

SANTOS PORT AUTHORITY					
	Instrumento Normativo de Processo			Código: TIC-140-016	
	Diretoria Responsável: <b>Presidência</b>		Unidade Responsável: <b>Superintendência de Tecnologia da Informação</b>		Elaboração: <b>Supervisão de Governança de TI</b>
	Início da vigência: <b>19/11/2021</b>	Próxima revisão: <b>19/11/2023</b>	Aprovação: Decisão Direxe: <b>484.2021</b>		Validação: <b>Superintendente de Tecnologia da Informação</b>
Processo: <b>Sistema de Gestão da Privacidade da Informação: Incidentes de Segurança da Informação e Incidentes de Violação de Dados Pessoais</b>				Versão: <b>1.3</b>	

# Instrumento Normativo de Processo Sistema de Gestão da Privacidade da Informação: Incidentes de Segurança da Informação e Incidentes de Violação de Dados Pessoais

## SUMÁRIO

<b>1. OBJETIVO .....</b>	<b>3</b>
<b>2. ABRANGÊNCIA.....</b>	<b>3</b>
<b>3. FUNDAMENTAÇÃO .....</b>	<b>3</b>
<b>4. DEFINIÇÕES .....</b>	<b>3</b>
<b>5. ARCABOUÇO LEGAL .....</b>	<b>6</b>
<b>6. DIRETRIZES .....</b>	<b>7</b>
<b>6.1. Diretrizes .....</b>	<b>7</b>
<b>6.2. Consenso / Aprovação .....</b>	<b>18</b>
<b>7. PAPÉIS E RESPONSABILIDADES.....</b>	<b>18</b>
<b>7.1. Da Unidade Responsável – Incidentes de Segurança da Informação .....</b>	<b>18</b>
<b>7.2. Da Unidade Responsável – Incidentes de Violação de Dados Pessoais.....</b>	<b>19</b>
<b>7.3. Das Unidades Executoras .....</b>	<b>20</b>
<b>8. DISPOSIÇÕES FINAIS .....</b>	<b>22</b>
<b>9. ANEXOS.....</b>	<b>22</b>

## 1. OBJETIVO

**1.1** Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.

**1.2** Estabelecer e manter a Equipe de Resposta a Incidentes (ERI).

**1.3** Estabelecer as regras relativas à gestão dos Incidentes de Violação de Dados Pessoais da SPA e mitigar os riscos ao negócio e aos ativos da SPA.

## 2. ABRANGÊNCIA

Este normativo se aplica a todos os empregados, incluindo os cedidos, aos estagiários e aos terceirizados que executem atividades nas instalações da Companhia.

Todas as unidade de gestão da Santos Port Authority (SPA), todos os sistemas corporativos que são utilizados em ambientes de produção na SPA, ativos de TI sob gestão da Superintendência de Tecnologia da Informação (SUPTI) e que estejam sujeitos a ameaças internas ou externas que possam explorar vulnerabilidades conhecidas e desconhecidas no ambiente de TI, bem como áreas Segurança da Informação, Tecnologia da Informação, Encarregado pelo Tratamento de Dados Pessoais, e demais Áreas de Negócio.

## 3. FUNDAMENTAÇÃO

Este documento está fundamentado na Política de Segurança e Privacidade, e Sistema de Gestão de Privacidade da Informação – SGPI da SPA, em vigor.

## 4. DEFINIÇÕES

Termo	Descrição
<b>Ameaça</b>	Risco ou potencial perigo de um incidente, que pode resultar em dano à SPA.
<b>Ativo</b>	Qualquer bem, material ou imaterial, que tenha valor para a SPA e precisa ser adequadamente protegido.
<b>Evento</b>	Qualquer ocorrência visível em uma rede ou sistema de informação. Exemplos: um usuário que acessa um arquivo compartilhado, um servidor que recebe uma solicitação para uma página da Web, um usuário que envia um e-mail ou um firewall que faz um bloqueio de uma tentativa de conexão, entre outros.

Termo	Descrição
<b>Evento adverso (ou ofensivo)</b>	Evento com consequências negativas. Exemplos: falhas do sistema de informação, uso não autorizado de privilégios de sistema de informação, acesso não autorizado a dados confidenciais ou execução de malware que destrói dados, entre outros.
<b>Eventos de segurança da informação</b>	Uma ocorrência no sistema, serviço ou estado da rede, indicando uma possível falha de Segurança da Informação, violação de políticas e/ou instrumentos normativos da SPA, ou falha de controles, ou uma situação prévia desconhecida que pode ser relevante para a segurança.
<b>Information Technology Infrastructure Library (ITIL)</b>	Conjunto de melhores práticas dos processos de gestão de serviços de Tecnologia da Informação (TI) de uma empresa.
<b>Item de configuração (IC)</b>	Refere-se a qualquer componente que necessita ser configurado com o objetivo de se entregar um serviço de TI. Os ICs normalmente incluem serviços de TI, hardware, software, pessoas e documentações formais, como documentação de processos e acordos de nível de Serviço.
<b>Incidente</b>	Qualquer interrupção não planejada no serviço de TI ou qualquer degradação na qualidade do serviço de TI ou falha de qualquer IC (mesmo que não tenha afetado o serviço ainda) utilizado para fornecer serviço de TI (ITIL).
<b>Incidentes de segurança da informação</b>	Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação e ativos de TIC, levando à perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade.
<b>Incidentes de segurança da informação envolvendo dados pessoais</b>	Tipo de incidente de segurança da informação, em que o ativo afetado envolve dados pessoais
<b>Informação</b>	Conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.

