Norma de Gestão de Incidentes

Manual de Processos e Práticas

Especificações do Documento	
Título	Norma de Gestão de Incidentes
Subtítulo	Manual de Processos e Práticas
Código	NRM-09

Histórico de Revisões			
Data	**Versão**	**Descrição**	**Responsável/Revisor**
08/12/2021	1	Versão inicial	Fábio Marques/Selmo Medeiros
05/12/2022	2	Primeira Revisão	Fábio Marques/Selmo Medeiros
07/06/2023	3	Segunda Revisão	Maurício T Daniel Tourinho/ Selmo Medeiros
07/06/2024	4	Terceira Revisão	Maurício T Daniel Tourinho/ Selmo Medeiros

finaşu / SOLUÇÕES FINANCEIRAS

Avenida Rio Branco, 185 - Sala 1803
Centro - Rio de Janeiro | RJ
CEP: 20.040-007

Sumário

1 Introdução

A Norma de Gestão de Incidentes (NRM-09) complementa a Política Geral de Segurança da Informação, este documento apresenta o plano de gestão de incidentes para violação de dados pessoais na Finasu. Todos os Controladores e Operadores de Dados Pessoais precisam estar preparados para diagnosticar, tratar e reportar incidentes de segurança da informação que possam envolver violações de dados pessoais. O tratamento de incidentes consiste na implementação de procedimentos e etapas para a resolução do incidente.

Desta forma, mantemos aderencia ao artigo 50 da Lei Geral de Proteção de Dados, o qual determina que os controladores e operadores precisam estar preparados para os incidentes que possam ocasionar uma eventual violação de dados pessoais, através de um plano de incidentes e remediação.

2 Propósito

2.1 Este documento tem como propósito apresentar e orientar sobre o processo de tratamento de incidentes visando reduzir ao máximo os impactos ao negócio da Finasu. A seguir constam tópicos relacionados ao processo de Gestão de Incidentes.

- ✓ Governança de TI
- ✓ Detecção de incidentes e violação de dados pessoas
- ✓ Procedimento de detecção e tratamento
- ✓ Tipo de incidentes
- ✓ Níveis de atendimento
- ✓ SLA
- ✓ Resolver o incidente, manter as evidências e registrar na base de conhecimentos

3 Escopo

3.1 Operações de tratamento de dados pessoais realizados pela Finasu, tanto em seu papel como controlador e operador.

- Os cenários de incidentes internos quando atua como controlador ecenários externos, no papel de operador;
- Classificação dos incidentes;
- Determinar os incidentes que geram necessidades de suporte, cuja níveisde atendimento que devem ser acionados;

4 Governança de TI

Com as constantes transformações no ambiente empresarial, cada vez mais é exigido da área de TI, formas ágeis, eficazes e flexíveis para o gerenciamento dos serviços. Neste contexto, as melhores práticas e modelos de Governança de TI auxiliam na gestão de processos e no gerenciamento das diversidades tecnológicas presentes nas corporações, fornecem técnicas de planejamento estratégico e possibilitam a disponibilidade de serviços com mais qualidade, agilidade e eficiência.

Este documento possui como base as melhores práticas de gestão com base no framework ITIL que descreve os processos necessários para gerenciar a TI eficientemente e eficazmente de modo a garantir os níveis de serviço acordados com os clientes internos e externos, bem como, agregar valor.

A figura abaixo apresenta o Mapa do framework ITIL 4, que contém os seguintes elementos: Princípios Orientadores, Quatro Dimensões do Gerenciamento de Serviço, o Sistema de Valor de Serviço (SVS), a Cadeia de Valor de Serviço (CVS), o Modelo de Melhoria Contínua, e as Práticas de Gerenciamento, Práticas de Gerenciamento de Serviços, onde o Gerenciamento de Incidentes está inserido, e as Práticas de Gerenciamento Técnico.

