PLANO DE RESPOSTA A INCIDENTES COM DADOS PESSOAIS

BARRETOS
PREFEITURA

CGM

Controladoria Geral do Município

Prefeita do Município da Estância Turística de Barretos
Paula Oliveira Lemos

Controladoria Geral do Município
Paulo Fernando Scannavino

Elaboração
Daniel Chiarelli

Contato
lgpd@barretos.sp.gov.br
(17) 3612-2021

1. Apresentação

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018), conhecida como LGPD, impõe aos agentes de tratamento de dados pessoais a responsabilidade de garantir a segurança dessas informações, conforme previsto no artigo 47. Essa obrigação de proteção permanece vigente mesmo após o término do tratamento dos dados. A ausência de medidas técnicas e administrativas adequadas para proteger os dados sob custódia do controlador pode ser tão prejudicial como um ataque cibernético..

O artigo 46 da LGPD reforça a necessidade de adotar precauções que protejam os dados pessoais de acessos não autorizados e de situações acidentais ou de tratamento inadequado. Essas precauções não se limitam apenas ao uso de tecnologias e padrões de segurança, mas também envolvem a elaboração, manutenção e revisão de documentos. Essas práticas visam otimizar os processos internos, resguardando a reputação da organização, bem como seus servidores, prestadores de serviço e colaboradores.

Este guia foi criado para auxiliar os profissionais responsáveis pelo tratamento de dados pessoais e demais servidores subordinados ao Encarregado da Proteção de Dados. Seu objetivo é incentivar a adoção de boas práticas de segurança e proteção de dados, especialmente no que tange à resposta a incidentes. As informações apresentadas serão constantemente atualizadas, incorporando melhorias e novas normas à medida que os processos de proteção de dados evoluem, assegurando uma abordagem dinâmica e eficiente na preservação dos dados pessoais.

Assim, ao seguir as diretrizes deste guia e adotar as diligências indicadas pela LGPD, as organizações estarão melhor preparadas para mitigar riscos, garantindo não apenas a conformidade legal, mas também a proteção eficaz de suas informações e a manutenção de sua credibilidade.

2. Objetivos

O Plano de Resposta a Incidente de Segurança tem como objetivo principal orientar a Controladoria-Geral do Município na gestão de situações de emergência e exceção. A intenção é garantir que as evidências sejam preservadas para auxiliar na prevenção de futuros incidentes e no cumprimento das exigências legais de comunicação e transparência.

Neste Plano define as funções e responsabilidades tanto individuais quanto das equipes, além das medidas a serem adotadas para que a Controladoria-Geral do Município responda de forma adequada a incidentes que envolvam dados pessoais e dados sensíveis. Ele deve ser seguido em conjunto com a Política de Segurança da Informação, garantindo uma abordagem integrada e alinhada às diretrizes de proteção de dados do município.

3. Definições

No contexto deste plano e com base na Lei Geral de Proteção de dados (Lei 13.709/2018 - LGPD), são definidos:

LGPD: Lei Federal nº 13.709/2018, que regula o tratamento de dados pessoais em meios físicos ou digitais, por pessoas físicas ou jurídicas, públicas ou privadas, visando proteger os dados pessoais.

ANPD: Autoridade responsável por fiscalizar e garantir o cumprimento da legislação de proteção de dados pessoais no Brasil.

Dado pessoal: Qualquer informação que permita identificar, direta ou indiretamente, uma pessoa, como nome, documentos, telefone, endereço, e-mail, etc.

Dado pessoal sensível: Informações sobre origem racial, religião, opinião política, saúde, dados genéticos ou biométricos.

Anonimização: Processo que impede a associação de um dado a uma pessoa, direta ou indiretamente.

Pseudonimização: Tratamento de dados que só permite a identificação por meio de informação adicional, mantida em ambiente seguro.
Titular: Pessoa física a quem se referem os dados pessoais.

Controlador: Pessoa ou entidade responsável pelas decisões sobre o tratamento de dados.

Operador: Pessoa ou entidade que realiza o tratamento de dados em nome do controlador (servidor não é operador).

Agentes de tratamento: O controlador e o operador.

Encarregado da Proteção de Dados: Responsável pela comunicação entre o controlador, os titulares e a ANPD.

Tratamento: Qualquer operação com dados pessoais, como coleta, armazenamento, eliminação, transmissão, etc.

Incidente: Ato ou evento que compromete a segurança de dados pessoais.

Incidente de segurança com dados pessoais: Violação de dados, como acesso não autorizado, perda, alteração ou vazamento.

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;

4. Incidentes com dados pessoais

Um incidente de segurança com dados pessoais é qualquer evento confirmado que envolve uma violação da segurança, resultando em destruição, perda, alteração, divulgação, uso ou acesso não autorizado a dados pessoais e dados pessoais sensíveis. Esses incidentes podem ser causados por: ações maliciosas, ataques cibernéticos ou furto de dispositivos de armazenamento. Também podem ser causados por eventos não intencionais, como erros humanos ou falhas de sistema. Tais ocorrências podem representar riscos significativos para os direitos e liberdades dos titulares dos dados.

