Plano de Resposta a Incidentes

PRI

Câmara Técnica sobre a Lei Geral de Proteção de Dados Pessoais
Conselho Nacional de Controle Interno

2024

Conaci
CONSELHO NACIONAL DE CONTROLE INTERNO

SUMÁRIO

Conaci
CONSELHO NACIONAL DE CONTROLE INTERNO

1. APRESENTAÇÃO

Em um ambiente cada vez mais digital e interconectado, as organizações enfrentam desafios crescentes no que diz respeito à segurança da informação e à proteção de dados pessoais. Com a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709/2018, tornou-se essencial que as instituições adotem medidas robustas e eficazes para garantir a privacidade e a segurança dos dados que processam, a fim de se adequarem às exigências legais e protegerem os direitos dos titulares.

Nesse cenário, o Plano de Resposta a Incidentes (PRI) surge como um instrumento fundamental, fornecendo uma estrutura clara e organizada para a identificação, análise e resolução de incidentes que envolvem dados pessoais. O PRI visa garantir que, em casos de violação de segurança ou privacidade, a organização seja capaz de agir de forma ágil e eficiente, em conformidade com os requisitos da LGPD. Assim, busca-se minimizar os danos aos titulares dos dados e à própria organização, preservando sua reputação e cumprindo com as obrigações legais.

Além disso, o PRI tem como propósito fomentar a cultura de segurança da informação dentro da organização, conscientizando as equipes envolvidas sobre as melhores práticas de resposta a incidentes. Com isso, assegura-se a integridade dos processos e a continuidade das operações, reduzindo significativamente os riscos associados a eventuais falhas de segurança e reforçando a confiança de clientes, parceiros e demais partes interessadas.

Para apoiar as organizações nesse processo, a Câmara Técnica da LGPD, do Conselho Nacional de Controle Interno (CONACI), disponibiliza um modelo de construção do Plano de Resposta a Incidentes (PRI). Este modelo oferece uma abordagem detalhada para a criação de um PRI eficaz, alinhado às diretrizes da LGPD, e serve como referência essencial para a implementação de boas práticas de proteção de dados pessoais.

2. PLANO DE RESPOSTAS A INCIDENTES

Este tópico tratará da estruturação do Plano de Resposta a Incidentes (PRI), destacando os componentes essenciais para garantir uma resposta organizada e eficaz a incidentes que envolvam dados pessoais. O objetivo é detalhar as principais seções que compõem o plano, oferecendo uma visão clara de cada uma delas e exemplificando sua aplicação prática. Dessa forma, busca-se assegurar que a resposta aos incidentes seja eficiente, em conformidade com a legislação vigente, e capaz de minimizar os impactos para a organização e os titulares dos dados.

Nos subtópicos a seguir serão tratadas as seções que devem compor o Plano de Resposta a Incidentes conforme a Figura 1:

Figura 1 - Estrutura do Plano de Resposta a Incidentes

2.1 Introdução

Nesta seção, é necessário elaborar uma introdução que explique a importância do Plano de Resposta a Incidentes (PRI) no contexto da segurança da informação e da conformidade com a Lei Geral de Proteção de Dados (LGPD). O objetivo é apresentar o plano, destacando sua relevância para a organização e seu compromisso em proteger dados pessoais, além de garantir uma resposta adequada e eficiente a incidentes.

A Introdução do PRI tem a função de contextualizar a criação deste documento, enfatizando a necessidade de uma abordagem estruturada para lidar com incidentes de segurança. O PRI assegura que a organização esteja devidamente preparada para responder rapidamente a violações de dados, preservando a integridade e a privacidade dos dados pessoais, ao mesmo tempo em que cumpre as exigências legais, especialmente as estabelecidas pela LGPD.

Abaixo segue exemplo de texto introdutório para o PRI:

A proteção de dados pessoais tornou-se um tema central no ambiente organizacional, especialmente com o avanço da transformação digital e o aumento das ameaças cibernéticas. Incidentes de segurança que envolvem o vazamento ou o uso indevido de dados pessoais podem resultar em prejuízos significativos para a organização e para os titulares dos dados. Nesse cenário, é imprescindível que as empresas adotem medidas proativas e estruturadas para lidar com possíveis violações de segurança, garantindo a conformidade com a Lei Geral de Proteção de Dados (LGPD).

O Plano de Resposta a Incidentes (PRI) é um documento essencial que estabelece um conjunto de diretrizes, procedimentos e responsabilidades a serem seguidos em caso de incidentes de segurança da informação. Ele visa assegurar que a organização esteja preparada para responder de maneira eficaz, minimizando os impactos e garantindo a proteção dos dados pessoais.

Além disso, o PRI define claramente as etapas que a equipe deve seguir, desde a identificação do incidente até a análise pós-incidente, promovendo uma abordagem coordenada e eficiente.

