GOVERNO DE SANTA CATARINA
SECRETARIA DE ESTADO DA ADMINISTRAÇÃO

Guia de Resposta a Incidentes de Segurança

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Versão 1.0
Florianópolis, fevereiro de 2022

GOVERNO DE SANTA CATARINA
SECRETARIA DE ESTADO DA ADMINISTRAÇÃO

GUIA DE RESPOSTA A INCIDENTES DE SEGURANÇA

SECRETARIA DE ESTADO DA ADMINISTRAÇÃO

Jorge Eduardo Tasca - Secretário da Administração

Luiz Antônio Dacol - Secretário-Adjunto da Administração

Comitê Gestor de Proteção de Dados Pessoais - CGPD/SC

Félix Fernando da Silva – Coordenador

Alessandro de Oliveira dos Santos

Elenise Magnus Hendler

Fernanda Donadel da Silva

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

Equipe Técnica de Elaboração

Alexandre Aguiar Moura

Fernando Zanner

Marcos Silvio da Rosa

Maurício de Alexandrino

GOVERNO DE SANTA CATARINA
SECRETARIA DE ESTADO DA ADMINISTRAÇÃO

Histórico de Versões

Data	Versão	Descrição	Autor
19/10/2021	1.0	Primeira versão do Guia Resposta a Incidentes.	Equipe Técnica de Elaboração
30/12/2021	1.1	Revisão do fluxo de atividades e descrições	Equipe Técnica de Elaboração
09/02/222	1.2	Correções sugeridas pelos membros do CGPD	CGPD
14/02/2022	1.3	Revisão e validação pelo Comitê Gestor de Proteção de Dados Pessoais	CGPD

SUMÁRIO

INTRODUÇÃO

Na administração pública o gerenciamento de resposta a incidentes de segurança deve incluir as estratégias, as habilidades, as pessoas, os processos e as ferramentas que os órgãos e entidades precisam prover para identificar, tratar e restaurar os serviços o mais rápido possível. Este Guia 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 Secretaria de Estado da Administração. De caráter orientativo, o propósito do presente guia é trazer uma visão macro sobre resposta a incidentes de segurança, para fomentar a adequação à Lei Geral de Proteção de Dados Pessoais. Cada órgão e entidade estadual é livre para adequar todas as proposições deste guia à sua realidade operacional.

Além disso, o guia também busca auxiliar tanto os profissionais que estão ou que serão designados ao tratamento de dados, assim como os profissionais responsáveis pelo tratamento de incidentes cibernéticos. Ressalta-se que a leitura deste guia não substitui a leitura dos documentos aqui referenciados ou de qualquer normativo já existente na administração pública estadual que verse sobre o assunto.

Este guia 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.

1 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 competem 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.

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: 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).

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS: 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 a 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 contenha 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.

2 INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

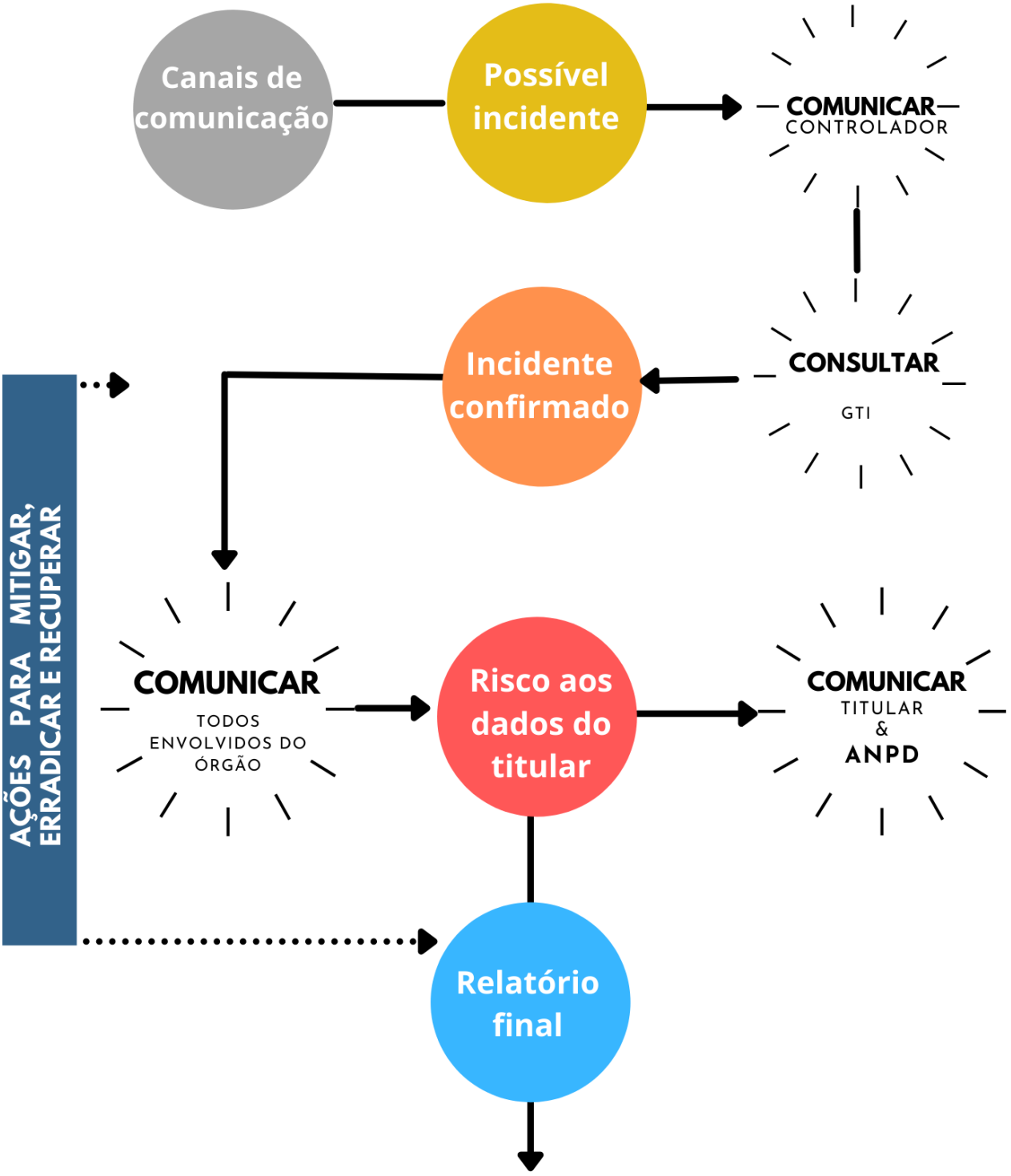
Conforme estabelecido no artigo 46 da LGPD, os agentes de tratamento devem adotar medidas de segurança para proteger os dados pessoais desde a concepção até a sua execução. Ainda, o artigo 50 do referido normativo estabelece que controladores e operadores poderão formular regras de boas práticas e de governança para o tratamento de dados pessoais, podendo ser implementado um programa de governança e privacidade que conte com planos 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** para obter informações iniciais sobre o impacto do ocorrido, tais como: fonte, 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** sobre o incidente para que este tome as devidas providências. O **Encarregado de Dados** deve também ser comunicado sobre o ocorrido.
3. **Consultar o Grupo de Trabalho Interno do órgão/entidade (GTI)** em caso de incidentes na rede computacional. O GTI deve dar ciência aos gestores das áreas afetadas.
4. **Comunicar a todos os envolvidos** (nos termos da LGPD), por parte do CONTROLADOR do dado, a existência do incidente.
5. **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** contendo os tipos de dados e a quantidade de titulares afetados. Deve também acompanhar um relatório técnico de tratamento que permita avaliar extensão e adequação de medidas para incidentes futuros.

