PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA

DA SECRETARIA DE ESTADO DA ADMINISTRAÇÃO - SEA/SC

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Versão 1.1

GOVERNO DE SANTA CATARINA
SECRETARIA DE ESTADO DA ADMINISTRAÇÃO

GOVERNO DE SANTA CATARINA
SECRETARIA DE ESTADO DA ADMINISTRAÇÃO

EQUIPE TÉCNICA DE ELABORAÇÃO

PAPEL	PESSOA DESIGNADA	SETOR / CONTATO
Controlador	Luiz Antônio Dacol	Secretário da Administração / Secretaria
Controlador Suplente		Secretário-Adjunto da Administração / Secretaria
Comitê Gestor de Proteção de Dados Pessoais - CGPD/SC	Félix Fernando da Silva – Coordenador Alessandro de Oliveira dos Santos Elenise Magnus Hendler Gisela de Souza Fonseca João Mário Martins Jucelito Darela Mendes Lisandro José Fendrich Luis Haroldo de Mattos Marina de Sousa Santos Garcia Rebelo Tayse Schristine Marian Borges Victor Martins Maeberg Yalle Hugo de Souza	Comitê Gestor de Proteção de Dados Pessoais - CGPD/SC / comitelgpd@sea.sc.gov.br
Encarregado de Dados Pessoais - DPO	Mylene Mendonça	encarregado@sea.sc.gov.br
Grupo de Trabalho Interno - GTI SEA	Mylene Mendonça Jucelito Darela Mendes Giovanna Gasparoto Paludo Gisele Faffe Pellegrini Karen Sabrina Bayestorff Duarte Laura Daiane Moraes Wolff Renata Schoeder Bion Simone da Silva Tabata Juliane Magrin Tayse Schristine Marian Borge Krause Victor Martins Maeberg Welliton Saulo da Costa	Grupo de Trabalho Interno - GTI SEA
Comitê de Segurança da Informação	Victor Martins Maeberg Daniel Pamplona Lisboa	Gerente de Infraestrutura e Segurança - GESIN Gerente de Tecnologia da Informação - GETIC
Jurídico	Elisângela Strada	Consultoria Jurídica - COJUR SEA cojur@sea.sc.gov.br
Relacionamento e atendimento	Encarregado de Dados OUVIDORIA	encarregado@sea.sc.gov.br cojur@sea.sc.gov.br http://ouvidoria.sc.gov.br/

SUMÁRIO

1. INTRODUÇÃO..... 1
2. OBJETIVOS..... 2
3. DEFINIÇÕES GERAIS..... 3
4. INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS..... 6
   - AVALIAR INTERNAMENTE O INCIDENTE..... 7
   - COMUNICAR O CONTROLADOR..... 8
   - CONSULTAR O GRUPO DE TRABALHO INTERNO DO ÓRGÃO/ENTIDADE (GTI)..... 8
   - COMUNICAR A TODOS OS ENVOLVIDOS.... 8
   - COMUNICAR À ANPD..... 9
   - EMITIR O RELATÓRIO FINAL..... 9
5. RESPOSTAS AOS INCIDENTES DE SEGURANÇA. 12
6. COMUNICAÇÃO À ANPD E TITULAR DE DADOS PESSOAIS..... 16
7. RELATÓRIO FINAL DO INCIDENTE..... 17

GOVERNO DE SANTA CATARINA
SECRETARIA DE ESTADO DA ADMINISTRAÇÃO

1. INTRODUÇÃO

Este Plano de Resposta a Incidentes de Segurança foi elaborado com base no guia utilizado pelo Governo Federal, constituindo-se como um complemento aos demais planos da POSIN (Política de Segurança da Informação), elaborados e publicados pela SEA (Secretaria de Estado da Administração de Santa Catarina).

O propósito do presente documento é trazer uma visão macro sobre resposta a incidentes de segurança específicos da Secretaria, para fomentar a adequação à Lei Geral de Proteção de Dados Pessoais.

O plano dispõe de medidas que devem ser adotadas no caso de uma situação de emergência ou evento de risco que possa ocasionar danos aos ativos tecnológicos da SEA, viabilizando, inclusive, a comunicação apropriada e tempestiva à ANPD, quando for o caso.

