Plano de Respostas a Incidentes - LGPD

Município de Paulo Bento - RS

Histórico de versões

Data	Versão	Descrição	Autor
04/08/2026	v.0.1	Elaboração e revisão final para envio ao Comitê Municipal de Gerstão de TI.	Daniel Marin
		Texto revisado com alterações aprovadas pelo Comitê Municipal de Gerstão de TI.	Membros do Comitê Municipal de Gerstão de TI

Sumário

1. Introdução

Este Plano de Respostas a Incidentes na qual é de natureza pertinente ao tratamento dos incidentes que envolvam os dados pessoais de acordo com a LGPD, faz parte de todo m processo que inadvetidamente é primaz e necessário, tendo em vista não somente o alinhamento com a legislação vientes, mas também a urgência e acompanhar o desenvolvimento da TI em todas às áreas.

Neste contexto urde, elucidar com clarea e objetividade alguns pontos introodutórios e propriamente conceituais, Nesta esteira então temos o seguinte: o incidente de segurança com dados pessoais é um evento adverso envolvendo dados de titulares (pessoas). 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. Enfim algo caracteristicamente anômalo no que tange a seguridade e confidencialidade de dados pessoais.

Os 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. Entretanto quando há à exploração da vulnerabilidade concernente, seja para fins idôneos ou inidôneos, então poderá assim resultar na configuração de um incidente e uma violação de privacidade flagrante.

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 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.

Levando em consideração os distintos dados com que a Prefeitura Municipal de Paulo Bento-RS trata diariamente, urde traçar minimamente um planejamento para intuir mitigar os riscos e balizar um plano de respostas a incidentes de vazamento de dados. Contudo o primeiro passo é ter a plena consciência dos riscos que cercam o aspecto correlato ao vazamento de dados sensíveis. E além de seguir os preceitos que estão avalizados na LGPD.

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 da Prefeitura de Paulo Bento – RS, além de fundamentar às ações de mitigância.

2. Objetivos

Traça-se como objetivo geral o seguinte:

- 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.

E para lograr êxito no quesito da objetivação central deste plano, serão seus eixos objetivais estratégicos e específicos os seguintes:

- 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;
- Mitigar os riscos concernentes ao vazamento de dados sensíveis da entidade.

3. Conceitos e Definições

Dentro deste contexto é deveras necessário minimamente conceituar alguns termos relativos a TI e a dados informacionais que fazem parte do campo da LGPD e suas áreas afins:

- **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:** 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;
- **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.

4. Panorama Relativo a Incidentes com Dados Pessoais

Considerando as definições da LGPD, um incidente de segurança é um acontecimento indesejado ou inesperado, passível portanto de 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. E que pode inadvertidamente vir a causar severos danos à organização e/ou a indivíduos.

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.

4.1 Indicadores relativos a vazamento de dados

Consoante aos estudos realizados no ano de 2025 sobre o tema pela IBM em diversos países, incluindo o Brasil, observa-se os seguintes percentuais em relação à ocorrência de vazamento de dados, conforme os indicadores abaixo afiançam:

Vetores Iniciais de Ataque no Brasil:

- Phishing: Representa 18% das violações, sendo o principal vetor inicial de acesso no país;
- Terceiros (Supply Chain): Comprometimento da cadeia de suprimentos representa 15% dos casos;
- Exploração de vulnerabilidades: Responsável por 13% dos incidentes.

Fatores Tecnológicos e Tendências Globais:

- Uso indevido de Inteligência Artificial: 13% das organizações relataram violações envolvendo modelos ou aplicações de IA (aumento impulsionado por shadow AI, onde sistemas são usados sem governança adequada);
- Proporção de organizações que relataram um incidente de segurança relacionado à IA e não possuíam controles adequados de acesso à IA: 97%;
- Falta de governança de IA: Globalmente, 63% das organizações violadas não possuíam políticas adequadas de governança de Inteligência Artificial para prevenir riscos;
- Ciclo de vida da violação de dados: 51% ataques maliciosos ou criminosos; 26% erro humano; 23% falha de TI;
- Identificação da violação: equipes e ferramentas de segurança da organização 50%; terceiro benigno 31%; divulgação pelo invasor 19%;
- Parcela das organizações que não se recuperaram totalmente de uma violação de dados: 65%;
- Parcela das violações de dados que resultam em multas: 32%;
- Das organizações que relataram incidentes de segurança em modelos ou aplicações de IA: fornecedor terceirizado entregue como SaaS 29%; interno 26%; software livre 26%; 19% fornecedor terceirizado, implementação local;
- Ataques orientados por IA (Parcela de violações envolvendo invasores que utilizaram a IA): 16%.

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:

- Falhas na configuração de infraestrutura em nuvem;
- Vulnerabilidades em softwares de terceiros e phishing;
- Informações de identificação pessoal (PII);
- Detalhes financeiros: são quaisquer dados relativos às finanças de um indivíduo ou organização, como registros fiscais, extratos bancários, faturas, etc;
- Credenciais de login: por exemplo, nomes de usuário e senhas que podem ser usados para realizar o controle de contas de e-mail ou contas de mídia social.

Ao obter qualquer uma das informações acima através do vazamento de dados, os cibercriminosos têm os meios para perpetrar outros crimes, incluindo roubo de identidade, fraude financeira e extorsão. É por isso que é essencial que indivíduos e empresas tomem cuidado para fortalecer a segurança cibernética na prevenção contra perda de dados.

