MUNICÍPIO DE ITAIPULÂNDIA

ESTADO DO PARANÁ

PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

ELABORAÇÃO E REVISÃO

Ouvidoria e equipe de Proteção de Dados Pessoais

SUMÁRIO

CONTEXTUALIZAÇÃO

A Lei nº 13.709/2018, Lei Geral de Proteção de Dados – LGPD, tem como um de seus pilares centrais a implementação de medidas de Segurança da Informação que podem trazer às entidades públicas e privadas, uma cultura de maior conscientização na área. A LGPD considera que, mais grave do que sofrer um ataque ou passar por um vazamento de dados, é não se prevenir e nem adotar as medidas e práticas necessárias e possíveis para a proteção dos seus dados e de todos os que são afetados por eventuais acessos não autorizados.

Um incidente de segurança com dados pessoais é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

Evitar esses eventos, passa pela necessidade de adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, de acordo com as regras de boas práticas de governança para o tratamento dedados pessoais.

Levando isso em consideração, a criação de estratégias e Planos para controle de danos é essencial, e é aí que entram os Planos de Respostas a Incidentes de Segurança em Dados Pessoais.

Resposta a Incidentes é o processo que descreve como uma organização deverá lidar com um incidente de segurança, seja ele um ataque cibernético, uma violação de dados, a presença de um aplicativo malicioso (como um vírus), uma violação das políticas e padrões de segurança da entidade, dentre outros. O objetivo é minimizar os danos que poderiam ser causados pelo incidente, reduzir o tempo de ação e os custos de recuperação.

O Plano de Respostas a Incidentes consiste em um documento interno que deve ser amplamente conhecido por todos os servidores e colaboradores e que dispõe sobre as medidas que devem ser adotadas no caso de um Incidente de Segurança em Dados Pessoais.

Atualmente, grande parte dos processos da Administração Municipal são informatizados, imprimindo maior eficiência e agilidade nos serviços que presta. Por isso mesmo, a criação e implementação de medidas de controle e segurança de dados, como o Plano de Resposta a Incidentes, é questão que impõe.

Este guia visa auxiliar os profissionais designados ao tratamento de dados pessoais e demais servidores que atuam subordinados ao controlador, incentivando a utilização de boas práticas de segurança e proteção de dados nos assuntos relacionados a respostas de incidentes.

As informações contidas neste guia serão atualizadas de forma contínua, buscando incorporar melhorias, conforme a publicação de novas normas e edificação dos processos de proteção de dados existentes.

OBJETIVO, ABRANGÊNCIA E VIGÊNCIA

O Plano em questão, tem o objetivo geral de orientar a Administração Municipal a responder às situações de emergência e exceção, de forma documentada, formalizada, ágil e confiável, além de resguardar as evidências que possam auxiliar na prevenção de novos incidentes e no atendimento às exigências legais de comunicação e transparência.

Neste plano serão estabelecidas funções e responsabilidades individuais e de equipes, bem como, as medidas a serem adotadas para que a Administração Municipal responda adequadamente a um incidente, sempre prezando pela integridade dos sistemas/processos, proteção de informações e privacidade dos seus titulares, possibilitando manter a confiabilidade dos serviços prestados.

O presente plano se aplica em qualquer caso de incidentes envolvendo Dados Pessoais e deverá ser observado em conjunto com as demais políticas da Administração Municipal e por todas as áreas, servidores, colaboradores e prestadores de serviços que possam vir a ter acesso às informações, arquivos e dados sob a responsabilidade da Controladora.

A implementação do PRI busca:

- Reduzir o impacto de incidentes de segurança da informação;
- Minimizar as interrupções nas operações da organização;
- Proteger a reputação da Administração Municipal;
- Assegurar a conformidade com a LGPD e outras leis de proteção de dados;
- Demonstrar proatividade e responsabilidade na proteção de dados pessoais;

TERMOS E DEFINIÇÕES

- **Agentes de tratamento:** corresponde ao controlador e operador em conjunto. Não são considerados controladores ou operadores os servidores ou as equipes de trabalho de uma entidade, 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 nacional;

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

- **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;

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

- **Dados pessoais sensíveis:** são dados pessoais que digam respeito a origem racial ou étnica, convicção religiosa, prática ou orientação sexual, informações médicas ou de saúde, como histórico médico e prontuário físico ou eletrônico, informações genéticas ou biométricas, crenças políticas ou filosóficas, filiação política ou sindical, número do seguro social, número da carteirinha do Plano de saúde e informações bancárias;

