GUIA DE RESPOSTA A INCIDENTE DE SEGURANÇA

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

CNPJ 21.071.712/0001-71

SPEEDIO

INTRODUÇÃO

Este Guia tem por finalidade apresentar orientações com o intuito de auxiliar a realizar a Gestão de Resposta à Incidentes de Segurança da Informação no âmbito da Empresa. A segurança da informação é uma preocupação crítica em um mundo cada vez mais digitalizado, onde as organizações enfrentam ameaças constantes de ataques cibernéticos e violações de dados. A capacidade de detectar, analisar e responder eficazmente a incidentes de segurança é essencial para proteger os ativos da empresa, garantir a continuidade dos negócios e manter a confiança dos clientes e parceiros.

Neste guia, você encontrará diretrizes detalhadas e melhores práticas que visam estabelecer um processo de resposta a incidentes sólido e eficiente. Abordaremos desde a formação da equipe de resposta até a documentação pós-incidente, passando pela classificação de incidentes, detecção, análise, contenção e recuperação.

A segurança da informação é uma responsabilidade de todos, e a adoção de práticas sólidas de resposta a incidentes é um passo fundamental em direção a um ambiente de negócios mais seguro e resiliente.

1. DEFINIÇÕES GERAIS

Agentes de Tratamento: São as partes envolvidas na operação de tratamento de dados pessoais, podendo ser controladores (ou operadores) que definem as finalidades e os meios do tratamento, ou processadores de dados que realizam o tratamento em nome do controlador.

Encarregado: Também conhecido como Data Protection Officer (DPO), é uma pessoa designada pela organização para supervisionar a conformidade com a LGPD e atuar como ponto de contato entre a organização, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Autoridade Nacional de Proteção de Dados (ANPD): É o órgão governamental responsável pela fiscalização e regulamentação da LGPD no Brasil. Sua função inclui orientar, fornecer diretrizes e aplicar penalidades em caso de violações da lei.

Dado Pessoal: Qualquer informação relacionada a uma pessoa física identificada ou identificável. Isso pode incluir informações como nome, endereço, número de telefone, endereço de e-mail, entre outras.

ETIR: Sigla para "Equipe de Tratamento de Incidentes de Resposta", que se refere à equipe responsável por lidar com incidentes de segurança da informação.

IDP: Sigla para "Incidente de Proteção de Dados", que é um evento que compromete a segurança ou a privacidade dos dados pessoais, podendo ser intencional ou acidental.

Incidente: Um evento que desvia do funcionamento normal de um sistema de informação, que pode indicar uma possível violação de segurança ou uma ameaça à confidencialidade, integridade ou disponibilidade dos dados.
Incidente de Segurança: Um evento que compromete a segurança da informação de uma organização, podendo envolver a exposição não autorizada de dados ou sistemas a riscos.

Incidente de Segurança com Dados Pessoais: Um incidente de segurança que envolve a exposição, vazamento ou acesso não autorizado a dados pessoais, conforme definido pela LGPD.

LGPD: Sigla para "Lei Geral de Proteção de Dados", que é a legislação brasileira que regula o tratamento de dados pessoais e estabelece direitos e obrigações relacionados à privacidade e à proteção de dados pessoais.

Relatório Final: Um relatório que contém todas as evidências e ações realizadas para o tratamento do incidente de segurança da informação. Esse relatório é emitido ao final das tratativas do incidente e serve como um documento detalhado que descreve a resposta e as medidas tomadas.

RIPD: Sigla para "Registro de Incidente de Proteção de Dados", que é um registro documentado de um incidente de segurança com dados pessoais, conforme exigido pela LGPD. O RIPD é uma parte importante da documentação de incidentes de segurança e é necessário para fins de conformidade com a lei.

2. INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

A segurança da informação é uma área que se concentra na proteção, armazenamento e transmissão segura de dados. Essa área de conhecimento está intimamente ligada ao comportamento e às ações das pessoas, uma vez que engloba o seu papel fundamental no processo de segurança. Além disso, a segurança da informação visa resguardar tanto os dados quanto às informações e os dispositivos que os abrigam.