A figura a seguir apresenta de maneira simplificada este processo:

FLUXOGRAMA DE NOTIFICAÇÃO DE INCIDENTES



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.**

2.1 - Avaliar internamente o incidente

A avaliação será feita pelo Controlador, que contará com as figuras do Encarregado de Dados, do Grupo de Trabalho interno e dos gestores dos sistemas afetados para realização desta tarefa.

Itens a serem avaliados:

a. **Qual vulnerabilidade foi explorada no incidente:** listar situações como: acesso indevido ou não autorizado aos dados pessoais; perda ou roubo de dados; ataques cibernéticos; erros de programação de aplicativos e sistemas internos; engenharia social; descartes indevidos; repasse indevido de dados pessoais; roubo, venda e utilização de dados tutelados pela entidade; comprometimento de senhas de acesso; entre outras.

b. **Fonte dos dados pessoais:** listar o meio em que foram obtidos os dados pessoais, tais como preenchimento de formulário eletrônico ou não eletrônico.

c. **Categoria de dados pessoais:**

- dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

- dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

d. **Extensão do vazamento:** realizar o dimensionamento da extensão do dano, quantificando, se possível, os titulares e os dados pessoais que tiveram a sua segurança comprometida no incidente.

e. **Avaliação do impacto ao titular:** avaliar quais os impactos que o incidente pode gerar aos titulares.

f. **Avaliação do impacto no serviço:** avaliar os impactos que o incidente pode gerar ao órgão/entidade, como perda de confiabilidade do cidadão, danos à imagem, ações judiciais e impacto total ou parcial nas atividades desenvolvidas.

Neste cenário, todos os passos devem ser devidamente documentados, desde o momento inicial de atuação até a contenção e os efeitos.

Exemplo de ações a serem feitas:

a) Registrar como se deu a comunicação do incidente, como este foi descoberto (resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento, data e hora da detecção, data e hora do incidente e sua duração);

b) Mencionar quais as causas preliminares identificadas;

c) Relatar as circunstâncias em que ocorreu a violação de segurança de dados pessoais (perda, roubo, cópia, vazamento, dentre outros);

d) Realizar reuniões/entrevistas com as pessoas envolvidas;

e) Identificar possíveis consequências e efeitos negativos sobre os titulares dos dados afetados;

f) Descrever quais os dados pessoais e informações afetadas (natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados);

g) Verificar se o sistema ainda está comprometido e o que deve ser feito para que novas ameaças sejam contidas (resumo das medidas implementadas até o momento para controlar os possíveis danos);

h) Relatar se foram tomadas medidas de segurança, técnicas e administrativas preventivas pelo controlador de acordo com a LGPD;

g) Possíveis problemas de natureza transfronteiriça;

i) Outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.