Termo	Descrição
<b>Encarregado pela proteção de Dados Pessoais (ETDP)</b>	Pessoa ou função responsável pela gestão dos dados pessoais tratados pela SPA, para atuar no canal de comunicação entre o controlador (no caso SPA), o titular dos dados e a ANPD. Esse papel é nomeado via portaria pelo Presidente da SPA.
<b>Resposta a Incidente</b>	Conjunto de atividades técnicas executadas para analisar, detectar, defender contra um incidente e responder a um incidente. Fonte <a href="https://blog.elearnsecurity.com/security-incidents-incident-handling-vs-incident-response.html">https://blog.elearnsecurity.com/security-incidents-incident-handling-vs-incident-response.html</a>
<b>Risco</b>	Combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos.
<b>Prevenção à violações de dados Pessoais</b>	Avaliações de impacto dos dados pessoais (Relatório de Impacto à proteção de Dados - RIPD) antes do início de qualquer projeto ou implementação de qualquer tecnologia que processe (tratamento) Dados Pessoais. As avaliações de impacto nos dados pessoais apresentam os riscos associados aos dados pessoais. Em caso de alto risco, medidas técnicas e organizacionais apropriadas serão adotadas para proteger dados pessoais contra destruição acidental ou ilegal, perda acidental, alteração, divulgação ou acesso não autorizado.
<b>RIPD</b>	Relatório de Impacto à proteção de Dados
<b>Registro de Violação de Dados Pessoais</b>	Coleção das comunicações de violações feitas à ANPD e das violações não comunicadas.
<b>Tratamento de Incidentes</b>	Resumo dos processos e ações predefinidas para lidar/gerenciar de forma eficaz um incidente. Fonte: <a href="https://blog.elearnsecurity.com/security-incidents-incident-handling-vs-incident-response.html">https://blog.elearnsecurity.com/security-incidents-incident-handling-vs-incident-response.html</a>
<b>ERI</b>	Equipe de Resposta a Incidente
<b>CERT</b>	Equivale ao ERI. <i>Computer Emergency Response Team</i>
<b>CSIRT</b>	Equivale ao ERI. <i>Computer Security Incident Response Team</i>
<b>Ciclo de Vida de resposta a Incidente (NIST)</b>	<ol style="list-style-type: none"> <li>1- Preparação,</li> <li>2- Detecção e Análise,</li> <li>3- Contenção, Erradicação/Remediação e Recuperação</li> <li>4- Atividades pós incidente</li> </ol>

Termo	Descrição
<b>SANS</b>	<i>SysAdmin, Audit, Network and Security</i> , Instituto especializado em treinamento em segurança da informação, e <i>cybersecurity</i> .
<b>NIST</b>	<i>National Institute of Standards and Technology</i> , é uma agência governamental não regulatória da administração de tecnologia do Departamento de Comércio dos Estados Unidos
<b>Etapas do plano de respostas a incidentes (SANS)</b>	<ol style="list-style-type: none"> <li>1. Preparação</li> <li>2. Identificação</li> <li>3. Contenção</li> <li>4. Erradicação</li> <li>5. Recuperação</li> <li>6. Lições aprendidas</li> </ol>
<b>Fases de Gerenciamento de Incidentes de segurança – ISO-27035</b>	<ol style="list-style-type: none"> <li>1. Planejar e preparar</li> <li>2. Detectar e reportar</li> <li>3. Avaliar e decidir</li> <li>4. Lições aprendidas</li> </ol>

## 5. ARCABOUÇO LEGAL

Leis, Normativos Externos, Ofícios e Resoluções	Ano	Assunto
<b>Lei nº 13.709</b>	2018	Lei Geral de Proteção de Dados Pessoais (LGPD).
<b>Resolução CGPAR Nº 11 DE 10/05/2016</b>	2016	Dispõe sobre o planejamento e implementação de práticas de governança de Tecnologia da Informação (TI) que atendam de forma adequada os padrões usualmente reconhecidos nesta área, pelas empresas estatais federais.
<b>ISO/IEC 27001:2013</b>	2013	<i>Information technology --Security techniques - Information security management systems -- Requirements</i>
<b>ISO/IEC 27002:2013</b>	2013	<i>Information technology --Security techniques --Code of practice for information security controls</i> (Tecnologia da Informação –Técnicas de Segurança –Código de práticas para controles de segurança da Informação)
<b>ISO/IEC 27005:2010</b>	2010	<i>Information technology --Security techniques - Information security risk management</i> (Tecnologia da Informação –Técnicas de Segurança – Gerenciamento Riscos Segurança Informação)
<b>ISO/IEC 27701:2019</b>	2019	<i>Information technology --Security techniques - Privacy Information Management System (PIMS)</i>

