Ministério do Meio Ambiente e Mudança do Clima
Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis
Ouvidoria

PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

2024

Ministério do Meio Ambiente e Mudança do Clima
Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis
Ouvidoria

PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

ELABORAÇÃO E REVISÃO
Ouvidoria
Equipe para Proteção de Dados
gov.br/ibama
lgpd@ibama.gov.br

SUMÁRIO

INTRODUÇÃO

Incidente de segurança com dados pessoais é um evento adverso envolvendo dados de titulares. Ele acontece quando algum tipo de uso não autorizado, destruição, perda, exposição, alteração, vazamento ou ataque compromete a confidencialidade, a integridade ou a disponibilidade de dados pessoais.

Incidentes podem decorrer de ações voluntárias ou acidentais que resultem em divulgação, alteração, perda ou acesso não autorizado a dados armazenados em sistemas de informação ou em banco de dados, publicação não intencional de dados dos titulares ou até mesmo no envio de informações para o destinatário incorreto.

Mas também podem ocorrer por meio de atos intencionais, como a invasão de um sistema de informação, o sequestro de dados (ransomware) ou o furto de um dispositivo de armazenamento de dados.

A mera existência de uma vulnerabilidade em um sistema de informação não constitui um incidente de segurança. A exploração da referida vulnerabilidade, no entanto, pode resultar em um incidente.

Um incidente de roubo de um dispositivo eletrônico, por exemplo, pode ou não ser capaz de causar um risco relevante aos titulares de dados. A avaliação vai depender do tipo de dado armazenado, do contexto da atividade de tratamento e do fato de os dados estarem ou não protegidos por criptografia.

São considerados incidentes capazes de causar risco ou dano relevante aqueles que possam causar aos titulares danos materiais ou morais, expô-los a situações de discriminação ou de roubo de identidade, especialmente se envolverem dados em larga escala, sensíveis e de grupos vulneráveis como crianças e adolescentes ou idosos.

Merecem destaque os seguintes exemplos de incidentes de segurança da informação:

- acesso de terceiro não autorizado na rede de computadores, que ocorre quando algum agente externo, ou mesmo um servidor ou terceirizado, acessa uma parte do sistema que não deveria;

- vírus e códigos maliciosos, cuja detecção requer o uso de ferramentas próprias, como antivírus;

- uso impróprio de sistemas ou de informações, que ocorrem quando um servidor ou terceirizado usa um e-mail corporativo para a promoção de negócios pessoais, ou quando instala uma ferramenta não autorizada no computador do Órgão ou utiliza um pen drive de forma não autorizada ou, ainda, quando imprime documentos sigilosos de forma não autorizada e os repassa para terceiros.

Considerando o volume de dados tratados pelo Ibama e a relevância de seu papel institucional na entrega de serviços públicos, é importante que o Órgão esteja consciente de que incidentes de segurança revestem-se de uma realidade possível, os quais devem ser evitados com medidas de salvaguarda e prevenção.

Por essa razão, é necessário que o Ibama esteja preparado para agir em caso de “violação da segurança que provoque, de modo acidental ou ilícito a destruição, a perda, a alteração, a divulgação ou o acesso não autorizados a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento” (definição constante no art. 4º do GDPR - General Data Protection Regulation - Regulamento Geral de Proteção de Dados).

Em atenção à Lei nº 13.709/2018, Lei Geral de Proteção de Dados - LGPD, que regula as atividades de tratamento de dados pessoais:

> *Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.*
> *§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:*
> *I - a descrição da natureza dos dados pessoais afetados;*
> *II - as informações sobre os titulares envolvidos;*
> *III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;*
> *IV - os riscos relacionados ao incidente;*
> *V - os motivos da demora, no caso de a comunicação não ter sido imediata; e*
> *VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.*
> *§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:*
> *I - ampla divulgação do fato em meios de comunicação; e*
> *II - medidas para reverter ou mitigar os efeitos do incidente.*
> *§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.*

Neste sentido, o presente Plano dispõe sobre as medidas que devem ser adotadas no caso de uma situação de emergência ou evento de risco que possam ocasionar danos aos ativos tecnológicos do Órgão, viabilizando, inclusive, a comunicação apropriada e tempestiva à Autoridade Nacional de Proteção de Dados - ANPD, quando for o caso.

OBJETIVOS

GERAL

Promover uma estratégia de comunicação para prevenção e ação efetiva nas respostas às situações emergenciais e imprevistas, de forma documentada, formalizada, rápida e confiável, resguardando as evidências que possam ajudar a prevenir novos incidentes e a atender às exigências legais de comunicação e transparência.

A fim de preservar a reputação das atividades prestadas pelo Ibama, evitar custos indesejados, minimizar a ocorrência de problemas legais e preservar a confiança dos usuários externos e internos.

ESPECÍFICOS

- Conferir clareza sobre o fluxo de procedimentos adequados e os responsáveis, no caso de incidentes.
- Assegurar respostas rápidas, efetivas e coordenadas.
- Evoluir continuamente com as lições aprendidas.

