Histórico de Revisões			
Revisão	**Data**	**Descrição**	**Aprovador**
00	25/10/2023	Emissão Inicial	José Francisco Ferreira Santos
01	21/05/2025	Revisão Geral	José Francisco Ferreira Santos

Sumário

1. Introdução

Toda empresa está suscetível a incidentes de segurança envolvendo dados pessoais, seja por conta de ataques hacker, vazamentos ou perda de dados na hora de atualizar sistemas, erros operacionais, falhas humanas dentre inúmeros outros possíveis fatores.

Para garantir a conformidade com a LGPD (Lei Geral de Proteção de Dados), mais especificamente com seu Artigo 50, parágrafo 2º, inciso I, que prevê a implementação de um programa de privacidade com plano de resposta a incidentes e remediação. Assim, este documento é fundamental para lidar com possíveis situações e minimizar os prejuízos aos titulares de dados.

Para facilitar esse processo, vamos auxiliá-lo no plano de resposta quando ocorrer um incidente de dados pessoais.

2. Notificação do incidente e acionamento do time de resposta

A notícia inicial do incidente pode vir de várias fontes, como por exemplo, colaboradores, parceiros ou outros terceiros, clientes, mídia, redes sociais e etc.

A identificação do vazamento deve ser comunicada imediatamente através do e-mail **privacidade@omegasaude.med.br.**

3. Avaliação do Incidente e da necessidade de comunicação à ANPD e aos titulares

O Encarregado de Dados da OMEGA deverá fazer uma avaliação detalhada do incidente, identificando se há riscos aos titulares de dados. Essa avaliação deve ser feita rapidamente, dado que, em alguns casos, os incidentes podem levar os dados a se espalharem em maiores proporções.

Identificados os riscos, é preciso notificar a ANPD no prazo de 02 (dois) dias úteis contados da data do conhecimento do incidente, e os titulares das medidas adotadas para a mitigação dos riscos e impactos decorrentes do incidente.

Assim, é preciso levantar o máximo de informações possível a respeito do incidente, por exemplo:

- Qual foi a causa do incidente?
- Quais foram as vulnerabilidades que levaram ao incidente?
- Quais setores da empresa foram afetados?
- Houve exposição, transferência ou sequestro de dados?
- Quais dados e quais titulares foram afetados?
- Quais colaboradores estão envolvidos?

É importante que o Encarregado de Dados sempre documente o incidente, ainda que seja feita a opção pela não comunicação à ANPD (em casos em que o risco seja de pequeno porte), como forma de demonstrar a conformidade com a lei, registrar o ocorrido exibindo-se as razões pelas quais foi feita esta opção.

Nos casos em que forem identificados riscos aos titulares de média a alta gravidade, caberá ao CONTROLADOR a notificação à ANPD por meio do formulário de comunicação de incidente de segurança com dados pessoais no link: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca e aos titulares envolvidos.

Caso contrário poderá preencher o formulário disponibilizado pela OMEGA.

4. Contenção e Erradicação

O objetivo é evitar que os danos causem maiores prejuízos.

Importante atuar na raiz do incidente e estabelecer maneiras de conter danos, como por exemplo, desabilitar sistemas, alterar programas, redefinir senhas, comunicar os envolvidos, além de poder aprimorar fluxos, processos e procedimentos para salvaguardar futuras ações similares.

Porém é muito importante procurar preservar as evidências que possam ajudar a identificar melhor o que ocorreu e os eventuais responsáveis.

5. Recuperação

Depois que o incidente estiver contido e erradicado, é preciso tentar restaurar dados e serviços.

Essa fase pode incluir a restauração de backups, clonagem de máquinas virtuais, reinstalação de sistemas, dentre outras medidas.

6. Avaliação e monitoramento

Para que o mesmo incidente não volte a ocorrer, todas as características do evento, incluindo as ameaças, o impacto e a probabilidade de recorrência, deverão ser documentadas. Um Plano de Recuperação deverá ser criado para o incidente após o restabelecimento normal dos serviços, caso ainda não tenha um elaborado.

É preciso lembrar que é importante manter o Programa de Adequação à Lei Geral de Proteção de Dados Pessoais atualizado, cabendo rever procedimentos de tempos em tempos, pois assim é possível identificar algumas vulnerabilidades promovendo já de antemão uma atuação preventiva para evitar incidentes de dados.