LGPD

LEI GERAL DE PROTEÇÃO DE DADOS

PLANO DE RESPOSTA A INCIDENTES - PRI

CGE
CONTROLADORIA E OUVIDORIA GERAL DO ESTADO
GOVERNO DO ESTADO DO CEARÁ

PLANO DE RESPOSTAS A INCIDENTES DA CONTROLADORIA E OUVIDORIA GERAL DO ESTADO DO CEARÁ – CGE/CE

GOVERNADOR
Elmano de Freitas da Costa

SECRETÁRIO DE ESTADO CHEFE DA CONTROLADORIA E OUVIDORA GERAL
Aloísio Barbosa de Carvalho Neto

SECRETÁRIO EXECUTIVO
Antônio Marconi Lemos da Silva

SECRETÁRIO EXECUTIVO DE PLANEJAMENTO E GESTÃO INTERNA
Marcelo de Sousa Monteiro

COMITÊ SETORIAL DE PROTEÇÃO DE DADOS PESSOAIS DA CGE

SECRETÁRIO EXECUTIVO DE PLANEJAMENTO E GESTÃO INTERNA
Marcelo de Sousa Monteiro

COORDENADOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
Marcos Henrique de Carvalho Almeida

ASSESSORA JURÍDICA
Ana Zélia Cavalcante Oliveira

ASSESSORA DE CONTROLE INTERNO
LARIÇA LOIOLA GONÇALVES ALEXANDRINO

AGOSTO/2024

SUMÁRIO

1.	**INTRODUÇÃO**	03
2.	**OBJETIVO**	04
3.	**DEFINIÇÕES**	04
4.	**PAPÉIS E RESPONSABILIDADES**	06
4.1	Encarregado de Dados Pessoais	06
4.2	Equipe Técnica de Respostas a Incidentes	07
4.3	Comitê Setorial de Proteção de Dados	08
4.4	Assessoria de Comunicação	09
4.5	Gestores de Sistemas	09
4.6	Controlador	10
5.	**ETAPAS DO PROCESSO DE RESPOSTAS A INCIDENTES**	10
5.1	Notificação	11
5.2	Identificação	11
5.3	Classificação	12
5.4	Contenção	13
5.5	Erradicação	13
5.6	Recuperação	14
5.7	Comunicação e Notificação	14
5.8	Revisão pós-incidente	16
5.9	Relatório de Incidentes	17
5.10	Fluxo do Processo	19
6.	**DISPOSIÇÕES FINAIS**	20
7.	**REFERÊNCIAS BIBLIOGRÁFICAS**	21

1.INTRODUÇÃO

O avanço tecnológico e a crescente digitalização dos serviços públicos trouxeram inúmeros benefícios à gestão e operação de diversas atividades, mas também expuseram as instituições a novos riscos e ameaças no ambiente cibernético. A Controladoria e Ouvidoria Geral do Estado do Ceará (CGE/CE), ciente de seu papel estratégico na garantia da segurança das informações e na prevenção de vazamentos de dados sensíveis, desenvolve o Plano de Resposta a Incidentes (PRI) como um instrumento fundamental para mitigar riscos e assegurar a continuidade das operações de maneira eficaz e organizada.

O PRI é um documento que estabelece diretrizes, responsabilidades e procedimentos a serem seguidos em caso de incidentes de segurança, como ataques cibernéticos, violações de dados ou falhas operacionais que possam comprometer a integridade, a confidencialidade e a disponibilidade das informações. Este plano visa fornecer uma resposta rápida e coordenada, garantindo a preservação dos ativos de informação e o cumprimento dos requisitos legais, especialmente os dispostos pela Lei Geral de Proteção de Dados (LGPD).

Por meio deste plano, a CGE 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 da sociedade, parceiros e demais envolvidos, demonstrando que a CGE está preparada para lidar com eventuais incidentes de forma responsável e transparente.

