Política de Respostas a Incidentes

Santo Caos

Programa de Conformidade LGPD 2021

INTRODUÇÃO

Esta Política tem como objetivo preparar a Santo Caos para lidar com a gestão de um incidente de segurança garantindo que responda de forma mais rápida, organizada e eficiente ao evento, minimizando suas consequências para todos os envolvidos.

O nível da resposta dependerá do tipo de dados e da complexidade do tratamento aplicado. Antes de mais nada, é necessário definir o que é um incidente. De maneira geral, um incidente é uma situação inesperada, capaz de alterar a ordem normal das coisas e, no caso da proteção de dados, colocar em risco dados pessoais dos indivíduos que se relacionam com a Santo Caos.

O National Institute of Standards and Technology (NIT), define um incidente de segurança como uma violação ou ameaça de violação da política de segurança computacional, política de uso aceitável ou padrões de prática de segurança. De acordo com o artigo 46 da Lei Geral de Proteção de Dados (LGPD),

> Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito.

Seguindo o disposto no artigo 48 da referida Lei, é obrigação do controlador comunicar à autoridade nacional e ao titular dos dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Devendo esta comunicação ser feita em prazo razoável, conforme definição da autoridade nacional, tendo em seu conteúdo, no mínimo:

- A descrição da natureza dos dados pessoais afetados;
- As informações sobre os titulares envolvidos; A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados;
- Os riscos relacionados ao incidente;
- Os motivos da demora, no caso de a comunicação não ter sido imediata;
- As medidas que foram ou que estão sendo tomadas para reverter ou mitigar os efeitos do prejuízo.

Com base no exposto, a Política de Resposta a Incidentes da Santo Caos, seguirá as etapas ilustradas na figura abaixo e descritas na sequência:

Figura 1: Etapas da Resposta a Incidentes.



1. PLANEJAMENTO

Consiste em identificar, prever e descrever possíveis situações de violação de dados, bem como as respectivas ações que deverão ser tomadas, os prazos e as formas de registro, garantindo que em situações reais se tenha um plano de ação previamente traçado. O planejamento deverá conter, no mínimo:

a. a previsão de possíveis situações de sinistros bem como as formas de monitoramento e a ação que deverá ser tomada em caso de sua ocorrência;

b. a definição da área que deverá ser informada em situação de ocorrência do sinistro e como reportar;

c. o detalhamento das ações necessárias deve levar em conta a criticidade do evento.

Exemplo de detalhamento de incidente:



2. IDENTIFICAÇÃO

Deve-se definir os critérios para detectar, identificar e registrar as situações de incidentes e descrever os recursos utilizados para a identificação de alertas de segurança e acionamento das equipes responsáveis para que sejam tomadas as devidas providências. Devem ser avaliadas todas as possíveis fontes capazes de representar uma ameaça à proteção de dados. Abaixo, algumas situações que devem ser consideradas suspeitas:

- Recebimento de e-mails com caracteres e/ou arquivos anexos suspeitos;
- Comportamento inadequado de dispositivos;
- Problema no acesso a determinados arquivos ou serviços;
- Roubo de dispositivos de armazenamento ou computadores com informações;
- Alerta de software antivírus;
- Consumo excessivo e repentino de memória em servidores ou computadores;
- Tráfego de rede incomum;
- Conexões bloqueadas por firewall;

Análise dos logs de tentativas de acesso não autorizado aos servidores. Situações de não cumprimento dos procedimentos internos também podem oferecer riscos à segurança dos dados pessoais, deste modo, a observação da Cartilha de Boas Práticas é de extrema importância. Todos os colaboradores e parceiros da Instituição são responsáveis por reportar qualquer tipo de eventos e fragilidades, que possam causar danos à segurança da informação. A notificação deve ser registrada por e-mail ao Encarregado de Proteção de Dados.