- **Encarregado ou Data Protection Officer (DPO):** é pessoa física designada pelo controlador, responsável por assegurar o cumprimento da legislação local aplicável e atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

- **Incidente:** qualquer ato, suspeita, ameaça ou circunstância que comprometa a confidencialidade, integridade ou a disponibilidade de informações que estão em posse do Município de Itaipulândia ou que ela venha a ter acesso;

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

- **LGPD:** acrônimo utilizado para identificação da Lei Geral de Proteção de Dados, a Lei nº 13.709/2018, que regula as atividades de Tratamento de Dados no Brasil.

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

- **Operador:** é toda pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados em nome do controlador. O operador será sempre uma pessoa distinta do controlador;

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

- **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;

- **Vazamento de dados:** qualquer quebra de sigilo ou disseminação 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.

- **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;

- **Titular de dados pessoais:** a pessoa natural a quem pertence o dado pessoal.

ATORES E RESPONSABILIDADES

Cada setor da administração municipal tem responsabilidades quando da ocorrência ou mera suspeita de um Incidente, devendo comunicar, imediatamente, o fato ao encarregado.

- **Notificador:** pessoa ou sistema de monitoração que notifica o incidente;

- **Encarregado pelo tratamento de dados pessoais ou Data Privacy Officer (DPO):** O Encarregado é a pessoa indicada pelo Controlador para atuar como ponto de contato entre a organização, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD).

- **Controlador:** O papel do Controlador no PRI, segundo a LGPD, é central e de grande responsabilidade. O Controlador é a pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No contexto de incidentes de segurança envolvendo dados, suas responsabilidades incluem:

a) notificar a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares dos dados sobre incidentes que possam acarretar risco ou dano relevante, isso inclui a descrição da natureza dos dados afetados, os titulares envolvidos, as medidas técnicas e de segurança adotadas, e os possíveis impactos;

b) acompanhar toda a execução do PRI e tomar decisões, quando necessário, sobre as ações e procedimentos a serem adotados em todas as etapas do Plano;

c) o Controlador deve revisar o incidente, analisar suas causas e decidir sobre ajustes nos procedimentos e sistemas para minimizar riscos de novos incidentes.

- **Equipe Técnica de Respostas a incidentes:** A Equipe Técnica de Resposta a Incidentes é formada por profissionais especializados em segurança da informação, com atuação predominantemente vinculada ao Setor de Tecnologia da Informação do ente. Esses especialistas são responsáveis por gerenciar todos os aspectos técnicos relacionados aos incidentes, assegurando a identificação precisa, a contenção eficaz, a erradicação completa dos problemas e a implementação de medidas preventivas para evitar futuros eventos de segurança.

- **Comissão Permanente Municipal de Proteção de Dados (CPMPD):** É a instância responsável pela adequação da Controladoria e Ouvidoria Geral às exigências da Lei Geral de Proteção de Dados Pessoais (LGPD), conforme estabelecido pela Portaria nº 872, de 25 de novembro de 2025. Esta comissão atua de forma a garantir que as práticas da Administração Municipal estejam em conformidade com os requisitos legais de proteção de dados, desempenhando um papel essencial no monitoramento e gestão de incidentes que possam comprometer informações pessoais.

COMUNICAR O ENCARREGADO DE DADOS

A notificação ao Encarregado de Dados quanto a eventual incidente de segurança com dados pessoais deverá ser feita via e-mail institucional, o mais rápido possível, para as providências previstas na LGPD e no portal da ANPD sobre comunicação de incidentes de segurança.

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. Nessas tarefas, a LGPD e os demais normativos infralegais vigentes sobre proteção de dados pessoais deverão ser sempre consultados e utilizados como balizas.

COMUNICAR O CONTROLADOR

O Encarregado de Dados Pessoais deve comunicar incidentes com dados pessoais ao Controlador o mais rápido possível, a fim de viabilizar que o Controlador possa comunicar a ANPD e ao titular de dados.

O controlador deverá ter cautela quanto ao julgamento acerca da relevância dos riscos e danos referentes ao incidente e, em caso de dúvida, a comunicação do incidente deverá ser realizada de forma breve.