Este plano será atualizado continuamente para incorporar melhorias, à medida que forem publicadas novas normas e que os processos de proteção de dados existentes sejam amadurecidos no contexto estadual.

GOVERNO DE SANTA CATARINA
SECRETARIA DE ESTADO DA ADMINISTRAÇÃO

2. OBJETIVOS

Objetivo geral: Orientar a todos da SEA em como responder as situações de emergência com incidentes de segurança da informação, de forma documentada, formalizada, rápida e confiável, ao passo em que resguarde as evidências que possam ajudar a prevenir novos incidentes e a atender às exigências legais de comunicação e transparência.

Objetivos específicos:

- Conferir clareza sobre o fluxo de procedimentos adequados e responsáveis no caso de incidentes;
- Preservar a reputação e imagem da SEA;
- Assegurar respostas rápidas, efetivas e coordenadas;
- Quantificar e monitorar desempenho;
- Evoluir continuamente com as lições aprendidas;
- Tornar a SEA referência em proteção de dados pessoais, no âmbito da Administração Pública do Estado de Santa Catarina.

3. DEFINIÇÕES GERAIS

Para auxílio na leitura deste guia, serão adotadas as seguintes definições no que se refere a incidentes ocorridos nos órgãos e entidades da administração pública estadual:

Agente de tratamento

São agentes de tratamento aqueles que podem ter alguma ação no tratamento de um incidente que coloque em risco a segurança dos dados pessoais. Tais agentes abrangem:

Controlador

Pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais; na administração pública estadual, os órgãos exercem as funções típicas do controlador.

Operador

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Observação: A depender do contexto, uma mesma operação de tratamento de dados pessoais pode envolver mais de um operador ou controlador (controladoria conjunta, ou co-controladores).

Encarregado

Também conhecido como DPO (Data Protection Officer), é a pessoa indicada pelo controlador e pelo operador para atuar como canal de comunicação com os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

ANPD

Os arts. 55-A e seguintes da LGPD definem a Autoridade Nacional de Proteção de Dados (ANPD) como entidade responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional, conforme as atribuições descritas no art. 55-J da LGPD e no Decreto nº 10.474, de 26 de agosto de 2020.

Dado pessoal

É toda informação relacionada à pessoa natural identificada ou identificável.

IDP

O Inventário de Dados Pessoais representa um artefato primordial para documentar o tratamento de dados pessoais realizados pela instituição.

Incidente

Evento, ação ou omissão que tenha permitido ou possa vir a permitir acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou, ainda, apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

Incidente de segurança

Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

Incidente de segurança com dados pessoais

Incidente de segurança à proteção de dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação de dados pessoais, sendo acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento ou qualquer forma de tratamento de dados ilícita ou inadequada, que tem a capacidade de pôr em risco os direitos e as liberdades dos titulares dos dados pessoais.

LGPD

Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), cujo objetivo é proteger os direitos fundamentais de privacidade e de liberdade de cada indivíduo.

Relatório final

Relatório que contém todas as evidências e ações realizadas para tratamento do incidente e que deve ser emitido ao final das tratativas.

RIPD

Conforme a LGPD, o Relatório de Impacto a Proteção de Dados (RIPD) é uma documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que tem o potencial de gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

GTI LGPD SEA

Grupo de Trabalho Interno instituído pela Portaria nº 738/2021, com o objetivo de promover a implementação das disposições da Lei nº 13.709/2018 - LGPD.

4. INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

Conforme estabelecido no artigo 46 da LGPD, os agentes de tratamento devem adotar medidas de segurança para proteger os dados pessoais desde a concepção até a sua execução. Ainda, o artigo 50 do referido normativo estabelece que controladores e operadores poderão formular regras de boas práticas e de governança para o tratamento de dados pessoais, podendo ser implementado um programa de governança e privacidade que conte com plano de resposta a incidentes e remediações.