		(Tecnologia da Informação –Técnicas de Segurança –Sistema de Gestao da Privacidade da Informação –SGPI)
--	--	---

## 6. DIRETRIZES

### 6.1. Diretrizes

#	Diretrizes
1.	<p>A Superintendência de Tecnologia da Informação (SUPTI) implementará e manterá uma ERI (ou CERT ou CISP) com as seguintes funções:</p> <ol style="list-style-type: none"> <li>1. “comando”:</li> <li>2. Planejamento:</li> <li>3. Monitoramento:</li> <li>4. Resposta:</li> <li>5. Implementação:</li> <li>6. Análise:</li> </ol>
1.1	<p>Atribuições função “<b>comando</b>”: Lidera e toma decisões sobre questões importantes relacionadas à resposta a incidentes de segurança da informação e cibersegurança.</p> <ol style="list-style-type: none"> <li>a. comprometer-se e apoiar a resposta a incidentes, incluindo o fornecimento dos recursos necessários (mão de obra, financeira e material);</li> <li>b. revisar e aprovar planos de resposta a incidentes e supervisionar a implementação;</li> <li>c. revisar e criticar os planos de resposta a incidentes;</li> <li>d. coordenar internamente e externamente a equipe.</li> </ol>
1.2	<p>Atribuições função <b>Planejamento</b>: Opera a resposta a incidentes.</p> <ol style="list-style-type: none"> <li>a. estabelecer os planos de resposta;</li> <li>b. implementar processos de segurança;</li> <li>c. ajustar as prioridades de risco;</li> <li>d. comunicar com organizações de nível superior e outras organizações de terceiros;</li> <li>e. apoiar a administração;</li> <li>f. discutir/registrar/aprovar relatórios de vulnerabilidade na SPA;</li> <li>g. realizar outras atividades dirigidas pelo “comando”.</li> </ol>

#	Diretrizes
1.3	<p>Atribuições função <b>Monitoramento</b>: Executa as atividades de monitoramento de segurança em tempo real.</p> <ul style="list-style-type: none"> <li>a. monitorar e operar diariamente;</li> <li>b. detectar a intrusão, registrar incidentes e executar as primeiras respostas;</li> <li>c. executar ou acompanhar as atualizações de segurança;</li> <li>d. implementar planos de resposta e outras salvaguardas;</li> <li>e. realizar suporte técnico;</li> <li>f. gerenciar instalações;</li> <li>g. realizar outras atividades dirigidas pelo “comando”.</li> </ul>
1.4	<p>Atribuições função <b>Resposta</b>: Fornece serviços como respostas em tempo real, suporte técnico.</p> <ul style="list-style-type: none"> <li>a. propagar e informar incidentes;</li> <li>b. analisar correlação entre sistemas de monitoramento;</li> <li>c. apoiar investigação e recuperação de incidentes;</li> <li>d. analisar vulnerabilidade no incidente alvo;</li> <li>e. realizar outras atividades dirigidas pelo “comando”.</li> </ul>
1.5	<p>Atribuições função <b>Implementação</b>: Executa a ação total da resposta a incidentes.</p> <ul style="list-style-type: none"> <li>a. analisar os requisitos de resposta a incidentes;</li> <li>b. determinar níveis de resposta a incidentes;</li> <li>c. implementar planos de resposta a incidentes;</li> <li>d. projetar planos de resposta a incidentes;</li> <li>e. resumir o trabalho e o relatório de resposta a incidentes;</li> <li>f. implantar e usar os recursos de resposta a incidentes;</li> <li>g. realizar outras atividades dirigidas pelo “comando”</li> </ul>
1.6	<p>Atribuições função <b>Análise</b>: Executa análise de incidentes</p> <ul style="list-style-type: none"> <li>a. planejar a análise de vulnerabilidade para a equipe;</li> <li>b. aprimorar as ferramentas de análise de segurança e a lista de verificação;</li> <li>c. melhorar as regras de monitoramento;</li> <li>d. publicar boletim informativo;</li> <li>e. realizar outras atividades dirigidas pelo comando.</li> </ul>

#	Diretrizes
2.	Os membros da ERI deverão ser formalizados via portaria DIPRE, sendo sua nomeação de ciência dos participantes e seus gestores, além de, previamente aprovada pelo CSI.
3.	Os seguintes setores deverão ser representados na ERI, ao menos com um membro titular e seu suplente: <ul style="list-style-type: none"><li>• Segurança cibernética (como coordenador);</li><li>• Segurança da Informação;</li><li>• Proteção de dados pessoais;</li><li>• Infraestrutura de TI;</li><li>• Suporte ao usuário (<i>service desk</i>);</li><li>• Desenvolvimento de Sistemas;</li><li>• Gestão de riscos e controles internos.</li></ul>
4.	Em caso de (e dependendo do tipo de) um Incidente de Segurança, não é obrigatório nem necessário a convocação de todos os membros da ERI, bem como membros de outras áreas podem ser convocados.
5.	A ERI tem duração permanente. Cabendo revisão anual de composição e nomeações por parte do CSI.