Nessa perspectiva, destacam-se cinco pontos cruciais que a Segurança da Informação busca preservar:

a) Integridade do Conteúdo: Isso envolve assegurar que a mensagem enviada pelo emissor seja recebida de forma completa e precisa pelo receptor, sem ter sido alterada durante a transmissão.
b) Irretratabilidade da Comunicação: Isso garante que nem o emissor nem o receptor possam alegar que uma comunicação bem-sucedida nunca ocorreu, tornando cada transação registrada e incontestável.
c) Autenticidade do Emissor e do Receptor: Isso visa garantir que a identidade de quem se apresenta como remetente ou destinatário da informação corresponda à pessoa ou entidade que alega ser, evitando falsificações e fraudes.
d) Confidencialidade do Conteúdo: Este ponto visa garantir que o conteúdo da mensagem só seja acessível aos destinatários autorizados, protegendo-o contra acesso não autorizado ou divulgação indevida.
e) Capacidade de Recuperação do Conteúdo pelo Receptor: Isso assegura que o conteúdo transmitido possa ser recuperado em sua forma original pelo destinatário, mesmo após a transmissão, para garantir que a informação seja utilizável e não tenha sido corrompida

O artigo 46 da Lei Geral de Proteção de Dados (LGPD) estabelece a obrigatoriedade para os agentes de tratamento de adotarem medidas de segurança, que englobam aspectos técnicos e administrativos, com o propósito de resguardar os dados pessoais contra acessos não autorizados, bem como prevenir situações acidentais ou ilícitas que possam resultar em destruição, perda, alteração, comunicação indevida ou qualquer outra forma de tratamento inadequado ou ilegal.

Essas medidas de segurança devem ser aplicadas ao longo de todo o ciclo de vida do produto ou serviço, desde a sua concepção até a sua execução. Essa abordagem

abrangente visa garantir a integridade e a privacidade dos dados pessoais em conformidade com as disposições da LGPD.

O artigo 50 da Lei Geral de Proteção de Dados (LGPD) estabelece que os controladores e operadores, dentro das suas respectivas competências, têm a prerrogativa de desenvolver diretrizes de boas práticas de governança para a manipulação de dados pessoais. Além disso, o parágrafo 2, inciso I, do mesmo artigo, prevê a obrigatoriedade de implementar um programa de governança em privacidade que inclua planos para responder a incidentes e procedimentos de remediação.

Em situações de incidentes que possam comprometer a segurança dos dados pessoais, é fundamental seguir procedimentos específicos. Estes procedimentos incluem:

a) **Realizar uma avaliação interna do incidente**, buscando obter informações iniciais, tais como o impacto do evento, a natureza, categoria e quantidade de titulares de dados pessoais afetados, a categoria e quantidade de dados afetados, as consequências do incidente para os titulares e para a entidade, bem como a sua criticidade e probabilidade. Além disso, é imperativo preservar todas as evidências relacionadas ao incidente.

b) **Comunicar imediatamente ao encarregado de dados** da entidade sobre a ocorrência do incidente, especialmente se ele envolver dados pessoais.

c) **Notificar o controlador,** conforme estabelecido pela LGPD, sobre a existência do incidente, sobretudo se ele envolver dados pessoais.

d) **Informar à Autoridade Nacional de Proteção de Dados** (ANPD) e ao titular dos dados pessoais sobre a existência do incidente, conforme previsto no artigo 48 da LGPD.

e) **Comunicar à Equipe Técnica de Incidentes em Redes de Informação** (ETIR) do órgão em caso de incidentes na rede computacional.

g) **Elaborar um relatório final** que engloba todas as informações coletadas, as ações tomadas para tratar eficazmente o incidente e quaisquer considerações relevantes para promover melhorias no processo de segurança de dados.

O prazo considerado razoável para a comunicação de um incidente seja de até 2 (dois) dias úteis. A equipe da Speedio deve agir com cautela ao avaliar a importância dos riscos e danos associados ao incidente. Em situações de dúvida, é aconselhável que a comunicação do incidente seja feita o mais rapidamente possível, a fim de evitar eventuais violações da LGPD.