Em caso de incidente que coloque em risco a segurança de dados pessoais devem ser realizados alguns procedimentos específicos que são listados abaixo:

1 AVALIAR INTERNAMENTE O INCIDENTE

Avaliar internamente o incidente para obter informações iniciais sobre o impacto do ocorrido, tais como:

- Origem;
- categoria;
- quantidade de titulares e de dados pessoais afetados;
- categoria e quantidade de dados afetados;
- consequências do incidente para os titulares e para a entidade;
- criticidade; e
- probabilidade.

Além disso, é necessário preservar todas as evidências do incidente.

2 COMUNICAR O CONTROLADOR

Comunicar o Controlador sobre o incidente para que este tome as devidas providências. O Encarregado de Dados deve também ser comunicado sobre o ocorrido.

3 CONSULTAR O GTI DO ÓRGÃO/ENTIDADE

Consultar o Grupo de Trabalho Interno do Órgão/Entidade em caso de incidentes na rede computacional. O GTI deve dar ciência aos gestores das áreas afetadas.

4 COMUNICAR A TODOS OS ENVOLVIDOS

Comunicar a todos os envolvidos (nos termos da LGPD), por parte do Controlador do dado, a existência do incidente.

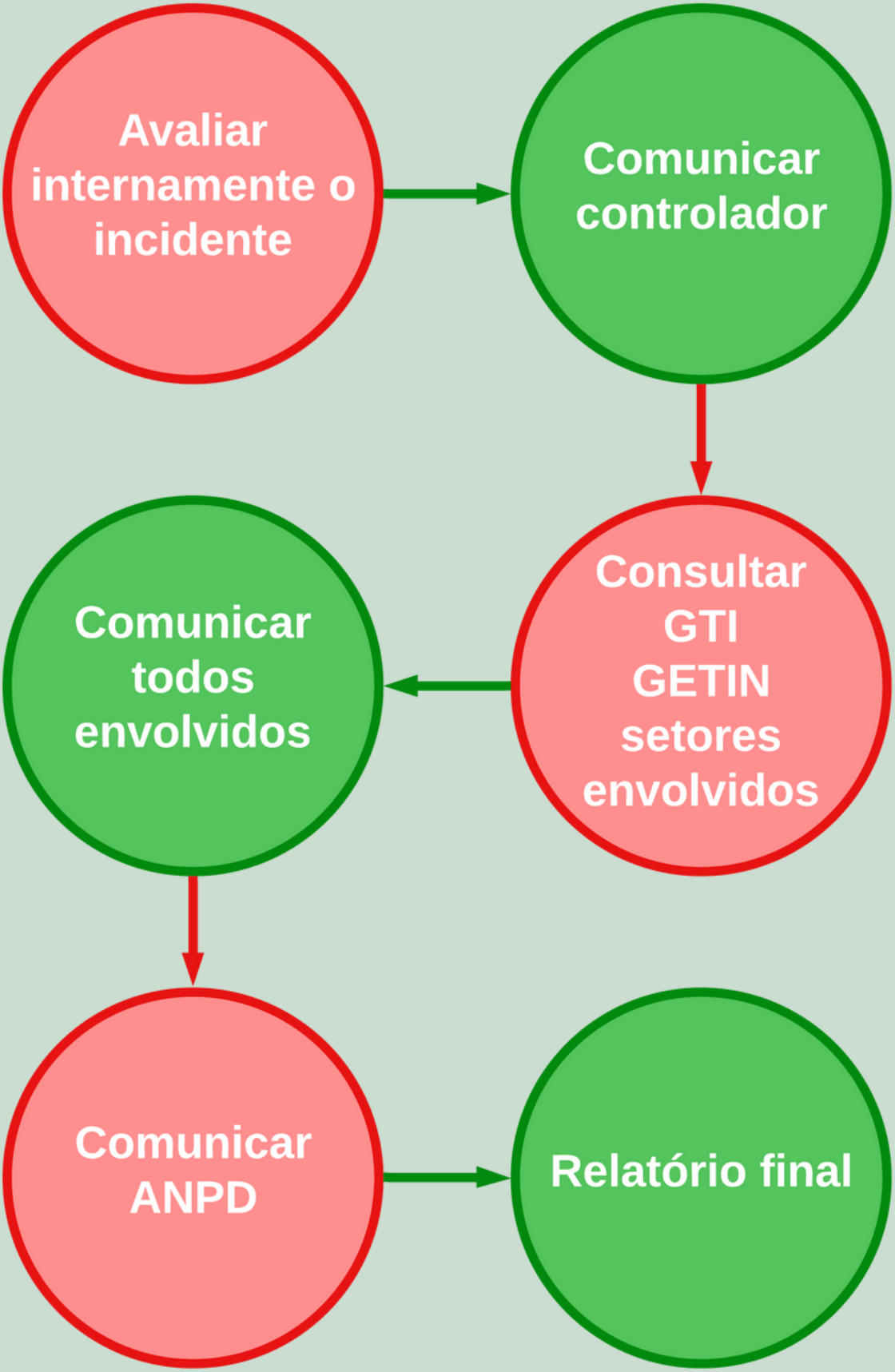
5 COMUNICAR À ANPD

Comunicar à ANPD e ao titular de dados pessoais (conforme art. 48 da LGPD) a existência do incidente e encaminhar o relatório inicial.

6 EMITIR O RELATÓRIO FINAL

Emitir o relatório final contendo os tipos de dados e a quantidade de titulares afetados. Deve também acompanhar um relatório técnico de tratamento que permita avaliar a extensão e adequação de medidas para incidentes futuros.