Por meio deste plano, a organização reforça seu compromisso com a segurança da informação e com a preservação dos direitos dos titulares dos dados. A implementação de um PRI robusto não apenas garante a conformidade com a LGPD, mas também fortalece a confiança de clientes, parceiros e demais stakeholders, demonstrando que a organização está preparada para lidar com eventuais incidentes de forma responsável e transparente.

2.2 Objetivo

Nessa seção, deve ser descrito o objetivo do PRI, exaltando os aspectos de proteção de dados pessoais, conformidade com a legislação vigente (em especial a LGPD), e a importância de uma resposta rápida e eficiente a incidentes de segurança.

Abaixo segue exemplo da seção Objetivo do PRI:

O objetivo principal do Plano de Resposta a Incidentes (PRI) é estabelecer um conjunto de procedimentos e ações padronizadas para lidar com incidentes de segurança da informação que envolvam dados pessoais, garantindo a rápida identificação, contenção, investigação e resolução do incidente, com o intuito de minimizar os riscos e impactos negativos para a organização e os titulares de dados.

A implementação do PRI busca:

- *Reduzir o impacto de incidentes de segurança da informação;*
- *Minimizar as interrupções nas operações da organização;*
- *Proteger a reputação da empresa e a confiança dos clientes;*
- *Assegurar a conformidade com a LGPD e outras leis de proteção de dados;*
- *Demonstrar proatividade e responsabilidade na proteção de dados pessoais.*

2.3 Definições

Nessa seção, você deve definir os principais termos utilizados no PRI, assegurando que todos os envolvidos compreendam claramente os conceitos relacionados à resposta a incidentes. O objetivo é evitar ambiguidades e padronizar o entendimento entre os membros da equipe.

Abaixo segue exemplo da seção Definições do PRI:

*a) **ANPD (Autoridade Nacional de Proteção de Dados):** A ANPD é o órgão responsável por zelar pela proteção dos dados pessoais no Brasil, fiscalizando e garantindo a aplicação da LGPD;*

*b) **Controlador:** O Controlador é a pessoa física ou jurídica, de direito público ou privado, responsável por tomar as decisões sobre o tratamento de dados pessoais;*

*c) **Encarregado de Dados Pessoais (ou DPO - Data Protection Officer):** O Encarregado é a pessoa indicada pelo Controlador e/ou pelo Operador para atuar como ponto de contato entre a organização, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);*

*d) **Equipe de Resposta a Incidentes:** A Equipe de Resposta a Incidentes é o grupo de profissionais designados para lidar com incidentes de segurança da informação dentro de uma organização;*

*e) **Incidente de Segurança:** Um Incidente de Segurança é qualquer evento que resulte na violação da confidencialidade, integridade ou disponibilidade de dados pessoais, podendo envolver vazamentos, acessos não autorizados, perdas, roubos ou exposições de dados;*

*f) **Operador:** O Operador é a pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador, seguindo as instruções dele;*

*g) **Plano de Resposta a Incidentes (PRI):** O Plano de Resposta a Incidentes (PRI) é um conjunto de procedimentos e diretrizes que define as etapas que uma organização deve seguir ao identificar um incidente de segurança.*

2.4 Atores e Responsabilidades

Nessa seção, você deve delinear os atores e responsabilidades de cada membro da equipe de resposta a incidentes. O objetivo é garantir que cada participante saiba exatamente suas atribuições durante a gestão de um incidente. Vale ressaltar que essa seção deverá ser construída observando a estrutura de cada organização e os recursos disponíveis relacionadas a atuação nas respostas a incidentes.

Abaixo segue exemplo da seção Atores e Responsabilidades do PRI:

No processo de resposta a incidentes, é fundamental definir claramente os atores envolvidos e suas respectivas responsabilidades, para garantir uma atuação rápida, eficaz e coordenada.

Ator	Função	Atribuições
Encarregado de dados pessoais	*desempenha um papel de liderança na proteção de dados e é o elo de comunicação entre a organização, os titulares de dados e a ANPD*	*Atuar como facilitador entre a equipe de resposta a incidentes e os gestores, garantindo que o plano seja seguido de forma adequada e que as ações estejam alinhadas com as exigências da LGPD;*
		Notificar a ANPD sobre qualquer incidente de segurança relevante, conforme exigido pela LGPD, e manter contato contínuo durante a resposta ao incidente;
		Garantir que os titulares de dados sejam informados sobre os incidentes que possam afetar seus dados pessoais, de forma clara e transparente;

