SANTA CATARINA

POLÍTICA DE RESPOSTAS A INCIDENTES LGPD / ISO 27035

Ordem dos Advogados do Brasil – Seção de Santa Catarina
Rua Paschoal Apóstolo Pítsica, 4860 – Agronômica – 88025-255 – Florianópolis – SC
Telefones: (48) 3239-3580 – Fax: (48) 3239-3559

A POLÍTICA:

Esta política norteará a gestão de incidentes em variadas esferas dentro do ambiente da OAB/SC. Conforme consta no artigo 50 da Lei Geral de Proteção de Dados, os controladores e operadores precisam estar preparados para os incidentes que possam ocasionar uma eventual violação de dados pessoais, através de um plano de incidentes e remediação.

O processo de resposta a uma violação envolve tarefas que não são necessariamente lineares, e as atividades descritas nesta política serão realizadas por membros específicos, definidos em conjunto com o Comitê de Segurança e o Encarregado de Dados.

Ao enfrentar um possível incidente, a organização gerencia a detecção do incidente, assegura que seus gestores colaborem e saibam suas funções, investiga, solicita a análise da equipe jurídica, gerencia as obrigações de comunicação e recupera-se da situação.

Embora todas essas etapas façam parte de uma resposta bem administrada, muitas delas devem acontecer em paralelo. Por isso, de maneira mais abrangente: operações seguras, notificar as partes competentes e corrigir as vulnerabilidades.

Segue em estrutura de tópicos as principais premissas elencadas para a gestão de incidentes na OAB/SC:

1. **PLANEJAMENTO E PREPARAÇÃO**
2. **PROCEDIMENTO DE DETECÇÃO E TRATAMENTO**
3. **CONTENÇÃO**
4. **RESPONSABILIDADES ESPECÍFICAS**
5. **RELATÓRIOS DE PROGRESSO**
6. **COMUNICAÇÕES SOBRE O INCIDENTE**
7. **TRIAGEM**
8. **ANÁLISE**
9. **NOTIFICAÇÕES**
10. **RESPOSTA**
11. **RELATÓRIOS**
12. **RESOLUÇÃO | EVIDÊNCIAS | BASE DE CONHECIMENTO**
13. **PÓS EVENTO**

Ordem dos Advogados do Brasil – Seção de Santa Catarina
Rua Paschoal Apóstolo Pítsica, 4860 – Agronômica – 88025-255 – Florianópolis – SC
Telefones: (48) 3239-3580 – Fax: (48) 3239-3559

1. PLANEJAMENTO E PREPARAÇÃO:

A preparação não impede um incidente, ao contrário da prevenção que se concentra nas tarefas e tecnologias que impedem a ocorrência de uma violação, a preparação se concentra nas medidas que devem ser tomadas para que a OAB/SC possa responder de forma ideal, ou seja, o que deverá ser feito quando a prevenção "falhar".

Na fase de preparação podemos incluir como pontos importantes e que devem ser realizados pela instituição independentemente da ocorrência ou não de um incidente:

1. Treinamento interno - deve ocorrer de maneira prévia ao incidente;

2. Implementação da presente Política de Resposta a Incidentes - as pessoas específicas que fazem parte do comitê de segurança devem ter conhecimento desta política;

3. Identificação dos principais gestores internos, que farão parte da resposta ao incidente - são aqueles que tiveram seu setor envolvido ou que integrem setores importantes para a investigação e resposta ao incidente;

4. Identificação e gerenciamento dos principais Operadores de Dados - muitas vezes o evento ocorre em um dos operadores, prestadores de serviços ou fornecedores, porém por força da lei, quem deverá respondê-lo é a instituição, por isso da importância de conhecê-los;

5. Análise das legislações aplicáveis - além da legislação específica de proteção de dados, é preciso identificar a legislação aplicável ao evento e aquela que a instituição está submetida.