#	Diretrizes
6.	<p>A ERI desenvolverá, implementará e manterá procedimentos para:</p> <ul style="list-style-type: none"> <li>○ Preparar e planejar a resposta a incidentes de SI, em complemento ao Instrumento Normativo de Processo Suporte de TIC, envolvendo usuários e equipe de TI para lidar com os incidentes caso ocorram;</li> <li>○ Monitorar, detectar, analisar e notificar eventos e incidentes de segurança da informação;</li> <li>○ Identificar incidentes de modo a caracterizá-los ou não como incidente de segurança da informação (e se envolve ou não dados pessoais) e quais eventos podem ser ignorados e quais devem ter ação imediata;</li> <li>○ Conter incidentes de segurança isolando ativos afetados para prevenir danos maiores;</li> <li>○ Erradicar o incidente eliminando a causa raiz do incidente de segurança;</li> <li>○ Prover a recuperação, colocando o ativo afetado em condições;</li> <li>○ Registrar as atividades de gerenciamento de incidentes;</li> <li>○ Documentar todos os detalhes do incidente de modo a observação de “Lições Aprendidas”.</li> <li>○ Manusear evidências forenses dos incidentes de segurança da informação quando aplicável;</li> <li>○ Respostas, incluindo escalação do incidente de 1º nível para os demais níveis e direcionamento para os setores adequados, recuperação de um incidente e comunicação com empregados e organizações internas e externas à SPA;             <ul style="list-style-type: none"> <li>○ Em caso de incidente envolvendo dados pessoais, comunicar ao ETDP, e passará a ser tratado também como Incidente de Violação de Dados Pessoais. Considerar que todos os empregados da SPA devem ser capazes de identificar um incidente de violação de dados pessoais, bem como estar atentos em reportar a ocorrência ao gestor de sua respectiva área, que deverá registrar a ocorrência de um incidente de segurança da informação envolvendo dados pessoais.</li> </ul> </li> <li>○ Garantias para:             <ul style="list-style-type: none"> <li>○ Estabelecer um ponto de contato para notificações e detecção de incidentes de segurança;</li> <li>○ Criar uma lista de contatos mantida com autoridades, grupos de interesses externos ou fóruns que tratem de questões relativas a incidentes de segurança da informação;</li> </ul> </li> </ul>

#	Diretrizes
7.	<p>Notificações de evento de segurança da informação incluem:</p> <ul style="list-style-type: none"> <li>○ Ineficácia do controle de segurança;</li> <li>○ Violação de disponibilidade, confidencialidade ou integridade da informação;</li> <li>○ Erros humanos;</li> <li>○ Não conformidade com políticas, instrumentos normativos ou normas;</li> <li>○ Violações de procedimentos de segurança física;</li> <li>○ Mudanças de sistema fora de controle;</li> <li>○ Mal funcionamento de <i>hardware</i> ou <i>software</i>;</li> <li>○ Violação de acesso.</li> </ul>
8.	<p>Notificações de fragilidades de segurança da informação.</p> <p>A SUPTI em conjunto com a Gerência de Carreira e Capacitação (GECAR) instruirá os empregados que usam os sistemas e serviços de informação da organização para notificarem e registrarem quaisquer fragilidades de segurança da informação, observada ou suspeita, nos sistemas ou serviços.</p>
9.	<p>Avaliação de decisão dos eventos de segurança da informação.</p> <p>Todos os eventos de segurança da informação serão avaliados e será decidido pela SUPTI se eles serão classificados como incidentes de segurança da informação.</p>
10.	<p>A resposta aos incidentes de segurança da informação deve considerar:</p> <ul style="list-style-type: none"> <li>○ Coleta de evidências, o mais rápido possível após o evento;</li> <li>○ Condução de análise forense de segurança da informação;</li> <li>○ Escalação, se requerido;</li> <li>○ Garantia de que todas as atividades de respostas sejam registradas para análise futura;</li> <li>○ Comunicação da existência do incidente de segurança da informação para pessoal interno ou externo, ou organizações que precisam tomar conhecimento do fato;</li> <li>○ Tratamento das fragilidades de segurança da informação encontradas que causaram ou contribuíram para o incidente;</li> <li>○ Encerramento e registro do incidente uma vez que ele foi tratado de forma bem-sucedida.</li> </ul>
11.	<p>Os conhecimentos obtidos da análise e resolução dos incidentes de segurança da informação serão documentados por meio de documento de <u>Lições Aprendidas</u> visando sua utilização para reduzir a probabilidade ou o impacto de incidentes futuros.</p>