2.1 Realizar uma Avaliação Interna do Incidente

Ao identificar um incidente de segurança, é fundamental conduzir uma avaliação interna abrangente para compreender a sua natureza e impacto. Siga os seguintes passos:

a) Identificar a Vulnerabilidade Explorada

- Determine qual vulnerabilidade foi explorada no incidente. Isso pode incluir:
    - Acesso indevido aos dados pessoais.
    - Roubo de dados.
    - Ataques cibernéticos, como invasões de sistemas.
    - Erros de programação em aplicativos e sistemas internos.
    - Técnicas de engenharia social.
    - Descarte inadequado de informações.
    - Repasse não autorizado de dados pessoais.
    - Roubo, venda ou uso indevido de dados sob responsabilidade da entidade.
    - Comprometimento de senhas de acesso.
    - Outros métodos de exploração de vulnerabilidades.

b) Identificar a Fonte dos Dados Pessoais

- Determine como os dados pessoais foram obtidos, identificando a fonte. Isso pode envolver:
    - Preenchimento de formulários eletrônicos ou não eletrônicos pelos titulares.
    - Uso de APIs (Interface de Programação de Aplicativos).
    - Compartilhamento de dados com terceiros.
    - Uso de XML e cookies.

c) Classificar a Categoria dos Dados Pessoais

- Categorize os dados pessoais afetados em:
    - Dados sensíveis.
    - Dados pessoais de crianças e adolescentes.

d) Mensurar a Extensão do Vazamento

- Quantifique o impacto do incidente determinando:

- O número de titulares de dados pessoais afetados.
- A quantidade de dados pessoais comprometidos.

e) Avaliar o Impacto para os Titulares

- Analise os potenciais impactos que o incidente pode causar aos titulares de dados, levando em consideração fatores como:
  - Potencial para roubo de identidade.
  - Exposição de informações sensíveis.
  - Riscos à privacidade.
  - Consequências financeiras.
  - Repercussões legais.

f) Avaliar o Impacto no Serviço

- Considere os impactos que o incidente pode ter na entidade, incluindo:
  - Perda de confiabilidade por parte dos cidadãos.
  - Possibilidade de ações judiciais.
  - Danos à imagem da instituição em âmbito nacional e internacional.
  - Prejuízos à entidade em contratos com fornecedores e clientes.
  - Impacto total ou parcial nas atividades desenvolvidas pela entidade.

Deve-se garantir a preservação de todas as evidências relacionadas ao incidente, bem como documentar minuciosamente todas as medidas tomadas desde o momento da sua identificação. Isso é essencial para que, caso seja necessário, seja possível demonstrar de maneira clara e precisa todas as ações empreendidas para compreender o incidente e mitigar seus efeitos. Essa documentação permitirá uma compreensão completa da sequência de ações realizadas para lidar com a situação.

Nesse contexto, é imperativo que todos os passos sejam devidamente registrados, desde o início da atuação até a contenção dos efeitos. Isso inclui, mas não se limita a:

a) Manter registros de todos os logs dos sistemas internos e externos envolvidos no incidente, para uma análise detalhada das atividades relacionadas ao evento.

b) Registrar todas as interações do time envolvido no tratamento do incidente, documentando todas as medidas adotadas, decisões tomadas e comunicações realizadas.

c) Documentar quaisquer contratações de ferramentas ou equipes de especialistas e auditores que tenham sido envolvidos de forma pontual no

tratamento do incidente, incluindo os detalhes das contratações e as ações executadas por essas partes.

d) Registrar atas de todas as reuniões relevantes realizadas ao longo do processo de resposta ao incidente, descrevendo os tópicos discutidos, as decisões tomadas e os responsáveis por cada ação.

À medida que o tratamento do incidente progride, é importante manter as informações da avaliação preliminar atualizadas, pois novos dados e descobertas podem surgir. Essa documentação detalhada não apenas auxilia na gestão eficaz do incidente, mas também fornece um histórico completo e confiável que pode ser útil para autoridades ou partes interessadas que venham a investigar o ocorrido no futuro.