6. Sigilo da investigação do incidente - processo de resposta a incidentes é um processo que exige a participação de pessoas específicas da instituição, e um dos motivos é por questões sigilosas e confidenciais, tendo em vista que o incidente ou violação ainda não foi comprovado, e por isso, precisa manter o máximo de sigilo possível para que a investigação corra de maneira segura, e sem gerar notícias falsas.

2. PROCEDIMENTOS DE DETECÇÃO E TRATAMENTO

Ordem dos Advogados do Brasil – Seção de Santa Catarina
Rua Paschoal Apóstolo Pítsica, 4860 – Agronômica – 88025-255 – Florianópolis – SC
Telefones: (48) 3239-3580 – Fax: (48) 3239-3559

2.1 O QUE SERÁ CONSIDERADO UM INCIDENTE DE SEGURANÇA

Após a notificação da ocorrência de um incidente de segurança, o Encarregado de Dados, juntamente com uma equipe designada para resolução deste evento, iniciará as identificações e investigação do incidente.

Para um gerenciamento eficaz de incidentes, é preciso saber que nem todo incidente de segurança pode provocar violação de dados pessoais. Em suma, toda a violação é um incidente, mas nem todo o incidente será uma violação:

Definição de incidente e violação:

- Incidente de segurança da informação: Ocorrência que indica violações da segurança da informação, com o rompimento da confidencialidade, integridade ou disponibilidade em relação aos dados pessoais.
- Violação de dados pessoais:É uma violação da segurança que provoca (de forma proposital ou não) uma das seguintes situações:
  - Destruição de dados pessoais;
  - Perda de dados pessoais;
  - Alteração de dados pessoais;
  - Divulgação de dados pessoais;
  - Outros tratamentos de dados pessoais não autorizados para aqueles dados em específico.

Informações podem ser comprometidas de várias maneiras, considerando confidencialidade, integridade e disponibilidade, alguns cenários podem ser considerados:

- Vazamentos fora da organização:
  - Furto ou perda de um equipamento;
  - E-mail enviado de forma errônea;
  - Dados enviados por aplicativos mensageiros não autorizados pela organização (ex: whatsapp).
  - Acesso aos dados pessoais por pessoa não autorizada.

Feita a identificação do incidente, o Encarregado de Dados juntamente com a equipe designada para a Resposta do Incidente, irá identificar se o ocorrido é de fato uma violação de dados pessoais. Mesmo que não tenha sido identificado uma violação ou o vazamento de dados sensíveis, ou situação que tenha gerado dano a titulares de dados, poderá haver a necessidade de um alerta, em relação ao evento.

3. CONTENÇÃO

Ordem dos Advogados do Brasil – Seção de Santa Catarina
Rua Paschoal Apóstolo Pítsica, 4860 – Agronômica – 88025-255 – Florianópolis – SC
Telefones: (48) 3239-3580 – Fax: (48) 3239-3559

Detectado o incidente de segurança, confirmado a violação de dados pessoais, será necessário conter os efeitos deste evento.

Contenção do incidente, tem o intuito de iniciar gerando ações que parem de gerar mais danos, podendo ser medidas paliativas para uma contenção rápida.

Durante a fase de investigação de um incidente, a contenção estará no centro das atenções da equipe de TI/Segurança juntamente com o Encarregado de Dados.

Pontos muito importantes precisam ser levados em consideração nesta fase:

1. A necessidade de evitar maiores perdas, tomando medidas apropriadas, é decisiva, isso inclui a segurança de áreas físicas e o bloqueio de acesso dos infratores aos dados impactados;

2. Correção de vulnerabilidades que permitiram que o infrator acessasse os sistemas:

2.1. Evitar que o invasor acesse ou faça extração de dados ou outras informações;

2.2. Evitar que o invasor destrua evidências valiosas e adultere os sistemas enquanto estão sendo analisados;

2.3. Evitar que o invasor use sistemas para atacar outros sistemas, protegendo os componentes organizacionais da instituição.