Ator	Função	Atribuições
Equipe Técnica de Resposta a Incidentes	*equipe formada por profissionais especializados em segurança da informação e TI, responsáveis por lidar com os aspectos técnicos do incidente*	*Detectar e analisar incidentes, utilizando ferramentas de monitoramento e técnicas de investigação para identificar a origem e o alcance do problema*
		Adotar ações imediatas para conter o incidente e mitigar seus efeitos, como isolar sistemas comprometidos, restringir acessos e interromper atividades prejudiciais;
		Remover as vulnerabilidades ou ameaças que causaram o incidente, garantindo que a fonte do problema seja completamente eliminada;
		Restaurar os sistemas afetados, garantindo que voltem a operar de maneira segura e normalizada, e evitar que o incidente se repita;
		Registrar detalhadamente todas as ações tomadas, erros identificados e soluções aplicadas durante o processo de resposta;
Equipe Jurídica	*desempenha um papel crucial na avaliação dos aspectos legais e regulatórios envolvidos no incidente*	*Verificar se as ações realizadas durante a resposta ao incidente estão em conformidade com as leis de proteção de dados, como a LGPD, e outras normativas aplicáveis;*
		Notificar a ANPD sobre qualquer incidente de segurança relevante, conforme exigido pela LGPD, e manter contato contínuo durante a resposta ao incidente;
		Garantir que os titulares de dados sejam informados sobre os incidentes que possam afetar seus dados pessoais, de forma clara e transparente;

Ator	Função	Atribuições
Equipe Comunicação	*responsável pela comunicação, em articulação com o Encarregado de Dados, com o público e outras partes interessadas durante e após um incidente*	*Garantir que todas as partes interessadas (internas e externas) sejam mantidas informadas sobre o incidente e as ações tomadas pela organização;*
		Ajudar a preparar e divulgar as comunicações aos titulares de dados afetados, garantindo que a informação seja clara, precisa e dentro do prazo estabelecido pela LGPD;
		Ajudar a proteger a reputação da organização, lidando com comunicações sensíveis e gerenciando possíveis crises de imagem causadas pelo incidente;
Controlador	*pessoa física ou jurídica, pública ou privada, responsável por tomar as decisões sobre o tratamento de dados pessoais*	*Determinar as ações globais em resposta a incidentes, considerando o impacto nos titulares de dados e na reputação da organização;*
		Certificar-se de que o Plano de Resposta a Incidentes (PRI) está em vigor e é seguido corretamente durante um incidente;
		Garantir que, em casos de incidentes graves que afetam os dados pessoais, os titulares sejam informados de maneira adequada e oportuna, conforme exigido pela LGPD;

Tabela 1 - Atores e Atribuições

2.5 Etapas do Plano de Resposta a Incidentes

Nessa seção, você deve descrever as etapas detalhadas que compõem o processo de resposta a incidentes, desde a identificação até a finalização. O objetivo é assegurar que todos os passos sejam seguidos para minimizar os impactos do incidente.

Abaixo segue exemplo da seção Etapas do PRI:

As etapas do Plano de Resposta a Incidentes (PRI) constituem um conjunto estruturado de ações e processos que devem ser seguidos para garantir uma resposta eficaz a incidentes de segurança. O objetivo dessas etapas é assegurar que a organização responda de maneira rápida, coordenada e adequada, minimizando os danos e restabelecendo a normalidade das operações, enquanto cumpre rigorosamente com as exigências legais, como as previstas pela Lei Geral de Proteção de Dados (LGPD). Cada etapa desempenha um papel fundamental para assegurar a eficiência do processo, desde a identificação inicial do incidente até a análise pós-incidente, promovendo a melhoria contínua da segurança.

A figura abaixo ilustra um resumo das etapas a serem percorridas no Plano de Respostas a Incidentes:

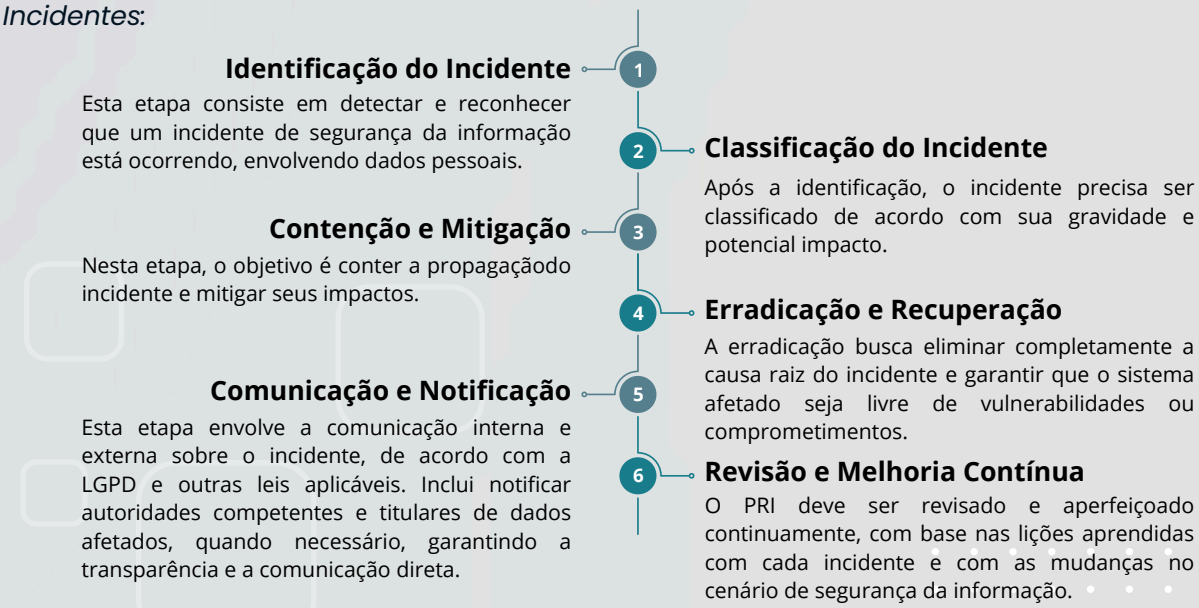


Figura 2 – Etapas do Plano de Resposta a Incidentes

1. *Identificação do Incidente*

a. ***Objetivo:*** *O objetivo principal dessa fase é identificar, de maneira precisa e oportuna, se um incidente de segurança ocorreu, além de identificar os casos que possam envolver dados pessoais. A identificação eficaz permite que as equipes de resposta tomem as medidas corretas para mitigar danos e garantir a conformidade com as obrigações legais impostas pela LGPD;*

b. ***Processo de identificação:*** *A identificação do incidente envolve a detecção de sinais ou evidências de que uma violação de segurança ocorreu ou está em andamento, a organização deve implementar ferramentas e processos de monitoramento contínuo para identificar possíveis incidentes de segurança de dados em tempo real. Isso inclui a utilização de sistemas de detecção e prevenção de intrusões (IDS/IPS), ferramentas de monitoramento de logs, firewalls, entre outros. Uma vez que os sistemas de monitoramento detectem uma possível anomalia ou evento suspeito, é fundamental que os dados de logs e alertas sejam analisados para determinar a natureza do incidente. Nessa fase, a equipe de segurança deve revisar logs de acesso a dados, auditorias de sistemas, tentativas de login suspeitas, comportamentos anômalos de usuários ou sistemas etc.;*

c. ***Coleta de informações:*** *Assim que o incidente for identificado, devem ser coletadas as informações relacionadas a origem do incidente (local onde ocorreu), ao tipo do incidente (violação de segurança, acesso não autorizado, vazamento de dados etc.), aos ativos afetados (sistemas, dados e serviços impactados) e impacto inicial percebido (indisponibilidade de serviços ou comprometimento de dados);*

d. ***Atores Participantes:*** *Equipe Técnica de Resposta a Incidentes.*

2. *Classificação do Incidente*

a. ***Objetivo:*** *O objetivo principal da classificação de incidentes é identificar rapidamente a gravidade, impacto e urgência do incidente, categorizando os incidentes de forma eficiente e precisa, facilitando uma resposta ágil e eficaz;*

b. ***Critérios de classificação:*** *Cada incidente deve ser classificado com base nos critérios Gravidade, Urgência, Impacto e Recorrência;*

c. ***Atores participantes:*** *Equipe Técnica de Resposta a Incidentes e Encarregados de Dados Pessoais (quando o incidente envolver dados pessoais).*

Seguem as tabelas com o modelo de classificação a ser seguido:

Critério	Baixo (1 ponto)	Médio (3 pontos)	Alto (5 pontos)
Gravidade	*Incidente menor, que não causa impacto significativo*	*Incidente com impacto moderado, que pode ser contido sem maiores danos*	*Impacto crítico para a organização, como perda de dados sensíveis ou interrupção de serviços essenciais*
Urgência	*Pode ser resolvido em prazo mais estendido*	*Deve ser tratado em curto prazo, mas não requer ação imediata*	*Necessita de ação imediata para evitar maiores danos*
Impacto	*Atinge uma pequena parte da organização com impacto restrito*	*Impacta uma parte significativa da organização, mas com danos limitados*	*Grande número de sistemas, usuários ou dados comprometidos*
Probabilidade de Recorrência	*Incidente isolado, com baixa probabilidade de repetição*	*Pode ocorrer novamente, mas de forma esporádica*	*Grande chance de ocorrer novamente se não for tratado adequadamente*

Tabela 2 - Critérios de Classificação de Incidentes

Classificação	Pontuação
Criticidade Muito Alta	*15 a 20 pontos*
Criticidade Alta	*10 a 15 pontos*
Criticidade Média	*5 a 10 pontos*
Criticidade Baixa	*0 a 5 pontos*

