PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA

Sumário:

1. OBJETIVO
2. ABRANGÊNCIA
3. DIRETRIZES DE GOVERNANÇA
4. PAPÉIS E RESPONSABILIDADES DO ENCARREGADO A INCIDENTES DE SEGURANÇA
5. INCIDENTES QUE SERÃO CONSIDERADOS
6. RECUPERAÇÃO
7. DISPOSIÇÕES FINAIS

1. OBJETIVO

Definir o plano de resposta a incidente de segurança do 2º Tabelionato de Alegrete.

Atender à Lei de Registros Públicos, Lei n. 8935/1994, Lei 13.709/2018 LGPD e Provimento 134/2022- CNJ

2. ABRANGÊNCIA

Esta Norma é um documento interno, com valor jurídico e aplicabilidade imediata, plena e indistinta. Ela deve ser de conhecimento e aplicação exclusiva ao encarregado nomeado pelo Tabelião.

3. DIRETRIZES DE GOVERNANÇA

O Encarregado de LGPD deve dispor de uma estrutura formalmente constituída de governança.

O Encarregado tem o papel fundamental de estipular e garantir a aderência às diretrizes da segurança da informação e privacidade de dados, além de auxiliar no estabelecimento de controles de segurança adequados para cada área.

4. PAPÉIS E RESPONSABILIDADES DO ENCARREGADO A INCIDENTES DE SEGURANÇA

O plano de resposta a incidentes de segurança com dados pessoais prevê a comunicação ao Juiz Diretor do Foro, a Corregedoria Geral da Justiça/RS, e à Autoridade Nacional de Proteção de Dados, no prazo máximo de 48 horas, nos termos do artigo 13 do Provimento 134, do CNJ, com esclarecimento da natureza do incidente e das medidas adotadas para a apuração das suas causas e a mitigação de novos riscos e dos impactos causados aos titulares dos dados.

Os incidentes de segurança com dados pessoais serão imediatamente comunicados pelos operadores ao controlador.

5. INCIDENTES QUE SERÃO CONSIDERADOS (ROL MERAMENTE EXEMPLICATIVO)

O encarregado deverá levantar o máximo de informação possível a respeito do incidente, identificando, por exemplo:

-Qual foi a causa do incidente;

-Quais foram as vulnerabilidades exploradas ou que levaram ao incidente;

-Se houve o uso de credenciais comprometidas e quais são essas credenciais;

-Quais sistemas, equipamentos e redes foram comprometidos;

-Quais setores do tabelionato foram afetados;

-Se houve exposição, transferência ou sequestro de dados;

-Quais dados e quais titulares, exatamente, foram afetados; etc.

Será documentado o incidente ainda que seja feita a opção pela não comunicação, como forma de demonstrar a conformidade com a lei, exibindo-se as razões pelas quais foi feita esta opção.

5.1. Contenção e erradicação

Essa é a fase de conter e erradicar o incidente, limitando os danos. A ação depende do incidente específico, mas o objetivo é evitar que ele cause mais prejuízos do que já causou.

Isso implica atuar na raiz do incidente e estabelecer formas de contenção (podendo até mesmo ser necessário desabilitar sistemas inteiros). Será importante, nesta etapa, procurar preservar as evidências que possam ajudar a identificar melhor o que ocorreu e os eventuais responsáveis.

6. RECUPERAÇÃO

Depois que o incidente estiver contido e erradicado, serão restaurados dados e serviços.

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

7. DISPOSIÇÕES FINAIS

O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com a Política e outras Normas e Procedimentos aplicáveis e relevantes adotados pela serventia.