#	Diretrizes
12.	<p>A coleta de evidências irá considerar itens referentes à:</p> <ul style="list-style-type: none"> <li>○ Cadeia de custódia;</li> <li>○ Segurança da evidência;</li> <li>○ Segurança das pessoas envolvidas;</li> <li>○ Papéis e responsabilidades das pessoas envolvidas;</li> <li>○ Competência do pessoal;</li> <li>○ Documentação;</li> <li>○ Resumo do incidente.</li> </ul>
13.	<p>Informações coletadas para gestão de incidentes de segurança em TI:</p> <ul style="list-style-type: none"> <li>• Descrição do incidente;</li> <li>• Setor onde ocorreu o incidente;</li> <li>• Dados para contato (telefone, email, etc);</li> <li>• Identificação de quem reportou e de quem atendeu;</li> <li>• Data do evento / Data de identificação;</li> <li>• Natureza do incidente (perda de serviços ou ativos, uso indevido de credenciais, violação ou tentativa de burla dos sistemas e controles, observação ou suspeita de fragilidade, acesso indevido, outros);</li> <li>• Causa raiz identificada;</li> <li>• Como foi detectado;</li> <li>• Ativos afetados;</li> <li>• Impacto;</li> <li>• Outras informações;</li> <li>• Causa raiz resolvida;</li> <li>• Data prevista da solução;</li> <li>• Data da solução;</li> <li>• Equipe de resposta;</li> <li>• Providências para investigação e setores envolvidos;</li> <li>• Lista de comunicação (pessoas, etc).</li> </ul>
<b>INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS</b>	
<b>IDENTIFICAÇÃO DO INCIDENTE DE VIOLAÇÃO DE DADOS PESSOAIS:</b>	
14.	<p>O Encarregado pelo Tratamento de Dados Pessoais deverá receber o chamado com as informações necessárias e avaliar se a ocorrência realmente configura um incidente de violação de dados pessoais.</p>

#	Diretrizes
15.	Para análise do incidente, o Encarregado pelo Tratamento de Dados Pessoais deve envolver a SUPTI, o responsável pela segurança da informação e, quando aplicáveis, a Tecnologia da Informação de terceiros envolvidos e outros agentes pertinentes.
16.	Se os dados pessoais envolvidos no incidente estiverem anonimizados, não serão considerados dados pessoais e deverá ser seguido o processo normal de gestão de incidentes de segurança da informação e não mais tratado como violação de dados pessoais.
<b>REGISTRO DO INCIDENTE DE VIOLAÇÃO DE DADOS PESSOAIS</b>	
17.	Incidentes ocorridos por ação ou omissão de agentes de tratamento (SPA ou fornecedores que realizem tratamento em nome da SPA) devem ser mantidos no Registro de Violação de Dados Pessoais.
18.	Quando o incidente tiver origem em um prestador de serviço, o Encarregado pelo Tratamento de Dados Pessoais deve avaliar, em conjunto com o gestor da área ou do agente de tratamento (fornecedor) originária do incidente de violação de dados, o tipo e o nível de risco criado pela violação.
19.	O Encarregado pelo Tratamento de Dados Pessoais determinará se existe um risco para os direitos e liberdades dos titulares dos dados. Os riscos contra os direitos e liberdades incluem, entre outros, perda de controle ou confidencialidade dos Dados Pessoais, reversão não autorizada de pseudonimização, danos à reputação, discriminação, roubo ou fraude de identidade, perda financeira e outras desvantagens econômicas ou sociais.
20.	O Encarregado pelo Tratamento de Dados Pessoais avaliará se a probabilidade e a gravidade dos riscos potenciais criam um risco classificado como alto. Essa avaliação deve envolver uma análise do tipo de violação; a natureza; sensibilidade e volume de dados pessoais afetados; a gravidade das possíveis consequências para os titulares dos dados; o número e as características dos titulares de dados afetados; as características do destinatário dos dados pessoais e a facilidade de identificação dos titulares dos dados.
21.	São riscos elevados, os decorrentes de processamento que utiliza novas tecnologias, ou métodos de processamento onde nenhuma avaliação de impacto na proteção de dados (RIPD) foi realizada antes da violação pelo controlador, ou quando uma avaliação de impacto nos dados (RIPD) se tornou necessária à luz do tempo decorrido desde o processamento inicial.