TERMOS E DEFINIÇÕES

Agentes de tratamento: corresponde ao Controlador e ao Operador em conjunto, não são considerados controladores ou operadores os indivíduos subordinados, tais como os funcionários, os servidores públicos ou as equipes de trabalho de uma organização, já que atuam sob o poder diretivo do agente de tratamento;

Anonimização: é a utilização de meios técnicos razoáveis e disponíveis por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

Ataque: evento de exploração de vulnerabilidades, ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível;

Autoridade Nacional de Proteção de Dados (ANPD): é o órgão da administração pública nacional responsável por fiscalizar e zelar pelo cumprimento da Lei Geral de Proteção de Dados em todo o território brasileiro;

Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico

Bot: código malicioso que permite ao invasor controlar remotamente o computador ou o dispositivo que hospeda;

Consentimento: a LGPD definiu algumas hipóteses para tratamento dos dados pessoais, sendo uma delas o consentimento. Entretanto, para a coleta desse consentimento, foram impostos alguns requisitos, devendo, a manifestação do consentimento, ser livre, informada e inequívoca;

Controlador: é toda pessoa física ou jurídica, de direito público ou privado, a quem competem decisões referentes ao tratamento de dados pessoais;

Dado anonimizado: é o dado pessoal que, apesar de estar relacionado a uma pessoa natural, passou por um processo de anonimização e não pode mais ser identificado;

Dados pessoais: qualquer informação relacionada a um indivíduo que possa ser usada para identificá-lo, direta ou indiretamente, por conta própria ou quando combinada com outras informações;

Dados que identificam uma pessoa natural: são as informações que identificam uma pessoa por si só (nome completo, caso não exista homônimo; número do CPF, do RG, do passaporte, entre outros);

Dados que possam identificar pessoa natural: são as informações que, somadas, passam a identificar alguém (primeiro nome, endereço, características físicas, entre outros);

Dados pessoais sensíveis: são dados pessoais que digam respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Data center: é um ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados e sistemas de ativos de rede;

Documento físico e documento digital: os documentos físicos são aqueles elaborados em suportes físicos, por exemplo, em papel. Já os documentos digitais são informações registradas, codificadas em forma analógica ou em dígitos binários, acessíveis e interpretáveis por meio de um equipamento eletrônico;

Encarregado pelo Tratamento de Dados Pessoais ou Data Privacy Officer (DPO): pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

Engenharia social: técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados;

Expurgo de dados: significa destruição segura e definitiva de informações, ou seja, quando os dados não existem mais ou não podem mais ser acessados pelo Controlador de qualquer forma;

GMT (Greenwich Mean Time): Horário Médio de Greenwich, baseado no primeiro meridiano de Greenwich, que passa pelo Observatório Real, perto de Londres;

Incidente: evento, ação ou omissão que tenha permitido ou possa vir a permitir acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou, ainda, apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

Incidente de segurança com dados pessoais: de acordo com a ANPD, incidente de segurança à proteção de dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação de dados pessoais, sendo acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento ou qualquer forma de tratamento de dados ilícita ou inadequada, que tem a capacidade de pôr em risco os direitos e as liberdades dos titulares de dados pessoais;

IP: Protocolo da Internet (Internet Protocol), número utilizado para identificar um dispositivo de tecnologia da informação em uma rede, ou Internet;

LGPD: Lei Geral de Proteção de Dados – Lei n. 13.709/2018 que possui, como objetivo, regulamentar as atividades que se utilizam de dados pessoais em território nacional, por pessoa natural ou jurídica de direito público ou privado, em ambientes físicos ou digitais. Dessa forma, a LGPD poderá compreender uma relação com estrangeiro, caso parte do processo seja realizado no Brasil. Importante mencionar que a LGPD foi elaborada para proteção de dados que identifiquem uma pessoa natural, e não informações sigilosas de empresas ou negócios**.**

Log: processo de registro de eventos relevantes num sistema computacional;

Malware: é um termo genérico para qualquer tipo de “malicious software” (“software malicioso”) projetado para se infiltrar em dispositivos eletrônicos sem o devido conhecimento do usuário. Existem muitos tipos de malware, e cada um funciona de maneira diferente na busca de seus objetivos;

Manifestação inequívoca: não pode haver dúvidas sobre a manifestação do consentimento do titular, ou seja, deve existir a certeza de que o titular consentiu com o tratamento dos seus dados pessoais;

Manifestação informada: antes de dar o consentimento, o titular deverá ter acesso prévio, completo e detalhado sobre o tratamento de seus dados pessoais, incluindo sua natureza, objetivos, métodos, duração, justificativa, finalidades, risco, responsabilidades dos agentes de tratamento e benefícios antes de proferir o Consentimento;

Manifestação livre: a manifestação do consentimento deve partir do titular sem que haja qualquer tipo de pressão ou direcionamento;

Operador: é toda pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador;

Pessoa natural: todos os seres humanos, independentemente de sexo, etnia, idade, orientação sexual, religião, nacionalidade, filiação partidária ou quaisquer outras características, possuindo direitos e obrigações;

Phishing: é uma técnica de engenharia social usada para enganar usuários de internet usando fraude eletrônica para obter informações confidenciais, como nome de usuário, senha e detalhes do cartão de crédito.