COMUNICAR A ANPD E AO TITULAR DE DADOS PESSOAIS

O art. 48 da LGPD determina que é obrigação do controlador comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

A ANPD estipula o prazo de 2 (dois) dias úteis para comunicação de incidente de segurança a proteção de dados.

Poderá ser acessado no site da ANPD ou por meio do link: https:/www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca, formulário modelo para notificação de incidentes de segurança com proteção de dados.

MACRO ETAPAS DO PROCESSO

Identificação

A identificação de qualquer Incidente de Segurança é aspecto chave para a boa implementação de um Plano de Respostas. É importante que se possa dispor das principais medidas de detecção e identificação de Incidentes, como ferramentas de monitoramento, eventos de log, mensagens de erro firewalls, etc. Também deve haver um trabalho maciço de sensibilização e capacitação de servidores, para que, proativamente, esses tenham a capacidade de identificar e informar eventual vazamento de dados, de que tenham conhecimento/acesso.

Preparação

Uma resposta a um incidente deve ser decisiva e executada prontamente. Como há pouco espaço para equívocos, é essencial que as práticas de emergência sejam exercitadas e os tempos de resposta medidos. Desta forma, é possível desenvolver uma metodologia que estimule a agilidade e a exatidão, minimizando o impacto da indisponibilidade de recursos e os potenciais danos causados pelo comprometimento do sistema/processos.

Contenção

Após a identificação de um incidente, o mesmo deve ser contido e, se for o caso, isolado, para que outros sistemas/processos não sejam afetados, evitando maiores danos ao ambiente. Essa etapa inclui a contenção de curto prazo, backup do sistema, contenção a longo prazo, dentre outros.

É importante que, durante a etapa de contenção, ocorra simultaneamente a adoção de medidas que permitam a documentação e o registro do incidente, devendo ser evitado que evidências e provas do ocorrido sejam destruídas ou perdidas.

Erradicação

Após a contenção da ameaça, a próxima etapa consiste da remoção da ameaça e restauração dos sistemas/processos afetados para que retornem ao seu estado original antes do incidente.

Recuperação

Nesta etapa, os sistemas/processos afetados retornarão, após testes e validações, ao ambiente de produção, ou, ao habitual andamento, com vistas a garantir que nenhuma ameaça permaneça.

Documentação do Incidente

O incidente deve ser documentado de forma detalhada, incluindo todas as ações implementadas nas etapas anteriores e as lições aprendidas com o caso.

Comunicações

A ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, deve ser comunicada à Autoridade Nacional de Proteção de Dados – ANPD e ao titular afetado. A depender da situação, as informações a serem prestadas à ANPD poderá ocorrer por meio de solicitações, comunicações ou auditorias, com a finalidade principal de demonstrar, para o órgão fiscalizador, a adequação (ou intenção de adequação) da Entidade aos ditames da lei.

DESCRIÇÃO DO PROCESSO

Início/Detecção

1. Um novo incidente é notificado por pessoa interna/externa à Administração Municipal ou por eventual alarme da monitoração. A comunicação inicial do incidente pode ser proveniente de qualquer fonte, tais como e-mails, telefone, “Fale Conosco”, Disk Denúncia, Sistemas internos (incluindo as recebidas pelo Encarregado quando se tratar de notificação do titular dos dados pessoais), devendo todas serem registradas, diretamente pelo Notificador.

Triagem

1. A Notificação é recebida pelo Encarregado de Dados, que deverá fazer a avaliação preliminar ou indicar a necessidade de composição de um Time de Resposta a Incidentes (TRI) para realizar a referida avaliação, descartando as notificações nulas ou claramente improcedentes. Em sendo desnecessária a composição do TRI, Encarregado de Dados assumirá as fases descritas no fluxo do processo que seriam de responsabilidade do TRI.
2. Na avaliação preliminar, devem ser buscadas informações sobre os sistemas/processos que foram alegadamente impactados, sua criticidade, quais os danos aparentes e o risco da situação se agravarem se não houver resposta imediata.
3. Conforme a avaliação preliminar, incidentes que não envolvem sistemas online e que seguramente não apresentam riscos aumentados pela falta de ação

imediata podem ser reencaminhados para tramites regulares dos setores pertinentes da Autarquia.