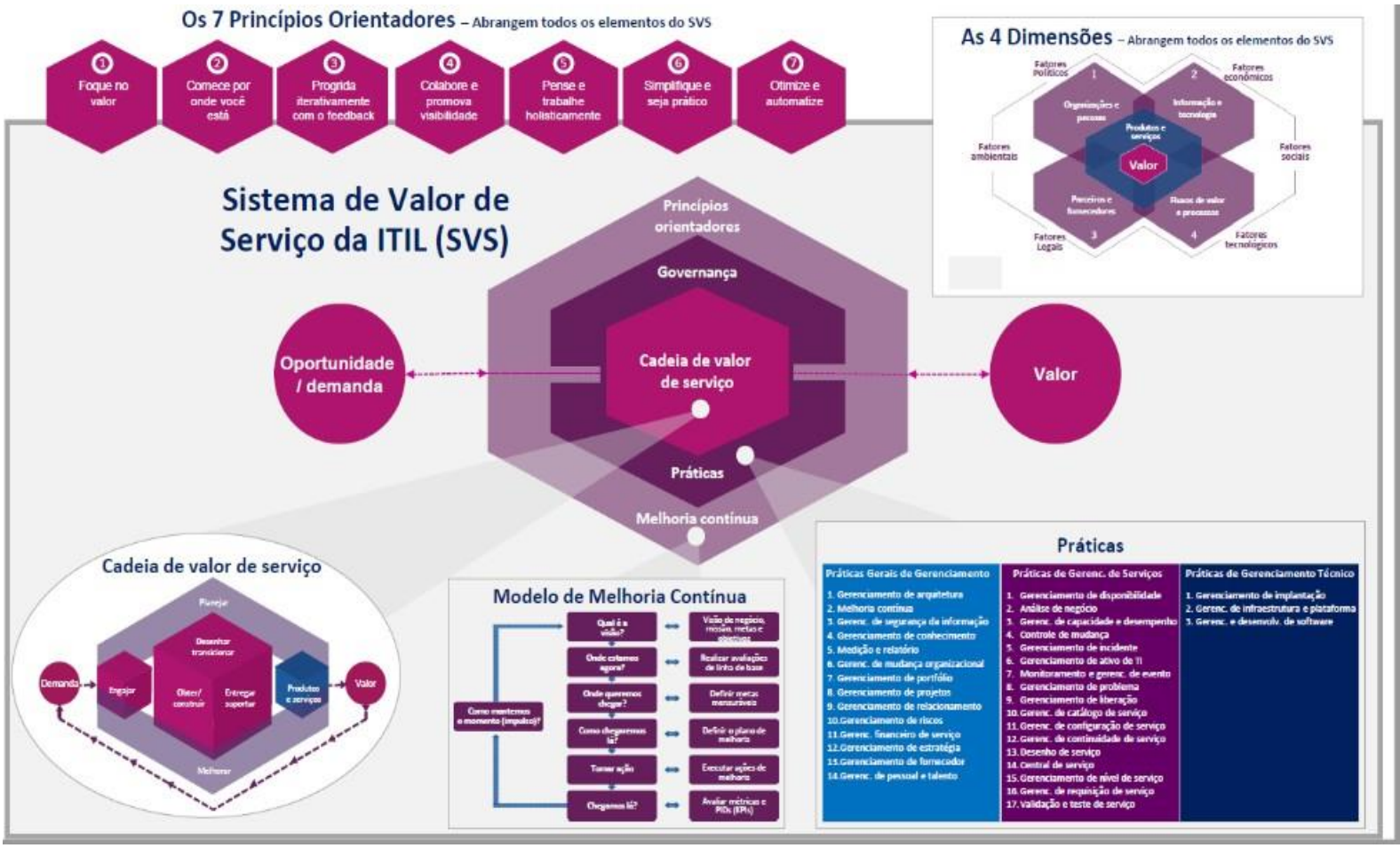


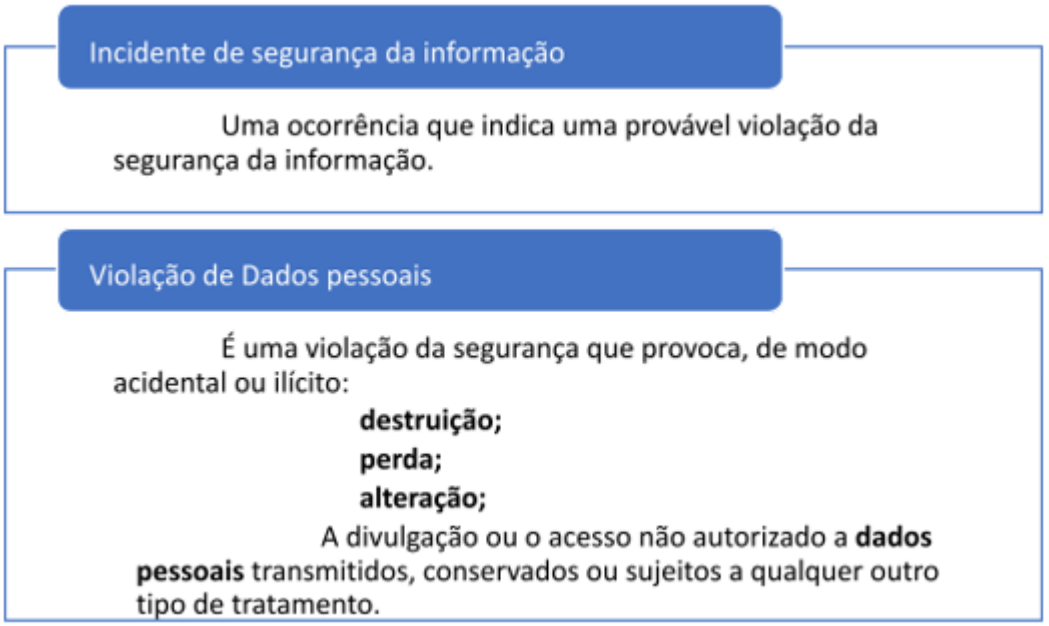
FIGURA 1- MAPA ITIL 4

Assim, no contexto de se buscar sempre a melhoria contínua, para lcançar o objetivo proposto, este documento irá abordar os seguintes tópicos:

- ✓ Detecção de Incidentes;
- ✓ Categorização;
- ✓ SLA;
- ✓ Análise de causa raiz;
- ✓ Gestão de conhecimento;
- ✓ Lições aprendidas e plano de ação;
- ✓ Notificação

5 Detecção de incidentes e violação de dados Pessoais

Para gerenciarmos os nossos incidentes de maneira eficaz, precisamos diferenciar que nem todo incidente de segurança da informação pode provocar uma violação de dados pessoais:



As informações podem ser comprometidas de diversas formas, ao considerarmos a confidencialidade, integridade e disponibilidade. Alguns exemplos, ilustram estes possíveis cenários:

- ✓ **Vazada fora da organização**: roubo de laptop, tablet, celular (WhatsApp com troca de informações sigilosas), e-mail com informações de clientes para pessoas fora da organização etc.;
- ✓ **Destruída ou danificada:** uma deleção acidental ou incorreta, funcionário mal-intencionado etc.;
- ✓ **Inacessível, bloqueada:** ataques, sequestros de dados, ransomware, indisponibilidade dos sistemas etc.

Os dados são comprometidos/violados sempre quando temos alguma ameaça e uma vulnerabilidade associadas.

6 Atores do Processo

- Autoridade Nacional de Proteção de Dados - ANPD: Órgão da administração pública que deve fiscalizar o cumprimento da LGPD. Analista de segurança: responsável por examinar e avaliar as causas e doincidente de segurança da informação;

- Encarregado de Proteção de Dados - EPD: Pessoa física ou jurídica indicada pelo controlador para atuar como ponto de comunicação entre o titular do dado e a ANPD;

- Controlador: Responsável por definir as operações de tratamento a serem realizadas.

7 Procedimento de detecção e tratamento

No caso de um incidente, a primeira medida a ser tomada é a contenção, ou seja, identificar onde ocorreu o mesmo e tomar as primeiras medidas para "estancar" o vazamento de dados.