Conforme estipulado no artigo 46 da LGPD, os agentes de tratamento devem implementar medidas de segurança técnicas e administrativas adequadas para proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas. Essas medidas devem ser aplicadas desde a concepção até a execução de produtos ou serviços.

Adicionalmente, a ANPD enfatiza que cabe ao controlador dos dados identificar, tratar e avaliar os riscos associados a incidentes de segurança que possam afetar suas operações de tratamento. Se os agentes de tratamento não cumprirem suas obrigações legais previstas na LGPD, podem enfrentar sanções administrativas ou civis. Uma gestão inadequada ou incorreta de incidentes pode resultar em penalidades.

5. Consequências de um vazamento de dados

Um incidente pode representar um risco ou causar danos significativos aos titulares, especialmente quando envolve dados sensíveis ou indivíduos em situação de vulnerabilidade, como crianças e adolescentes. Os danos podem incluir discriminação, violação de direitos à imagem e reputação, fraudes financeiras e roubo de identidade.

É importante considerar o volume de dados afetados, o número de indivíduos impactados, a boa-fé e as intenções de terceiros que tiveram acesso aos dados após o incidente, além da facilidade de identificação dos titulares por pessoas não autorizadas. Em caso de dúvida sobre a gravidade dos riscos e danos, recomenda-se a comunicação, conforme prevê o artigo 48 da Lei Geral de Proteção de Dados (Lei nº 14.709/2018), que estabelece a obrigação de notificar a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares quando houver risco ou dano relevante.

Nos casos em que um incidente comprometa a segurança dos dados pessoais, devem ser seguidos procedimentos específicos:

1. Avaliação interna do incidente: Coletar informações sobre o impacto do evento, a natureza, categoria e número de titulares afetados, assim como a categoria e quantidade de dados comprometidos. É vital preservar todas as evidências do incidente.

2. Comunicações necessárias: Informar o encarregado da proteção dos dados, a autoridade máxima, o Departamento de Informática , a ANPD e os titulares de dados pessoais sobre a existência do incidente que possa gerar risco ou dano relevante, conforme o artigo 48 da LGPD.

3. Relatório final: Emitir um relatório com todas as informações coletadas, as ações realizadas para tratar o evento e considerações para melhorar o atendimento a incidentes.

Quando a entidade tem conhecimento do incidente, deve ser realizada uma avaliação interna para identificar:

- Vulnerabilidades exploradas: Como acesso não autorizado, roubo de dados, ataques cibernéticos, erros de programação, engenharia social, descartes indevidos e comprometimento de senhas.

- Fonte dos dados: Meios de obtenção dos dados pessoais, como formulários eletrônicos ou não, API, compartilhamento de dados, XML e *cookies*.

- Categoria dos dados pessoais: Dados sensíveis, dados de crianças e adolescentes.

- Extensão do vazamento: Quantificar os titulares e os dados pessoais comprometidos no evento.

- Avaliação do impacto ao titular: Determinar os possíveis impactos que o incidente pode causar aos titulares.

- Avaliação do impacto no serviço: Analisar os efeitos que o incidente pode ter na entidade, como perda de confiabilidade, ações judiciais, danos à imagem, prejuízos em contratos e impacto nas atividades desenvolvidas.

É fundamental preservar o máximo de evidências do incidente e das medidas adotadas a partir do seu conhecimento, para demonstrar a cadeia de diligências realizadas a autoridades que possam investigar o ocorrido.

É essencial documentar todos os passos desde o início da atuação até a contenção do incidente e seus efeitos. Isso abrange:

- *Logs* de sistemas internos e externos envolvidos;
- Interações da equipe e medidas adotadas;
- Contratações de ferramentas e especialistas para o tratamento do incidente;
- Atas de reuniões relevantes.

As informações da avaliação preliminar podem ser atualizadas conforme o tratamento do incidente avança.

5.1. Relatório de impacto à proteção de dados pessoais (RIPD)

O Relatório de impacto à proteção de dados (RIPD) poderá ser solicitado nas seguintes situações:

1. **Tratamento de dados pessoais para fins específicos**:
   - **Segurança pública**: O RIPD pode ser solicitado quando o tratamento de dados pessoais é realizado com o objetivo de garantir a segurança da sociedade, como ações de policiamento, vigilância e prevenção de crimes.
   - **Investigação e repressão de infrações penais**: Quando os dados pessoais são utilizados em investigações criminais ou para a repressão de delitos, o RIPD se torna essencial para avaliar os riscos à privacidade dos envolvidos. Isso está de acordo com as exceções previstas no inciso III do art. 4º da LGPD, que reconhece a relevância da proteção de dados em contextos que envolvem a segurança pública e a ordem pública.
2. **Infrações à LGPD**:
   - O RIPD também pode ser solicitado em casos em que há indícios de infração à LGPD resultante do tratamento de dados pessoais por órgãos públicos. Esta solicitação é fundamentada nos artigos 31 e 32 da LGPD, que tratam da responsabilização de órgãos e entidades públicas. A análise do RIPD permitirá identificar se as medidas de segurança e proteção de dados estão sendo adequadas e se os direitos dos titulares estão sendo respeitados. Nesse contexto, o RIPD ajuda a entender a gravidade da infração e a necessidade de medidas corretivas.
3. **Determinação da ANPD**:
   - A ANPD tem a autoridade para requisitar o RIPD a qualquer momento, conforme estabelecido no art. 38 da LGPD. Essa solicitação pode ocorrer em resposta a incidentes de segurança, denúncias ou reclamações de titulares de dados, ou durante auditorias e investigações em andamento. A ANPD pode usar o RIPD como ferramenta para avaliar o impacto de incidentes na proteção de dados

pessoais e para assegurar que os responsáveis pelo tratamento estejam em conformidade com a legislação.

6. Comunicar às autoridades responsáveis

A notificação ao Encarregado de Dados sobre qualquer possível incidente de segurança envolvendo dados pessoais deve ser realizada o mais rápido possível, através do e-mail institucional. Essa medida é crucial para que sejam tomadas as providências necessárias.

O Encarregado da proteção de dados deve, com base nas informações coletadas internamente e nos critérios estabelecidos pelo órgão, pela ANPD, ou em conformidade com boas práticas, avaliar a necessidade e a profundidade da comunicação com a ANPD e com os titulares de dados. É essencial que a LGPD e outros normativos infralegais vigentes sobre proteção de dados pessoais sejam sempre consultados para orientar essa avaliação.

Além disso, o Encarregado da Proteção de Dados deve notificar a ANPD e os titulares de dados. Ele deve proceder com cautela ao avaliar a relevância dos riscos e danos associados ao incidente. Em caso de dúvida, a comunicação do incidente deve ser feita de forma rápida.

De acordo com o art. 48 da LGPD, é obrigação do Encarregado informar à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares sobre a ocorrência de qualquer incidente de segurança que possa acarretar risco ou dano significativo. Em situações excepcionais, o operador pode comunicar o incidente, que será analisado pela autoridade de proteção de dados.

7. Emissão do relatório final de incidente

É fundamental que todas as informações e evidências coletadas, assim como as ações realizadas durante o tratamento de um incidente de segurança relacionado à proteção de dados, sejam minuciosamente documentadas. Essa documentação é essencial para a elaboração de um relatório final que compile todos os aspectos do incidente.

O relatório deve atender aos seguintes requisitos:

1. **Considerações para melhoria contínua**: O documento deve incluir recomendações e observações que promovam a melhoria contínua dos processos de tratamento de incidentes, visando otimizar a resposta e prevenir futuros incidentes.

2. **Disponibilidade para consulta**: O relatório deve estar acessível para consultas futuras, especialmente no contexto de elaboração e atualização do Relatório de Impacto à Proteção de Dados (RIPD). Essa acessibilidade garante que as lições aprendidas e as medidas implementadas sejam incorporadas ao processo contínuo de gestão de dados.

A Autoridade Nacional de Proteção de Dados (ANPD) pode solicitar este relatório para diversas finalidades, incluindo:

- **Avaliação das ações tomadas**: A ANPD utilizará o relatório para avaliar as medidas adotadas durante um incidente em que dados pessoais foram expostos ou comprometidos, garantindo que as respostas estejam em conformidade com as exigências legais.
- **Publicação e atualização de normas**: As informações contidas no relatório poderão servir de base para a ANPD na formulação e atualização de normas relacionadas à proteção de dados, contribuindo para a evolução das práticas de segurança.
- **Cumprimento do princípio da responsabilização**: Conforme estabelece o art. 6º, inciso X da LGPD, o relatório é uma ferramenta que reforça o princípio da responsabilização, demonstrando que a entidade adotou medidas adequadas para proteger os dados pessoais.

- **Subsídio para Questionamentos**: O relatório pode ser utilizado como evidência em eventuais questionamentos, facilitando a comprovação de conformidade com a legislação e as políticas de proteção de dados.

A elaboração e a manutenção deste relatório são cruciais não apenas para a conformidade legal, mas também para a construção de uma cultura de proteção de dados dentro da organização, promovendo a confiança dos titulares e a integridade dos processos de tratamento de dados pessoais.

8. Canais de Comunicação

Os canais abaixo de contato poderão ser utilizados no processo de comunicação de incidentes:

ANPD
formulário de comunicação de incidentes disponível no link:
https:/www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca

Encarregado da Proteção de Dados
e-mail para: paulo.controladoria@barretos.sp.gov.br

Controladoria Geral do Município
e-mail: lgpd@barretos.sp.gov.br