Estratégias de contenção que devem ser utilizadas para proteger a instituição no momento em que o incidente está sendo investigado, conforme descreve a ISO 27035, no seu item 11.2.3:

- **Implementar bloqueios** técnicos, físicos ou administrativos;
- **Desconectar** (isolar, remover), a desconexão de um sistema que foi infectado da área de rede local pode ajudar a prevenir infecções no restante da rede;
- **Desligar** se for determinado que permitir que o sistema funcione irá destruir dados ou aplicativos no sistema, o mesmo deverá ser desligado como uma medida de contenção, com a aprovação da direção;
- **Mudança de roteamento** para que o invasor perca totalmente o acesso;
- **Desativação de conta,** desabilitando as contas de usuários que podem ter sido utilizadas no ataque.

A contenção é muito importante para que o evento não se propague, e para que seja possível a investigação do mesmo, porém, as ações acima mencionadas podem ser objeto de destruição de informações que podem ser necessárias para a avaliação do evento, por isso é necessário assegurar que todos os dados necessário foram coletados antes de qualquer ação de contenção alterações do

Ordem dos Advogados do Brasil – Seção de Santa Catarina
Rua Paschoal Apóstolo Pítsica, 4860 – Agronômica – 88025-255 – Florianópolis – SC
Telefones: (48) 3239-3580 – Fax: (48) 3239-3559

sistema.

4. RESPONSABILIDADES ESPECÍFICAS:

No decorrer da investigação do incidente, e após a confirmação da violação ou não, a administração da instituição deve priorizar a solução do evento alocando fundos e sendo necessário declarações públicas para que a situação se torne calma e transparente.
Há setores específicos na participação da investigação e resolução do evento, e seguem suas principais atribuições para a oportunidade:

Encarregado de Dados:

1. Deverá avaliar a necessidade de comunicação do incidente de violação de dados para a Autoridade Nacional de Proteção de Dados e titulares de dados pessoais e providenciar que isso seja feito caso necessário;
2. Deverá seguir com o processo de apuração até conclusão, indicando atividades para mitigar os riscos, sugestões de monitoramento, de controles internos e treinamentos.

Setor de TI:

1. Aprovar e empreender ações ou investimentos que promovam a melhoria contínua dos processos;
2. Auxiliar na análise dos incidentes de violação de dados pessoais por meio da apresentação de trilhas de auditorias dos sistemas sob gestão;
3. É a área responsável pelo gerenciamento de mudanças tecnológicas;
4. Caso o tratamento do incidente envolve impactos no ambiente de produção a equipe de gerenciamento de mudanças deve ser comunicada para notificar os gestores e usuários do recurso em questão sobre o ocorrido;
5. Auxiliar nos processos de investigação do incidente quando requerido;
6. Apoiar com as medidas técnicas necessárias para contenção/recuperação do incidente.

Time de resposta a incidentes (Comitê de Privacidade):

1. Monitorar continuamente o ambiente tecnológico do ponto de vista da segurança da informação, visando eventos que possam causar impacto na disponibilidade, integridade e

Ordem dos Advogados do Brasil – Seção de Santa Catarina
Rua Paschoal Apóstolo Pítsica, 4860 – Agronômica – 88025-255 – Florianópolis – SC
Telefones: (48) 3239-3580 – Fax: (48) 3239-3559

confidencialidade de dados pessoais que sejam tratados pela instituição;

2. Seguir todas as fases descrita nesse documento desde a identificação até a solução;
3. Comunicar às áreas responsáveis pelo gerenciamento de mudanças em caso de incidentes de violação de dados pessoais que envolvam impactos no ambiente de produção;
4. Conduzir em paralelo a este documento os procedimentos indicados nesta política;
5. Auxiliar nos processos de investigação do incidente quando requerido;
6. Apoiar com as medidas técnicas necessárias para contenção/recuperação do incidente.

Jurídico:

1. Se o incidente tiver consequências legais deve ser estabelecido um contato com os órgãos responsáveis pela apuração e aplicação, de penalidades (Autoridade se for o caso) para relato dos fatos e apresentação de indícios relativos ao incidente;
2. Auxílio na confecção de documentos relativos ao incidente;
3. Cabe zelar pela estratégia jurídica que tenha menor impacto e proteja a instituição.