Isso inclui, mas não se limita a:

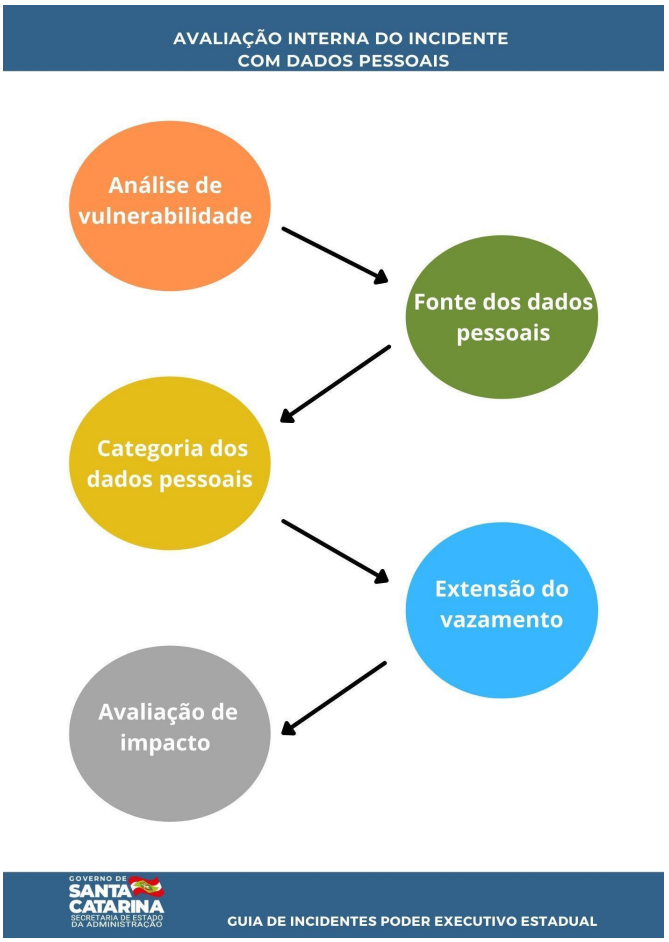
a. Todos os logs dos sistemas internos e externos envolvidos no incidente;

b. Interações do time envolvido e todas as medidas adotadas;

c. Eventuais contratações de ferramentas e equipes de especialistas e auditores para atuação pontual no incidente a ser tratado;

d. Atas das reuniões relevantes.

A figura a seguir demonstra, de forma ilustrativa, as atividades da avaliação interna acima abordadas:



2.2 - Comunicar o Controlador do órgão/entidade

É importante que os órgãos e as entidades da administração pública estadual criem mecanismos para facilitar que seus colaboradores internos (servidores, estagiários e terceirizados) notifiquem o Controlador e/ou o Encarregado de dados. O conhecimento de um incidente por qualquer colaborador, fornecedor ou parte interessada deve ensejar uma comunicação ao Controlador, o mais breve possível, para as providências previstas sobre comunicação de incidentes de segurança.

O Operador deve comunicar incidentes com dados pessoais ao Controlador de forma breve, a fim de viabilizar que ele exerça seu papel tempestivamente. Caso a relação entre Controlador e Operador seja feita em razão de contrato administrativo, tal obrigação de notificação tempestiva deve constar nas cláusulas contratuais.

2.3 - Consultar o Grupo de Trabalho Interno do órgão/ entidade (GTI)

O Controlador, por intermédio do Encarregado de Dados, pode consultar o GTI para obter detalhamento sobre o incidente e produzir o relatório de comunicação do incidente. Este relatório deverá minimamente descrever o incidente; se possível, indicar a sua origem ou a razão de não ser possível identificá-la; como foi detectado; quais foram os dados coletados e

preservados; outros dados julgados relevantes; quais foram as ações de tratamento e resposta ao incidente; como foram preservados os registros (ferramentas utilizadas); qual foi o local de armazenamento das informações preservadas.

2.4 - Comunicar a todos os envolvidos no órgão/entidade

- Quem?

  Controlador, Encarregado de Dados e setores afetados e, caso haja, operador de dados.

- Quando deve haver a comunicação?

  A comunicação deve ocorrer imediatamente após o conhecimento dos fatos. Contudo, a Lei 13.709/2018 traz exceções em seu artigo 4º.

2.5 - Comunicar à ANPD e ao titular de dados pessoais

A LGPD prevê, em seu art. 48, que, em caso de ocorrência de incidente, o controlador deve notificar tanto o titular como a Autoridade Nacional de Proteção de Dados (ANPD) em um prazo razoável, exceto nos casos em que a violação não apresente um risco de relevância aos direitos e liberdades dos indivíduos, como, por exemplo, quando os dados forem anonimizados ou criptografados.

A organização deve criar critérios, com base na LGPD, nos normativos e nas orientações da ANPD, que definam o que é um incidente que possa acarretar risco ou dano relevante aos titulares. Especialmente nos incidentes que envolvam dados do titular, é importante que se elabore um procedimento para potenciais questionamentos que venham a surgir.

Alguns questionamentos que podem auxiliar na determinação do risco:

1. Quais informações foram objeto do incidente?
2. O titular pode ser vítima de fraude em razão do incidente?
3. O incidente foi devidamente comunicado às autoridades?
4. O que o titular pode fazer em benefício da sua proteção?
5. Onde o titular pode obter mais informações sobre o incidente?

A **ANPD** disponibiliza um modelo 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 peticionamento eletrônico do Governo Federal, disponível no link https://www.gov.br/secretariageral/pt-br/sei-peticionamento-eletronico.

Conforme mencionado anteriormente, 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. A organização 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.