2. OBJETIVO

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, garantindo a rápida identificação, contenção,

investigação e resolução do incidente, com o intuito de minimizar os riscos e impactos negativos para a CGE e para 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 CGE;
- Assegurar a conformidade com a LGPD e outras leis de proteção de dados;
- Demonstrar proatividade e responsabilidade na proteção de dados pessoais;

3. DEFINIÇÕES

Para efeito deste Plano são adotadas as seguintes definições:

a) **Agente de Tratamento:** é um conceito fundamental na Lei Geral de Proteção de Dados (LGPD) e refere-se a qualquer pessoa, natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais. A LGPD divide os agentes de tratamento em dois tipos principais: o Controlador e o Operador;

b) **Ameaça**: qualquer circunstância ou evento potencialmente prejudicial que possa explorar uma vulnerabilidade e causar danos aos ativos de informação ou à operação da organização;

c) **Ataque:** qualquer ação ou conjunto de ações deliberadas realizadas com o objetivo de comprometer a confidencialidade, integridade ou disponibilidade de um sistema, rede, ou conjunto de dados.

d) **Autoridade Nacional de Proteção de Dados (ANPD):** órgão da administração pública federal responsável por fiscalizar e zelar pelo cumprimento da Lei Geral de Proteção de Dados em todo o território brasileiro;

e) **Controlador:** pessoa física ou jurídica, de direito público ou privado, a quem competem decisões referentes ao tratamento de dados pessoais.

f) **Dados Pessoais:** qualquer informação relacionada a um indivíduo que possa ser usada para identificá-lo, direta ou indiretamente, ou para entrar em contato, por conta própria ou quando combinada com outras informações;

g) **Dados Pessoas Sensíveis:** são dados pessoais que digam respeito a origem racial ou étnica, convicção religiosa, prática ou orientação sexual, informações médicas ou de saúde, como histórico médico e prontuário físico ou eletrônico, informações genéticas ou biométricas, crenças políticas ou filosóficas, filiação política ou sindical, número do seguro social, número da carteirinha do plano de saúde e informações bancárias;

h) **Encarregado de Dados Pessoais:** 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);

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

j) **Incidente de Segurança***:* qualquer evento ou ação que comprometa a confidencialidade, integridade ou disponibilidade dos dados ou sistemas de uma organização;

k) **Log:** processo de registro de eventos relevantes num sistema computacional;

l) **Malware:** qualquer tipo de software projetado para causar danos a um computador, servidor, rede ou dispositivo;

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

n) **Ransomware:** é um tipo de malware, ou software malicioso, que pode bloquear o acesso a dados ou criptografá-los, exigindo um resgate para restaurar o acesso**;**

o) **Vazamento de Dados:** qualquer quebra de sigilo ou vazamento de dados que possa resultar, criminosamente ou não, na perda, alteração, compartilhamento, acesso, transmissão, armazenamento ou processamento de dados não autorizado;

p) **Violação de Privacidade**: qualquer violação à legislação aplicável ou conduta e evento que resulte na destruição acidental ou ilícita dos dados, bem como sua perda, roubo, alteração, divulgação ou acesso não autorizado, danos ou desvio de finalidade em seu tratamento;

q) **Vírus:** programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos;

r) **Worm**: programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador;

4. PAPÉIS E RESPONSABILIDADES

A definição clara dos papéis envolvidos e de suas respectivas responsabilidades é fundamental para garantir a eficiência e a eficácia no tratamento de incidentes de segurança da informação. Cada ator desempenha um papel específico, alinhado às suas competências e funções, de modo a permitir uma resposta coordenada e ágil em situações críticas.

4.1 Encarregado de Dados Pessoais

O papel do Encarregado (ou Data Protection Officer - DPO) no processo de proteção de dados, especialmente na resposta a incidentes, é fundamental para garantir a conformidade com a LGPD. O Encarregado é a pessoa indicada pelo

Controlador para atuar como ponto de contato entre a organização, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD).

As suas principais atribuições relacionadas ao PRI são:

a) Atuar como facilitador entre a equipe técnica 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;
b) Preparar, em articulação com a Assessoria de Comunicação, a notificação a ANPD sobre qualquer incidente de segurança relevante, conforme exigido pela LGPD, e manter contato contínuo durante a resposta ao incidente;
c) Garantir que os titulares de dados sejam informados sobre os incidentes que possam afetar seus dados pessoais, de forma clara e transparente;

4.2 Equipe Técnica de Respostas a Incidentes

A Equipe Técnica de Resposta a Incidentes é formada por profissionais especializados em segurança da informação, com atuação predominantemente vinculada à Coordenadoria de Tecnologia da Informação e Comunicação (COTIC) da CGE. Esses especialistas são responsáveis por gerenciar todos os aspectos técnicos relacionados aos incidentes, assegurando a identificação precisa, a contenção eficaz, a erradicação completa dos problemas e a implementação de medidas preventivas para evitar futuros eventos de segurança.