RH:

1. Para incidentes de violação de dados pessoais que envolvam desvio de conduta do colaborador ou em desacordo com o código de ética, o colaborador será encaminhado para área de recursos humanos, a qual poderá se aprofundar na apuração e providências específicas.
2. Será responsável pela comunicação interna, sobre novas diretrizes no decorrer da investigação do incidente.

Financeiro/Administrativo: Assegurar recursos para financiar e operacionais para a resolução.

Comunicação: Estabelecer e manter uma mensagem positiva e consistente.

Atendimento: Tratar o tráfego de chamadas relativas à violação.

Além dos setores mencionados, é possível que seja necessária a contratação de agentes externos para auxiliar na resolução do evento.

Ordem dos Advogados do Brasil – Seção de Santa Catarina
Rua Paschoal Apóstolo Pítsica, 4860 – Agronômica – 88025-255 – Florianópolis – SC
Telefones: (48) 3239-3580 – Fax: (48) 3239-3559

5. RELATÓRIOS DE PROGRESSO

A importância dos relatórios no momento da investigação de um incidente é para que se possa identificar a evolução do evento.

O tipo de relatório e a frequência devem ser sempre personalizados para cada evento individual. Três tópicos com a resposta para as seguintes perguntas devem fazer parte de um relatório:

1. Para quem se destina o Relatório;
2. Quais as informações eles precisam saber;
3. Questões legais relativas a sigilo;
4. Questões relativas aos riscos do evento.

A frequência do envio de relatório nos primeiros dias e semanas pós evento são maiores, porém análises regulares devem ser programadas para atualizar os líderes operacionais, os executivos de alto escalão e outros envolvidos importantes sobre o status e o impacto do esforço de resposta a incidentes.

6. DAS COMUNICAÇÕES SOBRE O INCIDENTE:

6.1. Comunicação interna

A tentativa de impedir que os funcionários tomem conhecimento de um episódio de perda de dados não é prudente, tampouco viável. Muito pelo contrário, a transparência é fundamental para manter a integridade e a credibilidade.

Quando ocorrer uma violação, o funcionário precisa ser comunicado, inclusive com diretrizes específicas e proibições sobre divulgação externa, em relação ao evento que está em fase de investigação.

O anúncio interno deve ser feito em tempo hábil para evitar conflito com outras iniciativas da instituição, e também para evitar exposição legal negativa.

O setor de RH deve estar preparado para receber dúvidas em relação ao evento, e aos impactos sofridos pela instituição.

6.2. Comunicação externa:

Ordem dos Advogados do Brasil – Seção de Santa Catarina
Rua Paschoal Apóstolo Pítsica, 4860 – Agronômica – 88025-255 – Florianópolis – SC
Telefones: (48) 3239-3580 – Fax: (48) 3239-3559

A comunicação externa deve ser sempre muito bem alinhada internamente, e repassada para o setor que fará o atendimento ao público.

É importante que uma mensagem breve e em tempo hábil seja publicada para evitar qualquer especulação sobre o ocorrido, e tranquilizar clientes, parceiros, prestadores de serviços e terceiros.

As possíveis consequências de mensagens inconsistentes incluem incompreensões e suposições públicas, questões de responsabilidade legal, perda de confiança e confiabilidade por parte dos seus clientes.

7. TRIAGEM

Ao analisar e, eventualmente, identificar a causa-raiz após a coleta dos dados para um tipo de evidência de ataque, a propagação de danos pode ser bloqueada, e essa prática é conhecida como triagem.

Triagem é o processo de categorização, correlação, priorização e atributo de eventos recebidos, relatórios de incidentes, relatórios de vulnerabilidade e outras solicitações de informações gerais.