Avaliação

1. Nesta fase deve ser iniciada uma avaliação mais detalhada do incidente pelo DPO/TRI, classificando-o e definindo a sua criticidade.
2. A criticidade do incidente pode ser definida de acordo com as seguintes classificações:

Volume de Dados Pessoais expostos	Alto	Alta Gravidade	Alta Gravidade	Alta Gravidade
	Médio	Média Gravidade	Alta Gravidade	Alta Gravidade
	Baixo	Baixa Gravidade	Média Gravidade	Média Gravidade
		Baixa	Média	Alta
		Sensibilidade dos Dados Pessoais afetados		

Volume de Dados Pessoais expostos	
Criticidade	Descrição
Alto	Volume de Dados Pessoais afetado superior a 10% da base de dados da Controladora.
Médio	Volume de Dados Pessoais afetado inferior a 10% e superior a 2% da base de dados da Controladora.
Baixo	Volume de Dados Pessoais afetado inferior a 2% da base de dados da Controladora.

Sensibilidade dos Dados Pessoais afetados	
Criticidade	Descrição
Alta	Dados Pessoais de crianças/ adolescentes, dados Pessoais Sensíveis ou que possam gerar discriminação ao titular.
Média	Dados Pessoais imediatamente identificáveis (Ex.: nome, e-mail, CPF, endereço), combinados, ou não, com informações comportamentais (Ex.: histórico de atividades, preferências).
Baixa	Dados anonimizados, Dados Pessoais pseudonimizados (desde que a chave de desanonimização também não tenha sido comprometida), Dados Pessoais de difícil identificação (Ex.: IP)

3. Deve-se procurar identificar a causa do incidente, atores e ações envolvidas, vulnerabilidades exploradas, visando determinar ações para as demais fases. Pode ser importante engajar especialistas dos setores afetados para colaborar e isso deve ser feito a critério do DPO/TRI a qualquer momento que julgar adequado e viável.

Contenção, Erradicação e Recuperação

1. Os responsáveis pelos sistemas/processos impactados, devem ser acionados para se manifestarem sobre os procedimentos de resposta, contenção e erradicação.
2. 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, poderá ser realizado o desligamento dos sistemas inteiros ou de funcionalidades especificas e colocados avisos de indisponibilidade para manutenção. Todos os cuidados devem ser adotados para não impactar evidências que poderiam ser usadas para identificar autoria, origem e método usado para quebrar a segurança.
3. Em caso de incidente envolvendo máquinas virtuais, deve ser feito snapshot (registro do estado de um arquivo, aplicação ou sistema em um certo ponto no tempo) para posterior análise.
4. Em se tratando de incidentes não relacionados a recursos computacionais, mas essencialmente de atividade humana, os procedimentos podem envolver sindicância administrativa, processo administrativo disciplinar, entre outras medidas dispostas na legislação aplicável ao caso.
5. 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/processo.
6. Pode ser necessário o desenvolvimento e instalação de atualizações de aplicação ou do Sistema Operacional, ou elaboração de novas rotinas processuais.

Comunicações

1. Assim que possível, a situação deve ser encaminhada para análise do gestor responsável para avaliar se houve risco ou dano relevante aos titulares dos dados pessoais impactados.
2. Caso o gestor conclua que o incidente acarretou risco ou dano relevante aos titulares de dados pessoais, o Encarregado de Dados (DPO), deverá fazer as comunicações obrigatórias por Lei. Essas comunicações podem incluir agradecimentos ao notificador, informações para os titulares de dados e imprensa, bem como relatórios formais para a ANPD.

Documentação

1. O DPO/TRI deve documentar o incidente em base de conhecimentos apropriada, detalhando as informações obtidas, linha de tempo, atores envolvidos, evidencias, conclusões, decisões, autorizações e ações executadas.

2. Após a neutralização da ameaça, o Encarregado de Dados (DPO) deve elaborar um relatório circunstanciado de todas as medidas que foram adotadas, apresentando todas as informações relevantes, tais como, informações sobre o incidente em si (quando foi identificado, qual sua natureza, danos ou potenciais danos causados, a extensão, a relevância e a repercussão desses danos, etc); providências adotadas para preservação das evidências, procedimentos seguidos

para a contenção da crise; medidas de correção técnicas e de Governança adotadas; questionamentos e demandas externas (requerimentos de titulares de dados, autoridades e imprensa, bem como suas respostas); deliberações do TRI.

