo integrado que adota a BPMN como notação central para alinhar as diretrizes técnicas da norma ISO/IEC 27002 às obrigações legais da LGPD. Os autores argumentam que a capacidade da notação de representar responsabilidades e decisões a torna particularmente adequada para cenários que envolvem múltiplos atores institucionais e exigências jurídicas interdependentes [18].

No campo específico da proteção de dados, Araújo et al. (2021) propõem o método LGPD4BP, que orienta a adequação de processos de negócio por meio de um instrumento de avaliação e de um catálogo de padrões de modelagem em BPMN, abrangendo cenários como vazamento de dados e gestão de consentimento [1]. Um ponto de convergência com a presente pesquisa é que a validação do LGPD4BP ocorreu no contexto de uma instituição federal de ensino. Embora o foco daquele trabalho esteja na adequação de processos administrativos, a abordagem de traduzir princípios de privacidade em artefatos visuais constitui uma base metodológica relevante.

Essa perspectiva é convergente com a abordagem adotada neste estudo. A modelagem em BPMN do processo de resposta a incidentes da ETIR/UFSM, com a incorporação explícita dos requisitos da LGPD — inclue gatilhos de notificação, prazos legais e responsabilidades do controlador — busca produzir um artefato que seja simultaneamente compreensível para equipes técnicas, verificável por auditores de conformidade e aplicável em atividades de capacitação e simulação, conforme previsto na Medida 17.7 do Controle 17 do PPSI 2.0 [7].

2.5 Trabalhos Relacionados

A interseção entre a gestão de incidentes de segurança da informação e a proteção de dados pessoais configura um campo de pesquisa em consolidação, impulsionado pela entrada em vigor de regulamentações como o *General Data Protection Regulation* (GDPR) [22] e a Lei Geral de Proteção de Dados Pessoais (LGPD)[5]. Esta seção apresenta os principais trabalhos identificados na literatura que se aproximam do problema abordado neste estudo, organizados em três eixos temáticos: (i) modelos de integração entre gestão de incidentes e conformidade legal; (ii) estudos empíricos que evidenciam a lacuna entre normativos e prática organizacional; e (iii) pesquisas sobre segurança da informação em instituições públicas de ensino superior.

2.5.1 Modelos de Integração entre GIC e Conformidade Legal. [18] propuseram um modelo integrado para a gestão de incidentes de segurança da informação representado em notação BPMN, com o objetivo de articular as dimensões técnica, organizacional e legal da resposta em um fluxo único e verificável. O estudo identifica que

Table 2: Elementos BPMN utilizados no modelo proposto

Elemento	Tipo	Função no Modelo
Evento de início	Evento	Marca o gatilho do processo — detecção ou reporte de um incidente.
Evento de fim	Evento	Marca o encerramento do processo — após lições aprendidas ou arquivamento.
Evento intermediário temporizador	Evento	Representa prazos legais obrigatórios (ex.: 3 dias úteis para notificação à ANPD).
Evento intermediário de mensagem	Evento	Representa o envio ou recebimento de comunicações formais (ex.: notificação à ANPD, ao titular ou ao CTIR Gov).
Tarefa (Task)	Atividade	Representa uma ação executada por um ator do processo (ex.: classificar incidente, coletar evidências, elaborar relatório).
Subprocesso (Subprocess)	Atividade	Agrupa atividades de maior complexidade em um bloco expansível (ex.: avaliação de risco ou dano relevante).
Gateway exclusivo (XOR)	Gateway	Representa decisões com caminhos alternativos mutuamente exclusivos (ex.: "o incidente envolve dados pessoais?").
Gateway paralelo (AND)	Gateway	Representa atividades que devem ocorrer simultaneamente (ex.: contenção técnica e comunicação jurídica em paralelo).
Gateway baseado em evento	Gateway	Representa decisões condicionadas ao recebimento de um evento externo (ex.: resposta da ANPD).
Pool	Raia	Representa uma organização participante do processo (ex.: ETIR/UFSM).
Lane	Raia	Representa um ator ou área dentro de uma organização (ex.: Equipe de Tratamento (ETIR), DPO, área jurídica).
Fluxo de sequência	Conector	Representa a ordem de execução das atividades.
Fluxo de mensagem	Conector	Representa comunicações entre pools distintos.
Anotação de texto	Artefato	Registra informações complementares, como normas de referência ou prazos legais.

Fonte: Elaborado pelo autor com base em [16].

normas consolidadas, como a ISO/IEC 27002 e práticas do ITIL, não especificam como as atividades devem ser executadas em conformidade com as obrigações legais decorrentes da LGPD. Ao analisarem fluxos adotados por instituições públicas, os autores observaram lacunas relevantes, especialmente na ausência de mapeamento adequado das etapas de notificação à Agência Nacional de Proteção de Dados (ANPD) e aos titulares [18].

A principal contribuição do estudo reside na utilização da modelagem BPMN como mecanismo de integração entre requisitos técnicos e legais, configurando-o como o trabalho mais diretamente relacionado à presente pesquisa. A distinção fundamental, contudo, está no escopo de aplicação: enquanto Silva Filho e Afonseca propõem um modelo genérico e adaptável, este trabalho operacionaliza a integração no contexto específico das ETIRs em universidades federais, adotando o PPSI 2.0 como referência normativa e a ETIR/UFSM como cenário de aplicação.

Woods and Böhme [25] analisam a resposta a incidentes sob uma perspectiva jurídica, argumentam que a crescente judicialização desses eventos tem deslocado parte da condução da resposta para o domínio jurídico. Os autores identificam uma tensão estrutural entre a lógica técnica, orientada à contenção e recuperação rápida, e a lógica jurídica, que exige documentação rigorosa, controle de evidências e comunicação formal em prazos definidos. Essa tensão representa um dos principais desafios abordados neste trabalho, cuja proposta busca integrar essas dimensões em um fluxo único e coordenado.

Zaguir et al. [27] identificam a lacuna chamada *implementation roadmap gap*. O problema é a dificuldade de traduzir princípios legais em práticas operacionais concretas. Frameworks técnicos isolados não garantem conformidade regulatória. São necessários modelos de processos estruturados que conectem obrigações legais a atividades verificáveis. Nesse contexto, a modelagem em BPMN proposta neste trabalho insere-se como uma abordagem capaz de mitigar essa lacuna, ao formalizar e integrar os fluxos de resposta a incidentes com os requisitos legais da LGPD.

2.5.2 Lacuna entre Normas e Prática Organizacional. O Acórdão nº 1.372/2025 do Tribunal de Contas da União (TCU) constitui a evidência empírica mais abrangente disponível sobre o estado de conformidade com a LGPD na Administração Pública Federal [20]. Ao avaliar 387 órgãos e entidades, o levantamento identificou que as organizações ainda apresentam processos de resposta a incidentes pouco formalizados, com nível médio de maturidade na dimensão "Violação de Dados Pessoais" de aproximadamente 38%.

Os resultados indicam que apenas 32,82% das instituições possuem um Plano de Resposta a Incidentes formalizado que contemple vazamentos de dados pessoais. De forma ainda mais crítica,

64,6% das organizações auditadas (250 entidades) não estabeleceram processos padronizados para notificação à Agência Nacional de Proteção de Dados (ANPD) e aos titulares em caso de incidentes [20].

Esse cenário evidencia uma lacuna operacional significativa e uma baixa integração entre as equipes técnicas de segurança da informação e as áreas responsáveis pelas obrigações legais de privacidade.

Essa lacuna também é corroborada por estudos recentes conduzidos por Spósito et al. (2025), no âmbito da Universidade de Brasília, que analisaram 125 estudos primários sobre engenharia de requisitos de privacidade [19]. Os autores identificaram que, embora exista uma ampla variedade de técnicas, métodos, processos, frameworks e ferramentas voltados à privacidade, sua aplicação prática ainda é limitada, com predominância de estudos em contextos acadêmicos e baixa adoção na indústria.

Nesse sentido, o estudo evidencia dificuldades recorrentes na tradução de requisitos legais como os impostos pela LGPD em especificações técnicas operacionais, bem como na integração desses requisitos aos processos de desenvolvimento e gestão de sistemas. Essa constatação reforça a existência de uma lacuna estrutural entre os referenciais normativos e sua efetiva operacionalização nas organizações.

Dessa forma, observa-se que o principal desafio não reside na ausência de normas ou frameworks, mas na dificuldade de transformar essas diretrizes em processos estruturados, executáveis e auditáveis. Tal diagnóstico confere sustentação empírica ao problema de pesquisa deste trabalho, e reforça a necessidade de um modelo processual integrado que conecte, de forma sistemática, as dimensões técnica e legal da resposta a incidentes no contexto das ETIRs.

2.5.3 Segurança da Informação em Instituições Públicas de Ensino Superior. Ulven e Wangen (2021) revisaram sistematicamente os riscos cibernéticos em instituições de ensino superior (IES). O estudo identificou um perfil de risco distinto do setor corporativo. Fatores como alta rotatividade de usuários, recursos limitados e redes descentralizadas geram essa vulnerabilidade. Há um nítido *clash of cultures* entre as exigências de segurança e a cultura de abertura acadêmica [21]. Além disso, as IES atraem tanto o cibercrime financeiro quanto a espionagem estatal em busca de propriedade intelectual. Apesar deste cenário crítico, a resposta a incidentes nas universidades permanece reativa e ad hoc. Faltam processos formalizados e integração com os requisitos legais.

Nascimento e Silva (2023) analisaram repositórios institucionais sob a ótica da LGPD. O estudo demosntra que as IES enfrentam graves dificuldades operacionais com a lei. A falta de processos estruturados expõe estas instituições a sanções administrativas e danos reputacionais [14]. Para mitigar este cenário, as autoras recomendam o mapeamento dos dados e a padronização dos fluxos organizacionais. Esta constatação aplica-se ao contexto das ETIRs. O sucesso da resposta a incidentes depende deste conhecimento estruturado dos fluxos.

Araújo et al. (2021) propõem o método LGPD4BP baseado no princípio de *privacy by design*. O estudo prova a viabilidade de incorporar requisitos legais em processos de negócio via BPMN [1]. A estrutura fornece um instrumento de avaliação e um catálogo de modelagem para cenários de vazamento de dados e gestão de consentimento. Os autores validaram a proposta em uma instituição federal de ensino. Este cenário reforça a relevância da abordagem para esta pesquisa. Contudo, o método foca na adequação de processos administrativos. A solução não contempla o domínio crítico da resposta a incidentes de segurança.