A seguir são descritas as etapas do processo de tratamento:

1. O responsável técnico recebe o e-mail no contato@finasu.com.br e inicia o atendimento;

2. Comunicar imediatamente o fato ao DPO o ocorrido por meio do preenchimento de formulário interno de notificação de incidentes de segurança com violação de dados pessoais e a alta direção;

3. Apurar se o incidente ocorrido é considerado um caso grave de acordo com as prioridades de negócio e serviço e se inclui violação de dados pessoais. Se houver violação de dados pessoais, é necessário avaliar a natureza, categoria e quantidade de titulares de dados afetados, categoria e quantidade dos dados afetados, consequências concretas e prováveis; e direcionados a equipe adequada de gerenciamento de problemas. Ao longo da investigação, os envolvidos deverão ser

mantidos e informados sobre o status da apuração. Independente da classificação da gravidade do vazamento, de sua volumetria e de ter ocorrido ou configurar-se apenas de uma suspeita, as IF's deverão ser sempre comunicadas sobre a ocorrência identificada através do modelo descrito no item 14 deste documento.

4. Comunicar o incidente à Autoridade Nacional de Proteção de Dados (ANPD) por meio do **Formulário de Comunicação de Incidente de Segurança com Dados** Pessoais, cujo link encontra-se no site da ANPD(https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca)
   Esta notificação deverá ser efetuada em até 02 (dois) dias úteis.

   A comunicação deverá ser efetuada mesmo nos casos em que houver dúvida sobre a relevância dos riscos e danos envolvidos;

5. Comunicar de forma personalizada (nominal) o incidente aos titulares caso seja constatado risco ou danos relevantes aos mesmos. Essa comunicação deverá ser feita conforme o Modelo de Comunicação de Incidentes com Violação de Dados Pessoais de forma clara e precisa.

6. Realizar um workshop com os envolvidos para avaliar os fatos e conclusões na análise das causas do incidente bem como implementar procedimentos para o monitoramento preventivo.

O atendimento deve ser atualizado com as informações pertinentes e medidas para resolver o incidente, conter o dano e o plano de ação para que o problema não volte a ocorrer novamente. É válido realizar posteriormente a resolução do incidente uma reunião de lições aprendidas.