2.1 CATEGORIAS DA VIOLAÇÃO DE SEGURANÇA

A violação de segurança será classificada dentre as categorias citadas a seguir:

a. Material: quando o incidente envolve dados armazenados em dispositivos físicos. Exemplos: perda de portadores de dados, pastas de arquivos perdidas, smartphones perdidos etc.

b. Verbal: quando há vazamento de dados de forma verbal, seja por indiscrição (comentários acerca de dados pessoais que são percebidos por terceiros e utilizados em má-fé) ou de forma intencional, repassando indevidamente informações sigilosas.

c. Ciberespaço: quando o incidente está relacionado à Tecnologia da Informação. Nessa categoria enquadram-se o hackeamento, mau gerenciamento de patches, codificação incorreta, medidas de segurança insuficientes etc.

2.2 AVALIAÇÃO DA CRITICIDADE DE SEGURANÇA

Alguns fatores serão determinantes na definição da criticidade de um incidente:

I. A categoria da criticidade: de maneira genérica, o incidente será classificado em uma das categorias abaixo:

a. Risco Baixo: classificação utilizada quando o incidente de segurança de dados afetar apenas dados pessoais, não incluído o número do CPF;

b. Risco Moderado: classificação utilizada quando o incidente de segurança de dados afetar dados pessoais, incluído o número do CPF, e/ou pelo menos um dado sensível, não incluído raça, religião, nome social e dados de saúde;

c. Risco Alto: classificação utilizada quando o incidente de segurança de dados afetar dados pessoais, incluído o número do CPF e/ou mais que um dado sensível, incluindo raça, religião, nome social e dados de saúde.

II. Dados legíveis/ilegíveis: dados protegidos por algum sistema de pseudonimização (criptografia, por exemplo).

III. Volume de dados pessoais: expresso em quantidade de registros, arquivos, documentos e/ou em períodos de tempo (uma semana, um ano, etc.).

IV. Facilidade de identificação de indivíduos: facilidade com que se pode deduzir a identidade das pessoas a partir dos dados envolvidos no incidente.

V. Indivíduos com características especiais: se o incidente afeta pessoas com características ou necessidades especiais.

VI. Número de indivíduos afetados: dentro de uma determinada escala, por exemplo, mais de 100 indivíduos.

3. CONTENÇÃO

Após um incidente ser identificado como uma violação de segurança, o mesmo deverá ser contido para evitar que outros sistemas sejam afetados ou que ocasionem danos maiores, deve ser previsto ações para a contenção de curto prazo, backup do sistema e contenção a longo prazo. Durante a contenção, deve haver o registro do incidente e das medidas de contenção que foram adotadas, evitando ao máximo a perda de evidências e as provas do ocorrido. É importante lembrar da necessidade de trabalho colaborativo de toda a Santo Caos.

- Responsável pelo tratamento de dados da área afetada pelo incidente: a partir do momento que foi identificado um possível incidente de segurança de dados, a área responsável pela categoria de dados deve imediatamente informar o encarregado de dados para iniciar o processo de contenção.

- Operador: os operadores de dados, assim como os colaboradores internos, têm a responsabilidade de informar a ocorrência de incidente de segurança ao encarregado de dados, imediatamente.

- Encarregado da Proteção de Dados: após ser informado, o encarregado de proteção de dados deverá avaliar a existência do plano de ação para tal incidente

e iniciá-lo, e caso identifique o fato concreto de vazamento de dados pessoais, preencher o documento de Comunicação de Incidente de Segurança, para notificação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados.

4. ERRADICAÇÃO

Após a ameaça ter sido contida, é necessário proceder com a sua remoção e a restauração dos sistemas que foram afetados, de modo que voltem a operar em sua normalidade.

5. RECUPERAÇÃO

Os sistemas afetados são restabelecidos e voltam a operar em ambiente de produção. É necessário definir as ações que devem ser tomadas para que o sistema volte a sua normalidade. Deve ser realizada uma varredura para identificar as perdas ocorridas e como recuperar o que foi perdido.

6. LIÇÕES APRENDIDAS

É fundamental que os mesmos erros não voltem a acontecer. Assim, é necessário que os incidentes sejam documentados, especificando quais foram os procedimentos de respostas utilizadas para contorná-los, de forma a manter um histórico das ocorrências e das ações tomadas.