O propósito da triagem é entender o que está sendo relatado em toda a organização, e também permite uma avaliação inicial de um relatório recebido e determina em níveis de prioridade, e pode também nesta fase, ofertar um local para começar a documentação inicial e entrada de dados de um relatório ou solicitação, caso isto ainda não tenha sido feito na fase de detecção.

O processo de triagem envolve os seguintes estágios:

- Determinação da gravidade do incidente: baseada no impactos as atividades da organização, nos agentes de tratamento de dados envolvidos, no método de atividade de ataque usado, no tempo tempo dos ataques e no(s) número (s) de referência;
- Correlação com relatórios relacionados ao incidente;
- Para a **priorização** serão utilizados alguns critérios, que podem ser listados abaixo:
  - Nível de perigo para a vida humana;
  - Impacto na reputação;
  - Paradas ou danos na operação;
  - Proteção das informações confidenciais;
  - Limitação de perdas financeiras;
  - Manutenção da integridade da estrutura;
  - Ameaça a estrutura crítica;
  - Tipo da atividade;
  - Escopa da atividade;

Ordem dos Advogados do Brasil – Seção de Santa Catarina
Rua Paschoal Apóstolo Pítsica, 4860 – Agronômica – 88025-255 – Florianópolis – SC
Telefones: (48) 3239-3580 – Fax: (48) 3239-3559

○ Relacionamento com outras atividades contínuas relacionadas a segurança e não relacionadas a segurança;

● Atribuição: se as informações forem notáveis ou suspeitas, sao atribuídas a algum processo de análise e repassadas para este processo. Após a categorização, a prioridade, assim como a atribuição, podem ser alterados quando o evento é analisado no processo de resposta.

● Fontes de informações que podem ajudar no momento da triagem:

○ Fontes públicas (externas);

○ Fontes internas, podendo ser utilizadas relatórios de incidentes anteriores;

○ Fontes de inteligência sobre ameaças.

○ Descrição comum, caso seja confirmado um ataque, deverá identificar sua descrição comum (externamente);

○ prioridades organizacionais;

● Gerar informações sobre titulares envolvidos:

○ Obter informações sobre a quantidade de titulares envolvidos

○ Qual o tipo de dados pessoais afetados;

○ Existência de dados sensíveis afetados;

○ Existência de dados de menores afetados

○ Avaliação do impacto para a privacidade dos titulares de dados (riscos relevantes ou não)

○ Tipo de processamento que causou a violação (dados do RH, e-mail marketing etc...)

● Categorizar a violação de dados:

○ Material - Componentes queimados, perda de equipamentos;

○ Verbal - Indiscrições, vazamento intencional de informações confidenciais;

○ Cibersegurança - Codificação incorreta de sistemas, falta de aplicação de patches de segurança, falta de atualização de sistemas, ausência de medidas de segurança alinhadas às necessidades técnicas da instituição;

○ Indicação de medidas técnicas e de segurança alinhadas à proteção de dados;

○ Avaliação das melhores soluções para o incidente. Definindo horários de execução (para não prejudicar ainda mais a operação);

○ Documentar as soluções para posterior notificação;

○ Listar e documentar os riscos relacionados ao incidente;

Ordem dos Advogados do Brasil – Seção de Santa Catarina
Rua Paschoal Apóstolo Pítsica, 4860 – Agronômica – 88025-255 – Florianópolis – SC
Telefones: (48) 3239-3580 – Fax: (48) 3239-3559

- Documentar as medidas de contenção e reversão do incidente. Indicar se houve mitigação (ou não) dos riscos listados;
- Documentação e guarda de evidências, mantendo os registros ocorridos (LOGS, PRINTS etc...), para a correta prestação de contas.

Este conjunto de ações deve ser acompanhado pelo responsável técnico do setor de TI até a completa resolução. Com o conjunto de evidências obtidas, deve o encarregado de dados e a diretoria serem abastecidos de informações. A ação de manter o encarregado de dados abastecido de informações, permitirá que o mesmo proceda a notificação para a ANPD em até dois dias úteis.

