ICMBio
INSTITUTO CHICO MENDES
MMA

2025

PLANO DE RESPOSTA A

INCIDENTES COM DADOS PESSOAIS

EXPEDIENTE

Presidente do Instituto Chico Mendes de Conservação da Biodiversidade

Mauro Oliveira Pires

Chefe de Gabinete

Thais Ferraresi Pereirta

Encarregada pelo Tratamento de Dados Pessoais

Vanessa Simas Figueiredo

Encarregado Substituto pelo Tratamento de Dados Pessoais

Rafael Barbosa Chagas

Colaboração:

Gestor de Segurança da Informação - CGTI/DIPLAN/ICMBio

Mateus Sônego

Elaboração/Capa/Diagramação

Vanessa Simas Figueiredo

Revisão

Rafael Barbosa Chagas

Freida Freitas

SUMÁRIO

1. INTRODUÇÃO

Desde 2018, a Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD) – estabelece regras para o tratamento de dados pessoais e determina que os agentes de tratamento garantam sua segurança, inclusive após o encerramento do uso, prevenindo acessos não autorizados, perdas e tratamentos inadequados.

Com a Emenda Constitucional nº 115/2022, a proteção de dados pessoais tornou-se um direito fundamental, reforçando a importância de práticas seguras e responsáveis. Nesse contexto, a Autoridade Nacional de Proteção de Dados (ANPD) define diretrizes e procedimentos para prevenir, responder e mitigar riscos decorrentes de incidentes de segurança, conforme procedimentos específicos previstos na Resolução CD/ANPD nº 15, de 24 de abril de 2024, que aprova o Regulamento de Comunicação de Incidente de Segurança.

A ANPD considera incidente de segurança qualquer evento que envolva violação de dados pessoais — como vazamento, perda, alteração ou acesso indevido — e que possa gerar riscos aos direitos dos titulares.

Mais do que soluções tecnológicas, a proteção de dados exige governança, planejamento e procedimentos claros, bem como revisão contínua de práticas e fortalecimento da cultura institucional de segurança da informação.

Diante do volume e da natureza sensível dos dados tratados, é essencial que o Instituto Chico Mendes de Conservação da Biodiversidade – ICMBio disponha de um Plano de Resposta a Incidentes de Segurança de Dados Pessoais – PRI, que oriente a atuação diante de situações de risco, como ataques cibernéticos ou vazamentos.

Por meio deste Plano, o Instituto reafirma seu compromisso com a segurança da informação e com a proteção dos direitos dos titulares de dados pessoais. A adoção de um PRI de Dados Pessoais estruturado não apenas assegura a conformidade com a LGPD, como também fortalece a confiança da sociedade, de parceiros institucionais e dos próprios servidores, evidenciando que o Instituto está preparado para agir de forma responsável, eficiente e transparente diante de eventuais incidentes.

Proteger dados pessoais é, portanto, uma responsabilidade compartilhada, essencial para a confiança e integridade nas relações entre o poder público e a sociedade.

2. O PLANO

O Plano de Resposta a Incidentes de Segurança de Dados Pessoais tem como objetivo orientar a atuação do Instituto Chico Mendes diante de situações que envolvam risco ou violação de dados pessoais sob sua responsabilidade.

Trata-se de um instrumento estratégico que estabelece diretrizes para uma resposta rápida, adequada e transparente em casos como vazamentos de informações, acessos indevidos ou outros incidentes que possam comprometer a segurança dos dados.

A elaboração deste Plano busca prevenir danos, reduzir riscos e garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD), preparando servidores e colaboradores para agir corretamente e de forma coordenada em eventuais emergências.

O documento descreve as funções, responsabilidades e medidas preventivas e corretivas a serem adotadas, tanto individual quanto coletivamente, no tratamento de dados pessoais realizado pelo ICMBio.

Em consonância com a Política de Segurança da Informação do Instituto, com o art. 48 da LGPD e com o Regulamento de Comunicação de Incidente de Segurança — instituído pela Resolução CD/ANPD nº 15, de 24 de abril de 2024 —, o Plano consolida as práticas e orientações necessárias para assegurar a proteção e a governança dos dados pessoais.

Apresentado pela Ouvidoria do ICMBio, setor responsável pelo tratamento de dados pessoais no âmbito institucional, o Plano é destinado ao conhecimento e à aplicação por todos os servidores, terceirizados e colaboradores. Sua vigência é indeterminada, podendo ser revisado periodicamente ou sempre que houver necessidade de atualização.

Em caso de incidentes ou ameaças aos ativos tecnológicos do Instituto, o Plano define procedimentos de resposta e comunicação, incluindo, quando aplicável, a notificação tempestiva à Autoridade Nacional de Proteção de Dados (ANPD), assegurando a atuação responsável e a preservação da integridade institucional.