2.5.4 Síntese e Posicionamento da Pesquisa. A literatura apresenta avanços na integração entre segurança e proteção de dados. Contudo, as abordagens permanecem fragmentadas em três dimensões. As normas técnicas concentram-se na remediação operacional. Os instrumentos legais exigem documentação e comunicação formal. Estudos empíricos provam o grave descompasso entre estas duas esferas nas organizações públicas. Nas universidades públicas, esta lacuna é ainda mais evidente. A descentralização tecnológica e a baixa maturidade dos processos operacionais ampliam este problema.

O presente trabalho diferencia-se dos estudos anteriores ao combinar três elementos que, isoladamente, já aparecem na literatura, mas que não foram explorados de forma conjunta: (i) a modelagem em notação BPMN como mecanismo formal de integração; (ii) o referencial normativo específico do contexto federal brasileiro, representado pelo PPSI 2.0 e pela Resolução CD/ANPD nº 15/2024; e (iii) a aplicação em uma ETIR de universidade federal, com suas particularidades estruturais e operacionais. Essa combinação posiciona a pesquisa como uma contribuição original tanto do ponto de vista teórico quanto prático.

3 Metodologia

Esta seção detalha os procedimentos metodológicos da pesquisa. O texto aborda a classificação, o método aplicado, as etapas de desenvolvimento do modelo e os protocolos de validação com coleta de dados. Esta estrutura estabelece a base para integrar os requisitos da LGPD à gestão de incidentes cibernéticos na ETIR/UFSM.

3.1 Classificação da Pesquisa

A pesquisa é de natureza aplicada. Ela resolve um problema prático: a falta de fluxos operacionais que integrem respostas técnicas e legais a incidentes cibernéticos nas universidades federais [20, 27]. O conhecimento gerado tem aplicação imediata na ETIR/UFSM. A solução modelada supera a lacuna entre as diretrizes normativas e a prática operacional.

A abordagem do problema é qualitativa. O método permite compreender o contexto institucional da ETIR/UFSM. Ele possibilita interligar os processos reais aos requisitos do PPSI2.0, do PLANGIC e da Resolução CD/ANPD nº 15/2024. Métricas quantitativas falhariam em capturar a complexidade interpretativa destas obrigações legais.

Quanto aos objetivos, a pesquisa é exploratória e descritiva. A fase exploratória mapeia o descompasso entre a resposta técnica e a LGPD nas instituições públicas. A fase descritiva detalha a solução por meio da notação BPMN (*Business Process Model and Notation*). O modelo proposto expõe responsabilidades, decisões críticas e restrições legais de tempo.

Os procedimentos técnicos combinam três táticas: revisão de literatura, análise documental e modelagem de processos. As próximas subseções detalham o fluxo exato destas etapas.

3.2 Método de Pesquisa

A pesquisa combina o método de Estudo de Caso com a *Design Science Research* (DSR). Esta união permite construir e validar o artefato proposto na ETIR/UFSM.

O Estudo de Caso delimita a investigação ao contexto real da universidade. O método garante a análise profunda das particularidades institucionais na gestão de incidentes [26]. A escolha da UFSM como objeto de estudo justifica-se pela existência de uma estrutura formal de governança de segurança da informação, estabelecida pela Resolução UFSM nº 121, de 04 de abril de 2023, que institui a Política de Segurança da Informação (PoSIN) da instituição [23].

O normativo exige a manutenção permanente de uma ETIR (Art. 19). A norma também define a missão técnica de resposta a incidentes (Art. 51) sob um modelo de autonomia compartilhada (Art. 61). Este arcabouço fornece o respaldo exato para integrar o novo modelo à LGPD.

A *Design Science Research* fornece o arcabouço metodológico adequado para pesquisas focadas na criação de artefatos [10]. Neste caso, um modelo de processo em notação BPMN [10]. O percurso adapta as etapas clássicas de Hevner et al. (2004). A execução condensa-se em três fases diretas:

(1) **Conscientização do Problema**: etapa contemplada na Introdução e na Fundamentação Teórica (Seções 1 e 2), por meio da revisão da literatura, da análise do arcabouço normativo e da evidenciação empírica da lacuna existente, com destaque para os achados do Acórdão TCU nº 1.372/2025 [20].
(2) **Proposição do Artefato**: consiste no desenvolvimento do modelo de processo em BPMN que operacionaliza a integração entre os requisitos técnicos de resposta a incidentes e as obrigações legais da LGPD, tendo como referência os controles do PPSI 2.0 [7] e os prazos estabelecidos pela Resolução CD/ANPD nº 15/2024 [2]. Essa etapa é detalhada na Seção 3.4.
(3) **Avaliação do Artefato**: visa verificar a adequação, a clareza e a aplicabilidade do modelo proposto no ambiente da ETIR/UFSM. A avaliação é conduzida por meio de entrevistas semiestruturadas com especialistas da instituição, conforme protocolo detalhado na Seção 3.5.

3.3 Análise Documental

A pesquisa inclui uma análise documental de fontes normativas e orientativas. O método extrai informações estruturadas de documentos primários, como leis, resoluções e guias operacionais. Esta abordagem elimina a intermediação de interpretações de terceiros. A tática assegura fidelidade absoluta ao conteúdo normativo original.

3.3.1 Corpus Documental. O Quadro 3 relaciona os documentos que compuseram o corpus da análise documental, organizados por categoria.

3.3.2 Critérios e Procedimento de Análise. Cada documento foi analisado com foco em três dimensões:

- Definições e conceitos fundamentais adotados, especialmente aqueles relacionados à incidente de segurança, dados pessoais e obrigações de notificação;
- Fases, etapas ou atividades previstas no processo de resposta a incidentes;
- Atores, papéis e responsabilidades definidos para cada etapa.

As informações extraídas nessas três dimensões constituíram os insumos primários para o desenvolvimento do modelo BPMN. A leitura dos documentos foi orientada por um roteiro estruturado de questões analíticas:

- Quais atividades são exigidas em cada fase do ciclo de resposta?
- Quem é responsável por cada atividade?
- Quais são os prazos associados?
- Quais são os gatilhos para acionamento de obrigações legais?
- Quais informações devem ser registradas e comunicadas?

As respostas a essas questões foram sistematizadas em fichas de análise documental e posteriormente consolidadas no modelo proposto.

3.4 Desenvolvimento do Modelo BPMN

O modelo de processo proposto foi desenvolvido com base na literatura e na análise documental. O artefato utiliza a notação formal BPMN 2.0. A construção do diagrama ocorreu na ferramenta Bizagi Modeler.

3.4.1 Justificativa da Ferramenta. Foi adotado o Bizagi Modeler por três razões metodológicas. Primeiro, a plataforma é gratuita e suporta integralmente a especificação BPMN 2.0 [16]. Segundo, o software exporta arquivos nos formatos `.bpmn` e `.svg`. Esta funcionalidade garante a interoperabilidade do modelo e preserva a qualidade visual em documentos acadêmicos. Terceiro, a ferramenta suporta nativamente a modelagem de *pools*, *lanes*, eventos temporizados e subprocessos. Estes elementos gráficos são essenciais para representar com precisão os fluxos propostos na Seção 2.4.

3.4.2 Método de Construção. O desenvolvimento do modelo seguiu quatro etapas sequenciais. Na primeira etapa, foram identificados, a partir da análise documental, todos os requisitos normativos com implicação direta sobre o processo de resposta a incidentes — incluindo obrigações legais da LGPD, prazos da Resolução CD/ANPD nº 15/2024 e medidas do Controle 17 do PPSI 2.0. Na segunda etapa, esses requisitos foram mapeados às cinco fases do ciclo de resposta: prevenção, detecção, triagem e análise, resposta (contenção, erradicação e recuperação) e pós-incidente, definidas a partir da convergência entre o NIST SP 800-61r3, a ISO/IEC 27035-1:2023 e o PLANGIC, conforme sistematizado no Quadro 1. Na terceira etapa, os atores envolvidos foram identificados e organizados em raias (*pools* e *lanes*), com base nas responsabilidades definidas pelo PPSI 2.0 e pelo Guia de Resposta a Incidentes da SGD [8]. Na quarta etapa, o modelo foi construído no Bizagi Modeler, com a representação das atividades, eventos, *gateways* e conectores correspondentes a cada fase e requisito mapeado nas etapas anteriores.

3.4.3 Insumos Primários e Estrutura do Modelo. Três documentos orientaram a construção do modelo: o Guia de Resposta a Incidentes da SGD (v3.3)[8], o Guia do *Framework* PPSI2.0 (v1.2)[7] e o PGI-DP do MGI[6]. Juntos, eles cobrem as dimensões técnicas e as obrigações legais da LGPD. Estas fontes fundamentam todas as atividades, papéis e fluxos decisórios do artefato. O modelo possui

Table 3: Corpus da análise documental

Categoria	Documento	Ref.	Dimensões analisadas
Legislação	Lei nº 13.709/2018 — LGPD	[5]	Definições, obrigações, bases legais
Regulamentação	Resolução CD/ANPD nº 15/2024	[2]	Prazos, critérios, conteúdo da notificação
Framework normativo	Guia do *Framework* PPSI 2.0	[7]	Fases, atores, medidas
Guia operacional	Guia de Resposta a Incidentes — SGD v3.3	[8]	Fases, atividades
Plano governamental	PGI-DP/MGI	[6]	Integração LGPD
Norma técnica internacional	ISO/IEC 27035-1:2023	[12]	Ciclo de resposta
Guia técnico internacional	NIST SP 800-61r3	[15]	Boas práticas
Instrumento de coordenação	PLANGIC — GSI/PR	[9]	Papéis e escalonamento
Diagnóstico institucional	Acórdão TCU nº 1.372/2025	[20]	Lacunas
Normativo institucional	PoSIN/UFSM — Resolução nº 121/2023	[23]	Estrutura ETIR

Fonte: Elaborado pelo autor.

um *pool* principal para a ETIR/UFSM. Este espaço divide-se em quatro *lanes* de atores internos: Equipe de Tratamento (ETIR), Encarregado de Dados (DPO), Área Jurídica e Gestão Institucional. Um *pool* externo representa a ANPD. Este bloco captura o fluxo de solicitação de informações exigido pelo Art.8ºda Resolução CD/ANPD nº 15/2024.