Diante de todas as evidências, é importante que a entidade avalie a necessidade de elaborar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), conforme previsto na LGPD. A elaboração do RIPD pode ser solicitada em casos específicos, como tratamento de dados pessoais para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (exceções previstas pelo inciso art. 4o, inciso III da LGPD), em situações de infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 da LGPD, combinados), ou a qualquer momento, sob determinação da ANPD (art. 38).

2.2 Comunicar ao encarregado da entidade

Para a devida comunicação ao encarregado da entidade, é essencial seguir um procedimento adequado. O encarregado da proteção de dados, também conhecido como DPO (Data Protection Officer), desempenha um papel fundamental na supervisão e garantia do cumprimento das normas de proteção de dados pessoais. Portanto, ao identificar um incidente de segurança que envolva dados pessoais, é imperativo notificar prontamente o encarregado da entidade, fornecendo informações detalhadas sobre a natureza e o escopo do incidente.

Adicionalmente, o controlador deve disponibilizar um canal de comunicação apropriado no site da empresa e promover a divulgação interna do contato do encarregado, garantindo que os colaboradores tenham fácil acesso para relatar incidentes de segurança de dados pessoais. Isso permitirá uma resposta ágil e adequada em conformidade com as regulamentações da LGPD.

Para facilitar essa comunicação, considere que qualquer pessoa ou parte que tome conhecimento de um possível incidente deve informar imediatamente o encarregado do controlador. As informações para contato estão disponíveis no site da empresa e também podem ser acessadas por meio do **e-mail dpo@speedio.com.br.**

2.3 Comunicar ao controlador

O Operador deve comunicar incidentes com dados pessoais ao Controlador o mais rápido possível, a fim de viabilizar que o Controlador exerça seu papel tempestivamente. O controlador é responsável em comunicar incidentes com dados pessoais à ANPD e aos titulares de dados. No caso da Speedio atuar como operadora, a empresa deverá informar o controlador dentro dos termos do contrato ou relação firmada entre as partes, garantindo a conformidade com as obrigações estabelecidas.

2.4 Comunicar à ANPD e ao titular de dados pessoais

A ANPD estipula o prazo de 2 (dois) dias úteis para comunicação de incidente de segurança à proteção de dados. O art. 48 da LGPD determina que o controlador tem o dever de comunicar à ANPD e ao titular dos dados pessoais a ocorrência de incidente de segurança que tenha potencial de risco ou dano relevante ao titular. Nem sempre é necessário comunicar, depende do grau do incidente e das diretrizes estabelecidas.

Dessa forma, para avaliar o grau de risco, a organização em conjunto com o encarregado deve considerar e responder às seguintes questões:

a) Quais informações foram afetadas pelo incidente?

b) O titular pode estar em risco de fraude devido ao incidente?

c) O incidente foi comunicado adequadamente às autoridades?

d) Como o titular pode proteger seus dados?

e) Onde o titular pode obter informações adicionais sobre o incidente?

Essas perguntas servem como um ponto de partida e devem ser adaptadas às circunstâncias específicas do incidente para uma avaliação precisa.

Cabe ao Encarregado, diante das informações levantadas internamente e dos parâmetros estabelecidos pelo órgão, pela ANPD ou com base em boas práticas, avaliar a necessidade e a profundidade da comunicação com a ANPD e com os titulares de dados.

Para mais informações pode ser acessado no site da ANPD ou através do seguinte link:

https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis

2.5 Notificar os titulares de dados pessoais

De acordo com as normativas da LGPD, em caso de ocorrência de um incidente de segurança que possa gerar riscos ou danos relevantes, o controlador está obrigado a comunicar o titular dos dados. No entanto, quando o incidente não representa riscos ou danos relevantes, a notificação ao titular pode não ser necessária. Portanto, a relevância do risco determina a obrigação de comunicação ao titular.