4.2 Prevenção ao 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.

4.3 Consequências de um vazamento de dados ao 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.

2.2.1 Responsável legal caso ocorra 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 (...)

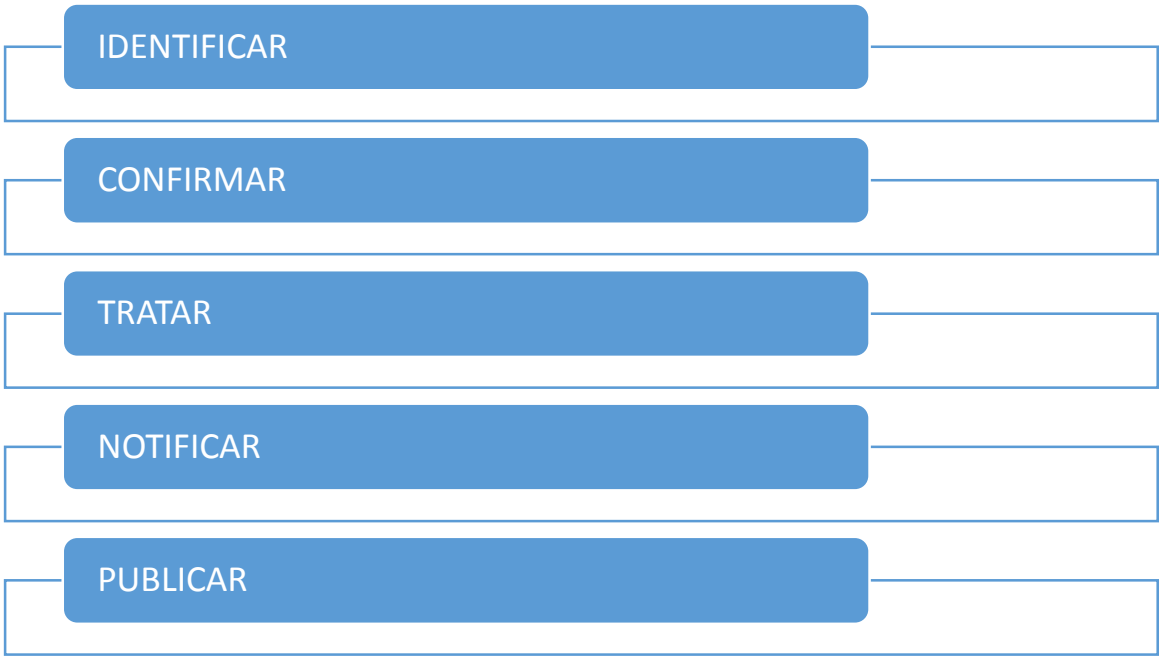
Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano."

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;
- O dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

5. Processo de Notificação e Tratamento

Detalharemos as etapas pertinentes ao processo que envolve a notificação e o tratamento de eventuais incidentes com dados pessoais:



Um incidente com dados pessoais pode ser notificado ao Encarregado pelo Tratamento de Dados Pessoais, por meio do e-mail: daniel.marin@paulobento.rs.gov.br.

Ou, por intermédio da Ouvidoria Municipal, pelo e-mail: ouvidoria@paulobento.rs.gov.br.

Recebida a notificação, 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 da Prefeitura de Paulo Bento;

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.

No tocante ao tratamento dos dados pertinente a resposta ao incidente, enseja-se seguir os seguintes passos, em que 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 à Prefeitura;

BAIXA (impacto mínimo): possível incidente, sistemas não críticos; investigações de incidentes ou de colaboradores;

6. Relatório final de ação, prevenção e aprendizado

Nesta etapa objetiva 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 a Prefeitura Municipal de Paulo Bento/RS, 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.

7. Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Comunicação de Incidentes de segurança. Disponível em: <https://www.gov.br/anpd/ptbr/assuntos/incidente-de-seguranca> Acesso em 16 de julho de 2026.

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-deabril-de-2024-556243024> Acesso em 17 de julho de 2026.

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: 26 de junho de 2026.

ENAP. Proteção de Dados Pessoais no Setor Público. Disponível em: <https://www.escolavirtual.gov.br/curso/290>. Acesso em: 02 de agosto de 2026.

GET PRIVACY. Perguntas e respostas sobre vazamento de dados pessoais. Disponível em:<https://getprivacy.com.br/perguntasrespostas-lgpd-vazamento-dedados/#:~:text=J%C3%A1%20um%20vazamento%20de%20dados,%C3%A0%20empresa%20controladora%20dos%20dados>. Acesso em 30 de julho de 2026.

IBM. Cost of a Data Breach Report 2025. Disponível em: < https://www.ibm.com/br-pt/reports/data-breach> Acesso em 02 de agosto de 2026.

GOVERNO FEDERAL. Guia de Resposta a Incidentes de Segurança. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-eprotecao-dedados/guias/GuiaderespostaaIncidentes_verso_Minuta_Finalversao_17121.pdf> Acesso em 22 de julho de 2026.

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-dedezembro-de-2022-452767918>. Acesso em 23 de julho de 2026.

LGPD BRASIL. Orientações sobre a criação de um plano de resposta a incidentes. Disponível em: <https://www.lgpdbrasil.com.br/plano-deresposta-a-incidentes-como-criar-um-adequado-para-a-sua-empresa/> Acesso em 23 de julho de 2026.

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-deseguranca-em-dados-pessoais/%20> Acesso em 04 de agosto de 2026.