O fluxo percorre as cinco fases do ciclo de resposta. Foram inseridos *gateways* explícitos para as decisões críticas. Estas acionam as obrigações legais, como a avaliação de risco e a necessidade de comunicação à ANPD e aos titulares. Fontes normativas ou acadêmicas justificam cada elemento do modelo. Foram incluídas anotações de texto no diagrama para registrar estas referências. Esta tática garante a auditoria e a rastreabilidade total do arcabouço normativo.

3.5 Validação do Modelo por Especialistas

A etapa de avaliação do artefato, prevista na *Design Science Research*, foi operacionalizada por meio de um processo de validação qualitativa junto a especialistas vinculados à ETIR/UFSM. O objetivo foi de verificar a adequação, a clareza e a aplicabilidade prática do modelo na universidade. A tática complementa a teoria normativa com a percepção de quem atua na linha de frente da LGPD e da gestão de incidentes.

3.5.1 Seleção dos Especialistas. A seleção dos participantes seguiu um critério intencional (*purposive sampling*), orientado pela relevância dos perfis para o objeto de estudo. Foram convidados três especialistas, cada um representou uma das dimensões institucionais diretamente implicadas no modelo proposto:

- **Coordenador da ETIR/UFSM**: responsável pela coordenação técnica da equipe de resposta a incidentes, com visão sobre os fluxos operacionais vigentes e as capacidades reais da equipe;
- **Gestor de Segurança da Informação**: responsável pela governança de segurança da informação na instituição, com conhecimento sobre o arcabouço normativo interno e o alinhamento com o PPSI 2.0;
- **Encarregado de Dados (DPO)**: responsável pelas obrigações legais decorrentes da LGPD, com visão sobre os requisitos de comunicação à ANPD e de proteção dos direitos dos titulares.

Essa composição assegura a cobertura das três perspectivas que o modelo busca integrar: a técnica, a de governança e a jurídico-normativa.

3.5.2 Instrumento de Coleta. A validação foi conduzida por meio de entrevista semiestruturada, modalidade que permite tanto a padronização das questões centrais quanto a exploração de aspectos emergentes identificados pelos participantes durante a análise do modelo [26]. O roteiro foi organizado em três blocos temáticos:

(1) **Adequação normativa**: o modelo incorpora corretamente os requisitos da LGPD e da Resolução CD/ANPD nº 15/2024 relevantes para a resposta a incidentes?
(2) **Clareza e usabilidade**: o modelo é compreensível para os profissionais que atuariam com ele no cotidiano? Os elementos BPMN utilizados representam adequadamente as atividades, decisões e responsabilidades envolvidas?
(3) **Aplicabilidade institucional**: o modelo é compatível com a estrutura organizacional, os recursos disponíveis e os fluxos de trabalho reais da ETIR/UFSM? Quais adaptações seriam necessárias para sua implementação prática?

O modelo BPMN foi compartilhado com os participantes previamente à realização da entrevista, em formato `.svg`. O envio incluiu um documento formal de apresentação. Este arquivo definiu os objetivos da pesquisa, a estrutura do artefato e as instruções de análise. As entrevistas foram realizadas no formato virtual. Cada sessão durou quarenta e cinco minutos. Todo o protocolo obedeceu aos princípios éticos de pesquisa com seres humanos.

3.5.3 Análise dos Dados. Os dados coletados nas entrevistas foram analisados por meio de análise de conteúdo temática [4]. Foram

definidas categorias *a priori* a partir dos três blocos do roteiro: adequação normativa, clareza e usabilidade, e aplicabilidade institucional. As contribuições dos especialistas foram sistematizadas para identificar pontos de convergência, divergências e sugestões de refinamento. A Seção 5 documenta e discute todos os ajustes finais aplicados ao modelo a partir desta validação.

3.6 Limitações do Método

A transparência acerca das limitações do método é fundamental para a manutenção do rigor acadêmico. Este estudo possui três limitações principais que precisam ser levadas em conta ao interpretar os resultados.

A primeira refere-se ao alcance da validação empírica. A avaliação baseou-se na percepção de especialistas da ETIR/UFSM, e não uma validação operacional completa. O método não incluiu a aplicação em cenários reais ou a observação direta dos fluxos operacionais da equipe. Trabalhos futuros devem aplicar simulações do modelo ou avaliar retrospectivamente incidentes geridos pela instituição.

A segunda limitação é a restrição do escopo normativo. A análise documental focou nos principais instrumentos normativos federais. O escopo abrangeu a LGPD, a Resolução CD/ANPD nº15/2024, o PPSI2.0 e o Guia da SGD. O método excluiu normativos internos detalhados da UFSM, como resoluções do Conselho Universitário e contratos com fornecedores. Trabalhos futuros devem incorporar esses documentos institucionais para aprimorar o modelo.

A terceira limitação envolve a generalização do artefato. A pesquisa utilizou a ETIR/UFSM como contexto prático inicial. Contudo, a base conceitual apoia-se em regulamentos federais. Esta característica permite aplicar a solução em outras universidades públicas. Entretanto, as instituições divergem em porte, recursos humanos e nível de maturidade cibernética. Estas variações exigem adaptações operacionais antes de replicar o fluxo em novos ambientes.

4 Modelo Proposto

Nesta seção, é apresentado o modelo de processo desenvolvido como artefato central desta pesquisa. O modelo representa, em notação BPMN 2.0, o fluxo de resposta a incidentes de segurança da informação da ETIR/UFSM, com a incorporação dos requisitos legais da Lei Geral de Proteção de Dados Pessoais (LGPD) e da Resolução CD/ANPD nº 15/2024. A seção está organizada em quatro partes: a visão geral do modelo, o detalhamento de cada fase do ciclo de resposta, a síntese dos requisitos normativos atendidos e as considerações sobre a implementação prática.

4.1 Visão Geral do Modelo

O modelo está organizado em duas pools (piscinas) que representam as organizações participantes do processo:

- **Pool ETIR/UFSM**: entidade responsável pela resposta ao incidente no âmbito institucional. Essa pool é subdividida em quatro lanes (raias), que segregam as responsabilidades internas:
  - **Equipe de Tratamento (ETIR)**: conjunto de profissionais que atuam de forma coordenada, conduzem as atividades técnicas de detecção, registro, classificação, análise, contenção, erradicação, recuperação e lições aprendidas, além de elaborar o Relatório de Tratamento do Incidente quando solicitado pela ANPD.
  - **Encarregado de Dados (DPO)**: responsável pelas obrigações legais decorrentes da LGPD - avaliação de risco ou dano relevante, elaboração e envio das notificações à ANPD e aos titulares, elaboração do Relatório Final de Incidente e guarda documental.
  - **Área Jurídica**: consulta facultativa pelo DPO para revisão jurídica das comunicações (não obrigatória).
  - **Gestão Institucional**: ciência das notificações e comunicações enviadas (não aprovação).
- **Pool ANPD**: representa a Agência Nacional de Proteção de Dados, destinatária das notificações de incidentes com dados pessoais e origem das solicitações de informações adicionais previstas no Art. 8º da Resolução CD/ANPD nº 15/2024.

As comunicações com o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) são representadas por uma tarefa de envio na lane da Equipe de Tratamento (ETIR), por se tratar de comunicação de saída que não demanda pool dedicado.

O fluxo do processo percorre as cinco fases do ciclo de resposta a incidentes - prevenção, detecção, triagem/análise, resposta (contenção, erradicação e recuperação) e pós-incidente. O acionamento ocorre por um evento de início na lane da Equipe de Tratamento (ETIR). A Figura 1 apresenta o diagrama BPMN completo. As subseções seguintes detalham cada fase com ênfase nos pontos de decisão (gateways) que ativam as obrigações legais da LGPD.

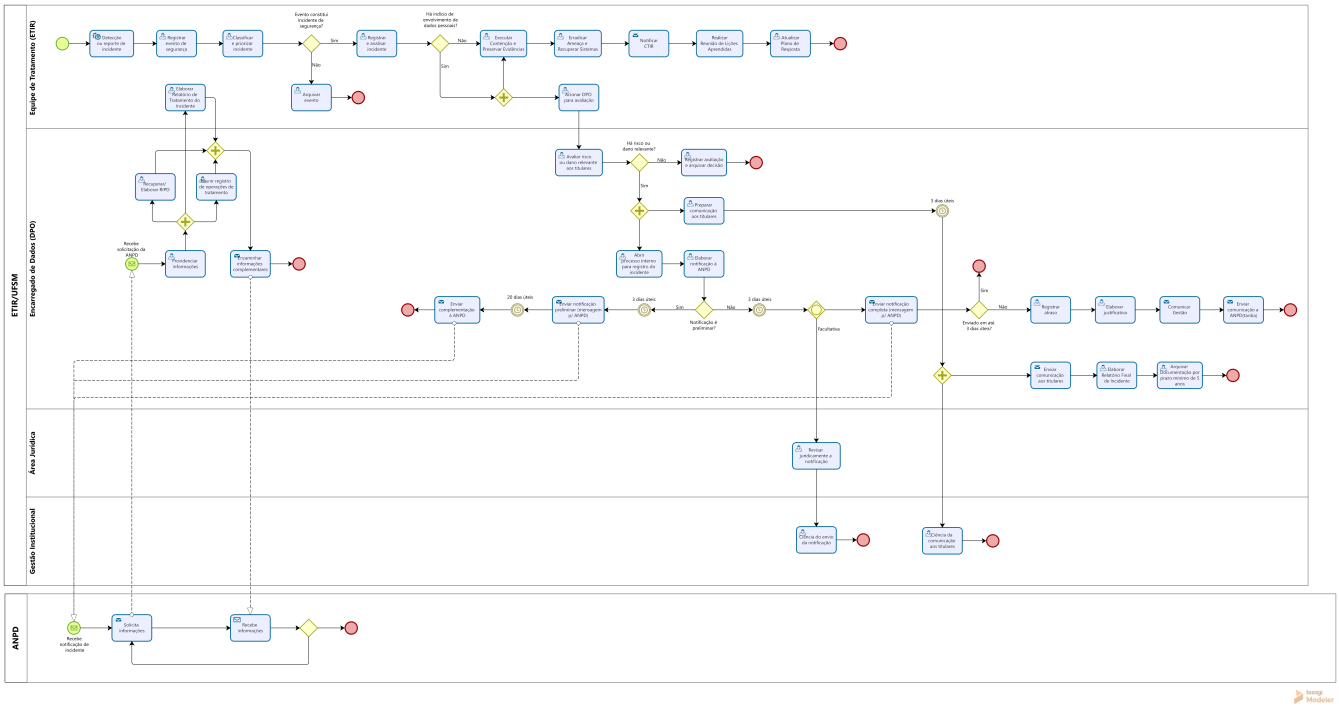

Figure 1: Modelo BPMN de resposta a incidentes integrado à LGPD — ETIR/UFSM.
Fonte: Elaborado pelo autor.