#	Diretrizes
22.	O Encarregado pelo Tratamento de Dados Pessoais facilitará a notificação para a ANPD e aos Titulares dos Dados Pessoais, conforme necessário, com base no nível de risco.
<b>CONTENÇÃO DO INCIDENTE DE VIOLAÇÃO DE DADOS PESSOAIS</b>	
23.	O Encarregado pelo Tratamento de Dados Pessoais deverá orientar os gestores e áreas responsáveis/afetadas pela violação de dados quanto às medidas corretivas a serem tomadas.
24.	O Gestor da Área originária do incidente de violação de dados deve tentar, junto com sua equipe, recuperar qualquer dado que tenha sido comprometido de forma a mitigar o risco ao máximo possível, com o apoio do Encarregado pelo Tratamento de Dados Pessoais e da Área de Segurança da Informação.
25.	O Encarregado pelo Tratamento de Dados Pessoais deverá estabelecer quem precisa ser informado internamente acerca da violação de dados e quais ações devem ser tomadas por quem foi informado.
26.	A Área de Segurança da Informação deverá apoiar com as medidas técnicas necessárias para contenção/recuperação do incidente, por exemplo, efetuar coleta de evidências de forma legal ou isolar recursos de tecnologia de modo a não perder dados relativos ao incidente.
<b>ANÁLISE DE RISCOS DA VIOLAÇÃO DE DADOS PESSOAIS</b>	

#	Diretrizes
27.	<p>De forma a analisar os riscos envolvidos no incidente de violação de dados, deverá ser feita pelo gestor da área uma avaliação do impacto da violação onde ocorreu o evento ou do agente de tratamento (fornecedor) originário do incidente de violação de dados (com apoio do Encarregado pelo Tratamento de Dados Pessoais) considerando as seguintes informações:</p> <ul style="list-style-type: none"> <li>• Que tipo e quais dados pessoais estão envolvidos?</li> <li>• Há dados pessoais sensíveis nesta violação?</li> <li>• Quais medidas de segurança são aplicáveis à área/recurso originário do incidente?</li> <li>• Quantos titulares foram afetados pela violação?</li> <li>• Em caso de compartilhamento indevido, quais informações um terceiro pode extrair da informação a qual teve acesso?</li> <li>• Foi possível identificar todos os envolvidos na violação de dados ocorrida?</li> <li>• Há informações de cadastro/contato de todos os envolvidos na violação de dados ocorrida?</li> <li>• A violação de dados ocorrida afeta algum direito do titular de dados pessoais garantido por legislação de proteção de dados nos territórios onde ocorreu a violação?</li> </ul>
<b>COMUNICAÇÃO PARA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)</b>	
28.	<p>Uma violação dos dados que represente risco relevante aos direitos e liberdades das pessoas físicas deve ser relatada à ANPD sem demora injustificada, dentro de até 48 horas depois que a SPA tomar conhecimento da violação, ou em outro prazo definido pela ANPD, se menor. Quaisquer possíveis motivos para demora na comunicação devem ser informados à ANPD. A comunicação deve ser realizada obedecendo-se os meios e ferramentas disponibilizadas pela ANPD.</p>
29.	<p>A SPA é considerada ciente de uma violação de dados pessoais quando existe um grau razoável de certeza de que ocorreu um incidente de segurança que levou ao comprometimento dos dados pessoais. A SPA também é considerada ciente quando um operador é informado; portanto, todos os contratos de processamento de dados devem exigir que o operador notifique imediatamente a SPA de uma violação.</p>
30.	<p>Um aviso parcial e incompleto deverá ser enviado para a ANPD, dentro do prazo previsto na diretriz 24, em casos de ocorrência de violações complexas que requeiram investigações detalhadas, ou quando ocorrerem várias violações semelhantes em um curto período de tempo.</p>

#	Diretrizes
31.	<p>A notificação para a ANPD deverá incluir:</p> <ul style="list-style-type: none"> <li>a) A descrição da natureza dos dados pessoais afetados;</li> <li>b) As informações sobre os titulares envolvidos;</li> <li>c) A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;</li> <li>d) Os riscos relacionados ao incidente;</li> <li>e) Os motivos da demora, no caso de a comunicação não ter sido imediata;</li> <li>f) As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo;</li> <li>g) Identificar pontos de contato para maiores detalhes;</li> <li>h) Descrever possíveis consequências do incidente de violação de dados;</li> <li>i) Descrever medidas para endereçar o incidente de violação de dados, incluindo medidas adotadas para mitigar possíveis efeitos adversos do incidente de violação de dados.</li> </ul>
<b>COMUNICAÇÃO AOS TITULARES DE DADOS PESSOAIS</b>	
32.	<p>Quando a violação oferecer um risco classificado como alto risco para os titulares de dados e pessoas afetadas, o Encarregado pelo Tratamento de Dados Pessoais deverá, com o apoio da Superintendência Jurídica (SUJUD) e da Superintendência de Comunicação Corporativa (SUCOC) elaborar plano de comunicação aos titulares de dados e pessoas envolvidas no incidente. Em seguida, o Encarregado pelo Tratamento de Dados Pessoais deverá solicitar a aprovação do Comitê de Segurança da Informação para executar o plano de comunicação. Esse processo deve ser executado sem demora injustificada.</p>