Pseudonimização: é a substituição de informação encontrável por identificadores artificiais, cifragem, codificação de mensagens e outros, sendo que o controlador mantém a informação em local separado;

Porta: uma porta de conexão está sempre associada a um endereço IP de um host e ao tipo de protocolo de transporte utilizado para a comunicação. Exemplo: o servidor de e-mail que executa um serviço de SMTP usa a porta 25 do protocolo TCP;

Privacy by default (privacidade por padrão): significa assegurar que são colocados em prática, dentro de uma organização, mecanismos para garantir que, por padrão, apenas será recolhida/coletada, utilizada e conservada, para cada atividade, a quantidade necessária de dados pessoais;

Privacy by design (privacidade desde a concepção): significa levar o risco de privacidade em conta em todo o processo de concepção de um novo produto ou serviço.

Relatório de impacto à proteção de dados pessoais (RIPD): quando o tratamento de dados puder gerar riscos à liberdade civil e aos direitos fundamentais do titular, o controlador deverá elaborar uma documentação contendo a descrição dos processos de tratamento de dados pessoais;

Ransomware: é um tipo de malware de sequestro de dados, feito por meio de criptografia, que usa como refém arquivos pessoais da própria vítima e cobra resgate para restabelecer o acesso a estes arquivos. O resgate é cobrado em criptomoedas, que, na prática, o torna quase impossível de se rastrear o criminoso.

Scripts: conjunto de instruções para que uma função seja executada em determinado aplicativo;

Sistemas: hardware, software, network de dados, armazenador de mídias e demais sistemas usados, adquiridos, desenvolvidos, acessados, controlados, cedidos ou operados pelo Ibama para dar suporte na execução de suas atividades;

Sniffing: corresponde ao roubo ou interceptação de dados capturando o tráfego de rede usando um sniffer (aplicativo destinado a capturar pacotes de rede);

Spam: termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas;

Spyware: programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros;

Titular de dados pessoais: a pessoa natural a quem pertence o dado pessoal;

Transferência internacional: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

Tratamento: qualquer operação ou conjunto de operações efetuadas sobre os dados, por meios automatizados ou não, incluindo, mas não se limitando, a coleta, gravação, organização, estruturação, alteração, uso, acesso, divulgação, cópia, transferência, armazenamento, exclusão, combinação, restrição, adaptação, recuperação, consulta, destruição ou anonimização;

Trojan (Cavalo de Troia): programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário;

Vazamento de dados: qualquer quebra de sigilo ou vazamento de dados que possa resultar, criminosamente ou não, na perda, alteração, compartilhamento, acesso, transmissão, armazenamento ou processamento de dados não autorizado;

Violação de privacidade: qualquer violação à legislação aplicável ou conduta e evento que resulte na destruição acidental ou ilícita dos dados, bem como sua perda, roubo, alteração, divulgação ou acesso não autorizado, danos ou desvio de finalidade em seu tratamento;

Vírus: programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos;

Worm: programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

ATORES E RESPONSABILIDADES

Comitê de Governança Digital (CGD): comitê de caráter estratégico e deliberativo, com a finalidade de aperfeiçoar os serviços relacionados à Tecnologia da Informação e Comunicação (TIC) desenvolvidos no Ibama, fortalecendo a utilização integrada de tecnologias da informação e comunicação para aprimorar o acesso à informação, transparência e a prestação de serviços ao público, deliberando sobre políticas, diretrizes e planos relativos à TIC e à Governança Digital.

Encarregado pelo Tratamento de Dados Pessoais ou Data Privacy Officer (DPO): pessoa indicada pelo controlador atuar como canal de comunicação entre a instituição, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). No Ibama essa função é assumida pelos titulares da Ouvidoria.

Equipe para Proteção de Dados (EIAPD): equipe responsável por implementar e acompanhar a adequação de serviços e processos internos à LGPD no Ibama, conforme Portaria nº 1.265/2021 - SEI nº 10043956.

Gestor de Segurança da Informação: pessoa designada pela alta administração como responsável pelas ações de segurança da informação no âmbito do órgão. No Ibama os indicados para essa função podem ser consultados por meio do processo SEI nº 02001.016022/2020-69.

Equipe de Tratamento de Incidentes em Redes Computacionais (ETIR): equipe responsável por receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança na rede computacional do Ibama, conforme Norma Complementar nº 10 da POSIC - SEI nº 11461146.

INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

1. O que é um incidente de segurança e um vazamento de dados pessoais?

Considerando as definições da LGPD, um incidente de segurança é um acontecimento indesejado ou inesperado, hábil a comprometer a segurança dos dados pessoais, de modo a expô-los a acessos não autorizados e a situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Vazamento de dados é um tipo de incidente de segurança que se refere especificamente à situação em que informações privadas e sigilosas são expostas publicamente ou a terceiros sem autorização.

Dessa forma, as informações podem ser acessadas, visualizadas, copiadas, vendidas, compradas e usadas para golpes financeiros, extorsões e tentativas de prejudicar as atividades e a imagem do Órgão, colocando pessoas e organização em risco.

2. Onde, quando e de que forma podem ocorrer vazamentos de dados?

De acordo com estudos realizados no ano de 2023 sobre o tema pela IBM em diversos países, incluindo o Brasil, observa-se os seguintes percentuais em relação à ocorrência de vazamento de dados:

- cerca de 80% envolvem perda ou roubo de dados pessoais de usuários dos serviços;
- 32% referem-se a propriedade intelectual;
- 24% a dados anonimizados de usuários;
- 23% a dados corporativos em geral e
- 21% a dados pessoais de colaboradores.