A FIGURA A SEGUIR APRESENTA DE MANEIRA SIMPLIFICADA ESTE PROCESSO:



ATENÇÃO!

O artigo 48 da LGPD afirma que em caso de incidente de segurança que venha a gerar risco ou dano considerado relevante aos titulares, **o controlador tem a obrigação de comunicar por meio do Encarregado de Dados à ANPD e ao titular dos dados pessoais. O prazo que a ANPD recomenda para essa comunicação é de 2 (dois) dias úteis.**

5. RESPOSTAS AOS INCIDENTES DE SEGURANÇA

A SEA vai dar respostas aos seus incidentes utilizando as orientações da POSIN e as fases dos NIST descritas abaixo e utilizando o fluxo detalhado e o checklist no final deste documento.

5.1. PREPARAÇÃO/NOTIFICAÇÃO

Esta fase é de suma importância, pois estabelece a capacidade de resposta para que a SEA esteja pronta para responder a incidentes, como também a evitá-los e garantir que sistemas, redes e aplicativos sejam suficientemente seguros. Na fase de preparação e notificação o DPO, GTI, CGPD, GESIN E GETIC estarão preparados para responder e dar os encaminhamentos para juntos atuarem na resposta aos incidentes.

5.2. ANÁLISE/AVALIAÇÃO

Os incidentes podem ser detectados por vários meios ou recebidos nos canais de comunicação da SEA. Assim que o órgão for notificado será iniciada uma avaliação mais detalhada do incidente pelo DPO, GESIN e GETIC, que farão a classificação e definirão a sua criticidade.