#	Diretrizes
33.	<p>Uma comunicação para o(s) Titular(es) dos dados pessoais, deve conter, no mínimo, em linguagem clara e simplificada:</p> <ul style="list-style-type: none"> <li>a) A descrição da natureza dos dados pessoais afetados;</li> <li>b) As informações sobre os titulares envolvidos;</li> <li>c) A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;</li> <li>d) Os riscos relacionados ao incidente;</li> <li>e) Os motivos da demora, no caso de a comunicação não ter sido imediata;</li> <li>f) As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo;</li> <li>g) Identificar pontos de contato para maiores detalhes;</li> <li>h) Descrever possíveis consequências do incidente de violação de dados;</li> <li>i) Descrever medidas para endereçar o incidente de violação de dados, incluindo medidas adotadas para mitigar possíveis efeitos adversos do incidente de violação de dados.</li> </ul>
34.	<p>A comunicação com os titulares dos dados deve ser entregue em mensagens personalizadas individuais, por meios que maximizem as chances de comunicação das informações a todos os titulares dos dados afetados - isso pode exigir a utilização de vários métodos de comunicação e o fornecimento de informações em formatos e idiomas alternativos, se necessário.</p>
35.	<p>Se a violação afetar um grande volume de registros de titulares de dados e dados pessoais, a SPA decidirá se uma notificação pública em massa é apropriada em vez de uma notificação personalizada individual com base em uma avaliação da quantidade de recursos necessários para notificar cada titular de dados individualmente e sobre a capacidade da SPA de fornecer adequadamente aos titulares dos dados a notificação dentro do prazo especificado.</p>
<b>DECISÃO DE NÃO COMUNICAR</b>	
36.	<p>Quando a ocorrência resultar em risco ou dando que não seja relevante aos titulares, conforme artigo 48 da LGPD.</p>
37.	<p>Para os casos de decisão pela não comunicação, a justificativa para essa decisão deve ser documentada e aprovada pelo Comitê de Segurança da Informação.</p>

#	Diretrizes
38.	A SPA deve continuar a monitorar as circunstâncias e os efeitos de uma violação e pode precisar fazer ou atualizar comunicações à ANPD ou ao Titular dos Dados à medida que novas informações surgirem.
39.	Todas as violações e as ações tomadas para responder às violações devem ser totalmente documentadas e registradas, mesmo que nenhuma comunicação seja necessária.
<b>COMUNICAÇÃO AO CONTROLADOR - SPA NA CONDIÇÃO DE OPERADOR</b>	
40.	Se os dados pessoais envolvidos no incidente estiverem sendo tratados pela SPA, na qualidade de operador, o controlador dos dados deverá ser comunicado sem demora injustificada, devendo a SPA cooperar com as informações necessárias, bem como com as autoridades fiscalizadoras, para a mais breve apuração, esclarecimento e solução do caso com total transparência.
<b>PÓS INCIDENTE - PRÓXIMOS PASSOS</b>	
41.	Após a correção de uma violação, a Equipe de Resposta a Incidentes deve se reunir para discutir as medidas ou procedimentos de segurança que precisam ser implementados para melhorar a segurança dos dados com base nas lições aprendidas.
42.	A Equipe de Resposta a Incidentes também deve refletir sobre a resposta geral à violação e políticas ou protocolos atualizados, conforme necessário, para melhorar as reações futuras à eventuais novas violações.

## 6.2. Consenso / Aprovação

Este Instrumento Normativo deve ser aprovado pela Diretoria Executiva.

## 7. PAPÉIS E RESPONSABILIDADES

### 7.1. Da Unidade Responsável – Incidentes de Segurança da Informação

Área	Atividades	Ferramenta
<b>Superintendência de Tecnologia da Informação (SUPTI)</b>	Aplicação das políticas e práticas de Segurança da Informação.	N/A

	<p>Responsável pelos controles tecnológicos que apoiam a proteção da informação de todas as Unidades de Gestão da SPA, nos aspectos de:</p> <ul style="list-style-type: none"> <li>• Identificação;</li> <li>• apresentação;</li> <li>• sustentação;</li> <li>• escolha;</li> <li>• implantação; e,</li> <li>• manutenção.</li> </ul>	
--	---	--

## 7.2. Da Unidade Responsável – Incidentes de Violação de Dados Pessoais

Área	Atividades	Ferramenta
<p><b>Encarregado pelo Tratamento de Dados Pessoais (ETDP)</b></p>	<ul style="list-style-type: none"> <li>• Receber as notificações de incidentes e prosseguir com o que for devido;</li> <li>• Avaliar a necessidade de comunicação do Incidente de Violação de Dados para Autoridade Nacional de Proteção de Dados e titulares de dados pessoais;</li> <li>• Iniciar processos de investigação do Incidente de Violação de Dados e indicar áreas envolvidas que deverão participar do processo.</li> <li>• Providenciar que seja feita a comunicação das violações de alto risco à ANPD e aos titulares de dados afetados sem demora injustificada.</li> </ul>	