3. ATORES E RESPONSABILIDADES

A definição clara de papéis e responsabilidades é essencial para assegurar a eficiência e a eficácia na gestão de incidentes de segurança da informação. Cada participante deve atuar de forma coordenada e alinhada às suas competências e atribuições, possibilitando uma resposta rápida, estruturada e integrada diante de situações críticas.

NOTIFICADOR

Pessoa ou sistema de monitoramento que notifica o incidente.

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 ICMBio, essa atribuição é exercida pela autoridade máxima da Autarquia.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS OU ANPD

É a autarquia de natureza especial responsável por fiscalizar e zelar pelo cumprimento da Lei Geral de Proteção de Dados em todo o território brasileiro.

GESTOR DA BASE DE DADOS OU À EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS (ETIR)

Unidade(s) organizacional(is) do ICMBio responsável(is) pelo processo/sistema que originou o incidente com dados pessoais.

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

É a pessoa designada pelo controlador para ser responsável por assegurar o cumprimento da legislação aplicável, além de atuar como contato para os titulares dos dados e para a Autoridade Nacional de Proteção de Dados Pessoais (ANPD). É responsável também por avaliar se há dano ou risco relevante a titular de dados pessoais e encaminhar comunicações formais de incidentes envolvendo dados pessoais. No ICMBio, essa atribuição é exercida pelos titulares da Ouvidoria.

4. INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

DEFINIÇÃO:

Trata-se de qualquer situação que coloque em risco a segurança dos dados pessoais, comprometendo os princípios de confidencialidade, integridade, disponibilidade ou autenticidade dessas informações.

Esses incidentes podem resultar de ações intencionais ou acidentais que levem à divulgação, alteração, perda ou acesso não autorizado aos dados pessoais, independente do meio em que estejam armazenados — físico ou digital.

Alguns exemplos de incidentes de segurança:

I. Violação de dados: acesso não autorizado a informações confidenciais (a exemplo de processos disciplinares, relatórios de auditoria, questões de Estado) que contenham dados pessoais ou dados pessoas sensíveis;

II. Vazamento de dados pessoais: divulgação não autorizada, por meios físicos ou digitais, de dados pessoais ou dados pessoais sensíveis;

III. Erros humanos: ações não intencionais que resultam em violações de segurança, como envio de documentos com dados pessoais/sensíveis para destinatários errados, publicação não proposital de dados pessoais de titulares;

IV. Ataques cibernéticos: incluindo malware, *ransomware* (sequestro de dados), ataques de *phishing* e engenharia social;

V. Negação de serviço: é uma tentativa maliciosa de sobrecarregar um servidor, rede ou serviço *online* com um volume excessivo de tráfego, impedindo que usuários legítimos acessem esses recursos. Os ataques são realizados por meio de uma rede de computadores comprometidos chamados de "*bots*" ou "zumbis", que são controlados remotamente por um invasor, objetivando tornar o serviço inacessível, causando prejuízo financeiros e de reputação para a vítima;

VI. Acesso físico ou lógico prejudicado ou impossibilitado: com relação ao sistema que armazena dados pessoais, comprometendo a integridade dos mesmos permanentemente;

VII. Intrusões de rede: acesso não autorizado a sistemas ou redes internas por meio de exploração de vulnerabilidades ou falhas de segurança;

VIII. Acesso não autorizado: tentativas de acesso físico ou lógico a sistemas que possuam dados pessoais ou dados pessoais sensíveis sem permissão adequada;

IX. Uso inapropriado: violação das Políticas de uso de dados, incluindo a Política de Segurança da Informação e a de Privacidade; e

X. Exploração de vulnerabilidades: aproveitamento de falhas de segurança em software, sistemas ou infraestrutura para obter acesso não autorizado a dados pessoais ou dados pessoais sensíveis.

ENTENDA:

O artigo 46 da Lei Geral de Proteção de Dados Pessoais (LGPD), determina que os agentes de tratamento (Controlador e o Operador) devem adotar medidas de segurança aptas a proteger os dados pessoais em todas as etapas do tratamento, desde a concepção até a execução das atividades.

Além disso, o artigo 50 da mesma lei prevê que controladores e operadores podem estabelecer regras de boas práticas e de governança voltadas ao tratamento de dados pessoais, incluindo a implementação de programas de governança e privacidade que contemplem planos de resposta a incidentes e ações de remediação.