Tabela 3 - Classificação de Incidentes

3. ***Contenção***

a. ***Objetivo:*** *Limitar a propagação do incidente e reduzir seu impacto antes de realizar uma correção definitiva. A contenção visa impedir que o incidente cause mais danos ou se espalhe para outros sistemas ou ativos, preservar evidências para investigação posterior, proteger a continuidade das operações essenciais e ganhar tempo para preparar uma resposta definitiva e desenvolver uma estratégia de erradicação;*

b. ***Procedimento de contenção:*** *Desconectar dispositivos comprometidos da rede para evitar a propagação, suspender contas comprometidas ou desativar acessos não autorizados, restringir o tráfego de rede de e para as áreas afetadas e configurar alertas em tempo real para detectar qualquer atividade suspeita ou tentativas de novos acessos.*

c. ***Atores participantes:*** *Equipe Técnica de Resposta a Incidentes.*

4. ***Erradicação e Recuperação***

a. ***Objetivo:*** *Depois que o incidente está sob controle, a próxima etapa é eliminar completamente a causa raiz do incidente e garantir que o sistema afetado esteja livre de vulnerabilidades ou comprometimentos. A erradicação visa a remoção total do incidente, garantindo que ele não volte a ocorrer;*

b. ***Procedimento de erradicação:*** *Usar ferramentas de antivírus, anti-malware e soluções de segurança especializadas para garantir a eliminação de todos os arquivos maliciosos, corrigir vulnerabilidades exploradas pelo incidente, como falhas de software ou sistemas desatualizados, atualizar credenciais comprometidas e implementar políticas de senhas mais seguras para evitar novos acessos não autorizados, ajustar as configurações dos dispositivos afetados para evitar futuras tentativas de exploração executar análises completas e testes de vulnerabilidades para assegurar que o incidente foi completamente removido e o sistema está seguro;*

c. ***Procedimento de recuperação:*** *Restaurar os sistemas e serviços afetados ao seu estado normal de operação, após a contenção e erradicação do incidente. Durante essa fase, o foco está em garantir que as operações voltem à normalidade de forma segura, minimizando o impacto no desempenho e protegendo contra novos ataques ou recorrências;*

d. ***Atores participantes:*** *Equipe Técnica de Resposta a Incidentes.*

5. *Comunicação e Notificação*

a. ***Objetivo:*** *O principal objetivo desta etapa é garantir que as partes interessadas sejam informadas de forma clara, rápida e precisa sobre o incidente, suas implicações e as ações tomadas para mitigar seu impacto, para minimizar o pânico e evitar informações incorretas, assegurar que as partes envolvidas saibam seu papel no processo de resposta, cumprir as obrigações legais e regulatórias e manter a transparência e a confiança dos envolvidos;*

b. ***Plano de comunicação:*** *Realizar um plano de comunicação adequado, identificando as partes interessadas, internas e externas, as frequências e prazos de comunicações, o conteúdo e as atualizações periódicas;*

c. ***Conteúdo da comunicação:*** *O conteúdo das mensagens deve ser claro, objetivo e adequado ao público-alvo. Alguns elementos-chave a serem incluídos são a descrição do incidente, o que aconteceu, quando e como foi identificado, o impacto, quais áreas, sistemas ou dados foram afetados, o que foi feito até o momento para conter e corrigir o incidente, quais são as etapas futuras para a erradicação e recuperação. No caso de dados pessoais, explicar se há risco para os usuários e se eles precisam tomar medidas adicionais (trocar senhas, monitorar atividades de conta, etc.), se há dados sensíveis e as categorias de dados afetados e o número de titulares afetados, distinguindo, quando possível, o número de menores de idade e idosos afetados.*

d. ***Comunicação nos casos de exposições de dados pessoais:*** *Se o incidente envolver a exposição de dados pessoais, há requisitos legais específicos para notificação, como estabelecido pela LGPD (Lei Geral de Proteção de Dados), incidentes que resultem em comprometimento de dados pessoais devem ser reportados à Autoridade Nacional de Proteção de Dados (ANPD) e comunicada aos titulares de dados pessoais.*

e. ***Prazo para notificação:*** *Conforme Resolução da ANPD nº 15/2024 - Regulamento de Comunicação de Incidente de Segurança, a comunicação deve ser feita à ANPD e aos titulares afetados em até três dias úteis, contados da data em que o controlador confirmar que o incidente afetou dados pessoais. As informações à ANPD podem ser complementadas em até 20 dias úteis contados da data do protocolo da primeira comunicação.*

f. ***Atores participantes:*** *Encarregado de Dados Pessoais, Controlador, Área Jurídica e Área de Comunicação;*