2.6 - Emitir o relatório final do incidente

É importante que todas as informações e evidências coletadas e as ações do processo de tratamento de incidente de segurança à proteção de dados sejam documentadas, de modo a possibilitar a elaboração de um relatório final do incidente, o qual será assinado pelo Controlador e pelo Encarregado de Dados. Nele devem estar contidas as devidas considerações para a promoção da melhoria contínua dos processos de tratamento de incidentes, bem como deve ficar disponível para consulta em caso de atualização do relatório de impacto à proteção de dados (RIPD). Este relatório, poderá, ainda, ser apresentado a autoridades policiais, órgãos reguladores ou demais envolvidos.

3 RESPOSTA A INCIDENTES CIBERNÉTICOS

3.1 – Planejamento de resposta a incidentes computacionais

Conforme disciplina a Instrução Normativa SEA nº 20/2021, **cada órgão deve criar uma Política de Segurança da Informação (POSIN)** composta por planos orientando a criação de procedimentos internos para o tratamento e respostas de incidentes, seja o incidente de proteção com dados pessoais ou não. Os modelos para que os órgãos e entidades da administração pública estadual possam definir as suas diretrizes estão disponíveis no link https://www.sea.sc.gov.br/diretoria-de-tecnologia-e-inovacao/lgpd/. O **NIST (National Institute Of Standards and Technology)**, no documento NIST.SP.800-61r2, também define que as organizações devem desenvolver a política de gestão de resposta a incidentes por intermédio dos seguintes mecanismos:

a. **Plano de resposta a incidentes:** criar planos de resposta a incidentes de acordo com vulnerabilidades conhecidas, serviço impactado, severidade do incidente. Se o órgão/entidade já criou os planos de continuidade de negócio e gestão de riscos, os incidentes estarão contidos neles. Importante que esses planos devem ser aprovados pela alta gestão do órgão/entidade.

b. **Equipes para o tratamento de incidentes computacionais:** criar e treinar equipes especializadas para o tratamento de incidentes computacionais, cabendo-lhes o papel de atuação para resolução do incidente, restauração do ambiente e comunicação interna e externa à organização. *Na POSIN, disponibilizada pela SEA, o modelo de Plano de Continuidade de Negócio orienta a criação de equipes para respostas aos incidentes.*

c. **Procedimentos internos e relatórios para ações de resposta:** criar plano de resposta a incidentes computacionais que contenha procedimentos com tarefas específicas a serem executadas por uma determinada equipe para a contenção e mitigação de incidentes e restauração dos serviços ao estado pré-incidente.

d. **Diretrizes e o plano de comunicação:** informar no plano de resposta a incidentes quando e como devem ser realizadas as comunicações de incidentes, seja com fornecedores, empresas e órgãos parceiros (a título de exemplo o CIASC - para auxiliar na resolução do incidente), seja com titular de dados, entidades de controle, como a ANPD, para informar sobre os impactos que o incidente pode gerar aos titulares de dados pessoais.

e. **Linhas de comunicação entre as equipes que podem atuar na resposta a incidentes:** estabelecer comunicação com outros departamentos internos da organização, tais como jurídico, de pessoal e de comunicação externa. Consultar POSIN do órgão/entidade para auxiliar nessa comunicação.

f. **Modelo estrutural das equipes de pessoas envolvidas:** consultar a POSIN ou definir qual modelo de equipe para tratamento de incidente será utilizado: **interno, misto ou terceirizada**:

- ✔ **Interno**: equipe de resposta a incidentes composta por servidores de

diversos departamentos.

- ✔ **Misto:** composta por servidores e terceirizados.
- ✔ **Terceirizada**: equipe é composta por terceirizados; neste modelo, é importante que a gerência da equipe seja exercida por um servidor.

g. **Serviços providos pela equipe de resposta a incidentes:** informar qual equipe é responsável por aquele determinado incidente e quais são os serviços que esta equipe deve prover; se necessário, informar também a quem a equipe deve recorrer caso necessite de recursos extras, tais como especialistas e equipamentos.

3.2 - Tratamento de incidentes computacionais

Cabe a cada órgão ou entidade tratar de seus incidentes e para isso pode se orientar na sua POSIN ou nas 4 fases do NIST, especificadas a seguir:

Preparação: criar e treinar equipes para atuar na resposta a incidentes e implementar controles com base em avaliações de risco.

Detecção e análise de incidentes: adotar meios para detecção de incidentes e analisar tais eventos, buscando documentar, priorizar e notificar; esta fase também pode ser executada em conjunto com a fase posterior.

Contenção, erradicação e recuperação: implementar ações para contenção, erradicação e recuperação do incidente e identificar as origens de ataques e coletadas as evidências.

Atividades pós-incidente: realizar atividades para melhorar o tratamento de novos incidentes.

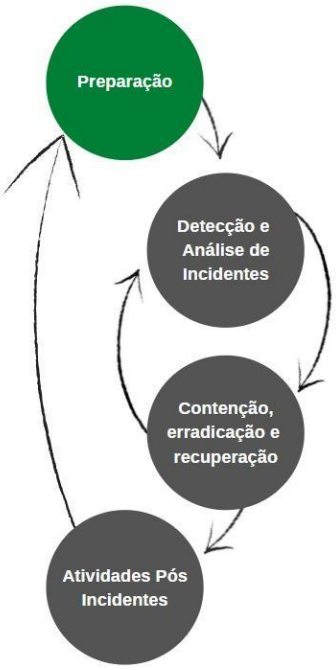
3.3.1 - Preparação

Esta fase é de suma importância, pois estabelece a capacidade de resposta para que o órgão ou entidade esteja pronto para responder a incidentes, como também a evitá-los e garantir que sistemas, redes e aplicativos sejam suficientemente seguros.