As suas principais atribuições relacionadas ao PRI são:

a) Detectar e analisar incidentes, utilizando ferramentas de monitoramento e técnicas de investigação para identificar a origem e o alcance do problema;

b) Adotar ações imediatas para conter o incidente e mitigar seus efeitos, como isolar sistemas comprometidos, restringir acessos e interromper atividades prejudiciais;
c) Remover as vulnerabilidades ou ameaças que causaram o incidente, garantindo que a fonte do problema seja completamente eliminada;
d) Restaurar os sistemas afetados, garantindo que voltem a operar de maneira segura e normalizada, e evitar que o incidente se repita;
e) Registrar detalhadamente todas as ações tomadas, erros identificados e soluções aplicadas durante o processo de resposta;

4.3 Comitê Setorial de Proteção de Dados Pessoais

O Comitê Setorial de Proteção de Dados Pessoais é a instância responsável pela adequação da Controladoria e Ouvidoria Geral do Estado (CGE) às exigências da Lei Geral de Proteção de Dados Pessoais (LGPD), conforme estabelecido pela Lei Estadual nº 18.699/2024. Este comitê atua de forma a garantir que as práticas da CGE estejam em conformidade com os requisitos legais de proteção de dados, desempenhando um papel essencial no monitoramento e gestão de incidentes que possam comprometer informações pessoais.

As suas principais atribuições relacionadas ao PRI são:

a) Comunicar o incidente de segurança ao Conselho Estadual de Proteção de Dados Pessoais (CEPD), nos casos em que o incidente possa ter repercussão direta sobre a proteção de dados pessoais, conforme disposto no Art. 7º, inciso VI, da Lei Estadual nº 18.699/2024. Tal comunicação é fundamental para garantir a transparência e a rápida ação corretiva em situações que envolvam a segurança de dados sensíveis;
b) Atuar em articulação com o Encarregado de Dados Pessoais garantindo que o plano seja seguido de forma adequada e que as ações estejam alinhadas com as exigências da LGPD;

4.4 Assessoria de Comunicação

A Assessoria de Comunicação é responsável por coordenar, em conjunto com o Encarregado de Dados, a comunicação com o público e outras partes interessadas durante e após a ocorrência de um incidente, garantindo clareza, transparência e alinhamento nas informações divulgadas.

As suas principais atribuições relacionadas ao PRI são:

a) Em conjunto com o Encarregado, colaborar na comunicação aos titulares dos dados afetados, assegurando que as informações sejam claras, precisas e transmitidas dentro dos prazos estabelecidos pela LGPD;
b) Ajudar a proteger a reputação da organização, lidando com comunicações sensíveis e gerenciando possíveis crises de imagem causadas pelo incidente;

4.5 Gestores de Sistemas

Os Gestores de Sistemas desempenham um papel crucial no Plano de Resposta a Incidentes (PRI), uma vez que possuem conhecimento operacional sobre os sistemas e aplicações sob sua responsabilidade. Suas atribuições dentro do PRI são essenciais para garantir a pronta resposta a incidentes, minimizando impactos e assegurando a continuidade das operações.

As suas principais atribuições relacionadas ao PRI são:

a) Atuar em colaboração com a Equipe de Resposta a Incidentes no esclarecimento de questões de negócios relacionadas aos sistemas, contribuindo na contenção, mitigação e recuperação dos sistemas afetados;

b) Autorizar ações que serão realizadas nos sistemas pela Equipe de Resposta a Incidentes, relacionadas a contenção, mitigação e recuperação dos sistemas afetados;

4.6 Controlador

O papel do Controlador no PRI, segundo a LGPD, é central e de grande responsabilidade. O Controlador é a pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No contexto de incidentes de segurança envolvendo dados, suas responsabilidades incluem:

a) notificar a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares dos dados sobre incidentes que possam acarretar risco ou dano relevante, isso inclui a descrição da natureza dos dados afetados, os titulares envolvidos, as medidas técnicas e de segurança adotadas, e os possíveis impactos;
b) acompanhar toda a execução do PRI e tomar decisões, quando necessário, sobre as ações e procedimentos a serem adotados em todas as etapas do Plano;
c) o Controlador deve revisar o incidente, analisar suas causas e decidir sobre ajustes nos procedimentos e sistemas para minimizar riscos de novos incidentes.