8. ANÁLISE

Uma análise tenta descobrir o impacto completo de um incidente dentro de uma organização, isto inclui a informação sobre ameaças e vulnerabilidade que podem ser utilizadas pelo Comitê de Segurança, conjuntamente com o Encarregado de Dados, para planejar a próxima ação, responder o incidente e recuperar-se do mesmo.
Uma análise é utilizada para determinar respostas e questões críticas sobre informações como as seguintes:

1. Qual é o problema?
2. Quem foi afetado?
3. Quão espalhado está o problema?
4. Qual é a seriedade do problema?
5. Quais as correções, soluções e alternativas estratégicas de mitigação que podem ser providas como resposta?

Após essas questões, há questões mais específicas em relação aos dados pessoais, que podem ser analisadas pelo Encarregado juntamente com o Comitê de segurança, definindo a gravidade perante a infraestrutura e negócio da instituição, bem como identificando possíveis impactos para os titulares de dados pessoais.
Análise de risco deverá contar com o apoio do representante da área originária da violação, com o apoio do encarregado de dados, considerando as seguintes questões:

a. Quais dados foram envolvidos na violação?
b. Há também dados sensíveis?
c. Quantos titulares de dados foram atingidos?

Ordem dos Advogados do Brasil – Seção de Santa Catarina
Rua Paschoal Apóstolo Pítsica, 4860 – Agronômica – 88025-255 – Florianópolis – SC
Telefones: (48) 3239-3580 – Fax: (48) 3239-3559

d. Quais são as medidas de segurança aplicáveis à área originária da violação?

e. Foi ou é possível identificar os envolvidos na violação?

f. Em de compartilhamento indevido das informações, o que o terceiro que as acessa poderia obter/extrair delas?

g. A violação afeta algum direito do titular de dados?

Feitas as devidas identificações, dependendo da gravidade da violação, a alta direção e comitê de segurança devem receber as comunicações sobre impacto ao negócio.
A alta direção deve ser notificada pelo encarregado de dados sobre as informações obtidas na fase de triagem e após análise do evento.

7.1. SLA - NÍVEL DE ACORDO DE SERVIÇO

A severidade dos incidentes devem nortear os prazos de atendimento. Para um melhor fluxo de trabalhos, o setor de TI definirá os prazos de respostas para diferentes níveis de severidade dos incidentes.

7.2 Armazenamento de evidências e resultados de análises

As evidências levantadas de um evento ocorrido dentro da instituição deverá ser mantida em segurança, para que possa ser utilizado futuramente como referência.

Inclusive a manutenção dos arquivos que foram objeto da análise, devem ser mantidos em segurança, conforme determina o item 10.6 da ISO 27035.

9. NOTIFICAÇÕES:

9.1. DECISÃO DE NÃO NOTIFICAÇÃO:

Após os estudos realizados, o Encarregado de Dados pode optar em não notificar a Autoridade e o titular de dados, nos casos em que a instituição está isenta do requisito de notificação obrigatória quando o risco para os titulares de dados for extremamente baixo.

A decisão de não notificar deverá ser registrada com fundamentos adequados, na ausência de justificação poderá haver exposição da instituição a riscos jurídicos e reputacionais sérios caso haja questionamento por titulares e autoridades.

Todos os incidentes, violações e as ações tomadas devem ser documentadas, mesmo que não haja a

Ordem dos Advogados do Brasil – Seção de Santa Catarina
Rua Paschoal Apóstolo Pítsica, 4860 – Agronômica – 88025-255 – Florianópolis – SC
Telefones: (48) 3239-3580 – Fax: (48) 3239-3559

necessidade de notificação, tudo devidamente inserido no formulário de incidentes de violação de dados.