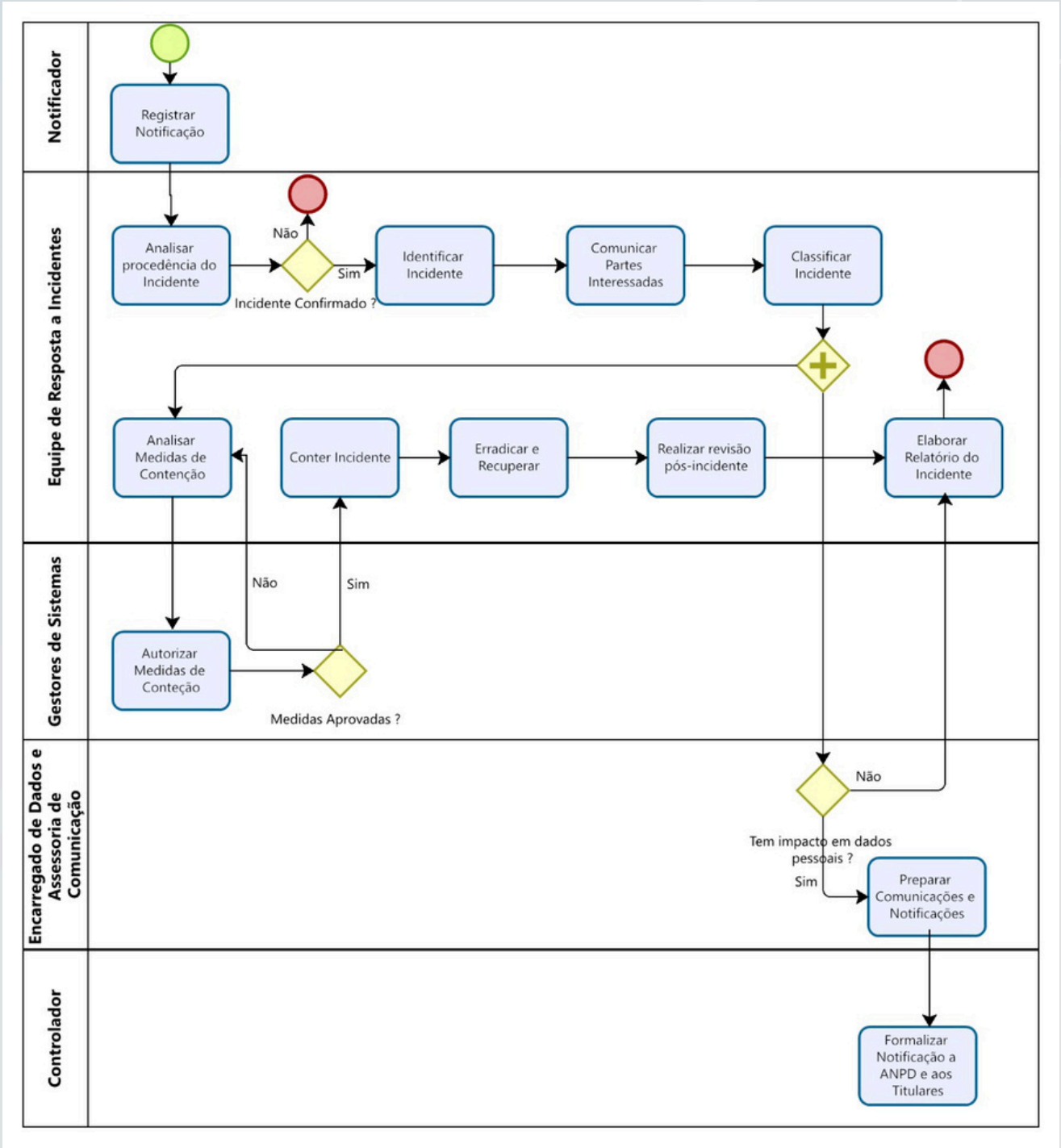
6. ***Melhoria Contínua***

a. ***Objetivo:*** *Essa fase ocorre após a recuperação completa do incidente e tem como objetivo analisar o que aconteceu, identificar falhas e pontos fortes na resposta, e implementar melhorias para prevenir ou mitigar incidentes futuros. Ela ajuda a fortalecer a capacidade da organização de lidar com ameaças, promovendo uma cultura de aprimoramento contínuo e aprendizado;*

