

PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA

versão 1.0 - 20/08/2021

1. OBJETIVO

Definir o plano de resposta a incidente de segurança do Tabelionato de Notas e Protesto de Porto Seguro/BA, de forma a atender a Lei de Registros Públicos, Lei n. 8.935/1994, Lei n.11.977/2009, Lei 9.492/97, Lei 13.709/2018 LGPD, Normas das Corregedorias, Geral e do Interior, de Justiça do Estado da Bahia e do Conselho Nacional de Justiça.

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 do Tabelionato de Notas e Protesto de Porto Seguro/BA.

3. DIRETRIZES DE GOVERNANÇA

O Encarregado do Tabelionato de Notas e Protesto de Porto Seguro/BA, conforme estipulado na Política de Segurança da Informação (PSI), 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 e processo do Tabelionato de Notas e Protesto de Porto Seguro/BA.

4. PAPÉIS E RESPONSABILIDADES DO ENCARREGADO A INCIDENTES DE SEGURANÇA

O plano de resposta a incidentes de segurança com dados pessoais envolve a comunicação ao Juiz Corregedor Permanente e à Corregedoria Geral da Justiça, no prazo máximo de 48 horas, 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. 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 pelo Tabelionato de Notas e Protesto de Porto Seguro/BA.

PREPARAÇÃO PRÉVIA

O Plano de Resposta a Incidentes de Segurança com dados pessoais é essencialmente um processo. Descreve a forma como o TABELIONATO DE NOTAS E PROTESTO vai responder às situações de emergência e exceção. Pela potencial gravidade, a resposta deve ser rápida e confiável, ao mesmo tempo resguardando evidências que possam ajudar a prevenir novos incidentes e atendendo as exigências legais de comunicação e transparência. Para o processo funcionar e ser estabelecido é pré-requisito a preparação prévia e contínua, atendendo os seguintes itens:

a) Identificação e Resposta a Incidentes. Este é um processo pelo qual todos os colaboradores devem estar cientes e treinados com acessos, habilidades, responsabilidades e conhecimentos chave para responder aos mais variados tipos de incidentes. Haverão reuniões periódicas para definir melhorias neste plano, verificação de pré-requisitos, mecanismos, atribuições, necessidade de preparo, bem como divulgação e treinamentos aos empregados. O Encarregado do Tabelionato de Notas e Protesto de Porto Seguro/BA será responsável pelo processo, juntamente com os demais Substitutos.

b) Instalação e divulgação dos mecanismos de comunicação de incidente. Devem ser criadas, disponibilizadas e publicadas as formas de notificação à Encarregado quando ocorrerem incidentes. Portanto, devem ser divulgados os e-mails: notas.portoseguro@gmail.com, bem como os contatos 73 9.9941-1924 e 73 3268-3536.

INICIO

1) Um novo incidente é notificado, por pessoa externa ou não a Tabelionato de Notas e Protesto de Porto Seguro/BA, usando um dos mecanismos de comunicação definidos. Notificação é recebida pelo Encarregado.

TRIAGEM

2) O Encarregado deve fazer a avaliação preliminar ou contatar imediatamente outro Acionador em condições de realizar a referida avaliação, descartando as notificações nulas ou claramente improcedentes, tomando os devidos cuidados.

3) Na avaliação preliminar, devem ser buscadas informações sobre os sistemas e dados que foram alegadamente impactados, sua criticidade, quais os danos aparentes e o risco da situação se agravar se não houver resposta imediata.

4) Conforme a avaliação preliminar, incidentes que não envolvem riscos aumentados pela falta de ação imediata podem ser reencaminhados para tramites regulares pelo Encarregado, caso o incidente envolva dados pessoais.

5) Em caso de incidentes que exigem resposta imediata ou melhor avaliação, o Encarregado deverá passar às fases seguintes.

AVALIAÇÃO

6) Nesta fase deve ser iniciada uma avaliação mais detalhada do incidente. Deve-se procurar identificar a causa do incidente, endereços IP e credenciais envolvidas, transações e transferências de dados irregulares, métodos e vulnerabilidades exploradas, visando determinar ações para as demais fases. Pode ser importante engajar especialistas dos sistemas afetados para colaborar e isso deve ser feito a critério do Encarregado a qualquer momento que julgar adequado e viável.

CONTENÇÃO E ERRADICAÇÃO

7) O objetivo das medidas de contenção e erradicação é limitar o dano e isolar os sistemas afetados para evitar mais danos. Aqui, conforme a necessidade e a autorização obtida, será realizado o desligamento dos sistemas inteiros ou de funcionalidades específicas, colocação de avisos de indisponibilidade para manutenção, paralisação dos procedimentos afetados, sempre que possível tomando cuidados para não impactar evidências que poderiam ser usadas para identificar autoria, origem e método usado para quebrar a segurança.

RECUPERAÇÃO

8) A recuperação é o conjunto de medidas para restaurar os serviços completamente, mas pode ser feita de forma gradual, conforme viabilidade e decisão do responsável pelo sistema.

9) O Encarregado tem a responsabilidade de passar as informações que obteve para o desenvolvimento da solução e sua instalação.

10) Para a recuperação devem ser tomadas medidas identificadas na Avaliação, tais como restauração de backups, clonagem de máquinas virtuais, reinstalação de sistemas,

LIÇÕES APRENDIDAS

11) Com o incidente contido e sua resolução encaminhada, o Encarregado deve agendar e conduzir uma reunião de Lições Aprendidas, com convidados a seu critério, com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os sistemas e processos, inclusive deste Plano de Resposta a Incidentes.

12) As melhorias sugeridas na reunião, com o devido consenso, devem ser encaminhadas aos responsáveis para definição sobre a adoção.

DOCUMENTAÇÃO

13) O Encarregado deve documentar o incidente em base de conhecimentos apropriada, detalhando as informações obtidas, linha de tempo, atores envolvidos, evidências, conclusões, decisões, autorizações e ações tomadas, inclusive as da reunião de lições aprendidas.

Comunicações

14) Assim que possível, no caso de incidente com vazamento de dados pessoais, o Encarregado deve avaliar e fazer as comunicações obrigatórias por Lei, se houverem, bem como informar e subsidiar os Encarregados de Tratamento de Dados dos controladores do sistema. Essas comunicações podem incluir agradecimentos ao notificador, informações para os titulares de dados, relatórios formais para a ANPD.

15) Os incidentes detectados serão comunicados, no prazo máximo de 48 horas, ao Juiz Corregedor Permanente às Corregedorias de Justiça, com esclarecimento da natureza do incidente e das medidas adotadas para a apuração das suas causas e a mitigação de novos riscos.

16) Os incidentes de segurança com dados pessoais serão imediatamente comunicados ao controlador.