Na fase de preparação cabe ao órgão ou entidade a **criação e treinamento de equipes para atuar na resposta a incidentes** e **implementar controles com base em avaliações de risco.**

Recursos e ferramentas recomendados para o tratamento de incidentes

A. **Agenda de contatos para resposta a incidentes:** contendo informações como telefone, e-mail, nome, órgão/entidade, vínculo, responsabilidade e informações de plantão (escala de trabalho). Contatos de membros da equipe e outras pessoas de dentro e fora da organização.
B. **Mecanismos de relatório de incidentes:** formulário on-line, sistema de mensagem, telefone ou e-mail são exemplos de mecanismos a serem adotados para permitir que pessoas relatem incidentes de modo anônimo (preferencialmente).
C. **Sistemas de rastreamento de problemas:** serve para rastrear informações de incidentes, status, ações, etc.



D. Canais de comunicação e locais seguros: smartphones para membros da equipe carregarem consigo o tempo inteiro, inclusive fora do expediente, para casos pertinentes ao contexto e comunicação segura. Utilização de programas com criptografia para a comunicação entre os membros da equipe e com contatos externos relativos à resposta de incidentes. Possuir uma sala ou espaço para comunicação e coordenação central, e um local para armazenamento seguro de evidências e outros dados sensíveis.

E. Estações para análise forense digital e/ou dispositivos de backup voltados a incidentes: criação de discos de imagem, preservação de logs dos sistemas, armazenamento de dados relevantes ao incidente.

F. Outros itens importantes: estação de trabalho para análise de segurança (pentest), mecanismos para restauração de dados em casos de malwares, acessórios para coleta de evidências, sistemas de detecção de intrusão, sistemas de prevenção de intrusão, mecanismos para análise de tráfego na rede, soluções de segurança endpoint, dispositivos de backup e restauração de dados.

Prevenção de Incidentes Computacionais

A. **Avaliação de riscos:** a avaliação de riscos deve ser realizada de forma periódica e constante, serve para determinar o risco de sistemas e aplicativos por meio de ameaças e vulnerabilidades presentes. Os riscos devem ser monitorados e priorizados pelo grau de dano em potencial, com intuito de serem mitigados o quanto antes.
B. **Segurança de equipamentos:** todos os equipamentos do órgão ou entidade devem conter sempre a sua última versão de atualização instalada, configurações adequadas à segurança, garantir que os usuários tenham regras bem definidas na questão de privilégios de acesso e uso dos equipamentos, possuir sistemas de monitoramento de segurança sobre os mesmos, isso diminui a chance de uma intrusão por meio de vulnerabilidades conhecidas e meios prováveis.
C. **Segurança de rede:** o perímetro de rede deve ser configurado para negar todas as atividades como padrão. Mediante necessidade de exceções, cada órgão ou entidade deve criar as suas próprias regras de acesso.
D. **Prevenção contra malware:** programas para detectar e conter malwares devem ser empregados no órgão ou entidade, em todos os níveis possíveis (sistemas operacionais, sistemas do usuário, servidores, redes e outros).
E. **Conscientização e treinamento de usuários:** todos os usuários da organização devem receber treinamento e conscientização sobre segurança da informação. Possuir uma política de segurança da informação dentro do órgão ou entidade, torná-la conhecida, difundida e aplicável no dia a dia.
F. **Treinamento da equipe:** os membros da equipe devem receber treinamento de segurança da informação e treinar periodicamente a resposta para possíveis incidentes.

3.3.2 - Detecção e análise de incidentes computacionais

Os incidentes podem ser detectados por vários meios. Dentre eles estão a monitoração automatizada e a manual dos recursos computacionais da organização:

A. Monitoração automatizada - por intermédio de softwares específicos.
B. Monitoração manual - relato de usuários por e-mail, central de atendimento, ferramenta de registro de incidentes e até mesmo de forma verbal.

Vetores de ataques

Um incidente pode acontecer de inúmeras maneiras. Portanto, é difícil desenvolver planos e procedimentos para a resposta de todos os incidentes que venham a ocorrer.

Alguns dos vetores mais comuns segundo o NIST são:

A. Dispositivos de armazenamento externo removíveis;
B. DDOS - ataque distribuído de negação de serviço;
C. Sítios da web;
D. E-mail;
E. Engenharia social;
F. Perda ou roubo de equipamentos; e
G. Uso inadequado de equipamentos.

Sinais de incidente computacional

Existem duas categorias de sinais de um incidente:

- Precursor: sinal de que um incidente pode ocorrer no futuro;
- Indicador: sinal de que um incidente já ocorreu ou está ocorrendo agora.

Análise

Por meio de uma análise inicial, a equipe deve obter informações suficientes para definir as atividades a serem executadas posteriormente, como contenção do incidente e análise detalhada dos efeitos deste.

