VERSÃO 1.0
17/03/2023

PLANO DE RESPOSTAS A INCIDENTES (IRP)

DPO – PORT. 270/2022- PMTR

APRESENTADO POR: ELISA GOMES

MUNICÍPIO DE TRÊS RIOS

PLANO DE RESPOSTA A INCIDENTES

O QUE É?

Incidente de segurança é qualquer ameaça ou episódio concreto de violação dos dados de uma instituição, resultando na perda de um ou mais dos pilares da segurança: *CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE.*

Responsabilidade ainda maior cabe à instituição quando a guarda das informações inclui dados pessoais e sensíveis dos usuários, clientes, parceiros e outros.

Um plano de resposta a incidentes em segurança de dados é um documento que indica como a empresa deverá agir frente a incidentes de segurança de TI, capaz de orientar uma resposta rápida e certeira a diferentes tipos de problemas como a presença de um malware, ataque cibernético ou qualquer situação de violação de dados.

COMO FUNCIONA?

O plano deve ser entendido como um instrumento interno da organização a ser conhecido por todos os colaboradores, contendo as seguintes informações:

- CONCEPÇÃO DA INSTITUIÇÃO SOBRE INCIDENTE DE SEGURANÇA
- PROCEDIMENTOS A SEREM SEGUIDOS FRENTE A UM INCIDENTE
- FERRAMENTAS E RECURSOS UTILIZADOS EM CADA CASO
- QUAIS PROFISSIONAIS RESPONSÁVEIS PELA MITIGAÇÃO DE INCIDENTES

ANTES DO INCIDENTE

Para ser colocado em prática um plano de resposta a incidentes é necessário que haja interatividade entre as áreas da instituição, tornando imprescindível instituir previamente um COMITÊ DE CRISE, onde os profissionais que vão atuar na mitigação dos incidentes devem ser designados antes que algo, de fato, aconteça.

Estas pessoas estão capacitadas inclusive para orientar o desenho do plano de respostas tornando-o efetivo e adequado à realidade da instituição.

Devem também conhecer profundamente a Política de Segurança da Informação, os Sistemas e Processos da instituição.

Composição do COMITÊ DE CRISE:

- DPO (LGPD)
- TI/SEGURANÇA (STIPD)
- JURÍDICO (PGM)
- COMPLIENCE (CONTROLE INTERNO)
- COMUNICAÇÃO (SECOM)

O mapeamento dos sistemas e processos são muito importante para gerar documentos previamente estruturados a fim de dar agilidade na atuação da equipe diante da crise, bem como para o envio de dados à ANPD.

DURENTE O INCIDENTE

O intuito do Plano de Respostas na LGPD é otimizar o processo durante o incidente, para isso é necessário **preservar evidências** que possam ser úteis depois.

Incidentes envolvendo violação de dados pessoais podem ser muito danosos, porém o descaso ou falta de preparo para resolvê-los se torna mais grave.

A **IDENTIFICAÇÃO, COLETA E PRESERVAÇÃO DAS EVIDÊNCIAS** é de vital importância no processo de mitigação de danos.

A identificação do responsável pelo vazamento ou a tentativa comprovada, por exemplo, é um argumento muito válido para evitar ou minimizar as sanções.

Nesta etapa o objetivo é a **Contenção dos Danos,** a **Erradicação** e a **Recuperação**, interromper os danos através dos recursos disponíveis, reconstruir o sistema ou processo, desligando coordenadamente os equipamentos suspeitos, limpando os dispositivos ou sistemas infectados, entre outras ações da Equipe de TI.

APÓS O INCIDENTE

Nesta fase do plano o Comitê de Crise deve reunir-se para debater sobre o incidente e todas as ações executadas, revisando os procedimentos e gerando um relatório completo, a fim de nortear novas ações mitigantes bem como aprimorar medidas preventivas.

O **RELATÓRIO FINAL DO INCIDENTE** deve informar sobre:

- O incidente, sua natureza e o tempo de identificação;
- Medidas tomadas para a preservação de evidências;
- Procedimentos adotados para a mitigação do incidente;
- Uma apresentação do Comitê de Crise e suas ações diante do incidente, bem como outros colabores envolvidos e suas ações;

- Os requerimentos dos titulares de dados, autoridades e imprensa, bem com as resposta fornecidas pela instituição;
- Medidas de correção técnicas e de Governança de TI;
- Análise e relatório das medidas que **poderiam** ser adotadas para evitar o incidente e que **devem** ser adotadas para evitar novas ocorrências;
- Balanço dos prejuízos causados pelo incidente.

COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA

De acordo com o Caput do artigo 48 da LGPD "***O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares***".

O elemento de mediação entre a instituição e o Governo é o Encarregado de Dados - DPO, que de acordo com uma série de determinações na Lei Geral de Proteção de Dados, comunica à ANPD – Agência Nacional da Proteção de Dados, órgão regulador Federa, através de formulário próprio, incidentes de segurança.

Além da comunicação à ANPD, elaborada a través da documentação com avaliação interna do incidente, medidas tomadas e análise de risco, para fins de cumprimento do principio de responsabilização e prestação de contas (Art. 6°, X da LGPD), deve-se comunicar também:

- O Controlador dos dados, no caso de a instituição ser o Operador;
- O Titular dos dados, em caso de risco ou dano relevante (Art. 48 da LGPD).

BENEFÍCIOS DE UM PLANO DE RESPOSTA A INCIDENTES

- Resposta rápida a incidentes;
- Evita a necessidade de um DR – Plano de Recuperação de Desastres;
- Facilidade na comunicação do incidente;
- Rápida retomada das atividades fim da instituição.

ETAPAS DO PLANO DE RESPOSTA

- ETAPA 1 - PREPARAÇÃO - COMITÊ DE CRISE
- ETAPA 2 - IDENTIFICAÇÃO/ COLETA/PRESERVAÇÃO
- ETAPA 3 - CONTENÇÃO DOS DANOS
- ETAPA 4 - ERRADICAÇÃO
- ETAPA 5 - RECUPERAÇÃO
- ETAPA 6 - AVALIAÇÃO E RELATÓRIO FINAL
- ETAPA 7 - COMUNICAÇÃO DE INCIDENTE À ANPD