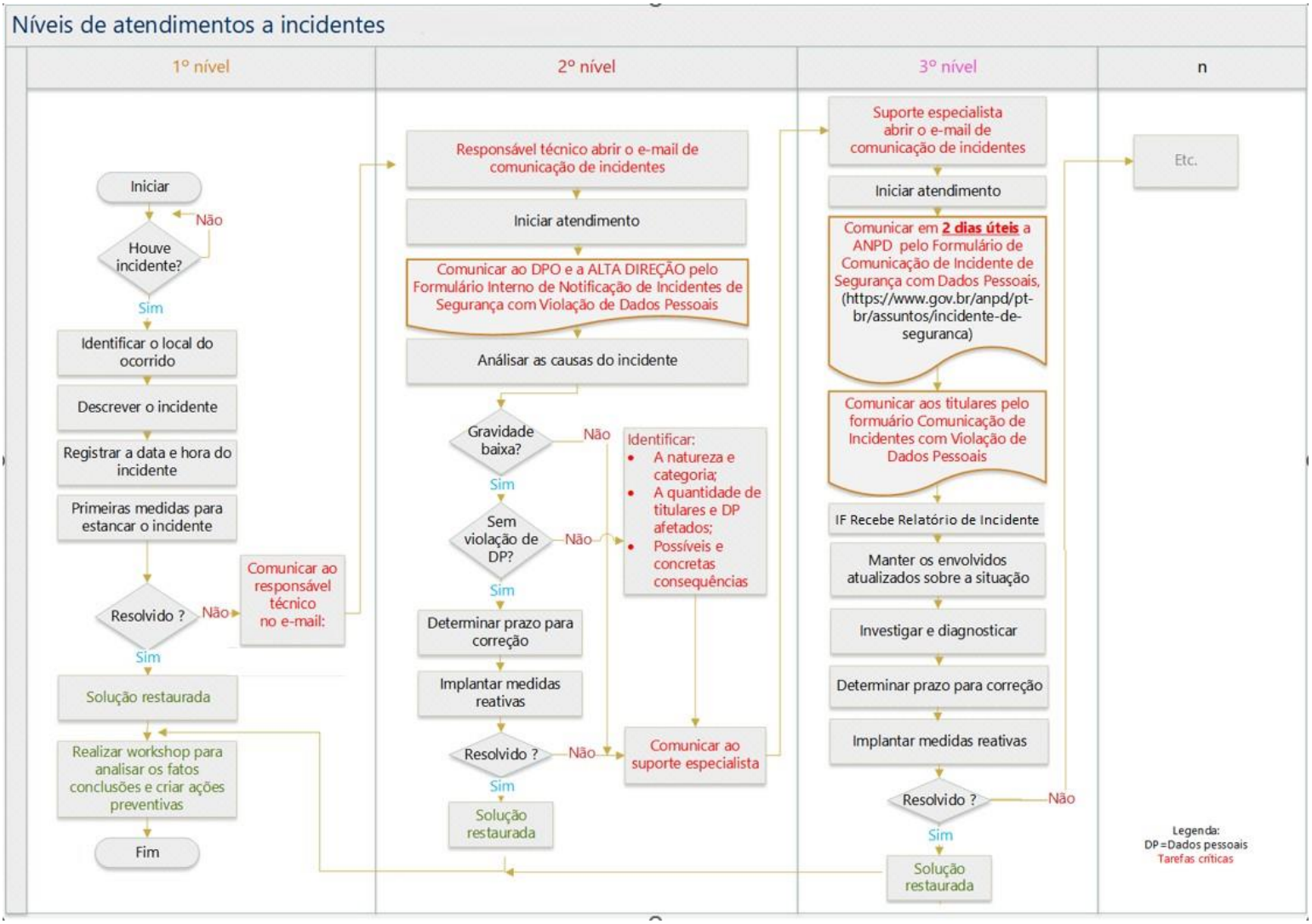
8 Tipo de Incidentes

Os seguintes eventos são considerados incidentes:

Incidentes	Tipo	Descrição
Acesso não Autorizado	Segurança da Informação	Tentativa não autorizada de acesso; falha no sistema que impede um acesso autorizado
Negação de serviço (denial of service)	Segurança da Informação	Tornar os recursos de um sistema indisponíveis através da geração de demanda insustentável pelo mesmo.
Vírus ou malwares	Segurança da Informação	Código malicioso, softwaremal-nocivo, intencionado ou malicioso.
Uso impróprio	Segurança da Informação	O Usuário viola as políticas de segurança da informação no uso de serviços de TI pessoais ou de terceiros.
Tentativa de intrusão	Segurança da Informação	Processo que varre redes de computadores para localizar serviços e portas lógicas ativas que podem ser exploradas.
Fraude (phishing)	Segurança da Informação	Atacante que tenta se passar por outrapessoa ou instituição para obter informações.
Conteúdo abusivo (spam)	Segurança da Informação	Envio de e-mails ou mensagens não solicitadas em massa geralmente com conteúdo publicitário.
Falha	TI	Defeito ou condição anormal em determinado equipamento ou sistema, que impede seu funcionamento normal. A partir da descrição da falha é possível categorizar o chamado,exemplos comuns: internet, rede com/sem fio, correio eletrônico,sistemas operacionais, impressoras e etc.
Requisição de serviços	TI	Solicitações feitas por usuários de serviços de TI, exemplos comuns: alteração de senha, solicitações de acesso, instalações e etc.
Requisição de informações	TI	Solicitações feitas por usuários sobre funcionamento ou dúvidas sobre serviços de TI.
Notificações demonitoramento	TI	Notificações de ferramentas de monitoramento sobre situações críticas de equipamentos ou serviços de TI.