4.1.1 Elementos de Controle de Prazo. O modelo incorpora eventos intermediários temporizadores que representam os prazos regulatórios estabelecidos pela Resolução CD/ANPD nº 15/2024:

- **3 dias úteis**: prazo para comunicação preliminar à ANPD e aos titulares, contado a partir da ciência do incidente (Art. 6º, caput e Art. 9º). Presente nos dois caminhos da vertente legal(notificação preliminar, notificação completa e comunicação aos titulares).
- **20 dias úteis**: prazo para complementação fundamentada das informações, conforme faculdade prevista no Art. 6º, § 3º. Este prazo é representado no fluxo de notificação preliminar (Caminho A da Fase 4 – Resposta), onde um evento temporizador de 20 dias úteis aciona as tarefas de Elaborar complementação fundamentada e Enviar complementação à ANPD.
- **5 anos**: prazo mínimo de guarda documental obrigatória, representado pela tarefa Arquivar Documentação por prazo mínimo 5 Anos na fase pós-incidente (Art. 10).
- **Prazo definido pela ANPD**: prazo estabelecido pela agência ao solicitar informações adicionais com base no Art. 8º, representado no subprocesso de atendimento à solicitação externa.

Além disso, o modelo contempla a previsão do Art. 6º, § 3º, que faculta ao controlador, de maneira fundamentada, complementar as informações em até 20 dias úteis. Essa possibilidade é representada no fluxo de notificação preliminar (Caminho A da Fase 4 - Resposta), onde um evento temporizador de 20 dias úteis aciona as tarefas de Elaborar complementação fundamentada e Enviar complementação à ANPD. Dessa forma, o diagrama reflete a faculdade legal, mas sem torná-la uma etapa obrigatória do fluxo principal.

4.1.2 Mapeamento Geral das Fases e Gateways. O Quadro 4 apresenta o mapeamento entre as cinco fases do modelo, as atividades principais de cada etapa e as obrigações legais incorporadas.

O Quadro 5 detalha os cinco gateways críticos do modelo, com sua respectiva base normativa e consequências no fluxo.

4.2 Detalhamento das Fases do Processo

4.2.1 Fase 1 – Preparação. A fase de Preparação compreende atividades contínuas e anteriores à ocorrência de qualquer incidente, com o objetivo de garantir a prontidão operacional e legal da ETIR/UFSM. Por sua natureza preventiva e cíclica, essa fase não integra o fluxo reativo representado na Figura 1, mas constitui pré-requisito indispensável para seu funcionamento. As atividades previstas são:

- Manter o inventário de ativos e o mapeamento de dados pessoais: tarefa baseada nos Controles 1 e 19 do PPSI 2.0 e no princípio da responsabilização (Art. 6º, inciso X, LGPD). O inventário alimenta a avaliação de impacto realizada na fase de Análise.
- Elaborar e revisar periodicamente o Plano de Resposta a Incidentes: documento formal exigido pelo PLANGIC e pelas Medidas 17.4 e 20.1 do PPSI 2.0. Essa atividade constitui o

Table 4: Mapeamento entre fases do modelo, atividades e obrigações da LGPD

Fase	Atividades principais	Obrigação legal incorporada
Preparação	Manter inventário de ativos e dados pessoais; elaborar Plano de Resposta; capacitar ETIR; estabelecer canais com DPO e Área Jurídica; definir critérios evento vs. incidente	Arts. 46 e 50, § 2º, I, "g", da LGPD; PPSI 2.0, Controles 1 e 19, Medidas 17.1, 17.2, 17.4, 17.7, 17.9, 20.1, 20.2 e 20.3
Detecção e Triagem	Detecção ou reporte; registro do evento; classificação e priorização; Gateway G1 (evento constitui incidente?)	Art. 46 da LGPD; PLANGIC (Item 4.1 - Triagem); PPSI 2.0, Medidas 17.3, 17.4 e 17.9; ABNT NBR ISO/IEC 27035-1:2023 (Seções 5.3 e 5.4).
Análise e Avaliação de Impacto	Registro e análise técnica do incidente; Gateway G2 (envolve dados pessoais?); acionamento do DPO; avaliação de risco ou dano relevante; Gateway G3 (risco relevante?); documentação da avaliação	Arts. 41, 46 e 48 da LGPD; Resolução CD/ANPD nº 15/2024, Arts. 5º e 10, § 1º, V; PLANGIC (Item 4.2 - Análise); PPSI 2.0, Medidas 20.1 e 21.5.
Resposta	Vertente técnica: contenção, preservação de evidências, erradicação, recuperação, notificação ao CTIR Gov. Vertente legal – notificação à ANPD: Gateway G4 (notificação é preliminar?). • Preliminar: elaborar e enviar notificação preliminar (3 dias); prazo de 20 dias; elaborar e enviar complementação. • Completa: elaborar e enviar notificação completa (3 dias); Gateway G5 (envio completo dentro do prazo?); se não, subfluxo de atraso. Vertente legal – comunicação aos titulares: preparar comunicação (3 dias); enviar; dar ciência à Gestão (sem gateway de aprovação).	Arts. 6º (inciso X), 48 e 50 da LGPD; Resolução CD/ANPD nº 15/2024, Arts. 6º, 7º e 9º; PLANGIC (Itens 5.1, 5.2 e 5.3); PPSI 2.0, Medidas 17.4 e 20.1.
Pós-incidente	Elaboração do Relatório Final (DPO); arquivamento por prazo mínimo de 5 anos; reunião de lições aprendidas e atualização do Plano de Resposta (Equipe de Tratamento e DPO); subprocesso de atendimento à solicitação da ANPD, acionado por Evento de Início de Mensagem (Recebe solicitação da ANPD) e com tarefas de envio de RIPD, registro de operações de tratamento e relatório de tratamento do incidente	Arts. 6º (inciso X), 37 e 38 da LGPD; Resolução CD/ANPD nº 15/2024, Arts. 8º e 10; PLANGIC (Item 6); PPSI 2.0, Medida 17.8; ABNT NBR ISO/IEC 27035-1:2023 (Seção 5.6).

Fonte: Elaborado pelo autor.

atendimento direto à exigência legal da LGPD de que a organização possua planos de resposta a incidentes e remediação (Art. 50, § 2º, inciso I, alínea "g").

- Capacitar membros da ETIR e demais stakeholders: atividade alinhada às Medidas 17.7, 20.2 e 20.3 do PPSI 2.0, com foco em planejar e conduzir exercícios simulados de tratamento de incidentes, bem como sensibilizar e treinar os agentes públicos sobre papéis e responsabilidades na resposta a incidentes com dados pessoais.
- Estabelecer canais de comunicação com o DPO e a Área Jurídica: tarefa que atende às Medidas 17.1 e 17.2 do PPSI 2.0 (exigência de informações de contato institucionais para notificação) e materializa o modelo de autonomia compartilhada definido na PoSIN/UFSM (Art. 61).
- Definir critérios formais para distinção entre evento e incidente: exigência da Medida 17.9 do PPSI 2.0.

Do ponto de vista legal, a fase de Preparação operacionaliza o dever geral de segurança estabelecido pelo Art. 46 da LGPD, aliado ao dever de governança exigido pelo Art. 50. A existência de uma fase preventiva estruturada é, portanto, simultaneamente uma boa prática técnica e uma exigência legal.

4.2.2 Fase 2 – Detecção e Triagem. Esta fase inicia com a chegada de um alerta ou notificação de possível incidente, representada por um evento de início na lane da Equipe de Tratamento (ETIR). As atividades desta fase são:

(1) Detecção ou reporte de incidente: tarefa que representa o acionamento do processo, podendo originar-se de sistemas automatizados, usuários ou comunicações externas, conforme a Medida 17.3 do PPSI 2.0 e a Seção 5.3 da ABNT NBR ISO/IEC 27035-1:2023.
(2) Registrar evento de segurança: tarefa que assegura a rastreabilidade do incidente no sistema de gestão, em atendimento ao Art. 46 da LGPD e à Medida 17.4 do PPSI 2.0.
(3) Classificar e priorizar incidentes: tarefa que utiliza os critérios definidos na fase de Preparação, que classifica o evento quanto à severidade e ao tipo de ameaça. Essa atividade é uma exigência explícita do Item 4.1 (Triagem) do PLANGIC, que determina à ETIR o estabelecimento de prioridades e a classificação do incidente cibernético em níveis (crítico, alto, médio ou baixo).

Table 5: Gateways críticos do modelo e suas implicações legais

ID	Pergunta decisória / Evento	Tipo BPMN	Base normativa	Consequências
G1	O evento registrado constitui um incidente de segurança?	Exclusivo (XOR)	PPSI 2.0, Medidas 17.4 e 17.9; ISO/IEC 27035-1:2023	Sim: avança para análise e verificação de escopo. Não: arquivamento com registro e encerramento.
G2	Há indício de envolvimento de dados pessoais?	Exclusivo (XOR)	Arts. 1º e 5º, inciso X e Art. 41 da LGPD; PPSI 2.0, Medida 20.1	Sim: bifurcação AND — aciona DPO e executa contenção técnica em paralelo; inicia contagem do prazo de 3 dias úteis. Não: fluxo exclusivamente técnico; comunicação ao CTIR Gov.
G3	Há risco ou dano relevante aos titulares?	Exclusivo (XOR)	Art. 48 da LGPD; Res. CD/ANPD nº 15/2024, Arts. 5º e 10, § 1º, inciso V	Sim: bifurcação AND — elaboração e envio de notificação à ANPD e preparação da comunicação aos titulares em paralelo. Não: avaliação documentada e arquivada; notificação dispensada.
G4	Notificação é preliminar?	Exclusivo (XOR)	Resolução CD/ANPD nº 15/2024, Art. 6º, caput, § 3º e 4º; orientação da ANPD sobre comunicação em etapas	Sim: fluxo de notificação preliminar (envio em 3 dias, complementação em até 20 dias). Não: fluxo de notificação completa.
G5	Notificação completa enviada em até 3 dias úteis? (aplica-se apenas ao fluxo completo)	Exclusivo (XOR)	Resolução CD/ANPD nº 15/2024, Art. 6º, caput e § 2º, inciso V	Sim: encerra o subfluxo da notificação completa; o processo prossegue pela vertente de comunicação aos titulares. Não: aciona subfluxo de gestão do atraso (registro, justificativa, comunicação à Gestão, envio tardio) e encerra o subfluxo.