No Brasil, as principais causas de vazamento de dados se referem a:

- 47% ataques maliciosos;
- 28% erros de sistema e
- 25% erro humano.

Dentre os ataques maliciosos estão ameaças como:

- malwares comuns e
- ransomwares, focados em sequestrar dados e exigir o pagamento de resgate.

Sendo identificados como os principais fatores que permitiram que elas fossem executadas:

- credenciais roubadas ou comprometidas;
- falhas na configuração de infraestrutura em nuvem;
- vulnerabilidades em softwares de terceiros e
- phishing.

3. Como evitar um vazamento de dados?

Para evitar a ocorrência de vazamentos de dados é necessário que a Intsituição adote as seguintes recomendações relacionadas à Segurança da Informação:

- investimento em ferramentas de prevenção contra ameaças, como firewall, antivírus corporativo (antiransomware), e-mail gateway e SIEM (gerenciador de eventos de segurança);
- manutenção de sistemas e softwares sempre atualizados;
- estabelecimento de políticas e ferramentas de autenticação e controle de acesso;
- garantia de segurança do acesso físico ao ambiente de TI;
- realização de análises de vulnerabilidade frequentemente;
- atenção às configurações de segurança de ambientes em nuvem;
- atenção à Política de Segurança da organização;
- promoção de campanhas de conscientização e treinamento de servidores e colaboradores, ensinando-os a reconhecer as principais ameaças, como phishing;
- cumprimento dos processos internos para comunicação e tratamento de incidentes de segurança, com especial atenção à avaliação quanto ao incidente envolver ou não dados pessoais.

4. Quais as consequências de um vazamento de dados para o Órgão?

Vazamento de dados podem acarretar diversas consequências, tais como:

- Sanções administrativas, como multas;
- Perdas financeiras por conta de negócios cancelados, fuga de investidores e vazamento de informações sensíveis à instituição;
- Quebra de confiança na relação com o usuário de serviços e com os titulares de dados em geral;
- Danos de reputação e imagem;
- Ações judiciais individuais e coletivas por parte dos titulares de dados e de entidades de defesa do consumidor.

De acordo com determinação prevista no artigo 42 LGPD, caso o usuário sofra algum dano como consequência do vazamento dos seus dados pessoais, ele pode acionar judicialmente o Órgão para garantir uma reparação.

> *"Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo."*

Se o titular sofreu um dano moral ou material por conta de um vazamento de dados, o recomendado é que ele entre em contato com o Órgão e busque uma reparação amigável.

Caso o contato seja infrutífero, o titular pode acionar a instituição judicialmente para garantir os seus direitos.

Por essa razão, a melhor opção é sempre agir de forma preventiva, adotando medidas para evitar qualquer tipo de incidente de segurança.

5. Quem responde legalmente caso ocorra um vazamento de dados?

Cabe destacar que a LGPD se refere apenas ao tratamento de dados pessoais, ou seja, a dados que identifiquem uma pessoa ou que, quando associados a outros dados, permitam identificar uma pessoa.

A Lei recomenda, em seu artigo 46, que os agentes de tratamento adotem medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais. Isso inclui protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Caso essas medidas não sejam adotadas e isso leve à uma violação da segurança dos dados, o controlador ou o operador terão que responder pelos danos causados.

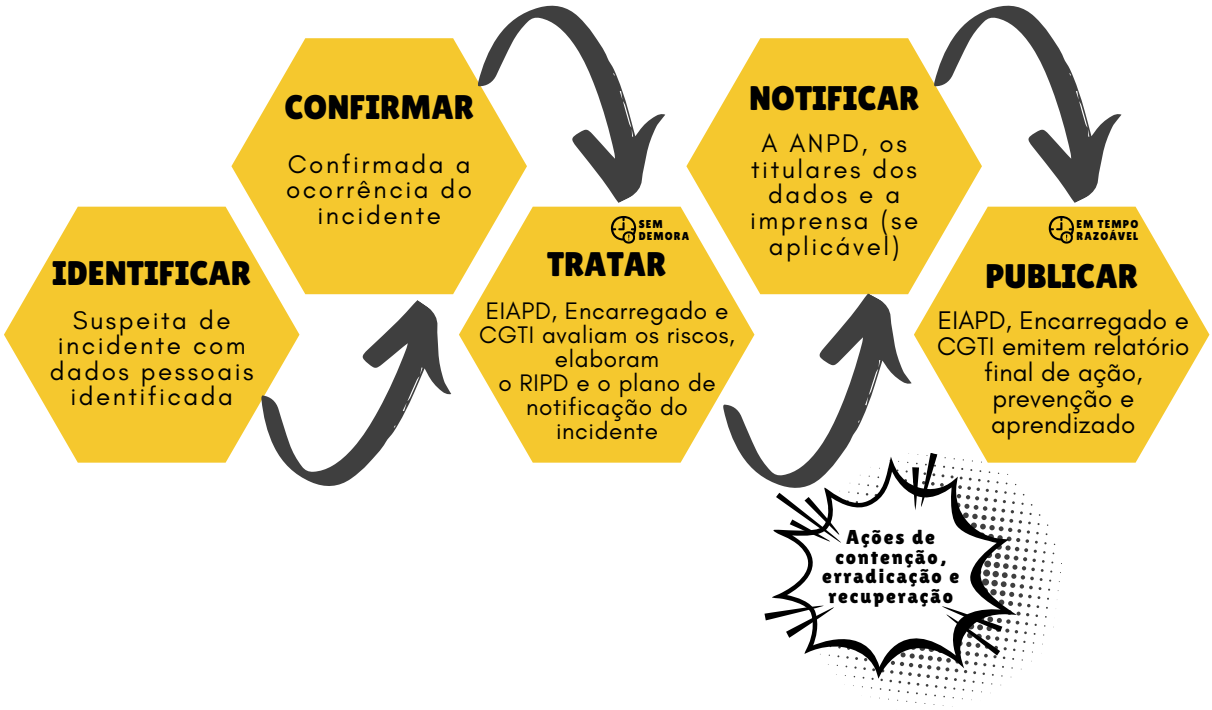
> *"Art.44 (...)*
> *Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano."*