<b>SUPTI</b>	<ul style="list-style-type: none"> <li>• Aprovar e empreender ações ou investimentos que promovam a melhoria contínua do processo.</li> <li>• Auxiliar na análise dos incidentes de violação de dados pessoais por meio da apresentação das trilhas de auditoria dos sistemas sob sua gestão;</li> <li>• Caso o tratamento do incidente envolva impactos no ambiente de produção a equipe de gerenciamento de mudanças deve ser comunicada para notificar os gestores e usuários do recurso em questão sobre o ocorrido;</li> <li>• Conduzir em paralelo a este normativo os procedimentos indicados na Política de Gestão de Incidentes de Segurança da Informação;</li> <li>• Auxiliar nos processos de investigação do incidente quando requerido;</li> <li>• Apoiar com as medidas técnicas necessárias para contenção/recuperação do incidente.</li> </ul>	
--------------	---	--

### 7.3. Das Unidades Executoras

Área	Atividades	Ferramenta
<b>SUPTI</b>	Fazer a gestão de incidentes de Segurança da Informação.	N/A
<b>Equipe de Resposta a Incidentes (ERI)</b>	<ul style="list-style-type: none"> <li>• Monitorar continuamente o ambiente tecnológico do ponto de vista de segurança da informação, visando identificar eventos que possam causar impacto na disponibilidade, integridade e confidencialidade de dados pessoais que sejam tratados pela SPA;</li> <li>• Seguir todas as fases descritas neste normativo desde a identificação até a solução do incidente;</li> <li>• Comunicar as áreas responsáveis pelo gerenciamento de mudanças em caso de incidentes de violação de dados pessoais que envolvam impactos no ambiente de produção;</li> <li>• Conduzir em paralelo a este normativo os procedimentos indicados na Política de</li> </ul>	

	<p>Gestão de Incidentes de Segurança da Informação;</p> <ul style="list-style-type: none"> <li>• Auxiliar nos processos de investigação do incidente quando requerido;</li> <li>• Apoiar com as medidas técnicas necessárias para contenção/recuperação do incidente</li> </ul>	
<p><b>Responsável pela Segurança da Informação</b></p>	<ul style="list-style-type: none"> <li>• Aprovar e empreender ações investimentos que promovam a melhoria contínua do processo;</li> <li>• Apoiar sempre que necessário na interação e no escalonamento com as demais áreas a fim de prover um atendimento mais rápido ao processo.</li> </ul>	
<p><b>Superintendência Jurídica (SUJUD)</b></p>	<ul style="list-style-type: none"> <li>• Se o incidente tiver consequências legais a SUJUD deve atuar junto aos órgãos responsáveis pela apuração e aplicação de penalidades (Agências Reguladoras e/ou Delegacias, se for o caso) em defesa dos interesses da SPA.</li> </ul>	
<p><b>Superintendência de Comunicação Corporativa (SUCOC)</b></p>	<ul style="list-style-type: none"> <li>• No caso de incidentes que tiverem desdobramentos para fora da SPA e que envolvam a imprensa ou comunidade externa, prestar suporte na elaboração do plano de comunicação aos titulares de dados e pessoas envolvidas no incidente.</li> </ul>	
<p><b>Comitê de Segurança da Informação (CSI)</b></p>	<ul style="list-style-type: none"> <li>• Tomar decisões sobre plano de comunicação aos titulares de dados;</li> <li>• Tomar decisões sobre plano de comunicação aos clientes e ao mercado.</li> </ul>	
<p><b>Gestores</b></p>	<ul style="list-style-type: none"> <li>• Garantir e gerenciar o cumprimento deste normativo e demais documentos complementares pelos seus subordinados;</li> <li>• Reportar incidentes de violação de dados;</li> <li>• Receber comunicação de incidentes de violação de dados por parte de empregados de sua área;</li> <li>• Para os incidentes de violação de dados pessoais que envolvam desvio de conduta do empregado ou em desacordo com o Código de Ética, encaminhar a solicitação de apuração à sua Superintendência direta, que remeterá à Corregedoria, para instauração de processo disciplinar, quando cabível, conforme previsto no Regulamento Interno de Pessoal - RIP.</li> </ul>	

	<ul style="list-style-type: none"> <li>• Receber comunicação de incidentes de violação por parte de agentes de tratamento (fornecedores) que estejam sob a sua gestão;</li> <li>• Auxiliar nos processos de investigação do incidente.</li> </ul>	
<b>Empregados</b>	<ul style="list-style-type: none"> <li>• Estar ciente e manter-se atualizado com este normativo e demais documentos complementares;</li> <li>• Reportar incidentes de violação de dados ao gerente de sua área;</li> <li>• Auxiliar nos processos de investigação do incidente quando requerido.</li> </ul>	

## 8. DISPOSIÇÕES FINAIS

Os casos excepcionais ou não previstos neste Instrumento Normativo deverão ser submetidos à análise e aprovação da Diretoria Executiva.

Qualquer atividade que desrespeite as disposições estabelecidas neste normativo ou em quaisquer dos documentos complementares da SPA deve ser considerada uma violação e tratada pela SPA a fim de apurar as responsabilidades dos envolvidos de acordo com as "Medidas Disciplinares" visando aplicação de sanções cabíveis previstas em cláusulas contratuais e na legislação vigente.

## 9. ANEXOS

N/A