Diretrizes de Notificações de Incidentes

SANTOS BEVILAQUA ADVOGADOS

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio de Janeiro/RJ

santosbevilaqua.com.br

Sumário

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

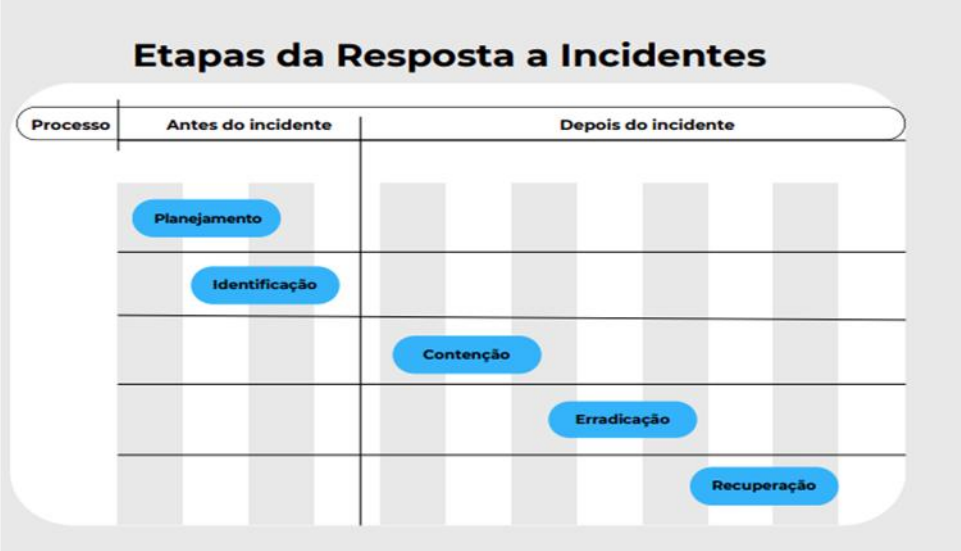
Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio de Janeiro/RJ

santosbevilaqua.com.br

1 Etapas da Resposta a Incidentes

Figura 1:Etapas da Resposta a incidentes



2 Política de Notificação de Incidentes

2.1 Planejamento

Este plano visa estabelecer um protocolo para lidar com violações de dados, incluindo a identificação e previsão de possíveis cenários, as ações a serem tomadas, os prazos e os métodos de registro. O objetivo é garantir que, em caso de violação, haja um plano de ação predefinido. O planejamento deve incluir, no mínimo:

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio de Janeiro/RJ

santosbevilaqua.com.br

2.1.1 Previsão e monitoramento de riscos

⇒ Identificar os possíveis cenários de violação de dados, como ataques cibernéticos, vazamentos de informações, perdas de dispositivos;

⇒ Definir formas de monitoramento para detectar precocemente esses riscos, como softwares de segurança, firewalls, logs de acesso;

⇒ Descrever as ações a serem tomadas em cada cenário de violação, incluindo medidas de contenção, investigação, recuperação e notificação.

2.1.2 Notificação e Comunicação

⇒ Definir a área responsável por ser informada em caso de violação de dados, como a equipe de segurança da informação, o responsável pela proteção de dados;

⇒ Estabelecer os procedimentos para reportar a ocorrência de uma violação, incluindo os canais de comunicação (telefone, e-mail, sistema interno) e as informações que devem ser fornecidas (data, hora, tipo de violação, dados afetados).

2.1.3 Ações Proporcionais à Criticidade

- Detalhar as ações necessárias para lidar com cada tipo de violação, levando em consideração a criticidade do evento, ou seja, o impacto que a violação pode causar à organização (perda de dados sensíveis, danos à reputação, prejuízos financeiros).
- As ações devem ser proporcionais à gravidade da violação, desde medidas mais simples, como a troca de senhas, até medidas mais complexas, como a investigação forense e a notificação às autoridades competentes.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio de Janeiro/RJ

santosbevilaqua.com.br

3 Identificação

É imprescindível definir os critérios para identificar, detectar e registrar incidentes de segurança, descrevendo os recursos para identificar alertas e acionar as equipes responsáveis para a devidas providências. os potenciais fontes de ameaça à proteção de dados devem ser avaliadas. 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.

A análise dos registros de acesso aos servidores é essencial para identificar tentativas não autorizadas. O não cumprimento dos procedimentos internos também coloca em risco a segurança dos dados pessoais. Todos os colaboradores são responsáveis por comunicar quaisquer eventos e fragilidades que possam prejudicar a segurança da informação, por meio de e-mail para o Encarregado de Proteção de Dados.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio de Janeiro/RJ

santosbevilaqua.com.br

3.1 Categorias da Violação De Segurança

As violações de segurança serão categorizadas da seguinte forma:

⇒ Física: Incidentes envolvendo dados em dispositivos físicos, como perda de mídias de armazenamento, pastas ou smartphones.

⇒ Verbal: Vazamento de dados por meio de conversas, seja por indiscrição ou repasse intencional de informações sigilosas.

⇒ Cibernética: Incidentes relacionados à Tecnologia da Informação, como ataques de hackers, falhas na gestão de patches, erros de código ou medidas de segurança inadequadas.

3.2 Avaliação da Criticidade De Segurança

3.2.1 Categoria de Risco

Risco Baixo: O incidente afeta apenas dados pessoais que não incluem o número do CPF.

Risco Moderado: O incidente afeta dados pessoais, incluindo o número do CPF, e/ou pelo menos um dado sensível (exceto raça, religião, nome social e dados de saúde).

Risco Alto: O incidente afeta dados pessoais, incluindo o número do CPF, e/ou mais de um dado sensível, incluindo raça, religião, nome social e dados de saúde.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio de Janeiro/RJ

santosbevilaqua.com.br

3.2.2 Legibilidade dos Dados

Dados protegidos por criptografia ou outros sistemas de pseudonimização serão considerados como de menor risco.

3.2.3 Volume de Dados

A quantidade de registros, arquivos, documentos e/ou o período em que os dados foram expostos (por exemplo, uma semana, um ano) serão considerados.

3.2.4 Facilidade de Identificação

A facilidade com que a identidade dos indivíduos pode ser deduzida a partir dos dados afetados será avaliada.

4 CONTENÇÃO

Uma vez identificado um incidente como violação de segurança, a primeira providência é interromper sua propagação, prevenindo que outros sistemas sejam atingidos ou que os danos se intensifiquem. Para isso, devem ser planejadas ações de contenção imediata, backup do sistema e contenção a longo prazo. Durante o processo de contenção, é essencial documentar o incidente e as medidas tomadas, zelando pela preservação das evidências. A colaboração de todos os membros do comitê de segurança da informação é fundamental.

5 ERRADICAÇÃO

Com a ameaça sob controle, é imprescindível eliminar os riscos e restaurar os sistemas afetados, permitindo que voltem a funcionar como antes.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio de Janeiro/RJ

santosbevilaqua.com.br

6 RECUPERAÇÃO

Os sistemas afetados são restabelecidos e voltam a operar em ambiente de produção. É necessário definir as ações para que o sistema volte à normalidade, incluindo uma varredura para identificar as perdas e como recuperar o que foi perdido.

Para evitar a repetição dos mesmos erros, é fundamental que os incidentes sejam documentados, especificando os procedimentos de resposta utilizados para contorná-los. Isso permite manter um histórico das ocorrências e das ações tomadas, aprendendo com cada incidente e aprimorando os processos de segurança.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio de Janeiro/RJ

santosbevilaqua.com.br