5. ETAPAS DO PROCESSO DE RESPOSTA A INCIDENTES

Este tópico descreve o conjunto de fases estruturadas que guiam a atuação da CGE diante de um incidente de segurança. Esse processo é composto por etapas essenciais, que incluem a Identificação do incidente, com a coleta de informações iniciais e a análise da sua gravidade; a Contenção, que visa impedir a propagação e os danos; a Erradicação, que busca remover a causa raiz do incidente; a Recuperação, onde são restabelecidos os serviços e sistemas

afetados de maneira segura; e, por fim, a Revisão Pós-Incidente, que envolve a documentação e análise das ações tomadas para aprimorar os procedimentos futuros. Cada etapa segue um fluxo coordenado, com a participação de equipes técnicas e gestoras, garantindo uma resposta rápida, eficaz e alinhada às políticas de segurança da informação e conformidade legal.

5.1 Notificação

Um novo incidente é notificado, por pessoa externa ou não à CGE ou por alarme de monitoramento da CGE. A comunicação inicial do incidente pode ser proveniente de qualquer fonte, tais como e-mails, telefone, manifestação de ouvidoria (incluindo as recebidas pelo Encarregado quando se tratar de notificação do titular dos dados pessoais), devendo todas serem cadastradas no sistema de abertura de chamados da CGE.

5.2 Identificação

A partir da notificação recebida, inicia-se a atividade de identificação do incidente, que consiste em confirmar de maneira precisa e oportuna, se um incidente de segurança ocorreu, além de identificar os casos que possam envolver dados pessoais. A identificação do incidente envolve a detecção de sinais ou evidências de que uma violação de segurança ocorreu ou está em andamento.

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).

A etapa de Identificação é crítica para reconhecer rapidamente a presença de um incidente e iniciar o processo de resposta de forma coordenada e eficaz, minimizando danos e permitindo uma recuperação mais rápida

5.3 Classificação

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.

Cada incidente deve ser classificado com base nos critérios Gravidade, Urgência, Impacto e Recorrência, conforme modelo abaixo:

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

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

Essa classificação deve ser realizada pela Equipe Técnica de Resposta a Incidentes e pelo Encarregado de Dados Pessoais.

5.4 Contenção

A etapa de Contenção consiste em 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.

Os procedimentos a serem executados nesta etapa podem incluir:

a) desconectar dispositivos comprometidos da rede para evitar a propagação;
b) suspender contas comprometidas ou desativar acessos não autorizados;
c) 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;

5.5 Erradicação

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.

Os procedimentos a serem realizados nessa etapa podem compreender:

a) usar ferramentas de antivírus, anti-malware e soluções de segurança especializadas para garantir a eliminação de todos os arquivos maliciosos;
b) corrigir vulnerabilidades exploradas pelo incidente, como falhas de software ou sistemas desatualizados;
c) atualizar credenciais comprometidas e implementar políticas de senhas mais seguras para evitar novos acessos não autorizados;

d) 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;

5.6 Recuperação

Essa etapa tem como objetivo 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.

Os procedimentos a serem realizados nessa etapa podem compreender:

a) reinstalar ou recuperar sistemas e serviços afetados a partir de backups seguros;
b) garantir que as versões restauradas estejam livres de comprometimentos ou vulnerabilidades;
c) comparar os dados restaurados com os backups ou versões anteriores para garantir a integridade e evitar perda de informações;
d) implementar monitoramento em tempo real nos sistemas recuperados para detectar qualquer atividade anômala ou indício de reinfecção;

5.7 Comunicação e Notificação

O principal objetivo desta etapa é garantir que as partes interessadas sejam informadas de maneira clara, rápida e precisa sobre o incidente, suas implicações e as ações tomadas para mitigar seu impacto. Isso visa minimizar o pânico, evitar a disseminação de informações incorretas, assegurar que todos compreendam seu papel no processo de resposta, cumprir as obrigações legais e regulatórias, além de manter a transparência e a confiança de todos os envolvidos.