5.3. CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO

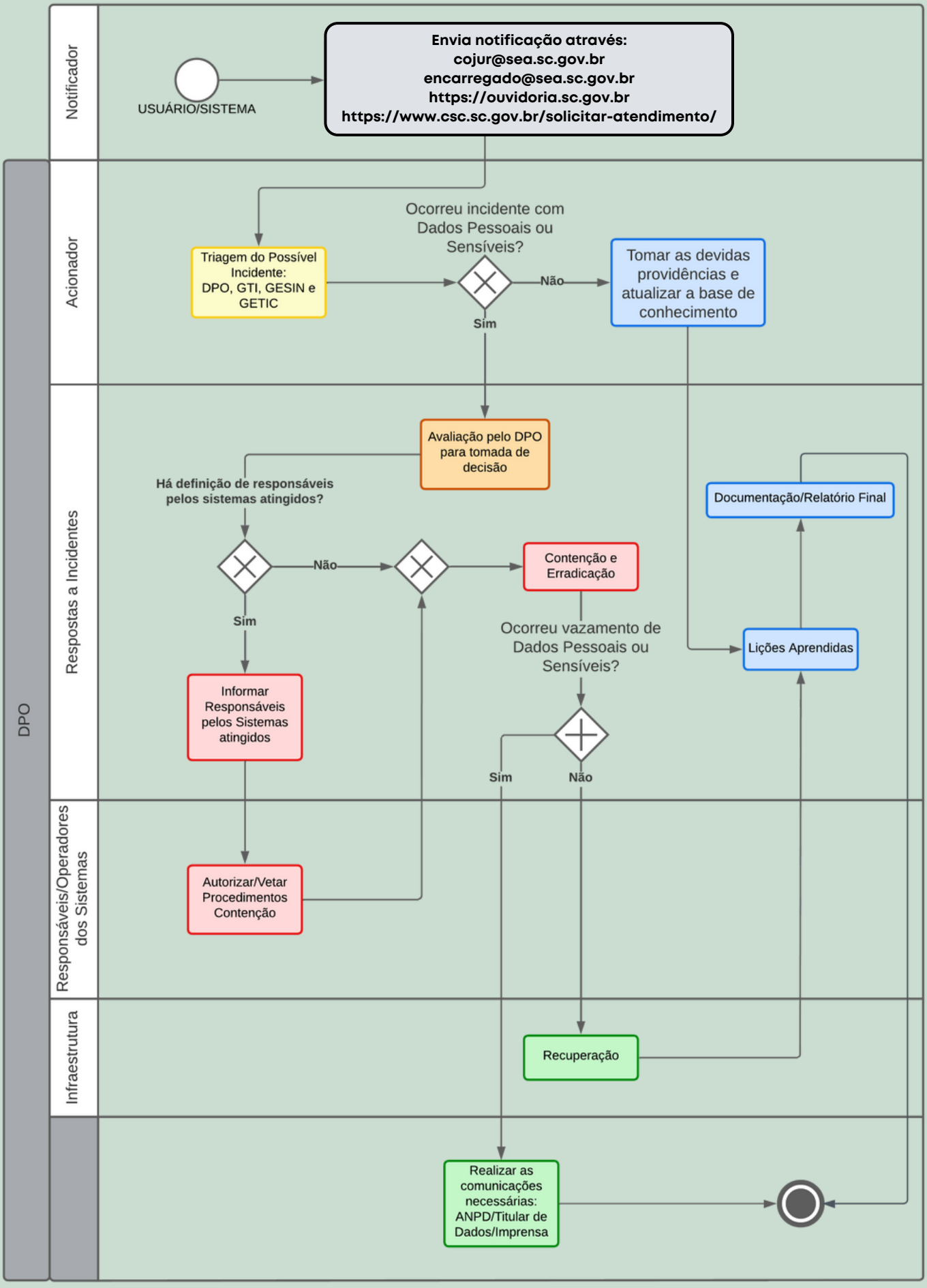
Os responsáveis pelos sistemas/processos impactados devem ser acionados para se manifestarem sobre os procedimentos de resposta, contenção e erradicação.

O objetivo das medidas de contenção e erradicação é limitar o dano e isolar os sistemas afetados para evitar mais danos. Aqui, conforme a necessidade e a autorização obtida, poderá ser realizado o desligamento dos sistemas inteiros ou de funcionalidades específicas e colocados avisos de indisponibilidade para manutenção. Todos os cuidados devem ser adotados para não impactar evidências que poderiam ser usadas para identificar autoria, origem e método usado para quebrar a segurança.

5.4. ATIVIDADES PÓS-INCIDENTE

Na fase de atividades pós-incidente, serão implementadas algumas atividades em busca da melhoria contínua de seus processos de resposta a incidentes, além de definir procedimentos para retenção de evidências e uso dos dados coletados em incidentes.