Contudo, os agentes de tratamento não serão responsabilizados caso consigam provar que:

- não realizaram o tratamento de dados pessoais que lhes é atribuído;
- embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
- o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

PROCESSO DE NOTIFICAÇÃO E TRATAMENTO DO INCIDENTE

Apresentam-se a seguir as etapas do processo de notificação e tratamento do incidente com dados pessoais:



Identificação do incidente

Um incidente com dados pessoais pode ser notificado à Equipe para Proteção de Dados - EIAPD e ao Encarregado pelo Tratamento de Dados Pessoais, por meio de:

- Formulário de Notificação de Incidentes de Segurança e Vazamento de Dados Pessoais, disponível no SEI Ibama;
- Plataforma Fala.BR; ou
- email lgpd@ibama.gov.br.

Processo de identificação do incidente

Titular de dados

Encarregado e EIAPD

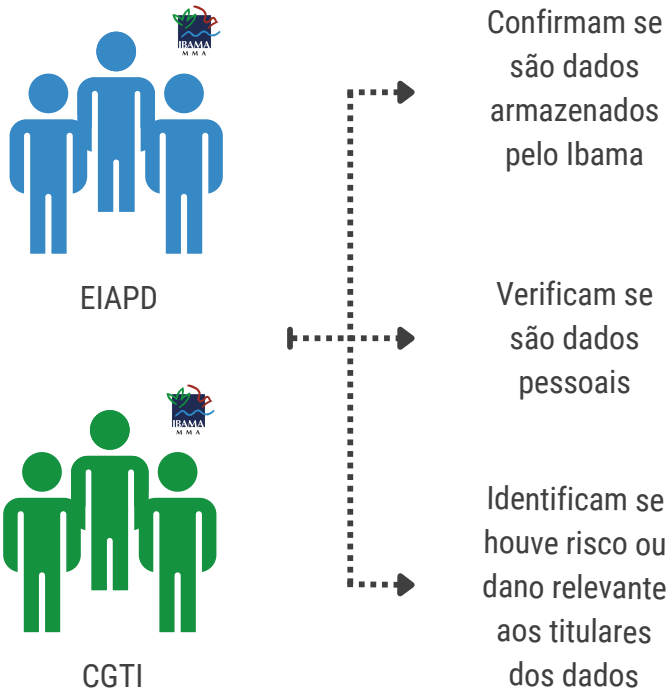
Confirmação da ocorrência do incidente

Recebida a notificação, a Equipe para Proteção de Dados - EIAPD, com o apoio da Coordenação-geral de Tecnologia da Informação - CGTI, deverá imediatamente identificar os dados vinculados ao incidente, analisando cautelosa e detalhadamente, todas as informações envolvidas no episódio, a fim de:

1. Confirmar se os dados compõem ou não a base de dados do Ibama;
2. Verificar se os dados do incidente são ou não caracterizados como dados pessoais, relacionados à pessoa natural identificada ou identificável, de acordo com o art. 5º, I, LGPD;
3. Identificar se houve algum tipo de tratamento dos dados pessoais, que acarrete risco ou dano relevante aos titulares dos dados, como, por exemplo:
    - A invasão dos sistemas utilizados pelo Prevfogo por um agente malicioso que realize a cópia não autorizada da base de dados contendo dados pessoais de brigadistas, tais como peso, altura, tipo sanguíneo, medidas corporais, atestados médicos e os expõe a risco de danos morais;

- A indisponibilidade prolongada do sistema de Cadastro, Arrecadação e Fiscalização (Sicafi) em razão de um incidente de sequestro de dados, impedindo o acesso aos dados ou a realização de procedimentos, pode expor dados pessoais sensíveis dos titulares e causar-lhes riscos de fraudes e danos materiais;
- A perda ou roubo de documentos ou dispositivos de armazenamento de dados que contenham dados pessoais protegidos por sigilo profissional, cópia de documentos de identificação oficial e dados de contato dos titulares pode expô-los a riscos reputacionais e de sofrer fraudes financeiras.

Processo de confirmação da ocorrência do incidente



Tratamento de resposta ao incidente

1. Avaliação do incidente

Confirmada a ocorrência do incidente, a Equipe para Proteção de Dados - EIAPD, juntamente com a Coordenação-geral de Tecnologia da Informação - CGTI, deverá iniciar a avaliação do incidente para a apuração da gravidade dos dados envolvidos. O documento, específico e direcionado à sinalização de criticidade e gravidade do evento, permitirá que o Ibama entenda melhor os riscos aos quais está sujeito, possibilitando uma melhor compreensão do tratamento que deverá dar à comunicação com os titulares dos dados vazados e às autoridades competentes.