A comunicação aos titulares de dados deve ser feita de forma clara e simples, utilizando uma linguagem acessível. Essa comunicação deve incluir, quando aplicável, os elementos previstos no §1º do Art. 48 da LGPD, que são:

- Descrição geral do incidente e data da ocorrência: Deve-se informar o que aconteceu de maneira geral e quando o incidente ocorreu.
- Natureza dos dados pessoais afetados e riscos relacionados ao incidente: É importante especificar que tipos de dados pessoais foram afetados e quais são os riscos potenciais associados ao incidente.
- Medidas tomadas e recomendadas para mitigar os efeitos do incidente: Descreva as ações que foram tomadas para lidar com o incidente e quais medidas os titulares podem adotar para reduzir os impactos.
- Contato do encarregado ou ponto de contato: Forneça as informações de contato do encarregado de proteção de dados ou outro ponto de contato para que os titulares possam obter mais informações sobre o incidente.

- Outras informações auxiliares: Inclua qualquer informação adicional que possa ajudar os titulares a prevenir possíveis danos ou entender melhor a situação.

A transparência e a clareza na comunicação são essenciais para que os titulares possam tomar medidas apropriadas para proteger seus dados pessoais e seus interesses.A comunicação deve ser feita de forma individual e diretamente aos titulares, sempre que possível.Se, pela natureza do incidente, não for possível identificar individualmente os titulares afetados, devem ser comunicados todos os presentes na base de dados comprometida.

3. RESPOSTA A INCIDENTES CIBERNÉTICOS

Refere-se aos processos e tecnologias de uma organização para detectar e responder a ameaças cibernéticas, violações de segurança ou ataques cibernéticos.

Descreve a forma como a Speedio vai responder às situações de emergência e exceção. Pela potencial gravidade, a resposta da Companhia deve ser rápida e confiável, ao mesmo tempo resguardando evidências forenses que podem 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:

- **Preparação:** a entidade deve criar e treinar equipes para atuar na resposta a incidentes, além de limitar o número de incidentes, selecionando e implementando controles com base em avaliações de risco.
- **Detecção e análise de incidentes:** a entidade deve adotar meios para detecção de incidentes e analisar tais eventos, buscando documentar, priorizar e notificar; esta fase também pode ser executada em conjunto com a fase posterior.
- **Contenção, erradicação e recuperação**: Fase em que são implementadas ações para contenção, erradicação e recuperação do incidente; aqui, também são identificadas as origens de ataques e coletadas as evidências. Após a detecção e a análise do incidente, devem ser realizadas ações buscando a remediação ou a restauração dos recursos atacados e, quando possível, a recuperação de tais recursos ao estado anterior ao ataque. Para isso, devem ser seguidos os procedimentos já estabelecidos internamente para resposta a incidentes.
- **Atividades pós-incidente:** a entidade deve realizar atividades para melhorar o tratamento de novos incidentes.

3.1 Início

Notificação: Um novo incidente é notificado, por pessoa externa ou não a Companhia ou por alarme da monitoração, usando um dos mecanismos de comunicação definidos. Notificação é recebida por Acionador do "CSIRT". Triagem

Acionar do "CSIRT" (Computer Security Incident Response Team): O "CSIRT" 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.

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

Análise da avaliação preliminar: Conforme a avaliação preliminar, incidentes que não envolvem sistemas online e que seguramente não apresentam riscos aumentados pela falta de ação imediata podem ser encaminhados para trâmites regulares da Companhia pela Equipe de Segurança da Informação e Encarregado pelo Tratamento de Dados Pessoais, caso o incidente envolve dados pessoais.

Consequências: Em caso de incidentes que exigem resposta imediata ou melhor avaliação, o "CSIRT" deve ser acionado e passamos às fases seguintes.

Avaliação: 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 "CSIRT" a qualquer momento que julgar adequado e viável.

Contenção e Erradicação: Devem ser acionados os responsáveis pelos sistemas impactados, conforme indicado na documentação, que irão orientar e se manifestar sobre os procedimentos de contenção e erradicação.