9 Níveis de atendimento

Neste cenário de suporte dos incidentes internos com violações de dados pessoais, iremos considerar os níveis de atendimento baseados nas melhores práticas da ITIL, que contemplam 3 níveis, demonstrados no fluxo a seguir:



De acordo com o cenário, podemos caracterizar os 3 níveis da seguinte forma:

- Nível 1: Possui conhecimento básico das soluções e informações para prestar um primeiro atendimento. Além disso, registra as informações relevantes do chamado/e-mail e se não consegue resolver reporta para o nível 2;

- Nível 2: Possui conhecimento aprofundado das soluções e especificidades dos clientes e está apto para verificar o problema na causa raiz, desta forma, tem habilidade para resgatar um log, executar um procedimento de ajuste, realizar uma atualização, verificar algum componente da arquitetura que pode ter contribuído para o acontecimento relatado. Desta forma, se o mesmo não consegue identificar a causa do problema informado, ou verifica algum erro crítico do sistema, irá reportar para o nível 3;

- Nível 3: É referente ao suporte especialista, que pode envolver até o fornecedor de soluções, ex: AWS. Poderá ser aberto um help desk com o fornecedor que analisará a fundo a causa raiz e a possível resolução.

10 SLA

No Gerenciamento de Incidentes, temos o SLA (Service Level Agreement) que permite que a TI decida em conjunto quais serviços devem ser fornecidos, bem como, o tempo de resolução para cada solicitação realizada e o tempo para restabelecimento do serviço em caso de indisponibilidade e seus respectivos custos.

Atualmente, a severidade de situações ocorridas para incidentes de segurança da informação com violação de dados pessoais para que seja atendida da maneira mais breve e eficaz possível, deve ser classificado e controlado pela como:

- **Severidade 1**: Comprometimento das informações pessoais que geraram alguma perda, alteração, roubo, uso indevido, compartilhamento não autorizado ou até vazamentos. Sempre que comprometida a confidencialidade, integridade e disponibilidade de informações que incluam dados pessoais é necessário considerar as violações de dados pessoais e estar alerta o tratamento necessário de acordo com a LGPD e diretrizes deste plano.

No cenário em que atuamos como operador, devemos analisar a severidade para cada exemplo de incidente no seu segmento de negócio e aplicações e assim, definir o tempo a ser acordado para resolução do ocorrido, com base na prioridade e criticidade.

11 Resolver o incidente, manter as evidências e registrar na base de conhecimentos

O time responsável pela resolução do incidente, poderá atuar conforme solução descrita na base de erros conhecidos e registrar, no histórico, as ações realizadas e medidas que foram implementadas.

Ao assegurar que o incidente foi corrigido, o responsável pela resolução deve sempre registrar o incidente na base de erros, conhecido como uma base de conhecimentos, e manter as soluções mapeadas com o seu devido passo a passo.

Para a LGPD, a prestação de contas é fundamental, pelo quedevemos manter armazenados todos os logs, prints, evidências, e-mails.

12 Plano para mitigação dos efeitos e suas respectivas consequências

Esta atividade inclui a reunião de lições aprendidas, as medidas para reverter ou mitigar os efeitos do incidente, o plano de ação com a solução definitiva e o seu devido acampamento/monitoramento até a aplicação da medida e mitigação do risco ou redução até um nível aceitável.

Os resultados devem ser integrados ao plano do projeto e ao relatório de impacto.

13 Procedimento para notificação

Ao longo da detecção do incidente e resolução, as notificações devem estar sendo preparadas por parte do(a) EPD e o Comitê de Privacidade a notificação para comunicação da violação de dados pessoais à Agência Nacional de Proteção de Dados, os titulares afetados e as IFs.

O prazo é de 02 dias úteis e precisamos estar sempre atentos às mudanças caso seja definido um prazo diferente. Não notificar no prazo estipulado pela agência e com todas as informações necessárias, poderá gerar penalizações.

Para tanto é recomendável que se utilize as orientações no modelo abaixo no item 14 intitulado **"Procedimento para criação da Notificação".**

É preciso ressaltar que a própria ANPD permite que sejam feitas comunicações parciais sobre o incidente, sejam ela preliminares ou complementares. Assim, apesar do prazo curto para enviar a notificação, é importante que não sejam dadas informações que não refletem o cenário real do incidente ocorrido, concendendo sempre a máxima transparência.

14 Procedimento para criação da Notificação

14.1 O reporte de um incidente de Segurança da Informação que envolve dados pessoais deve seguir o preenchimento das informações definidas pela Autoridade Nacional de Proteção de Dados – ANPD.