É importante destacar que as comunicações relacionadas aos incidentes podem ocorrer em todas as etapas do Plano, com o objetivo de manter as partes interessadas informadas sobre os procedimentos em andamento. Nesse sentido, é fundamental elaborar um plano de comunicação adequado, que identifique claramente as partes interessadas, internas e externas, defina a frequência e os prazos das comunicações, além de garantir que o conteúdo seja relevante e atualizado periodicamente.

Seguem as diretrizes que devem ser seguidas nesta etapa:

a) **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;
b) **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. Além disso, deve se indicar o número de titulares cujos dados são tratados nas atividades afetadas pelo incidente. Informar uma pessoa ou equipe que possa ser contatada para obter mais detalhes ou esclarecimentos;
c) **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;

d) **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;

5.8 Revisão pós-incidente

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.

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 CGE de lidar com ameaças, promovendo uma cultura de aprimoramento contínuo e aprendizado.

Seguem as diretrizes que devem ser seguidas nesta etapa:

a) avaliar o desempenho da equipe de resposta a incidentes (IRT), revisando se as ações tomadas seguiram os procedimentos estabelecidos no Plano de Resposta a Incidentes (PRI);
b) verificar se a comunicação interna e externa foi eficaz, oportuna e clara durante todas as fases do incidente;

c) identificar se houve falhas ou lacunas no PRI, como falta de procedimentos ou áreas que necessitem de ajustes ou melhorias;

5.9. Relatório de Incidentes

O Relatório de Incidentes do Plano de Resposta a Incidentes (PRI) tem como principal objetivo documentar de maneira detalhada e estruturada todo o processo de resposta ao incidente, desde sua identificação até a resolução. Ele visa fornecer uma visão completa das ações executadas, analisar as causas do incidente, avaliar os impactos para a organização e sugerir medidas corretivas e preventivas. Além de servir como um registro oficial para consulta futura, o relatório é fundamental para identificar falhas nos procedimentos e possibilitar a melhoria contínua das práticas de segurança da informação, garantindo maior eficiência e conformidade legal em incidentes subsequentes

Para elaboração do Relatório de Incidentes:

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 vírus, 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