A avaliação deverá identificar:

1. O contexto da atividade de tratamento de dados;
2. A classificação do incidente:
    - Conteúdo abusivo: spam, assédio, etc.;
    - Código malicioso: bot, worm, vírus, trojan, spyware, scripts;
    - Prospecção por informações: varredura, sniffing, engenharia social;
    - Tentativa de intrusão: tentativa de exploração de vulnerabilidades, tentativa de acesso lógico;
    - Intrusão: acesso lógico indesejável, comprometimento de conta de usuário, de aplicação;
    - Indisponibilidade de serviço ou informação: negação de serviço, sabotagem;
    - Segurança da informação: acesso não-autorizado à informação, modificação não autorizada da informação;
    - Fraude: violação de direitos autorais, fingir ou falsificar identidade pessoal ou institucional, uso de recursos de forma não-autorizada;
    - Outros: incidente especificamente categorizado.

3. As categorias e quantidades de titulares afetados;
4. Os tipos e quantidade de dados violados;
5. Os potenciais danos materiais, morais, reputacionais causados aos titulares;
6. Se os dados violados estavam protegidos de forma a impossibilitar a identificação de seus titulares;
7. As medidas de mitigação adotadas após o incidente.

Em função da combinação desses critérios, realizar a classificação de criticidade do incidente de acordo com as definições a seguir:

- ALTA (impacto grave): incidente que afeta sistemas relevantes ou informações críticas, com potencial para gerar impacto negativo sobre o Ibama;
- MÉDIA (impacto significativo): incidente que afeta sistemas ou informações não críticas, sem impacto negativo ao Ibama;
- BAIXA (impacto mínimo): possível incidente, sistemas não críticos; investigações de incidentes ou de colaboradores; investigações de longo prazo envolvendo pesquisa extensa e/ou trabalho forense detalhado.

2. Confecção de parecer técnico

Em seguida, a Equipe para Proteção de Dados - EIAPD juntamente com a Coordenação-geral de Tecnologia da Informação - CGTI, providenciará a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), a fim de demonstrar a coleta de evidências técnicas necessárias à formatação de prova sobre o incidente, apontar eventuais falhas de segurança que permitiram ou contribuíram com a ocorrência do incidente e direcionar as correções necessárias, fundamentais para que o Ibama evolua em relação às boas práticas de governança em privacidade.

3. Criação do plano de comunicação do incidente

Adicionalmente, a Equipe para Proteção de Dados - EIAPD providenciará, em parceria com a Coordenação-geral de Tecnologia da Informação - CGTI e a Assessoria de Comunicação - ASCOM, a elaboração de um plano de comunicação do incidente, composto de documentos a serem enviados à ANPD, aos titulares de dados e à impresa, caso necessário.