Visando tornar a análise de incidentes mais fácil e eficaz, seguem alguns sinais de alerta segundo o NIST:

A. Perfis de redes e sistemas;
B. Comportamento normal;
C. Obtenção e retenção de log;
D. Correlação de eventos;
E. Relógio dos hosts sincronizados;
F. Base de conhecimento de informações;

G. Motores de busca da Internet;
H. Analisadores de pacotes;
I. Filtro de alarmes;
J. Ajuda de terceiros.

Documentação

A partir do momento em que há suspeita de um incidente, a equipe de resposta a incidentes deve registrar todas as ações relativas a este. Usar uma ferramenta de rastreamento de problemas anteriores pode ajudar bastante na resolução de novos incidentes, além de prover dados para fiscalização e controle da equipe de resposta a incidentes, buscando garantir a resolução e tratamento de incidentes em tempo hábil. Este sistema de rastreamento de problemas pode conter as seguintes informações:

A. Status atual dos incidentes: novo, em andamento, encaminhado para investigação, pendente de informações ou ações de terceiros, resolvido, fechado etc.;
B. Resumo do incidente;
C. Indicadores relacionados ao incidente;
D. Outros incidentes relacionados a este evento específico;
E. Ações realizadas pela equipe de resposta e demais equipes que venham atuar neste incidente;
F. Cadeia de escalonamento, se aplicável;
G. Avaliações de impactos relacionados ao incidente;
H. Informações de contato com outras equipes envolvidas, terceiros e organizações parceiras;
I. Relação de evidências coletadas durante o tratamento do incidente;
J. Comentários e notas das pessoas que atuaram no incidente;
K. Próximas etapas a serem executadas após a resolução do incidente.

Priorização

A priorização do tratamento de incidentes é importante e as seguintes informações devem ser utilizadas para a definição da ordem de prioridade em seu tratamento:

A. Impacto no negócio: a equipe de resposta a incidentes deve, diante das opções para tratamento, mensurar os impactos que tais alternativas possam gerar tanto para a própria organização, como para outros entes parceiros;
B. Impacto em dados e informações: a equipe responsável tem o papel de identificar e avaliar os recursos disponíveis, bem como a relevância da recuperação do incidente para a organização;
C. Recuperabilidade: a equipe de resposta a incidentes deve priorizar a resposta a cada incidente de acordo com as estimativas de impacto e os recursos e esforços necessários para a sua recuperação.

Notificação

Convém que o plano de resposta a incidentes informe qual equipe é responsável pela notificação do incidente logo após a análise e a priorização, e quem deve ser notificado. A seguir, são listados exemplos de atores que devem ser notificados em caso de incidentes:

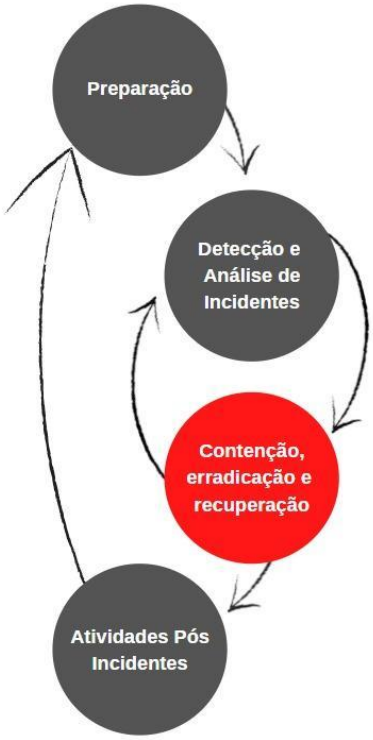
A. Diretor de tecnologia da Informação ou cargo similar;
B. Chefe de segurança da informação;
C. Líder técnico de segurança da informação;
D. Equipes internas de resposta a incidentes;
E. Responsável pelo recurso afetado;
F. Recursos humanos (em casos que envolvam funcionários);
G. Departamento de Comunicação Social;
H. Departamento jurídico;
I. Encarregado, controlador, ANPD e titulares de dados (em caso de incidentes envolvendo dados pessoais);
J. Polícia Civil (quando houver indícios de crimes).

Durante o tratamento do incidente, a equipe responsável pela comunicação pode utilizar de alguns meios para notificar os indivíduos e atualizar o relatório de tratamento de incidentes. Alguns desses meios são:

A. E-mail;
B. Site e portal de comunicação;
C. Ligação telefônica;
D. Aplicativos de mensagens instantâneas;
E. SMS;
F. Reuniões;
G. Avisos em quadros e cartazes.

3.3.3 - Contenção, erradicação e recuperação

Na fase de contenção, erradicação e recuperação devem ser realizadas ações buscando a remediação ou a restauração dos recursos atacados e, quando possível, a recuperação de tais recursos ao estado anterior ao ataque. Para isso, devem ser seguidos os procedimentos já estabelecidos internamente para resposta a incidentes.



Estratégia de contenção

A. Mensurar danos potenciais e/ou roubo de recursos;
B. Necessidade de preservação de evidências;
C. Disponibilidade do serviço;
D. Tempo e recursos para implementar a estratégia;
E. Eficácia da estratégia (contenção parcial ou total);
F. Duração da solução de contorno.

Coleta e manuseio de evidências

A. Identificação (endereços IP e MAC, porta de rede, sistema operacional, nome do host, localização);
B. Nome de quem realizou o manuseio da evidência;
C. Hora e data de cada ocorrência;
D. Locais onde as evidências foram armazenadas.