Fonte: Elaborado pelo autor com base na LGPD e na Resolução CD/ANPD nº 15/2024.

O primeiro ponto de decisão crítico é o Gateway G1 ("Evento constitui incidente de segurança?"), do tipo exclusivo (XOR), fundamentado na Medida 17.9 do PPSI 2.0 e nas diretrizes de avaliação da ABNT NBR ISO/IEC 27035-1:2023. Quando o evento não atende aos critérios definidos, ele é encerrado com registro e arquivamento. Caso seja confirmado como incidente, o fluxo avança para a fase de Análise.

4.2.3 Fase 3 – Análise e Avaliação de Impacto. Nesta fase, as lanes da Equipe de Tratamento (ETIR) e do DPO atuam de forma colaborativa para determinar a natureza e o impacto do incidente. A atividade inicial é o Registro e análise do incidente, conduzida pela Equipe de Tratamento (ETIR), que identifica o vetor de ataque, os sistemas afetados e o escopo do comprometimento. Esta etapa é fundamentada tecnicamente no Item 4.2 (Análise) do PLANGIC e na Medida 20.1 do PPSI 2.0, que exige o adequado registro do incidente com foco em proteção de dados.

O segundo ponto de decisão crítico é o Gateway G2 ("Há indício de envolvimento de dados pessoais?"), do tipo exclusivo (XOR), baseado no próprio escopo de aplicação material da LGPD. Este é o principal gatilho legal do modelo. A resposta afirmativa bifurca o fluxo em um gateway paralelo (AND). Duas vertentes são acionadas: a técnica, pela ETIR, e a jurídico-normativa, pelo DPO. A partir deste ponto, inicia-se também a contagem do prazo de três dias úteis para a comunicação à ANPD, conforme o Art. 6º da Resolução CD/ANPD nº 15/2024. Quando o incidente não envolve dados pessoais, o fluxo segue pela dimensão técnica, com comunicação ao CTIR Gov por meio da tarefa Notificar CTIR.

Subfluxo LGPD - Avaliação de Risco ou Dano Relevante. Quando o Gateway G2 indica envolvimento de dados pessoais, o DPO é acionado pela tarefa Acionar DPO para avaliação. Esta ação materializa o comando do Art. 41 da LGPD e atende à Medida 21.5 do PPSI 2.0, que determina à organização solicitar a assistência e a orientação do encarregado em decisões estratégicas referentes ao tratamento de dados. Em seguida, o encarregado conduz a tarefa Avaliar risco ou dano relevante aos titulares, obrigatória nos termos do Art. 48 da LGPD e do Art. 5º da Resolução CD/ANPD nº 15/2024. O modelo inclui anotação de texto com os fatores agravantes definidos pela referida Resolução.

O terceiro ponto de decisão é o Gateway G3 (“Há risco ou dano relevante?”), do tipo exclusivo (XOR). Quando o risco não é caracterizado, a avaliação é documentada e arquivada pela tarefa Registrar avaliação e arquivar decisão, em atendimento ao Art. 10, § 1º, inciso V, da Resolução CD/ANPD nº 15/2024. O fluxo legal é, então, encerrado, enquanto a vertente técnica prossegue. Quando o risco é considerado relevante, um novo gateway paralelo (AND) bifurca o processo em duas atividades simultâneas e independentes, ambas sujeitas ao prazo de 3 dias úteis: a elaboração da notificação à

ANPD e a preparação da comunicação aos titulares, descritas na fase seguinte.

4.2.4 Fase 4 – Resposta. A fase de Resposta é executada em duas vertentes paralelas, coordenadas pelo gateway AND de abertura acionado pelo G2 e, quando há risco relevante, pelo AND acionado pelo G3. A integração dessas duas frentes no desenho do processo atende à Medida 20.1 do PPSI 2.0, que exige que o plano de resposta aborde funções e responsabilidades sobre a eventual comunicação à ANPD e aos titulares.

Vertente Técnica (Equipe de Tratamento (ETIR)):.

- Executar contenção e preservar evidências: ações imediatas para interromper a progressão do incidente, com preservação obrigatória das evidências que possam subsidiar processos administrativos ou judiciais, conforme as diretrizes do Item 5.1 do PLANGIC, o Art. 46 da LGPD e a Medida 17.4 do PPSI 2.0 (que exige o adequado registro das evidências do incidente).
- Erradicar ameaças e recuperar sistemas: a remoção completa do agente causador e a restauração das operações a partir de backups íntegros obedecem às atividades dos Itens 5.2 e 5.3 do PLANGIC.
- Notificar o CTIR Gov: comunicação obrigatória ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, conforme a Medida 17.2 do PPSI 2.0 e a exigência do Item 5.3 do PLANGIC, que determina o envio de um relatório detalhado após o término do processo de recuperação.

Vertente Legal (DPO, Área Jurídica e Gestão Institucional): Após o AND de abertura do G3, dois fluxos são executados em paralelo; a notificação à ANPD e a comunicação aos titulares.
Caminho A – Notificação à ANPD Logo após o G3 (Sim), o DPO avalia se dispõe de todas as informações necessárias para uma notificação completa. O Gateway G4 (XOR), "Notificação é preliminar?", define o fluxo:

- **Fluxo de notificação preliminar**
  (1) Elaborar notificação preliminar à ANPD: preenchimento do formulário resumido com a justificativa da indisponibilidade de informações completas, conforme orientação da ANPD em sua página oficial de comunicação de incidentes [3].
  (2) Evento temporizador de 3 dias úteis: prazo para envio da preliminar (Art. 6º, caput, da Resolução CD/ANPD nº 15/2024) .
  (3) Enviar notificação preliminar à ANPD (evento de mensagem para a pool da ANPD).
  (4) Evento temporizador de 20 dias úteis: prazo para complementação fundamentada (Art. 6º, § 3º, da Resolução).
  (5) Elaborar complementação fundamentada (DPO).
  (6) Enviar complementação à ANPD.
  (7) Encerramento do subfluxo preliminar (não há gateway de verificação de atraso neste caminho, pois o envio da preliminar dentro dos 3 dias já cumpre a obrigação legal).
- **Fluxo de notificação completa**
  (1) Elaborar notificação completa à ANPD: produção do relatório com os elementos mínimos exigidos pelo Art. 6º, § 2º, da Resolução CD/ANPD nº 15/2024. O controlador pode também, nesta etapa, solicitar à autoridade o sigilo de informações protegidas, em observância ao Art. 7º da Resolução.
  (2) Evento temporizador de 3 dias úteis.
  (3) Um gateway OR Inclusivo permite que o DPO, facultativamente, submeta a notificação à Área Jurídica para revisão. Caso opte pela revisão, o fluxo segue para a tarefa "Revisar juridicamente a notificação" e depois para o envio. Caso contrário, o fluxo segue diretamente para o envio.
  (4) Enviar notificação completa (mensagem p/ ANPD).
  (5) Gateway G5 (XOR) – "Notificação completa enviada em até 3 dias úteis?"
    – **Sim:** o subfluxo de notificação completa é encerrado; o processo principal prossegue pela vertente de comunicação aos titulares e pós-incidente.
    – **Não:** aciona o subfluxo de gestão do atraso: Registrar atraso → Elaborar justificativa → Comunicar Gestão Institucional → Enviar comunicação à ANPD (tardia). Em seguida, o subfluxo é encerrado.

    Esse tratamento de exceção garante a transparência e a documentação adequada, em conformidade com o Art. 6º, § 2º, inciso V, da Resolução.

Nota: O G5 aplica-se apenas ao envio da notificação completa. O fluxo preliminar não possui essa verificação, pois a comunicação preliminar já satisfaz o prazo legal, e a complementação tem prazo próprio de 20 dias.
Caminho B – Comunicação aos titulares O fluxo da comunicação aos titulares é acionado pelo AND do G3, podendo passar por um gateway convergente que recebe eventuais retornos de revisão (quando o DPO optar por consultar a Área Jurídica antes do envio, de forma facultativa).

(1) Preparar comunicação aos titulares (DPO): elaboração da comunicação com linguagem simples e acessível, em cumprimento ao Art. 9º da Resolução CD/ANPD nº 15/2024.
(2) Evento temporizador de 3 dias úteis.
(3) Analisar comunicação aos titulares (DPO): o DPO pode, se julgar necessário, submeter a comunicação a uma revisão da Área Jurídica ou da Gestão, porém não há gateway obrigatório de aprovação. O DPO tem autonomia para enviar a comunicação diretamente.
(4) Enviar comunicação aos titulares (DPO).
(5) Dar ciência à Gestão Institucional: tarefa paralela ou subsequente que informa a alta administração sobre o envio da comunicação, para fins de governança e prestação de contas (Art. 50 da LGPD), sem que isso constitua etapa de aprovação.

Após a conclusão de ambas as vertentes (técnica e legal), seus fluxos convergem para a fase pós-incidente.

4.2.5 Fase 5 – Pós-incidente. A fase de Pós-incidente é responsável por consolidar aprendizados e assegurar o cumprimento das obrigações de documentação e prestação de contas (Art. 6º, inciso X, da LGPD). Ela é distribuída entre as lanes da Equipe de Tratamento (ETIR) e do DPO, com a possibilidade de acionamento condicional de solicitações externas.

Na lane do DPO:

(1) Elaborar Relatório Final de Incidente: documento único que consolida as ações técnicas, a avaliação de risco, as comunicações realizadas e as evidências coletadas. Embora a resposta a incidentes seja um esforço colaborativo, a consolidação final é de responsabilidade do DPO, que traduz os insumos técnicos fornecidos pela Equipe de Tratamento (ETIR) para a linguagem de conformidade legal exigida pela LGPD. Quando houver atendimento a uma solicitação da ANPD (Art. 8º), o Relatório de Tratamento do Incidente elaborado pela Equipe de Tratamento (ETIR) servirá como insumo primário para este Relatório Final.
(2) Arquivar Documentação por 5 Anos: tarefa que atende ao Art. 10 da Resolução CD/ANPD nº 15/2024.
(3) Subprocesso de Atendimento à Solicitação da ANPD (Art. 8º): A comunicação é modelada por meio de um Evento de Início de Mensagem (Recebe solicitação da ANPD), posicionado na lane do DPO. A solicitação origina-se na tarefa Solicita informações, localizada na pool da ANPD, e chega ao DPO por meio de um fluxo de mensagem (seta tracejada). Uma vez acionado, o subprocesso executa tarefas amparadas nos Arts. 37 e 38 da LGPD, tais como:
    - Providenciar informações (DPO);
    - Recuperar/Elaborar RIPD (DPO): recuperação ou elaboração do Relatório de Impacto à Proteção de Dados Pessoais (Art. 38 da LGPD), documento preventivo que descreve os processos de tratamento e as salvaguardas adotadas pela organização;
    - Reunir registro de operações de tratamento (DPO): em cumprimento ao Art. 37 da LGPD;
    - Elaborar Relatório de Tratamento do Incidente (Equipe de Tratamento (ETIR)): documento reativo que detalha o evento adverso ocorrido e as providências de contenção e mitigação adotadas.
    - Encaminhar informações complementares (DPO): envio das informações à ANPD, respeitando o prazo definido pela autoridade. Essa distinção reflete a diferença fundamental entre o RIPD (preventivo) e o relatório de tratamento (reativo). Ambos são instrumentos de accountability que a ANPD pode requerer a qualquer momento, conforme o Art. 8º.