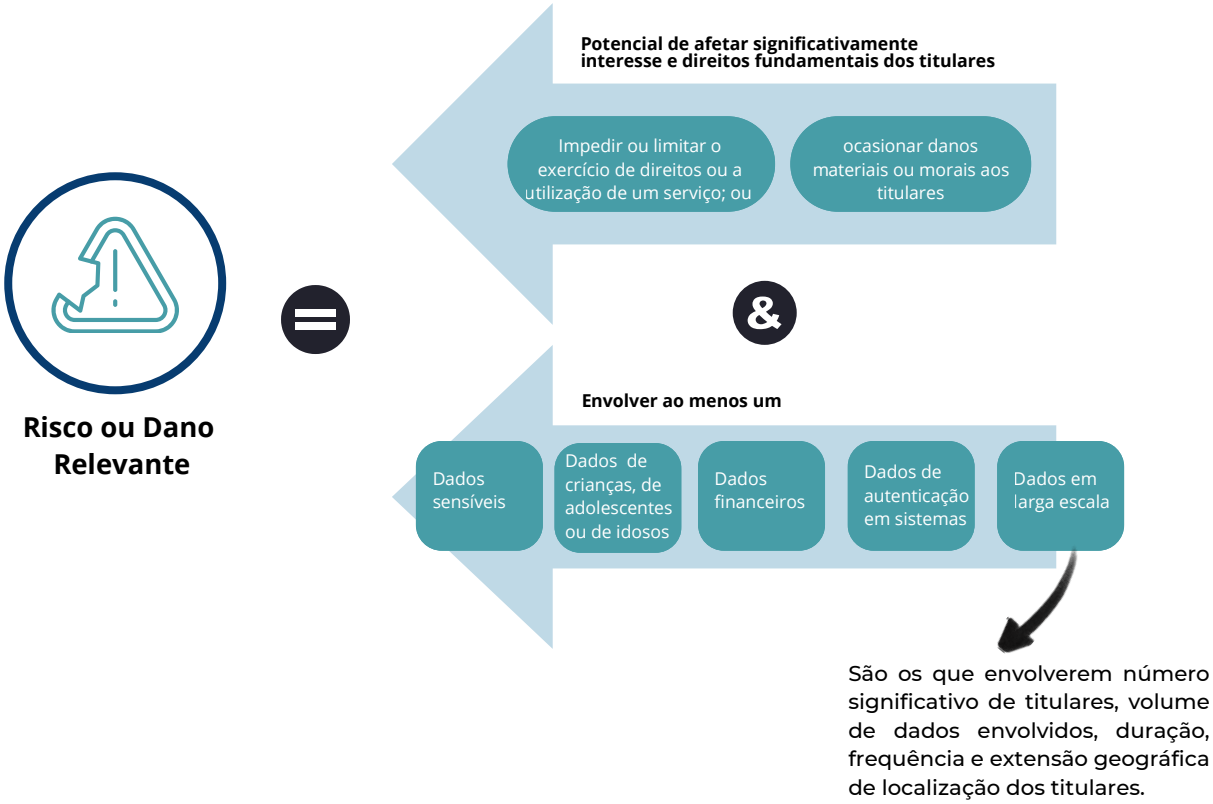
5. NEM TODO INCIDENTE DE SEGURANÇA DEVE SER COMUNICADO

Compete ao controlador, com o auxílio da avaliação do encarregado, decidir sobre os riscos e impactos do incidente aos titulares e a necessidade de efetuar a comunicação. Dessa forma, é essencial que, antes de proceder à comunicação, o controlador realize uma análise conforme o art. 5º da Resolução CD/ANPD nº 15/2024, que esclarece o conceito de risco e de dano relevante aos titulares, ao estabelecer que:

> "O incidente de segurança pode acarretar risco ou dano relevante aos titulares quando puder afetar significativamente interesses e direitos fundamentais dos titulares e, cumulativamente, envolver, pelo menos, um dos seguintes critérios: dados pessoais sensíveis; dados de crianças, de adolescentes ou de idosos; dados financeiros; dados de autenticação em sistemas; dados protegidos por sigilo legal, judicial ou profissional; ou dados em larga escala".

Um incidente precisa ser comunicado se atender, cumulativamente, aos seguintes critérios:

5.1. O QUE É CONSIDERADO UM RISCO OU DANO RELEVANTE?



ENTENDA:

Nem todo incidente de segurança da informação envolve dados pessoais. Incidentes que envolvam somente dados anonimizados ou que não estejam relacionados a pessoas naturais identificadas ou identificáveis não precisam ser comunicados à ANPD.

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.

5.2. O QUE DEVE SER CONSIDERADO NA AVALIÇÃO DE RISCO DE UM INCIDENTE COM DADOS PESSOAIS?

Na avaliação de risco de um incidente, devem ser considerados, entre outros aspectos:

- o contexto da atividade de tratamento dos dados;
- as categorias e o número de titulares afetados;
- a natureza, as categorias e a quantidade de dados pessoais violados;
- os potenciais danos materiais, morais ou reputacionais aos titulares;
- se os dados violados estavam protegidos de forma a impedir a identificação dos titulares; e
- as medidas de mitigação adotadas pelo controlador após a ocorrência do incidente.