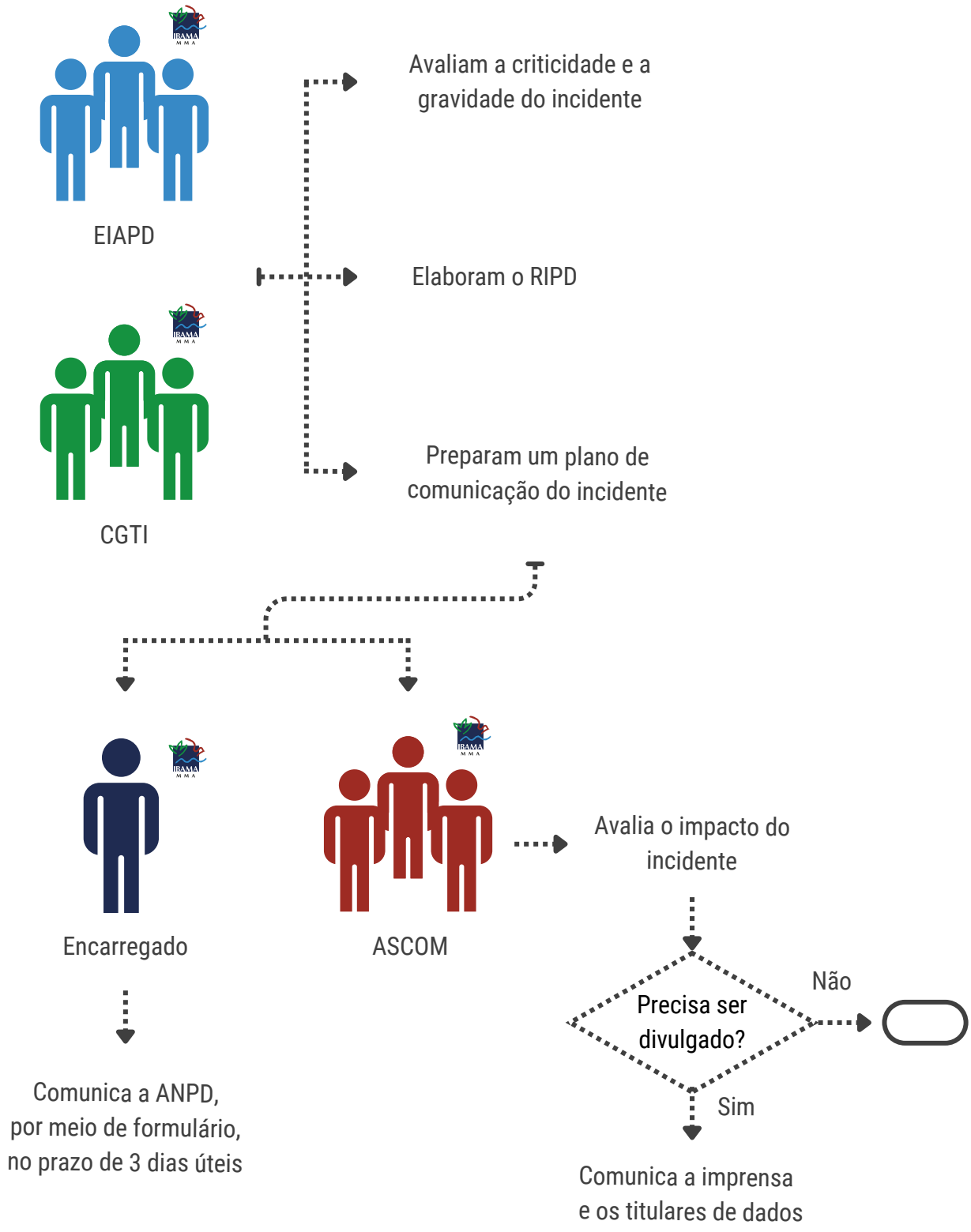
Notificação do incidente

Em atenção às disposições normativas que versam sobre a comunicação do incidente, sob pena de aplicação de sanções em face do Órgão pela ANPD, visando preservar os direitos dos titulares e tentar diminuir os possíveis prejuízos que um incidente de segurança possa causar, observando o prazo recomendado de 3 (três) dias úteis da ciência do fato, o Ibama providenciará a comunicação do incidente de segurança, nos seguintes termos:

Para quem?	Quem?	Como?
ANPD (necessário)	Encarregado	• Por meio do preenchimento de formulário disponibilizado para ser protocolado por peticionamento eletrônico no sistema SUPER da ANPD (https://www.gov.br/anpd/pt-br/canais_atendimento/peticionamento-eletronico-anpd)
Imprensa (se aplicável)	ASCOM	• Através de canais já habitualmente utilizados pelo Ibama para se comunicar com a imprensa

Para quem?	Quem?	Como?
Titular de dados (se aplicável)	ASCOM	• De forma individual e diretamente aos titulares, sempre que possível. • Por meio de e-mail, carta ou mensagem eletrônica ou através de outro canal já habitualmente utilizado pelo Ibama para se comunicar com o titular. • Caso não seja possível individualizar os titulares afetados, a comunicação deverá ser direcionadas a todos cujos dados estejam presentes na base de dados violada. • Excepcionalmente, e de forma justificada, pode ser feita a comunicação indireta por meio de publicação em meios de comunicação. O meio utilizado deve ser capaz de alcançar o maior número possível de titulares, e deve ser dado o devido destaque à divulgação. • O comunicado deve fazer uso de linguagem clara e conter as seguintes informações: ◦ a descrição da natureza e da categoria de dados pessoais afetados; ◦ as medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; ◦ os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares; ◦ os motivos da demora, no caso de a comunicação não ter sido feita no prazo de 3 (três) dias úteis; ◦ as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis; ◦ a data do conhecimento do incidente de segurança; e ◦ o contato para obtenção de informações e, quando aplicável, os dados de contato do encarregado (Plataforma Fala.BR ou email lgpd@ibama.gov.br).

Processo de tratamento de resposta e notificação do incidente



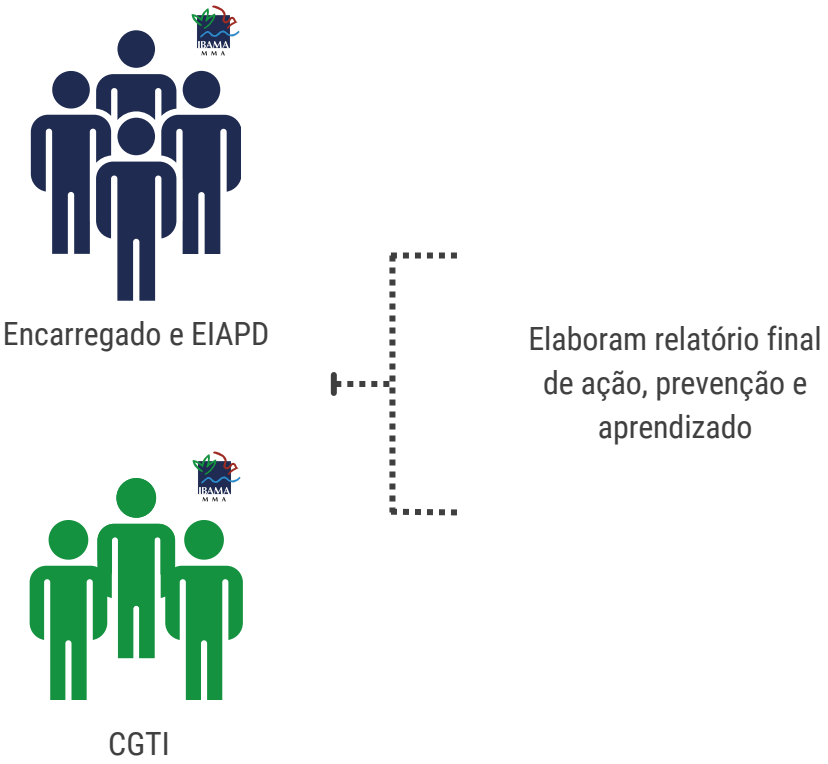
Elaboração de relatório final de ação, prevenção e aprendizado

Esta última etapa visa registrar a ocorrência do incidente e as providências adotadas, a partir da elaboração de um relatório circunstanciado, detalhando os resultados identificados, a fim de que o Ibama adote as medidas necessárias para a prevenção de novos episódios envolvendo vulnerabilidades tecnológicas.