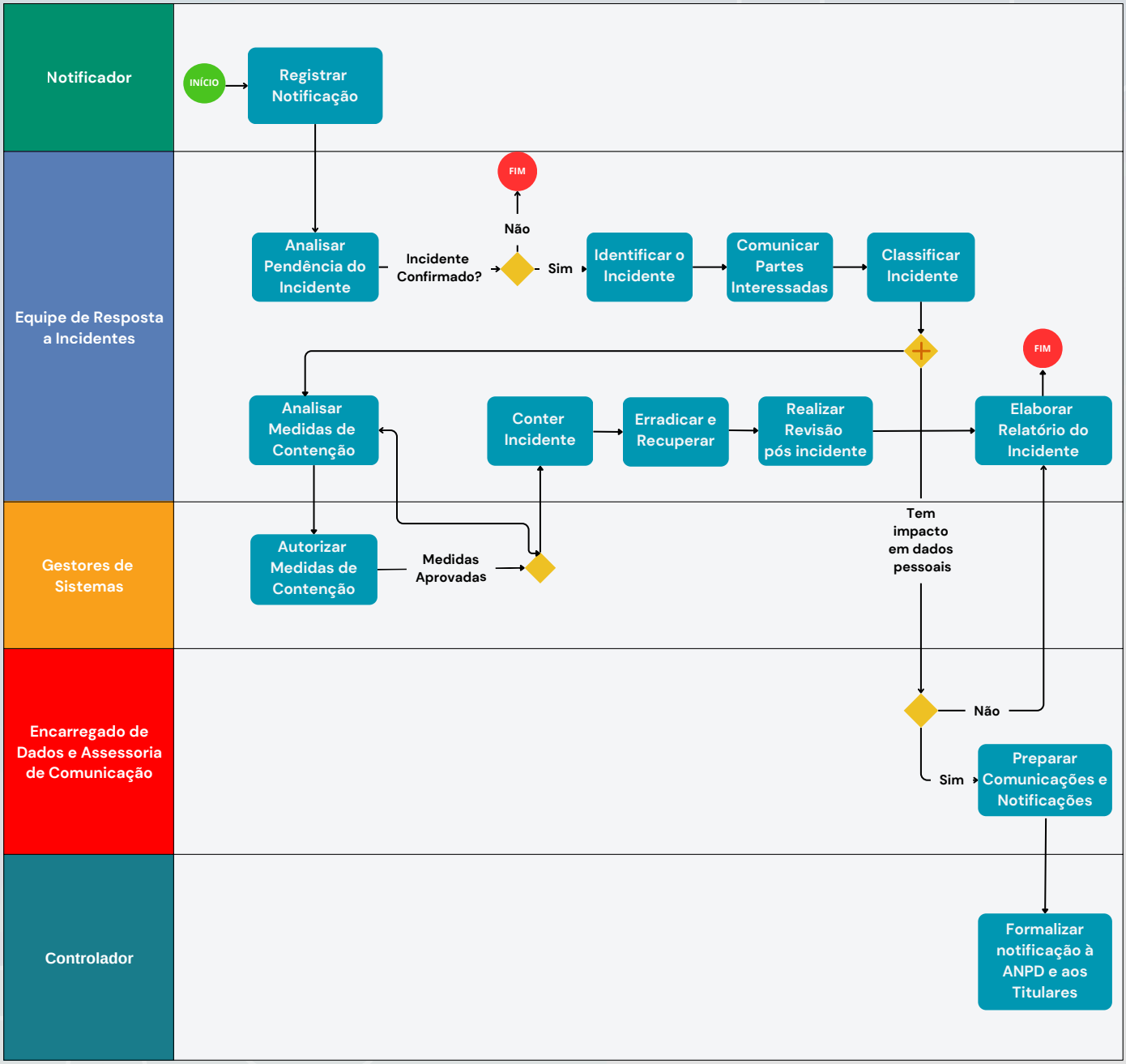
b. ***Reunião de revisão pós-incidente:*** *A reunião de revisão pós-incidente ou Post-Mortem. Essa reunião envolve a análise detalhada do incidente e da resposta aplicada, revisar as etapas do incidente: detecção, contenção, erradicação, recuperação e comunicação, Identificar lacunas e problemas que surgiram durante a resposta e propor soluções para melhorar a prontidão e a capacidade de resposta da organização no futuro;*

c. ***Atores participantes:*** *Equipe Técnica de Resposta a Incidentes, Controlador e Encarregado de Dados.*

7. *Fluxo das Etapas do Plano de Resposta a Incidentes*



7. *Fluxo das Etapas do Plano de Resposta a Incidentes*



2.6 Relatório Final

O Relatório Final é uma etapa crucial do Plano de Resposta a Incidentes (PRI), pois serve para documentar de forma completa e detalhada todo o ciclo de resposta a um incidente. Este relatório deve ser elaborado após a contenção, erradicação e recuperação dos sistemas afetados, fornecendo uma visão abrangente do incidente e das ações tomadas para lidar com ele. O objetivo do Relatório Final é não apenas registrar as ocorrências e medidas adotadas, mas também servir como uma ferramenta de aprendizado para a organização, ajudando a identificar melhorias e prevenir incidentes futuros.
Abaixo segue exemplo da seção Relatório Final do PRI:

Relatório Final:

a) ***Documentar o incidente:*** *Relatar de maneira precisa e objetiva todas as fases do incidente, desde sua detecção até a conclusão do processo de resposta, registrar o momento exato em que o incidente foi detectado e o tempo de resposta inicial, descrever o tipo de incidente, como vazamento de dados, ataque de ransomware, falha de sistema, entre outros, detalhar a causa raiz do incidente, como falha humana, vulnerabilidade de software, ataque externo, etc e especificar quais sistemas, redes ou dados foram comprometidos durante o incidente;*

b) ***Analisar o impacto****: Fornecer uma análise detalhada dos danos causados pelo incidente, incluindo a extensão da violação de dados pessoais, o impacto operacional e financeiro e os prejuízos à reputação da organização, avaliar se houve comprometimento de dados pessoais, detalhando o tipo de dado afetado e o número de titulares envolvidos, explicar as interrupções causadas nas operações da organização e o tempo necessário para retomá-las, Estimar os custos relacionados ao incidente, incluindo perdas financeiras diretas, custos de mitigação e possíveis multas e Analisar o impacto na imagem e reputação da organização, especialmente se os titulares de dados ou o público foram afetados;*

*c) **Avaliar a eficácia da resposta**: Verificar como as ações de resposta, contenção e recuperação foram conduzidas, avaliando a eficiência do PRI e identificando pontos fortes e fracos, detalhar as ações tomadas para conter o incidente e impedir que ele se espalhasse para outras áreas da organização, descrever como a causa do incidente foi eliminada, incluindo a remoção de ameaças ou correção de vulnerabilidades e informar como os sistemas e dados afetados foram restaurados à sua condição operacional normal, incluindo o tempo de recuperação;*

*d) **Analisar comunicação**: descrever as ações de comunicação realizadas com os titulares de dados afetados, explicando o que foi informado e em qual prazo, relatar se a Autoridade Nacional de Proteção de Dados (ANPD) foi notificada e quais informações foram prestadas, conforme as exigências da LGPD e Registrar como a equipe interna foi informada e envolvida no processo de resposta ao incidente;*

*e) **Recomendar melhorias:** Com base na análise do incidente, propor melhorias no PRI, nas políticas de segurança da organização e nas medidas preventivas a serem adotadas para evitar novos incidentes, realizar uma análise crítica de como a resposta ao incidente foi conduzida, identificando o que funcionou bem e o que pode ser melhorado, destacar as principais lições aprendidas com o incidente, que possam ser usadas para aprimorar a prevenção e a resposta a futuros incidentes e sugerir alterações ou aprimoramentos no Plano de Resposta a Incidentes, com base na análise do incidente;*

3. CONSIDERAÇÕES FINAIS

Este documento apresenta um modelo do Plano de Resposta a Incidentes (PRI), desenvolvido com o objetivo de servir como referência para os membros do Conselho Nacional de Controle Interno (CONACI). Ao longo deste trabalho, foram detalhadas as principais etapas e elementos que compõem um PRI eficaz, alinhado às diretrizes da Lei Geral de Proteção de Dados (LGPD) e às melhores práticas de segurança da informação. O objetivo central é garantir que as organizações estejam preparadas para lidar de forma eficiente com incidentes de segurança, mitigando riscos e assegurando a proteção dos dados pessoais sob sua responsabilidade.

É importante destacar que o presente modelo não deve ser visto como uma solução única ou definitiva, mas sim como uma base estruturada que pode ser adaptada conforme as necessidades específicas de cada organização. A realidade operacional, o porte e o nível de maturidade em segurança da informação podem exigir ajustes no PRI, adequando-o à sua capacidade técnica, organizacional e legal. Dessa forma, este documento oferece flexibilidade para que cada membro faça as adaptações necessárias, de modo a garantir que o plano reflita a realidade de sua organização e atenda aos seus desafios específicos.

Além de fornecer um guia para a resposta a incidentes, este trabalho visa promover uma cultura de segurança da informação e conformidade com a LGPD entre membros do CONACI. A implementação de um PRI bem estruturado não apenas ajuda a minimizar os danos causados por incidentes de segurança, mas também reforça a confiança dos cidadãos, parceiros e demais partes interessadas na capacidade das instituições de proteger dados sensíveis e reagir de forma adequada a eventuais violações.

Em conclusão, espera-se que este modelo de PRI sirva como um ponto de partida valioso para as organizações, orientando a criação ou aprimoramento de seus próprios planos de resposta a incidentes. A adaptação às particularidades de cada instituição é fundamental para garantir a efetividade do plano, sempre com o objetivo de fortalecer a segurança da informação e garantir a conformidade com as exigências legais e regulatórias vigentes.

4. REFERÊNCIAS

Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados;

Resolução da ANPD nº 15/2024 - Regulamento de Comunicação de Incidente de Segurança;

ISO/IEC 27035:2011 - Tecnologias da Informação - Segurança - Gestão de Incidentes de Segurança da Informação;

Manual de Boas Práticas para a Proteção de Dados Pessoais: Disponível em: https://www.gov.br/anpd/pt-br/assuntos/normas-e-legislacao/orientacoes/manual-de-boas-praticas-para-a-protecao-de-dados-pessoais;

Câmara Técnica sobre a Lei Geral de Proteção de Dados Pessoais
Conselho Nacional de Controle Interno (Conaci)