Na lane da Equipe de Tratamento (ETIR):

(1) Realizar Reunião de Lições Aprendidas: atividade prevista na ISO/IEC 27035-1:2023 e no PLANGIC, com registro formal das melhorias identificadas.
(2) Atualizar Plano de Resposta a Incidentes: retroalimentação do processo de preparação, fecha o ciclo de melhoria contínua, conforme exigido pela Medida 17.8 do PPSI 2.0 e pelo Item 6 do PLANGIC.

O processo encerra-se com eventos de fim em cada uma das lanes do DPO e da Equipe de Tratamento (ETIR), após a conclusão de todas as atividades pós-incidente.

4.3 Síntese dos Requisitos Normativos Atendidos pelo Modelo

A conformidade regulatória em segurança da informação e privacidade não se materializa apenas pela existência de políticas, mas pela sua integração aos processos de trabalho. Com o objetivo de demonstrar a rastreabilidade entre as exigências legais e a solução técnica, o Quadro 6 sumariza como os principais pontos da LGPD, da Resolução CD/ANPD nº 15/2024, do PLANGIC e do PPSI 2.0 foram operacionalizados e convertidos em artefatos e decisões no modelo BPMN proposto.

Table 6: Requisitos normativos atendidos pelo modelo BPMN

Requisito Normativo	Fonte	Como o modelo atende
Dever geral de segurança (medidas técnicas e administrativas)	Art. 46, LGPD	Fluxo completo de resposta, com segregação de responsabilidades e preservação de evidências.
Comunicação de incidente à ANPD – prazo de 3 dias úteis	Art. 6º, caput, Res. ANPD 15/2024	Evento temporizador de 3 dias no fluxo de notificação (tanto preliminar quanto completa).
Comunicação em duas etapas (preliminar + complementar)	Art. 6º, § 3º, Res. ANPD 15/2024; orientação da ANPD	Gateway G4 separa os fluxos; no preliminar, temporizador de 20 dias para complementação.
Tratamento de exceção por atraso na notificação completa	Art. 6º, § 2º, inciso V, Res. ANPD 15/2024	Gateway G5 com subfluxo de gestão do atraso (registro, justificativa, comunicação à Gestão, envio tardio).
Comunicação aos titulares em até 3 dias úteis	Art. 9º, Res. ANPD 15/2024	Evento temporizador de 3 dias no fluxo de comunicação aos titulares; envio direto pelo DPO com ciência à Gestão (sem gateway de aprovação).
Avaliação de risco ou dano relevante (critérios do Art. 5º)	Art. 5º, Res. ANPD 15/2024	Gateway G3 com anotação dos fatores agravantes; tarefa de documentação da avaliação.
Conteúdo mínimo da notificação	Art. 6º, § 2º, Res. ANPD 15/2024	Tarefa de elaboração de notificação com campos padronizados (formulário da ANPD).
Solicitação de informações adicionais pela ANPD (registro de operações, RIPD, relatório de tratamento)	Art. 8º, Res. ANPD 15/2024	Evento de Início de Mensagem que captura a solicitação da ANPD; Gateway Paralelo (AND) que aciona três tarefas paralelas (RIPD, registro de operações, relatório de tratamento); sincronização e envio com prazo definido pela ANPD.
Guarda de registros por prazo mínimo de 5 anos	Art. 10, Res. ANPD 15/2024	Tarefa Arquivar Documentação por prazo mínimo de 5 anos (ou conforme tabela de temporalidade do CONARQ) na fase pós-incidente, na lane do DPO.
Formalização da ETIR e definição de responsabilidades	Medida 0.8 e Controle 17(Medidas 17.1 e 17.2), PPSI 2.0	Lanes segregadas para Equipe de Tratamento (ETIR), DPO, Área Jurídica e Gestão Institucional.
Comunicação com CTIR Gov	Medida 17.2, PPSI 2.0; PLANGIC	Tarefa Notificar CTIR na lane da Equipe de Tratamento (ETIR).
Plano de resposta formalizado e testado; melhoria contínua	Controle 17, Medidas 17.7 e 17.8, PPSI 2.0	Atividades de preparação, reunião de lições aprendidas e atualização do Plano de Resposta.
Autonomia do DPO e governança	Art. 41 e Art. 50, LGPD	DPO decide sobre o envio de notificações e comunicações; Gestão recebe ciência.

Fonte: Elaborado pelo autor.

4.4 Considerações sobre a Implementação Prática

O modelo proposto foi concebido como um artefato TO-BE e representa a situação desejada de integração entre a resposta técnica e as obrigações legais. Para sua efetiva implantação na ETIR/UFSM, recomenda-se:

- Formalização normativa interna: a publicação de portaria ou resolução pela Reitoria, a validação do fluxo e o estabelecimento de prazos internos máximos para cada etapa são essenciais para garantir a adesão institucional e o cumprimento de prazos. Essa medida atende ao Art. 50 da LGPD (governança) e ao Acórdão TCU nº 1.372/2025.
- A capacitação dos membros da ETIR, do DPO e demais stakeholders não apenas nos elementos BPMN e nos prazos e critérios da Resolução CD/ANPD nº 15/2024, mas também em seus respectivos papéis de atuação conjunta, em atendimento direto às Medidas 20.2 e 20.3 do PPSI 2.0
- A adoção de uma ferramenta de workflow que suporte a execução do modelo para automatizar notificações e gateways temporais (ex.: uso de plataformas de orquestração de processos ou sistemas de ticket com plugins BPMN). A automação sistêmica é fundamental para assegurar o "adequado registro das evidências no sistema de gestão", conforme exigido pela Medida 17.4 do PPSI 2.0, e para materializar o princípio da responsabilização e prestação de contas (Art. 6º, inciso X, da LGPD).
- A realização periódica de simulações (tabletop exercises) baseadas no modelo que visa testar a integração entre a resposta técnica e o acionamento legal, conforme previsto na Medida 17.7 do PPSI 2.0 e recomendado pela norma ABNT NBR ISO/IEC 27035-1:2023.

O modelo unifica a equipe técnica sob a designação "Equipe de Tratamento (ETIR)", conforme o Art. 51 da PoSIN/UFSM. Na implantação, a UFSM pode desdobrá-la em duas frentes: a Equipe Central (coordenação, triagem e CTIR Gov) e a Equipe Descentralizada (contenção e recuperação local), nos termos do Art. 53. Esse refinamento não altera o fluxo e pode ser incorporado em normativos internos.

A validação qualitativa do modelo com os especialistas da UFSM, que é apresentada e discutida na Seção 5, traz também contribuições empíricas sobre as barreiras institucionais e os aprimoramentos que o modelo ainda precisa para se adequar plenamente à realidade operacional da instituição.

5 Resultados e Discussão

Este capítulo analisa os resultados da validação do modelo BPMN proposto, confrontando-os com a literatura e com as evidências empíricas sobre a maturidade da gestão de incidentes na Administração Pública Federal. Discutem-se a adequação normativa, a clareza, a usabilidade e a aplicabilidade institucional do artefato, além dos desafios para sua implementação na ETIR/UFSM. Ao final, são apresentadas as limitações do estudo, as recomendações para trabalhos futuros.

5.1 Síntese da validação

A validação do modelo foi conduzida por meio de entrevistas semiestruturadas com três especialistas da UFSM: o Coordenador da ETIR, o Gestor de SI e a Encarregada de Dados (DPO). O roteiro de perguntas seguiu os três blocos definidos na metodologia (Seção 3.5.2): adequação normativa, clareza e usabilidade, e aplicabilidade institucional.

Os três especialistas possuem atuação direta e continuada nas dimensões técnica, operacional e jurídico-normativa da gestão de incidentes na UFSM, o que os qualifica para avaliar o modelo nas três dimensões propostas na metodologia.

De modo geral, os especialistas reconheceram que o modelo atende plenamente às obrigações da LGPD e da Resolução CD/ANPD nº 15/2024. Todos os dispositivos avaliados (Arts. 46, 48, e os Arts. 5º, 6º, 8º, 9º e 10 da Resolução) foram considerados corretamente representados, o que era esperado em razão da análise documental prévia(Seção 3.3).

As principais contribuições positivas apontadas foram:

- A divisão clara de responsabilidades entre as raias (Equipe de Tratamento, DPO, Área Jurídica, Gestão Institucional).
- O uso do fluxo paralelo (AND) que permite a contenção técnica e a comunicação legal ocorrerem simultaneamente, sem que uma etapa trave a outra.
- A previsão do subprocesso do Art. 8º (solicitação de informações adicionais pela ANPD), elogiado como um dos pontos fortes do modelo.

5.2 Adequação normativa do modelo

A validação confirmou que o modelo incorpora corretamente os requisitos legais aplicáveis à resposta a incidentes com dados pessoais. O Coordenador da ETIR, o Gestor de SI e a DPO atestaram que todos os gatilhos e prazos estão representados de acordo com a Resolução CD/ANPD nº 15/2024. O Gestor de SI destacou, em particular, a importância do tratamento de atraso e do loop de reprovação como mecanismos de conformidade.

A DPO destacou que, na prática da UFSM, a notificação à ANPD já é realizada em duas etapas: preliminar (dentro de 3 dias) e complementar (em até 20 dias), conforme faculta o Art. 6º, § 3º da Resolução. Essa constatação levou à inclusão, no modelo, de um gateway específico ("Notificação é preliminar?"), de temporizadores de 3 e 20 dias e de tarefas para a elaboração e envio da complementação, alinhando o artefato à realidade operacional da instituição.