Observações complementares

Paralelamente à execução do Plano de Respostas a Incidentes, diversas ações devem ser desenvolvidas, antes, durante e depois da ocorrência de um incidente, conforme:

Durante o incidente: Identificação, coleta e preservação das evidências:

Como já mencionado, um aspecto essencial da Resposta aos Incidentes é a coleta e preservação de evidências que possam vir a ser úteis ou necessárias para a Entidade, por exemplo, para demonstrar às autoridades que houve uma resposta adequada e que o incidente foi tratado com a seriedade necessária.

Especialmente no contexto da LGPD e da ANPD, as providências adotadas pela Entidade, para conter o Incidente e seus danos, podem ser definitivas para a minimização das sanções e multas, eventualmente, aplicadas ao caso concreto. Tais evidências também se prestam a possibilitar a identificação/responsabilização do usuário causador do vazamento de dados pessoais. Diversas decisões na União Europeia, em decorrência da GDPR (General Data Protection Regulation ou Regulamentação Geral de Proteção de Dados da União Europeia), demonstram que, mais grave do que o incidente em si, é o fato de a organização desprezá-lo.

Após o incidente: Elaboração de relatório final do incidente e revisão dos procedimentos:

O relatório, além de ter uma função de comprovação das medidas levadas a efeito pela Entidade, é importante para que se possa compreender as causas do incidente, avaliar a aderência e efetividade do Plano de Respostas a Incidentes e analisar a atuação dos responsáveis.

No que tange à Comunicação de Incidente de Segurança, prevista na LGPD, cujo conteúdo mínimo está definido no artigo 48, temos:

> *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.*
>
> *I – a descrição da natureza dos dados pessoais afetados;*

Não basta apontar se os dados pessoais são convencionais (art. 5º, I) ou sensíveis (art. 5º, II), mas deve-se arrolar, com precisão, as espécies: contas de e-mail, dados de cartão de crédito, senhas, informações de geolocalização, etc., para que o titular tenha uma ideia, ainda que estimada, dos riscos existentes ou dos danos possíveis.

> *II – as informações sobre os titulares envolvidos;*

É a descrição, precisa ou estimada, de quais e quantos titulares foram afetados.

> *III – a indicação das medidas técnicas e de segurança utilizadas para a proteção;*

Observados os segredos comercial e industrial, a LGPD exige, em seu art. 46, que os agentes de tratamento (controlador e operador) adotem medidas de segurança (técnicas e administrativas) para a proteção de dados pessoais. Tais medidas

devem ser descritas, para se demonstrar o compliance com a lei. Obviamente, essa descrição minuciosa admite algumas limitações, como os segredos comercial e industrial, que devem ser poupados para a preservação do negócio. A depender do tipo de incidente e, em havendo o risco de ser repetido, a descrição de determinadas medidas de segurança adotadas também poderia ser ocultada, segundo a técnica da "segurança por obscuridade" (Security Through Obscurity – STO), que teria o condão de privar o adversário/atacante de qualquer informação que possa ajudá-lo a comprometer a organização.

IV – os riscos relacionados ao incidente;

Trata-se de uma análise prospectiva do incidente, levando em consideração, principalmente, os itens I e II. Poderá mencionar, também, os danos que já ocorreram, como a destruição ou codificação de dados.

V – os motivos da demora, no caso de a comunicação não ter sido imediata;

É a justificativa, devidamente fundamentada, da não apresentação imediata da notificação. Poderá decorrer, por exemplo, da complexidade e extensão (número de titulares afetados, quantidade de dados, etc.) do incidente.

VI – as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Aqui devem ser mencionadas, de forma clara e objetiva, e sem exagero de expressões técnicas, as condutas que foram e que serão implementadas para eliminar ou minimizar os efeitos do incidente, como o contato com as autoridades policiais, determinação de troca de senhas pelos usuários, a atualização de sistemas e servidores, etc.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

O RIPD poderá ser solicitado nas seguintes hipóteses:

- Para tratamento de dados pessoais realizados 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);
- Quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 da LGPD, combinados); e
- A qualquer momento, sob determinação da ANPD (art. 38).

Em síntese, o RIPD é um documento que pode ser solicitado pela ANPD e servirá de subsídio para o processo de gestão de incidentes com dados pessoais.