Identificar a origem de ataques

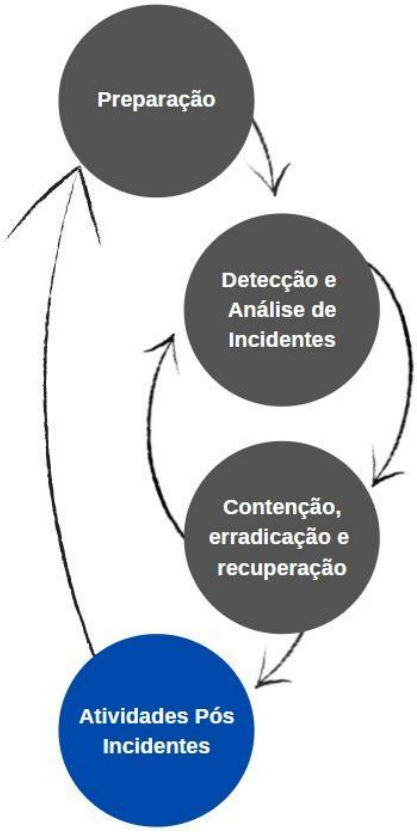
A. **Validação do endereço IP**: utilizar técnicas para identificar e validar o endereço de IP do host de ataque;
B. **Pesquisa de endereço de IP**: realizar uma pesquisa do IP do atacante em motores de busca;
C. **Banco de dados de incidentes:** identificar semelhanças com eventos antigos;
D. **Monitorar canais de comunicação:** verificar canais utilizados com frequência em ataques.

Erradicação e recuperação

A. Eliminar resquícios do incidente, como exclusão de malware, exclusão de contas violadas;
B. Recuperação dos sistemas para seu estado normal (pode envolver ações como alteração de senhas de rede, reconfiguração de regras de firewall, restauração de backup, reconstrução de sistemas e de toda base de dados, instalação de patches de segurança, substituição de arquivos corrompidos por versões limpas);
C. Priorizar o aumento dos níveis gerais de segurança e correções.

3.3.4 - Atividades pós-incidente

Na fase de atividades pós-incidente, deve-se implementar 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.



Lições aprendidas

A. Onde, quando, como e o que de fato aconteceu?
B. Qual a eficácia da equipe neste(s) evento(s)?
C. Foram seguidos procedimentos já documentados?
D. Algum procedimento não estava documentado?
E. Quais informações anteriores foram necessárias?
F. Algo prejudicou a recuperação?
G. O que pode ser atualizado para melhorar o tratamento?
H. Como melhorar o compartilhamento de informações?
I. Quais ações corretivas devem ser tomadas?
J. Quais alarmes e indicadores devem ser observados?
K. Quais recursos adicionais podem ser utilizados?

Usando dados coletados

Todas as atividades devem ser arquivadas e usadas como base histórica.

É fundamental que os dados coletados estejam inalterados, íntegros e sejam armazenados de forma adequada para serem analisados e agreguem ainda mais valor.

Retenção de evidência

A. **Judicialização**: armazenar as evidências de um incidente deve ser uma atividade que leva em consideração que tais evidências podem ou devem ser consultadas durante um processo judicial;
B. **Retenção:** é preciso elaborar procedimentos para a retenção que definam quanto tempo certos tipos de dados devem ser mantidos;
C. **Custo:** é necessário determinar o custo monetário de manter as evidências seguras e acessíveis.

3.4 - Compartilhamento de Informações

É importante que seja compartilhado o máximo de informações possível entre as equipes integrantes, mas tal compartilhamento deve ser cauteloso para não expor informações consideradas sensíveis. Todas as equipes devem cumprir requisitos de confidencialidade para que os dados não sejam vazados, gerando ainda mais impactos.

3.5 - Recomendações

1. Ter um plano de gerenciamento de risco que contemple ameaças e vulnerabilidades à segurança da informação, bem como medidas de proteção de dados, privacidade e procedimentos relativos à identificação, análise e avaliação de riscos.
2. Possuir o inventário de dados pessoais e implementar um processo de avaliação de risco (e.g. Relatório de Impacto à Proteção de Dados).
3. Realizar treinamentos constantes com o objetivo de propagar novos conhecimentos para a equipe.
4. Garantir a implementação de medidas de segurança da informação adequadas, com o objetivo de prevenir a ocorrência de incidentes de segurança.
5. Fazer com que comportamentos anormais de recursos de tecnologia sejam rapidamente identificados.
6. Correlacionar eventos distintos a fim de encontrar características comuns entre tais eventos.
7. Criar, manter e usar uma base de conhecimento com informações sobre incidentes.
8. Registrar todas as informações do evento a partir do momento em que há uma suspeita da ocorrência de um incidente.
9. Quando houver incidentes simultâneos, priorizar o tratamento de incidentes com base em características já estabelecidas como relevantes ou não.
10. Criar, documentar e seguir procedimentos de resposta a incidentes durante o tratamento de incidentes.
11. Realizar reuniões internas para identificar melhorias no processo de resposta a incidentes.
12. Participar de grupos de discussão entre organizações que atuam com resposta a incidentes, antes da ocorrência de um evento.
13. Efetuar consulta jurídica interna antes de participar de grupos de discussões, pois o compartilhamento de algumas informações pode constituir infração à legislação e a contratos.
14. Buscar o equilíbrio entre os benefícios do compartilhamento de informações e as desvantagens de compartilhar informações confidenciais e sensíveis.
15. Em caso de incidentes que gerem impactos a dados pessoais, elaborar o plano de comunicação entre equipes internas e atores externos, tais como a ANPD e os titulares de dados pessoais.