COMUNICAÇÃO

Tipo de comunicação:

☐Completa. ☐Parcial.

Para comunicação parcial:

☐Preliminar. ☐Complementar.

CRITÉRIO PARA A COMUNICAÇÃO:

☐O incidente de segurança pode acarretar risco ou dano relevante aos titulares.

☐Não tenho certeza sobre o nível de risco do incidente de segurança.

AGENTE DE TRATAMENTO

O notificante é:

☐Controlador. ☐Operador.

Se operador, informar se já houve comunicação ao controlador:

Dados do agente de tratamento:

Número do CPF ou CNPJ:	
Nome ou Razão Social:	
Natureza da Organização (Pública ou Privada):	
Endereço:	
Cidade:	
Estado:	
CEP:	
Telefone:	
E-mail:	

DADOS DO NOTIFICANTE:

Nome:	
E-mail:	
Telefone:	

DADOS DO ENCARREGADO:

☐Mesmos dados do notificante.

Nome:	
E-mail:	
Telefone:	

INCIDENTE DE SEGURANÇA

Descrever de forma resumida como o incidente de segurança com dados pessoais ocorreu.

Quando o incidente ocorreu?

[Data e hora]

☐Não tenho conhecimento.
Justifique:

☐Não tenho certeza.
Justifique:

Quando a organização teve ciência do incidente de segurança?

[Data e hora]

Descrever como a organização teve ciência do incidente de segurança.

Se a comunicação inicial do incidente não foi comunicada no prazo sugerido de 2 dias úteis após ter tomado ciência do incidente, justifique os motivos.

Se o incidente não foi comunicado de forma imediata após a sua ciência, justifique os motivos da demora.

Qual a natureza dos dados afetados?

☐Origem racial ou étnica.
☐Convicção religiosa.
☐Opinião política.
☐Filiação a sindicato.
☐Filiação a organização de caráter religioso, filosófico ou político.
☐Dado referente à saúde.
☐Dado referente à vida sexual.
☐Dado genético ou biométrico.
☐Dado de comprovação de identidade oficial (Por exemplo, nº RG, CPF, CNH).
☐Dado financeiro.
☐Nomes de usuário ou senhas de sistemas de informação.
☐Dado de geolocalização.

Outros:

Qual a quantidade de titulares afetados?

QUAL A CATEGORIA DOS TITULARES AFETADOS?

☐Funcionários
☐Crianças ou adolescentes
☐Clientes
☐Prestadores de serviço
☐Corretores / Parceiros
☐Prospects/Clientes Potenciais

MEDIDAS DE SEGURANÇA UTILIZADAS PARA A PROTEÇÃO DOS DADOS

Quais medidas de segurança, técnicas e administrativas, foram tomadas para prevenir a ocorrência do incidente de segurança?

Quais medidas de segurança, técnicas e administrativas, foram tomadas após a ciência do incidente de segurança?

Quais medidas de segurança, técnicas e administrativas, foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo do incidente de segurança aos titulares dos dados?

O agente de tratamento realizou relatório de impacto à proteção de dados pessoais?

RISCOS RELACIONADOS AO INCIDENTE DE SEGURANÇA

Quais as prováveis consequências do incidente de segurança para os titulares afetados?

Considerando os titulares afetados, na sua avaliação, o incidente pode trazer consequências transfronteiriças?

COMUNICAÇÃO AOS TITULARES DE DADOS

Os titulares foram comunicados sobre o incidente de segurança com dados pessoais?

☐Sim
☐Não

Forneça detalhes.

Caso os titulares afetados não tenham sido informados, quais são os motivos que justificam a não comunicação ou o seu retardo?

15 Sanções e Punições

15.1 Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

16 Revisões

16.1 Esta norma é revisada com periodicidade mínima anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

17 Validade

17.1 Esta norma entrará em vigor, a partir da primeira aprovação de liberação com data informada em seu histórico.

18 Gestão da Norma

18.1 A norma NRM-09 é aprovada pelo Comitê Gestor de Segurança da Informação e apresentada à Diretoria para conhecimento.

18.2 A presente norma foi aprovada no dia 08/12/2021 e revisada em 07/06/2024.