É necessário identificar a origem de ataques durante o tratamento de incidentes. Não obstante, embora isso seja importante, a equipe de resposta a incidentes deve manter o
enfoque na contenção, na erradicação e na recuperação.

A seguir, são enumeradas algumas das atividades mais comuns para identificar a origem de um ataque:

a) Validação do endereço IP: utilizar técnicas para identificar e validar o endereço de IP do host de ataque.

b) Pesquisa de endereço de IP: realizar uma pesquisa do IP do atacante em motores de busca pode levar a mais informações sobre o ataque.

c) Banco de dados de incidentes: alguns grupos realizam a coleta e consolidação de eventos que ocorreram em diferentes organizações, gerando um banco de dados de incidentes. A organização também pode consultar sua base particular de incidentes para identificar semelhanças com eventos antigos.
d) Monitorar canais de comunicação: a equipe de resposta a incidentes pode monitorar canais de comunicação que são utilizados com frequência em ataques.

Depois da contenção, a erradicação pode ser necessária para eliminar resquícios do incidente, como exclusão de malware, exclusão de contas violadas, e identificação e tratamento das vulnerabilidades exploradas.

Na erradicação, é importante identificar todos os recursos da organização que possam ser corrigidos. Podem ocorrer incidentes em que a erradicação é executada como uma etapa separada, mas continua fazendo parte do processo de recuperação.

Durante a recuperação, os sistemas são restaurados para seu estado normal, e os administradores dos sistemas devem confirmar se tais sistemas estão operando de maneira adequada. A recuperação pode envolver ações como alteração de senhas de rede, reconfiguração de regras de firewall, restauração de backup, reconstrução de sistemas e de toda base de dados, instalação de patches de segurança, substituição de arquivos corrompidos por versões limpas. Evidências coletadas no início da tratativa do incidente podem ser utilizadas para determinar qual o estado em que os recursos devem ser entregues à operação após a recuperação.

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 especificas, colocação de avisos de indisponibilidade para manutenção, sempre que possível tomando cuidados para não impactar evidências que poderiam ser usadas para identificar autoria, origem e método usado para quebrar a segurança.

Máquinas virtuais: Em caso de incidente envolvendo máquinas virtuais, deve ser feito snapshot das mesmas para posterior análise.

3.2 Recuperação

Acionar o Plano de Continuidade de Negócio dos sistemas impactados: Eles devem ser iniciados, conforme especificado no plano.

Recuperação: 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. Para a recuperação devem ser tomadas medidas identificadas na Avaliação, tais como restauração de backups, clonagem de máquinas virtuais e instalação de sistemas. Pode ser necessário o desenvolvimento e instalação de atualizações de aplicação ou do Sistema Operacional, por isso esta fase pode ser prolongada, de acordo com a priorização dada.

Responsabilidade do "CSIRT": O "CSIRT" tem a responsabilidade de passar as informações que obteve para o desenvolvimento da solução e sua instalação.

3.3 Lições Aprendidas

Com o incidente contido e sua resolução encaminhada, o "CSIRT" 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. 16) As melhorias sugeridas na reunião, com o devido consenso, devem ser encaminhadas aos responsáveis para definição sobre a adoção.

Após a ocorrência de um incidente, por exemplo, a organização deve mapear as vulnerabilidades exploradas e aplicar as devidas correções em todos os seus sistemas, elevando o nível de segurança.

Reuniões periódicas ou até mesmo após a ocorrência de um incidente são importantes para revisar como o evento ocorreu, o que foi feito durante as tratativas e se as ações surtiram efeito positivo.

Os relatórios dessas reuniões podem ser utilizados para atualizar os procedimentos operacionais já existentes, além de servirem como artefatos iniciais para a elaboração de novos procedimentos operacionais. Podem também ser disponibilizados de forma segura para consulta posterior em casos de incidentes semelhantes.

3.4 Documentação

O "CSIRT" 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.

É aconselhável manter um registro detalhado de todas as evidências, o que abrange inclusive informações sobre:
a) Identificação (endereços IP e MAC, porta de rede, número de série, sistema operacional, nome do host, localização);
b) Nome, matrícula, equipe e organização do indivíduo que realizou qualquer manuseio da evidência;
c) Hora e data de cada ocorrência de manipulação da evidência;
d) Locais onde as evidências foram armazenadas e podem ser acessadas.