Um ponto de refinamento adicional surgiu na fala da DPO: a necessidade de explicitar a abertura de um processo administrativo interno para consolidar o dossiê do incidente, em atendimento ao Art. 37 da LGPD (registro das operações de tratamento). Esse ajuste foi incorporado ao modelo (Seção 4.1) e fortalece a rastreabilidade e a *accountability*.

5.3 Clareza e usabilidade

A clareza do diagrama BPMN foi avaliada como boa, porém com ressalvas. O Coordenador e o Gestor de SI apontaram que a região de aprovações finais apresenta muitas linhas cruzadas, o que pode

dificultar a leitura por profissionais não familiarizados com a notação. Esse comentário levou a uma reorganização parcial do layout no Bizagi, mas manteve a estrutura lógica do fluxo.

A principal sugestão de melhoria veio da DPO e do Gestor de SI: a necessidade de identificar as ferramentas utilizadas em cada tarefa. Essa recomendação foi incorporada à Seção 4.4 como uma orientação para a UFSM.

Quanto à legibilidade geral, os três especialistas concordaram que o modelo é adequado à complexidade do processo e que não há excesso de informações. A renomeação da raia "Analista de Incidentes" para "Equipe de Tratamento (ETIR)" – sugerida pelos especialistas – foi adotada e contribuiu para uma representação mais fiel da estrutura organizacional da UFSM.

5.4 Aplicabilidade institucional e desafios de implementação

A DPO e os especialistas da ETIR apontaram que o modelo é compatível com a estrutura da PoSIN/UFSM e com as ferramentas utilizadas internamente. No entanto, destacaram desafios importantes:

- A equipe técnica da ETIR é enxuta e sobrecarregada, e a operacionalização do fluxo exigirá capacitação imediata e mudança de cultura (evitar que a TI só avise o DPO após o relatório final estar pronto).
- O prazo de três dias úteis para a notificação, embora legal, é desafiador diante da necessidade de aprovações internas e da ocorrência de feriados, greves ou dias facultativos.
- A formalização normativa (portaria ou resolução) é imprescindível para definir prazos internos (SLAs) e responsabilidades.

Esses desafios não invalidam o modelo, mas indicam que sua implementação bem-sucedida dependerá de um compromisso institucional com a alocação de recursos, treinamento e automação de workflows.

5.5 Comparação com trabalhos relacionados

O modelo proposto avança em relação aos estudos anteriores em pelo menos três aspectos.

Primeiro, enquanto Silva Filho & Afonseca (2025) [18] propuseram um modelo genérico e adaptável de integração entre a ISO/IEC 27002 e a LGPD, o presente trabalho operacionaliza a integração no contexto específico das ETIRs de universidades federais, adotando o PPSI 2.0 como referencial normativo e utilizando a UFSM como estudo de caso. Essa contextualização aumenta a relevância prática do artefato para o público-alvo.

Segundo, Woods & Böhme (2022) [25] identificaram uma tensão estrutural entre a lógica técnica da resposta a incidentes (contenção rápida) e a lógica jurídica (documentação rigorosa). O modelo BPMN aqui apresentado resolve essa tensão por meio de um fluxo paralelo (AND), no qual a contenção técnica e a comunicação legal ocorrem simultaneamente, sem que uma atividade dependa da conclusão da outra. Essa solução de modelagem é inovadora no âmbito da gestão de incidentes no setor público brasileiro.

Terceiro, Zaguir et al. (2024) [27] denominaram *implementation roadmap gap* a dificuldade de traduzir princípios legais em práticas operacionais. O presente trabalho demonstra que a modelagem em BPMN, quando ancorada em uma análise documental sistemática, é capaz de preencher essa lacuna, fornecendo um artefato visual e auditável que conecta diretamente cada requisito normativo a atividades e decisões concretas.

Além disso, o estudo alinha-se às recomendações de Spósito et al. (2025) [19], que apontam a necessidade de maior integração entre requisitos de privacidade e processos organizacionais, bem como de validação empírica desses artefatos junto aos profissionais da área. Diferentemente do método LGPD4BP de Araújo et al. (2021) [1], que se concentra na adequação de processos administrativos em geral, o presente modelo foca no domínio crítico da resposta a incidentes de segurança com dados pessoais, oferecendo uma solução validada para o contexto das ETIRs.

Esses avanços, aliados à validação empírica com os profissionais da ETIR e da DPO da UFSM, posicionam o modelo como uma contribuição original e aplicável ao contexto das instituições públicas de ensino superior.

5.6 Limitações do estudo e trabalhos futuros

Este estudo apresenta as seguintes limitações, que devem ser consideradas na interpretação dos resultados:

- **Validação baseada em percepção:** A avaliação do modelo restringiu-se a entrevistas com três especialistas, sem implementação em um incidente real. Estudos futuros poderiam conduzir simulações (*tabletop exercises*) ou um piloto operacional.
- **Escopo normativo restrito:** A análise concentrou-se nos documentos federais (LGPD, Resolução ANPD, PPSI 2.0, PLANGIC, PoSIN). Normativos internos detalhados (contratos com operadores, regimentos internos) não foram examinados, mas podem influenciar a implementação.
- **Generalização limitada:** Embora o modelo seja baseado em regulamentações federais, sua aplicação a outras universidades exigirá adaptações ao porte, à maturidade cibernética e à estrutura organizacional de cada instituição.

Com base nos achados e nas limitações, sugerem-se as seguintes direções para pesquisas futuras:

- **Automação e simulação:** Implementar o modelo em uma ferramenta de workflow e medir o impacto no cumprimento dos prazos legais.
- **Detalhamento da estrutura mista da ETIR:** Desdobrar a raia "Equipe de Tratamento" em Equipe Central e Equipe Descentralizada, conforme previsto na PoSIN/UFSM, e validar esse refinamento em simulações.
- **Validação em múltiplas instituições:** Aplicar o modelo em outras universidades federais e órgãos públicos para verificar sua generalização e identificar adaptações necessárias.
- **Avaliação longitudinal:** Acompanhar a utilização do modelo ao longo de incidentes reais, documentando gargalos, desvios e lições aprendidas.

5.7 Síntese da discussão

A validação empírica do modelo BPMN demonstrou que o artefato é normativamente consistente e atendeu a todos os requisitos da LGPD e da Resolução CD/ANPD nº 15/2024 avaliados. As contribuições dos especialistas da ETIR e da DPO permitiram refinar o modelo em aspectos práticos fundamentais: a separação entre a

notificação preliminar e a completa, o tratamento de exceção por atraso apenas na notificação completa, a autonomia do DPO na comunicação aos titulares (com ciência, não aprovação, da Gestão), e a abertura de processo administrativo para consolidação do dossiê.

Os principais desafios de aplicabilidade residem na insuficiência de recursos humanos e de automação, bem como na tensão entre o prazo regulatório de três dias úteis e a capacidade operacional atual da UFSM. Essas barreiras não invalidam o modelo; ao contrário, evidenciam a necessidade de investimentos institucionais paralelos para que o *dever ser* normativo se converta em prática efetiva.

O modelo, portanto, cumpre seu papel como artefato *TO-BE* – um guia para o estado desejado que, ao mesmo tempo, explicita as lacunas a serem superadas. A pergunta de pesquisa que orientou este trabalho foi respondida. O diagrama BPMN resultante não apenas documenta o fluxo integrado, mas serve como instrumento de governança, capacitação e eventual automação, e pode ser adotado como referência não apenas pela UFSM, mas por outras instituições públicas que enfrentam desafios semelhantes na integração entre resposta técnica e obrigações legais de privacidade.

6 Considerações Finais

Este trabalho partiu de uma pergunta de pesquisa objetiva: como integrar, de maneira prática e estruturada, os requisitos da LGPD aos processos de gestão de incidentes de segurança da informação, considerando as particularidades do setor público?

A resposta produzida é um modelo de processo em notação BPMN 2.0, desenvolvido a partir de análise documental sistemática e validado empiricamente com especialistas da ETIR/UFSM, que integra a dimensão técnica da resposta a incidentes às obrigações legais da LGPD e da Resolução CD/ANPD nº 15/2024.

A fundamentação teórica evidenciou que o arcabouço normativo brasileiro é abrangente em suas diretrizes, mas deixa uma lacuna operacional significativa na sua tradução em fluxos concretos de trabalho. Essa lacuna, empiricamente confirmada pelo Acórdão TCU nº 1.372/2025, que apontou que 64,6% das organizações federais auditadas não possuem processos padronizados de comunicação à ANPD, foi o ponto de partida e a principal motivação deste estudo.

O modelo proposto estrutura o ciclo de resposta em cinco fases, com responsabilidades segregadas em quatro *lanes*: Equipe de Tratamento (ETIR), Encarregado de Dados (DPO), Área Jurídica e Gestão Institucional. Entre seus principais diferenciais técnicos e normativos, destacam-se:

(1) o *gateway* paralelo (AND) que permite a contenção técnica e a comunicação legal ocorrerem simultaneamente, eliminando a dependência sequencial que compromete o cumprimento dos prazos legais;
(2) a distinção entre notificação preliminar e complementar à ANPD, com temporizadores de 3 e 20 dias úteis, alinhada à prática real da UFSM e ao Art. 6º, § 3º, da Resolução;
(3) o tratamento de exceção por atraso na notificação completa, com registro de justificativa e comunicação à Gestão Institucional;
(4) a autonomia do DPO na comunicação aos titulares, substituindo a aprovação institucional por uma notificação de ciência à Gestão, em conformidade com o Art. 41 da LGPD; e
(5) o subprocesso de atendimento à solicitação da ANPD (Art. 8º), com execução paralela das tarefas de RIPD, registro de operações de tratamento e relatório de tratamento do incidente.

A validação empírica, conduzida por meio de entrevistas semiestruturadas com o Coordenador da ETIR, o Gestor de SI e a Encarregada de Dados (DPO) da UFSM, confirmou a consistência normativa do modelo. Todos os dispositivos avaliados foram considerados corretamente representados. Mais relevante do que essa confirmação, porém, foram as contribuições que emergiram das entrevistas e que motivaram refinamentos substantivos no artefato: a separação entre os fluxos de notificação preliminar e complementar, a supressão do *gateway* de aprovação obrigatória da Gestão para a comunicação aos titulares e a incorporação da abertura de processo administrativo interno para consolidação do dossiê do incidente. Esses ajustes ilustram o ciclo de avaliação e refinamento característico da *Design Science Research* e conferem ao modelo aderência à realidade operacional da instituição.