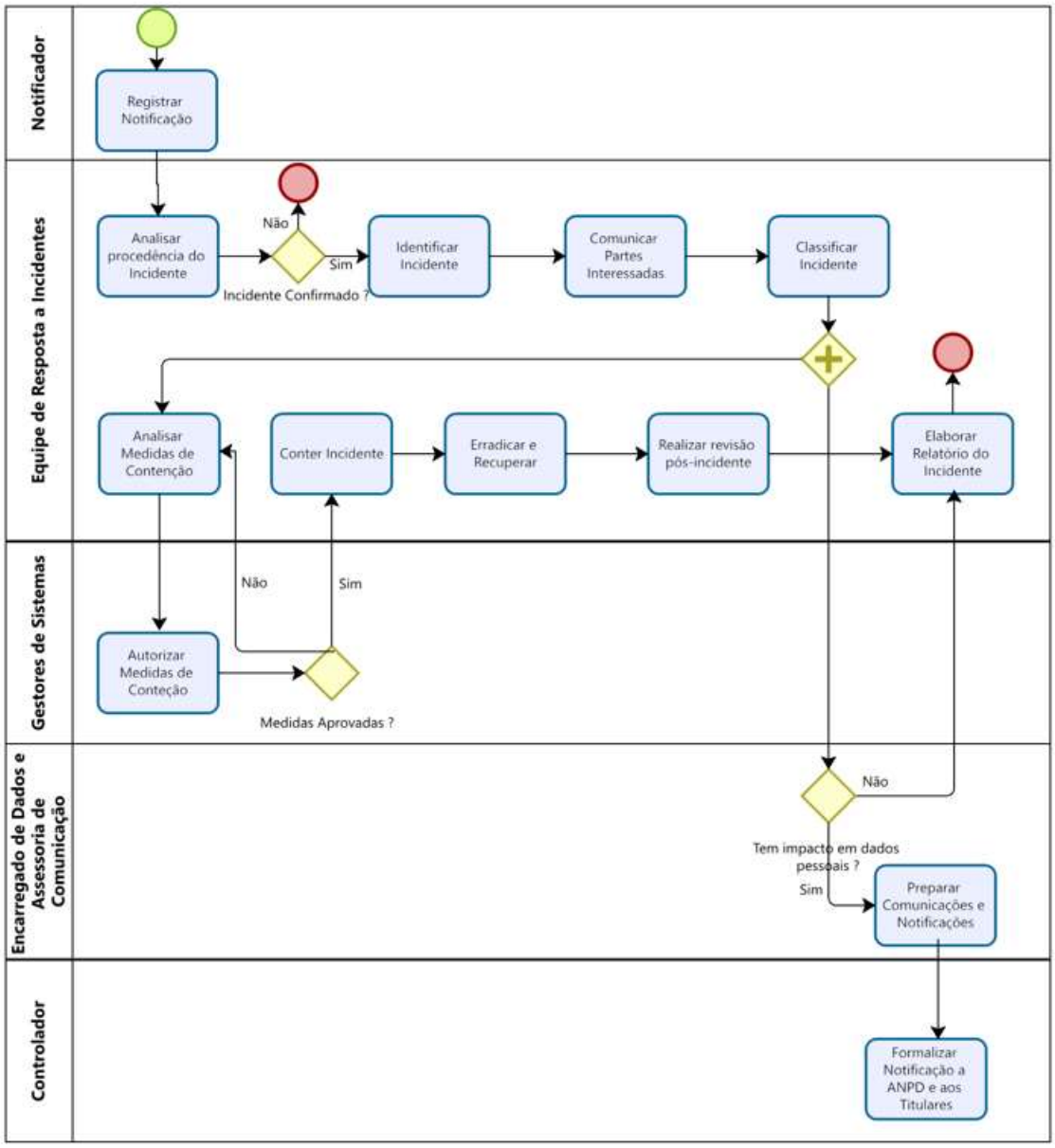
tempo necessário para retomá-las, Estimar os custos relacionados ao incidente, incluindo perdas financeiras diretas, custos de mitigação e possíveis multas e Analisar o impacto na imagem e reputação da organização, especialmente se os titulares de dados ou o público foram afetados;

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:** propor melhorias no PRI, nas políticas de segurança da CGE 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;

5.10. Fluxo do Processo de Resposta a Incidentes



6. DISPOSIÇÕES FINAIS

A Controladoria e Ouvidoria Geral do Estado (CGE) destaca a importância deste Plano como um instrumento estratégico para a proteção das informações e a continuidade dos serviços críticos da organização. A implementação de um

processo estruturado para o tratamento de incidentes fortalece a capacidade da CGE de responder de forma ágil e eficaz às ameaças que possam comprometer a segurança de seus dados e sistemas.

A execução bem-sucedida do PRI exige o comprometimento de todos os envolvidos, desde a alta gestão até os servidores que operam os sistemas, assegurando que as responsabilidades estejam claramente definidas e que as equipes sejam devidamente capacitadas. A integração entre as áreas técnica, operacional e estratégica é essencial para o alinhamento das ações de resposta e para a minimização dos impactos de possíveis incidentes.

É importante ressaltar que o PRI não é um documento estático. Ele deve ser revisado e aprimorado continuamente, à medida que novas ameaças e tecnologias emergem, e conforme a CGE acumula experiências no tratamento de incidentes. Além disso, a conformidade com a Lei Geral de Proteção de Dados (LGPD), a CGE reafirma o compromisso da instituição com a segurança da informação e a proteção de dados pessoais.

Por fim, o sucesso na resposta a incidentes depende da prevenção, da rápida detecção e da capacidade de adaptação frente a um cenário de ameaças em constante evolução. O PRI da CGE reflete o compromisso da organização em promover uma cultura de segurança da informação robusta e em garantir a integridade, a confidencialidade e a disponibilidade dos dados, contribuindo para a transparência e a confiança pública nos serviços prestados.

7. REFERÊNCIAS BIBLIOGRÁFICAS

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

Lei Estadual Nº 18.699/2024 – Modelo de Governança da Proteção de Dados do Poder Executivo Estadual;

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

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

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