9.2 NOTIFICAÇÃO AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANEXO I

Ao longo da detecção da violação de dados e resolução, as notificações devem paralelamente estar sendo preparadas por parte do Encarregado de dados e do Comitê de Privacidade a notificação para comunicação da violação de dados pessoais à Agência Nacional de Proteção de Dados. A ANPD fornece instruções sobre como enviar as notificações no link:

- https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca

A notificação à ANPD deve ocorrer através do uso do link a seguir:

- https://www.gov.br/secretariageral/pt-br/sei-peticionamento-eletronico

O prazo é de 02 dias úteis, sendo necessário monitorar possíveis mudanças provenientes da ANPD (Autoridade Nacional de Proteção de Dados), que podem resultar em prazos diferentes. Não notificar no prazo estipulado pela autoridade e com todas as informações necessárias, poderá gerar penalizações.

8.3 NOTIFICAÇÃO AOS TITULARES DE DADOS

Os titulares deverão ser notificados caso a violação de dados traga riscos ou danos para o titular dos dados. Ao notificar os titulares, deverá a notificação ter a citação dos seguintes itens:

- Quais dados pessoais foram comprometidos;
- Quais prejuízos para os direitos e liberdades das pessoas físicas;
- Qual o impacto na privacidade e proteção dos dados pessoais;
- Medidas tomadas.

10. RESPOSTA

A contenção já realizada, e caso não tenham sido atendidas todas as premissas narradas, deve ser retomada a ação de contenção, para iniciar a resposta ao incidente.

O principal propósito de uma resposta a um incidente é conter, erradicar e recuperar um incidente, os objetivos primários para o processo de respostas são:

Ordem dos Advogados do Brasil – Seção de Santa Catarina
Rua Paschoal Apóstolo Pítsica, 4860 – Agronômica – 88025-255 – Florianópolis – SC
Telefones: (48) 3239-3580 – Fax: (48) 3239-3559

- Parar ou minimizar os efeitos ou danos do ataque, mantendo a continuidade da missão operacional;
- Assegurar a recuperação efetiva e oportuna dos sistemas, de forma a prevenir que incidentes semelhantes ocorram novamente;
- Reforçar a postura defensiva e a prontidão operacional da organização;
- Assegurar que atividades de resposta ocorram de uma maneira que protejam quaisquer dados, de acordo com seu nível de sensibilidade;
- Oferecer apoio a caracterização de ataques rápidas e completa;
- Desenvolver e implementar cursos de ação;
- Remediar ou mitigar a atividade;
- Recuperar os sistemas para o nível operacional normal;
- Melhorar os processos de infraestrutura e de tratamento de incidentes.

Erradicação é a eliminação de componentes do incidente, como código maliciosos, contas e senhas comprometidas, ou outros sistemas e informações comprometidas. O objetivo da erradicação é remover permanentemente os dados armazenados digitalmente em alguma forma de mídia.

Já a recuperação é a restauração de um serviço, dados ou sistema ao seu estado operacional normal. A recuperação pode fazer parte de um planejamento geral de continuidade das atividades para toda a organização.

A ISO 27035 prevê todo o processo de erradicação e recuperação de um incidente de segurança, e por isso a mesma deverá ser consultada pela equipe responsável, sempre que necessário.\

11. RELATÓRIOS

A geração de relatório de incidentes é uma parte importante da avaliação e das decisões de incidentes para coordenar as respostas corretas. É uma parte essencial das operações de incidentes que os canais e formatos de geração de relatórios sejam estabelecidos para obter rápidas respostas a um incidente. Além disso, as organizações analisam incidentes para descobrir questões ou problemas que coloquem seus clientes e outros clientes em risco.

Dependendo do contexto e das características do incidente, pode ser necessário gerar relatório para terceiros. As partes terceiras, podem ser partes interessadas, como clientes, fornecedores, etc.

Principais requisitos e orientações para elaborar um relatório:

Ordem dos Advogados do Brasil – Seção de Santa Catarina
Rua Paschoal Apóstolo Pítsica, 4860 – Agronômica – 88025-255 – Florianópolis – SC
Telefones: (48) 3239-3580 – Fax: (48) 3239-3559

- Fornecer a definição de um incidente para a organização;
- Fornecer uma explicação sobre por que convém que um indivíduo ou grupo tenha um relatório;
- Identificar para quem ou para onde convém que o relatório seja enviado;
- Fornecer uma explicação sobre como relatou o evento;
- Fornecer uma descrição das situações críticas que devem ser incluídas no relatório;
- Fornecer uma explicação de quando relatar.