Esse documento tem como objetivos:

- avaliar o processo de tratamento do incidente e verificar a eficácia das soluções adotadas;
- relacionar e documentar as falhas e os recursos inexistentes ou insuficientes, para que sejam providenciados em futuras ocasiões;
- compartilhar as lições aprendidas, com outros atores se necessário, com o objetivo de discutir erros e dificuldades encontradas na atenuação do evento ocorrido, propor melhoria na infraestrutura computacional e nos processos de resposta a incidentes;
- comunicar a área de negócio afetada sobre as decisões tomadas para prevenção de incidentes da mesma natureza, buscando implementar melhorias na infraestrutura de segurança; e
- realizar os ajustes necessários no Programa de Governança em Privacidade - PGP.

Processo de elaboração de relatório final de ação, prevenção e aprendizado



REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Comunicação de Incidentes de segurança. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca> Acesso em 23 de janeiro de 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Resolução CD/ANPD nº 15, de 24 de abril de 2024. Aprova o Regulamento de Comunicação de Incidente de Segurança. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024> Acesso em 30 de abril de 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato20152018/2018/lei/l13709.htm>. Acesso em: 15 de dezembro de 2023.

ENAP. Proteção de Dados Pessoais no Setor Público. Disponível em: <https://www.escolavirtual.gov.br/curso/290>. Acesso em: 13 de dezembro de 2023.

GET PRIVACY. Perguntas e respostas sobre vazamento de dados pessoais. Disponível em:<https://getprivacy.com.br/perguntas-respostas-lgpd-vazamento-de-dados/#:~:text=J%C3%A1%20um%20vazamento%20de%20dados,%C3%A0%20empresa%20controladora%20dos%20dados>. Acesso em 14 de dezembro de 2023.

GOVERNO FEDERAL. Guia de Resposta a Incidentes de Segurança. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/GuiaderespostaaIncidentes_verso_Minuta_Finalversao_17121.pdf> Acesso em 15 de dezembro de 2023.

GOVERNO FEDERAL. Plano de Gestão de Incidentes Cibernéticos para a administração pública federal - Plangic - Portaria GSI_PR nº 120, de 21 de dezembro de 2022. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-120-de-21-de-dezembro-de-2022-452767918>. Acesso em 15 de dezembro de 2023.

IBAMA. Política de Segurança da Informação e Comunicações do Ibama (POSIC). Disponível em:<https://www.gov.br/ibama/pt-br/acesso-a-informacao/documentos-oficiais/politica-de-seguranca-da-informacao-e-comunicacoes-do-ibama-posic>. Acesso em 07 de dezembro de 2023.

IBM. Cost of a Data Breach Report 2023. Dispon'ivel em: <https://www.ibm.com/reports/data-breach> Acesso em 15 de dezembro de 2023.

LGPD BRASIL. Orientações sobre a criação de um plano de resposta a incidentes. Disponível em: <https://www.lgpdbrasil.com.br/plano-de-resposta-a-incidentes-como-criar-um-adequado-para-a-sua-empresa/> Acesso em 07 de dezembro de 2023.

OPICE BLUM. Orientações sobre o que fazer diante de um incidente de segurança em dados pessoais. Disponível em: <https://opiceblum.com.br/o-que-fazer-diante-de-um-incidente-de-seguranca-em-dados-pessoais/%20> Acesso em 23 de janeiro de 2024.

REDE GOVERNANÇA BRASIL. Cartilha de Governança em Proteção de Dados para Municípios / Lucas Paglia, Bruno Ferola, Fábio Xavier. Salvador, BA; Brasíllia, DF: Editora Mente Aberta; Rede Governança Brasil, 27 de outubro de 2021. [E-book].

SERPRO. Orientações sobre o que fazer em caso de violação de dados pessoais. Disponível em: <https://www.serpro.gov.br/menu/noticias/noticias-2022/o-que-fazer-em-caso-de-violacao-de-dados-pessoais#:~:text=Comunicar%20%C3%A0%20ANPD%20e%20ao,e%20presta%C3%A7%C3%A3o%20de%20contas%20(Art.)>. Acesso em 07 de dezembro de 2023.

TRIBUNAL REGIONAL DO TRABALHO DA 15º REGIÃO. Plano de Resposta a Incidentes de Segurança. Disponível em: <https://trt15.jus.br/sites/portal/files/roles/institucional/gestao-estrategica/lgpd/Plano%20de%20Resposta%20a%20Incidentes%20de%20Seguran%C3%A7a.pdf>. Acesso em 24 de janeiro de 2024