ABAIXO O FLUXO COMPLETO PARA RESPOSTAS A INCIDENTES



6. COMUNICAÇÃO À ANPD E TITULAR DE DADOS PESSOAIS

A comunicação à ANPD deve ser imediata e será realizada por intermédio do Encarregado de Dados designado pela SEA. A ANPD disponibiliza um Formulário de comunicação de incidente de segurança com dados pessoais que pode ser acessado por meio do link: https://www.gov.br/anpd/pt-br/assuntos/atual-formulario-de-comunicacao-de-incidentes-de-seguranca-com-dados-pessoais_01-03-2021-4.docx

A comunicação ocorre pelo encaminhamento do documento pelo sistema eletrônico do Governo Federal, disponível no link: https://www.gov.br/secretariageral/pt-br/sei-peticionamento-eletronico

Cabe ao controlador comunicar ao titular dos dados pessoais a ocorrência de incidente de segurança que tenha potencial de lhe gerar riscos ou danos relevantes. Tal notificação deve ser realizada de maneira transparente, podendo ser realizada por meios diversos, incluindo mensagens diretas (e-mails, SMS), banners, notificações em sites, comunicações postais e anúncios. O Controlador, com o apoio do Encarregado de Dados e GTI, deverá avaliar o risco no âmbito interno, com objetivo de estipular se há ou não risco ou dano relevante para a comunicação do incidente ao titular, sendo necessário justificativa para os casos em que se decidir por não comunicar o incidente.

7. RELATÓRIO FINAL DO INCIDENTE

Após a coleta de todas as informações e evidências, o Encarregado de Dados com o apoio do GTI, irá concluir o Relatório Final do Incidente.

O Relatório final será realizado com base em todas as evidências coletadas desde a identificação do incidente até o final das apurações. Nesse documento constará, além de todas as informações sobre o incidente, todas as propostas de melhorias e/ou aquisições sugeridas para redução dos riscos de novas ocorrências. O relatório, além de ter uma função de comprovação das medidas tomadas pela SEA frente às autoridades, é importante para que todos os envolvidos e demais servidores possam aprender com o ocorrido, podendo compreender suas causas, bem como avaliar em que sentido seu Plano de Respostas a Incidentes e seus procedimentos foram efetivos ou não, analisando a atuação dos responsáveis.

O relatório final do incidente será assinado pelo Controlador e pelo Encarregado de Dados e deve ficar disponível para consulta em caso de atualização do relatório de impacto à proteção de dados (RIPD). Esse relatório poderá, ainda, ser apresentado a autoridades policiais, órgãos reguladores ou demais envolvidos.

A SEGUIR, APRESENTA-SE UM CHECKLIST PARA VERIFICAÇÃO DO TRATAMENTO DE INCIDENTES.

	Ação	Realizado?
Detecção e análise		
1.	Determinar se ocorreu um incidente	
1.1	Analisar os precursores e os indicadores	
1.2	Buscar por informações correlatas	
1.3	Realizar pesquisa do incidente (via mecanismos de busca e bases de conhecimento)	
1.4	Documentar, investigar e reunir e evidências assim que a equipe identificar a ocorrência do incidente	
2.	Priorizar o tratamento com base em sua relevância (impacto de negócio, impacto de informação e recuperabilidade)	
3.	Comunicar o incidente às equipes internas envolvidas e, quando necessário, aos atores externos	
Contenção, erradicação e recuperação		
4.	Coletar, preservar, proteger e documentar as evidências	
5.	Conter o incidente	
6.	Erradicar o incidente	
6.1	Identificar e mitigar todas as vulnerabilidades exploradas	
6.2	Remover malware, materiais impróprios e outros componentes	
6.3	Se mais hosts afetados forem descobertos (por exemplo, novas infecções por malware), repetir as etapas de detecção e análise (1.1, 1.2) para identificar todos os outros hosts afetados, para então conter (5) e erradicar (6) o incidente em tais hosts	
7	Recuperar-se do incidente	
7.1	Retornar os sistemas afetados ao estado operacional	
7.2	Confirmar se os sistemas afetados estão funcionando normalmente	
7.3	Se necessário, implementar monitoração adicional para encontrar futuras atividades relacionadas	
Atividades pós-incidente		
8.	Criar o relatório de acompanhamento	
9.	Realizar uma reunião de lições aprendidas (tal reunião é obrigatória para incidentes graves e opcional para os demais incidentes)	