3.5 Comunicações

Assim que possível, no caso de incidente com vazamento de dados pessoais, o Encarregado de Tratamento de Dados (DPO) 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 ANDP.

3.6 Priorização

A priorização do tratamento de incidentes é importante para a correta alocação de recursos em áreas e sistemas que sejam chave para o contexto da APF. As seguintes informações devem ser utilizadas para a definição da ordem de prioridade no tratamento dos incidentes:

a) Impacto no negócio: a equipe de resposta a incidentes deve considerar como o incidente em tratamento pode impactar negativamente o negócio da organização, devendo realizar uma avaliação que leve em consideração os impactos futuros que o incidente pode trazer à organização. A seguir, compartilha-se uma tabela com os possíveis níveis de impacto no negócio:

Categoria	Definição
Nenhum	Não afeta a capacidade da organização de fornecer todos os serviços a todos os usuários.

Baixo	Efeito mínimo; a organização ainda pode fornecer todos os serviços essenciais para todos os usuários, mas perdeu eficiência.
Médio	A organização perdeu a capacidade de fornecer um serviço crítico a um subconjunto de usuários do sistema.
Alto	A organização não é mais capaz de fornecer alguns serviços essenciais a nenhum usuário.

b) Impacto em dados e informações: incidentes podem afetar a confidencialidade, a integridade e a disponibilidade dos dados e informações de uma organização. A equipe de resposta a incidentes deve, diante das opções para tratamento, mensurar os impactos que tais alternativas possam gerar tanto para a própria organização como para outros entes parceiros. A seguir, compartilha-se uma tabela com os possíveis níveis de impacto em dados e informações:

Categoria	**Definição**
Nenhum	Nenhuma informação relevante foi exposta, alterada, excluída ou de alguma maneira comprometida.
Violação de privacidade	Informações confidenciais de identificação pessoal (DP) de contribuintes, funcionários, beneficiários etc. foram acessadas ou expostas.
Violação Proprietária	Informações proprietárias não classificadas, como informações de infraestrutura crítica protegida (PCII), foram acessadas ou expostas.
Perda de Integridade	Informações confidenciais ou proprietárias foram alteradas ou excluídas.

c) Recuperabilidade: os impactos de um incidente determinam os recursos e o tempo necessários para a recuperação. A equipe responsável tem o papel de identificar e avaliar os recursos disponíveis, bem como a relevância da recuperação do incidente para a organização. Compartilha-se a seguir uma tabela com níveis de recuperabilidade.

Categoria	Definição
Regular	O tempo de recuperação é previsível com os recursos existentes.
Suplementado	O tempo de recuperação é previsível com recursos adicionais.
Estendido	O tempo de recuperação é imprevisível; recursos adicionais e ajuda externa são necessários.
Não Recuperável	A recuperação do incidente não é possível (por exemplo, dados confidenciais expostos e postados publicamente); lançar investigação.

A capacidade de recuperação de um incidente determina os possíveis procedimentos que a equipe de resposta a incidentes deve seguir para o tratamento. Um incidente de alto impacto aos negócios da organização e de fácil recuperação pode ser aquele em que a equipe de resposta a incidentes atue primeiro, tratando e solucionando o incidente. No entanto, pode haver casos de vazamento de dados pessoais em que seria necessário envolver não só pessoas e equipes internas da organização, mas titulares de dados e órgão de fiscalização (ANPD). Dessa forma, a comunicação e a recuperação podem ser realizadas de forma simultânea.

A equipe de resposta a incidentes deve priorizar a resposta a cada incidente de acordo com as estimativas de impacto e os recursos e esforços necessários para a sua recuperação.

Data	Versão	Descrição	Autor
23/11/2023	1.1	Primeiro Guia de Resposta a Incidentes de Segurança	Natanael Freitas (CTO), Raimundo Pessoa e Sara Marina P. Brizolla.