O armazenamento dos relatórios deve ser organizado e de fácil acesso às pessoas interessadas. Segundo definição da ISO 27035, poderá ser: **armazenamento quente**, que otimiza o acesso regular, com funcionalidade de leitura, gravação rápida e responsiva e outras; **armazenamento frio**, que otimiza para dados acessados com menos frequência e possui um período mínimo de armazenamento de um mês; **arquivo**, é o mais adequado para a retenção de dados a longo prazo.

12. RESOLUÇÃO | EVIDÊNCIAS | BASE DE CONHECIMENTO

A equipe responsável pela resolução do evento, violação ou vazamento de dados, poderá atuar conforme solução descrita em base de erros conhecidos da instituição ou procedimento operacional específico e registrar, em um histórico, as ações realizadas e medidas que foram implementadas.

Ao assegurar que evento foi controlado ou resolvido, o responsável pela resolução deve registrar em uma base de erros conhecidos, como uma base de conhecimentos e manter as soluções mapeadas com o seu devido passo a passo. As atualizações da situação do incidente são recomendáveis, especialmente se envolver danos ao comunicante.

A instituição de maneira geral, deve ter o aprendizado (lições aprendidas) para evitar novas ocorrências de mesma natureza, e utilizando como exemplo a situação ocorrida para evitar futuros incidentes.

13. PÓS EVENTO:

Após o evento e a resposta a equipe de resposta do incidente (Encarregado e Comitê de Privacidade) deve ser reunir para discutir sobre as medidas de segurança e procedimentos que precisam ser implementados para melhorar a segurança dos dados com base nas lições aprendidas.

Deve ser feita uma reflexão sobre a resposta geral à violação e políticas ou protocolos atualizados,

Ordem dos Advogados do Brasil – Seção de Santa Catarina
Rua Paschoal Apóstolo Pítsica, 4860 – Agronômica – 88025-255 – Florianópolis – SC
Telefones: (48) 3239-3580 – Fax: (48) 3239-3559

conforme necessário, para melhorar as relações futuras às violações.

Após uma violação a equipe deve reforçar a comunicação dentro da instituição e investir em treinamentos, tanto para aplicação desta política quanto para mitigar o risco de um novo incidente.

14. DISPOSIÇÕES FINAIS:

A presente política deve ser lida e interpretada sob a égide das leis brasileiras e em conjunto com as normas e procedimentos da instituição.

Esta política será utilizada e seguida pela equipe definida para responder ao incidente de segurança.

Questões relacionadas a esta política podem ser esclarecidas junto ao Encarregado de dados dpo@oab-sc.org.br.

Esta política passa a vigorar na OAB/SC a partir do dia 01/04/2024.

Ordem dos Advogados do Brasil – Seção de Santa Catarina
Rua Paschoal Apóstolo Pítsica, 4860 – Agronômica – 88025-255 – Florianópolis – SC
Telefones: (48) 3239-3580 – Fax: (48) 3239-3559

15. REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Comunicação de incidentes de segurança. 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em: 10 set. 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ISO/IEC 27035-3: GESTÂO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÂO PARTE 3. 1 ed. São Paulo: Abnt, 2021. 47 p.

IAPP_Gestao-do-Programa-de-Privacidade_Segunda-edicao_PT-1.0 - Edição e revisão de texto: Julia Homer - Indexação: Hyde Park Publishing Services - ISBN: 978-1-948771-52-8

Ordem dos Advogados do Brasil – Seção de Santa Catarina
Rua Paschoal Apóstolo Pítsica, 4860 – Agronômica – 88025-255 – Florianópolis – SC
Telefones: (48) 3239-3580 – Fax: (48) 3239-3559