4 CONSIDERAÇÕES FINAIS

Neste guia foram compartilhadas algumas das melhores práticas visando à adequação de organizações da administração pública estadual com intuito de auxiliar na elaboração do plano de resposta a incidentes de segurança e proteção de dados pessoais. Tais práticas seguem diretrizes e obrigações estipuladas na Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), no Decreto nº 1.184, de 1º de março de 2021, na Instrução Normativa nº 20, de 20 de outubro de 2021 e em outros atos normativos vigentes.

No processo de adoção de diretrizes sobre resposta a incidentes, aconselha-se que os órgãos e entidades busquem continuamente a conformidade com os normativos vigentes e com as melhores práticas que venham a ser adotadas ao longo do tempo, de maneira que a gestão de incidentes se mantenha efetiva, relevante e atualizada.

ANEXO I - Caso Prático

Em um cenário hipotético onde o órgão X sofreu um ataque do tipo ransomware, tendo uma de suas bases de dados totalmente copiadas e criptografadas por criminosos, os hackers solicitaram resgate, contudo, os gerentes do órgão haviam contratado meses antes um sistema de anti ransomware, o qual foi acionado logo após o incidente, corrigindo os dados criptografados. Dessa maneira, não se fez necessário o pagamento de resgate.

Quando os criminosos descobriram que não receberiam o dinheiro, resolveram divulgar os dados roubados na rede mundial de computadores (internet). Entre os dados divulgados, constavam dados pessoais e dados sensíveis.

Assim que o órgão soube do agravante, começou a tomar outras medidas para a resposta do incidente.

Inicialmente o gestor responsável pelo sistema realizou a comunicação com o DPO, que deu início as etapas seguintes:

- Avaliar internamente o incidente para obter informações iniciais sobre o impacto do ocorrido; fonte, categoria e quantidade de titulares de dados pessoais afetados;
- Levantar as consequências do incidente para os titulares e a entidade, criticidade e probabilidade; além disso, é necessário preservar todas as evidências do incidente.
- Solicitar manifestação do setor especialista no assunto para auxiliar na avaliação e providências a serem tomadas.
- Consultar o setor de tecnologia da informação do órgão/entidade em caso de incidentes na rede computacional - o mesmo irá dar ciência aos gestores.
- Comunicar a todos os envolvidos (nos termos da LGPD) por parte do CONTROLADOR do dado, a existência do incidente, como a autoridade máxima da entidade/órgão e gestores.
- Comunicar à ANPD e ao titular de dados pessoais (conforme art. 48 da LGPD) a existência do incidente.
- Emitir o relatório final contendo todas as ações realizadas para o tratamento efetivo do incidente e as considerações necessárias para promover a melhoria contínua no atendimento.

Perguntas que devem ser respondidas:

1. **Qual base de dados foi acessada indevidamente?** Para saber quais foram os titulares afetados a serem contatados.
2. **Por qual vetor de ataque se deu o incidente?** Foi detectado que o servidor, um Windows Server 2008, responsável pela base de dados, continha uma vulnerabilidade que permitia o acesso remoto de usuários não autorizados ao sistema, logo depois do incidente a equipe corrigiu a brecha atualizando o sistema.
3. **Após a coleta de informação inicial, qual a correção emergente do incidente?** O órgão deu início a comunicação com os responsáveis pela resposta do incidente.
4. **Quais lições aprendidas?** O relatório final deve conter esta resposta.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Autoridade Nacional de Proteção de Dados. Comunicação de incidentes de segurança. Disponível em: < https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca >. Acesso em: 19 out. 2021.

BRASIL. Presidência da República. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm >. Acesso em: 20 out. 2021.

BRASIL. Secretaria de Governo Digital. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd >. Acesso em: 20 out. 2021.

ESTADO DE SANTA CATARINA. Comitê Gestor de Proteção de Dados (CGPD). Disponível em: <https://www.sea.sc.gov.br/diretoria-de-tecnologia-e-inovacao/lgpd>. Acesso em 22 out. 2021.

ESTADO DE SANTA CATARINA. Decreto nº 282, de 27 de setembro de 2019. Dispõe sobre a disponibilização e compartilhamento de bases de dados no âmbito da Administração Pública Estadual. Disponível em: < http://server03.pge.sc.gov.br/LegislacaoEstadual/2019/000282-005-0-2019-007.htm >. Acesso em: 22 out. 2021.

ESTADO DE SANTA CATARINA. Decreto nº 844, de 18 de setembro de 2020. Institui o Comitê Gestor de Proteção de Dados no âmbito do Poder Executivo Estadual. Disponível em: < http://server03.pge.sc.gov.br/LegislacaoEstadual/2020/000844-005-0-2020-008.htm >. Acesso em: 22 out. 2021.

ESTADO DE SANTA CATARINA. Decreto nº 1.184, de 1º de março de 2021. Dispõe sobre proposições gerais objetivando a implementação da Lei federal nº 13.709, de 2018, no âmbito do Poder Executivo Estadual. Disponível em: < http://server03.pge.sc.gov.br/LegislacaoEstadual/2021/001184-005-0-2021-005.htm >. Acesso em: 22 out. 2021.

ESTADO DE SANTA CATARINA. Instrução Normativa nº 20, de 20 de outubro de 2021. Disciplina a elaboração da Política de Segurança da Informação – POSIN. Disponível em: < http://server03.pge.sc.gov.br/LegislacaoEstadual/2021/000020-009-0-2021-004.htm >. Acesso em: 22 out. 2021.