Do ponto de vista da aplicabilidade institucional, a validação também revelou desafios concretos: a equipe técnica da ETIR é enxuta; o prazo de três dias úteis para a notificação é crítico diante da dinâmica de feriados e da necessidade de alinhamento entre áreas; e a implementação efetiva exigirá formalização de normativa interna, capacitação específica e suporte de ferramentas de automação de *workflow*. Esses obstáculos não invalidam o modelo, ao contrário, evidenciam com precisão onde o investimento institucional deve ser priorizado para que o dever ser normativo se converta em prática efetiva.

No plano das contribuições teóricas, o trabalho avança em relação à literatura em três dimensões. Primeiro, contextualiza a integração entre LGPD e resposta a incidentes para o ambiente específico das ETIRs de universidades federais, superando o escopo genérico do modelo de Silva Filho e Afonseca (2025) [18]. Segundo, propõe uma solução estruturada para a tensão entre lógica técnica e lógica jurídica identificada por Woods e Böhme (2022) [25], ao modelar os dois fluxos em paralelo por meio de um *gateway* AND. Terceiro, demonstra empiricamente que a modelagem em BPMN, quando ancorada em análise documental sistemática, é capaz de preencher o *implementation roadmap gap* apontado por Zaguir et al. (2024) [27], fornecendo um artefato visual, rastreável e auditável que conecta cada requisito normativo a atividades e decisões concretas.

Do ponto de vista prático, o modelo constitui um instrumento de governança, capacitação e eventual automação, aplicável não apenas à UFSM, mas a outras instituições públicas de ensino superior que enfrentam desafios semelhantes na integração entre resposta técnica e obrigações legais de privacidade. Sua fundamentação em normativos de aplicação federal assegura potencial de replicação, com as adaptações necessárias ao porte e à maturidade de cada instituição.

Este estudo apresenta limitações que devem orientar pesquisas futuras. A validação baseou-se na percepção de especialistas, sem a implementação em cenários reais ou a observação direta dos fluxos operacionais. O escopo normativo restringiu-se aos principais instrumentos federais, sem aprofundamento em normativos internos da UFSM além da PoSIN. Estudos futuros poderão avançar na automação do fluxo em ferramentas de *workflow*, no detalhamento

da estrutura mista da ETIR (Equipe Central e Descentralizada, conforme o Art. 53 da PoSIN/UFSM), na condução de simulações (*table-top exercises*) baseadas no modelo e na validação em outras universidades federais e órgãos públicos.

Por fim, declara-se que o uso da ferramenta de inteligência artificial generativa NotebookLM restringiu-se a atividades de revisão textual, sem emprego na geração de conteúdo científico, em conformidade com as diretrizes éticas vigentes para a pesquisa [17].

References

[1] Eric Araújo, Jéssyka Vilela, Carla Silva, and Carina Alves. 2021. Are My Business Process Models Compliant With LGPD? The LGPD4BP Method to Evaluate and to Model LGPD Aware Business Processes. In *Proceedings of the XVII Brazilian Symposium on Information Systems (SBSI 2021)*. ACM, Uberlândia, Brazil, 46:1–46:9. doi:10.1145/3466933.3466982

[2] Autoridade Nacional de Proteção de Dados (ANPD). 2024. *Resolução CD/ANPD nº 15, de 24 de abril de 2024 — Regulamento de Comunicação de Incidentes de Segurança.* Technical Report. ANPD, Brasília, DF. https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024

[3] Autoridade Nacional de Proteção de Dados (ANPD). 2026. Comunicado de Incidente de Segurança (CIS). https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 25 maio 2026.

[4] Laurence Bardin. 2016. *Análise de Conteúdo.* Edições 70, São Paulo. Tradução Luís Antero Reto e Augusto Pinheiro.

[5] Brasil. 2018. Lei nº 13.709, de 14 de agosto de 2018 — Lei Geral de Proteção de Dados Pessoais (LGPD). https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[6] Brasil. Ministério da Gestão e Inovação em Serviços Públicos (MGI). 2025. *Plano de Gestão de Incidentes com Dados Pessoais (PGI-DP).* Technical Report. Coordenação-Geral de Proteção de Dados Pessoais – CGPDP/SSC/MGI, Brasília, DF. https://www.gov.br/gestao/pt-br/assuntos/noticias/2026/janeiro/plano-de-gestao-de-incidentes-com-dados-pessoais.pdf

[7] Brasil. Secretaria de Governo Digital / Ministério da Gestão e Inovação em Serviços Públicos. 2026. *Guia do Framework de Privacidade e Segurança da Informação — PPSI 2.0.* Technical Report. SGD/MGI, Brasília, DF. https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0/arquivos/guiafwppsi2-0-v1-2-30012026.pdf Versão 1.2, 30 jan. 2026.

[8] Brasil. Secretaria de Governo Digital (SGD/MGI). 2024. *Guia de Resposta a Incidentes de Segurança.* Technical Report. Diretoria de Privacidade e Segurança da Informação – SGD/MGI, Brasília, DF. https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_resposta_incidentes.pdf Versão 3.3.

[9] Gabinete de Segurança Institucional da Presidência da República (GSI/PR). 2022. *Plano de Gestão de Incidentes Cibernéticos para a Administração Pública Federal (Plangic).* Technical Report. GSI/PR, Brasília, DF. https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/plano-de-gestao-de-incidentes-ciberneticos-plangic/plangic.pdf

[10] Alan R. Hevner, Salvatore T. March, Jinsoo Park, and Sudha Ram. 2004. Design Science in Information Systems Research. *MIS Quarterly* 28, 1 (2004), 75–105. doi:10.2307/25148625

[11] IBM Security. 2025. *Cost of a Data Breach Report 2025.* Technical Report. IBM Corp. https://www.ibm.com/reports/data-breach

[12] International Organization for Standardization. 2023. *ISO/IEC 27035-1:2023 — Information Security Incident Management — Part 1: Principles and Process.* Technical Report. ISO, Geneva, Switzerland. https://www.iso.org/standard/78973.html

[13] Reza Montasari. 2023. Emerging Cybersecurity Attacks in the Era of Digital Transformation. In *2023 IEEE International Conference on Cyber Security and Resilience (CSR).* IEEE, Washington, DC, USA, 275–280. doi:10.1109/CSR57506.2023.10224900

[14] Bruna Laís Campos do Nascimento and Edilene Maria da Silva. 2023. Lei Geral de Proteção de Dados (LGPD) e repositórios institucionais: reflexões e adequações. *Em Questão* 29 (2023), e–127314. doi:10.1590/1808-5245.29.127314

[15] Alex Nelson, Sanjay Rekhi, Murugiah Souppaya, and Karen Scarfone. 2025. *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.* Technical Report NIST SP 800-61 Rev. 3. National Institute of Standards and Technology, Gaithersburg, MD, USA. doi:10.6028/NIST.SP.800-61r3

[16] Object Management Group (OMG). 2011. *Business Process Model and Notation (BPMN) Version 2.0.* Technical Report formal/2011-01-03. OMG, Needham, MA, USA. https://www.omg.org/spec/BPMN/2.0/PDF

[17] Rafael Cardoso Sampaio, Marcelo Sabbatini, and Ricardo Limongi. 2024. *Diretrizes para o uso ético e responsável da Inteligência Artificial Generativa: um guia prático para pesquisadores.* Sociedade Brasileira de Estudos Interdisciplinares da Comunicação – Intercom, São Paulo. https://portcom.intercom.org.br/ebooks/arquivos/livro-diretrizes-ia.pdf Livro eletrônico (PDF).

[18] Marcelo dos Santos Silva Filho and Ulisses Rodrigues Afonseca. 2025. Un Modelo Integrado para la Gestión de Incidentes en Seguridad de la Información. *Revista Foco* 18, 4 (2025), e8378. doi:10.54751/revistafoco.v18n4-154

[19] Stefano Luppi Spósito, João Francisco Gomes Targino, Geovana Ramos Sousa Silva, Laerte Peotta, Daniel de Paula Porto, Fábio Lúcio Lopes Mendonça, and Edna Dias Canedo Canedo. 2025. A Comprehensive Review of Techniques, Methods, Processes, Frameworks, and Tools for Privacy Requirements. *Journal of Internet Services and Applications* 16, 1 (2025), 508–529. doi:10.5753/jisa.2025.5252

[20] Tribunal de Contas da União (TCU). 2025. *Acórdão nº 1.372/2025 — Plenário: Auditoria sobre a Implementação dos Dispositivos da LGPD na Administração Pública Federal.* Technical Report. TCU, Brasília, DF. https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/*/NUMACORDAO%253A1372%2520ANOACORDAO%253A2025/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0 Relator: Min. Walton Alencar Rodrigues. TC 009.980/2024-5.

[21] Joachim Bjørn Ulven and Gaute Wangen. 2021. A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet* 13, 2 (feb 2021), 39. doi:10.3390/fi13020039

[22] European Union. 2018. General Data Protection Regulation (GDPR). *Intersoft Consulting* 1, 1 (2018), 1–100. https://gdpr-info.eu/

[23] Universidade Federal de Santa Maria. 2023. Resolução nº 121, de 04 de abril de 2023: Define a Política de Segurança da Informação (PoSIN) no âmbito da Universidade Federal de Santa Maria. https://www.ufsm.br/pro-reitorias/proplan/resolucao-ufsm-n-121-2023. Acesso em: [17/04/2026]..

[24] Universidade Federal de Santa Maria (UFSM). 2025. UFSM em Números. Portal Institucional UFSM. https://portal.ufsm.br/ufsm-em-numeros Coordenadoria de Planejamento Informacional, Pró-Reitoria de Planejamento. Acesso em: mar. 2026.

[25] Daniel W. Woods and Rainer Böhme. 2022. Incident Response as a Lawyers' Service. *IEEE Security & Privacy* 20, 2 (mar 2022), 68–74. doi:10.1109/MSEC.2021.3096742

[26] Robert K. Yin. 2015. *Estudo de Caso: Planejamento e Métodos* (5 ed.). Bookman, Porto Alegre.

[27] Nival Arteiro Zaguir, Guilherme Henrique Magalhães, and Mauro de Mesquita Spinola. 2024. Challenges and Enablers for GDPR Compliance: Systematic Literature Review and Future Research Directions. *IEEE Access* 12 (2024), 81608–81630. doi:10.1109/ACCESS.2024.3406724