Um mesmo tipo de incidente pode ou não ser considerado capaz de gerar risco ou dano relevante, a depender da combinação desses fatores.

Por exemplo, o roubo de um dispositivo eletrônico pode representar, ou não, um risco significativo aos titulares, conforme o tipo de dado armazenado, o contexto da atividade de tratamento e o nível de proteção aplicado, como o uso de criptografia.

São considerados incidentes com potencial de causar risco ou dano relevante aqueles que possam acarretar prejuízos materiais ou morais aos titulares, expô-los a situações de discriminação ou possibilitar o roubo de identidade — especialmente quando envolverem dados sensíveis, tratados em larga escala ou pertencentes a grupos vulneráveis, como crianças, adolescentes ou pessoas idosas.

6. PROCESSO DE NOTIFICAÇÃO E TRATAMENTO DO INCIDENTE

Em caso de suspeita de incidente que coloque em risco a segurança de dados pessoais, devem ser realizados alguns procedimentos específicos.

6.1. NOTIFICAÇÃO DO INCIDENTE

Qualquer pessoa, de dentro ou de fora do Instituto Chico Mendes, que identifique ou suspeite da ocorrência do incidente envolvendo dados pessoais poderá comunicar ao Encarregado pelo Tratamento de Dados Pessoais, por meio de:

- Formulário de Comunicação de Incidentes de Segurança e Vazamento de Dados Pessoais, disponível no SEI do ICMBio, com encaminhamento para a Ouvidoria;
- E-mail do Encarregado de Dados: lgpd@icmbio.gov.br; ou
- Plataforma Fala.BR (https://falabr.cgu.gov.br/web/home): Reclamação/ Denúncia.

Incidentes de vazamento de dados pessoais que envolvam infraestrutura de TI devem ser comunicados, simultaneamente, à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), por meio do e-mail etir@icmbio.gov.br.

Nos casos de notificações realizadas por e-mail ou pela Plataforma Fala.BR, o comunicante deverá preencher e anexar o Formulário de Comunicação de Incidentes de Segurança e Vazamento de Dados Pessoais constante no Portal do ICMBio, aba Lei Geral de Proteção de Dados Pessoais, disponível no link (https://www.gov.br/icmbio/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-lgpd). Consulte o modelo do Formulário de Comunicação no anexo deste Plano, página 30.

ENTENDA:

O notificante deve fornecer informações completas para que a demanda seja analisada. Caso os dados sejam insuficientes, incoerentes ou pouco claros, ele será solicitado a apresentar esclarecimentos ou documentos complementares. A Ouvidoria (unidade responsável por garantir a conformidade do ICMBio com a LGPD) também poderá entrevistá-lo para obter mais detalhes.

6.2. ANÁLISE PRÉVIA

Após o recebimento da notificação do incidente, o encarregado de dados deverá:

- criar um processo sigiloso no Sistema Eletrônico de Informações (SEI), contendo, caso haja, o Formulário de Comunicação de Incidentes de Segurança e Vazamento de Dados Pessoais preenchido;
- encaminhar o processo ao Gestor da Base de Dados ou à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), caso envolva infraestrutura de TI, como base de dados de sistemas computacionais; e
- Comunicar o Gestor da Base de Dados ou a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) sobre o envio do processo no SEI, indicando a necessidade de tratamento urgente.

Na análise prévia, o Gestor da Base de Dados ou a ETIR realiza uma avaliação interna para que sejam obtidas informações como:

a. Qual vulnerabilidade foi explorada no evento, abrangendo situações como: acesso indevido aos dados pessoais; roubo de dados; ataques cibernéticos; erros de programação de aplicativos e sistemas internos; engenharia social; descartes indevidos; repasse de dados pessoais; roubo, venda e utilização de dados tutelados pela entidade; comprometimento de senhas de acesso; e outras.

b. Fonte dos dados pessoais: meio pelo qual foram obtidos os dados pessoais, tais como preenchimento de formulário eletrônico ou não eletrônico por parte do titular, API, uso compartilhado de dados, XML e cookies.

c. Categoria dos dados: os tipos de dados foram comprometidos (ex: dados sensíveis, dados de crianças, dados financeiros).

d. Extensão do vazamento: quantificar os titulares e os dados pessoais que tiveram a sua segurança violada neste evento.

e. Avaliação do impacto:

- ao titular: avaliar quais são os efeitos, resultados ou prejuízos que o incidente pode gerar aos titulares.
- no serviço: avaliar os impactos que o incidente pode gerar à entidade como perda de confiabilidade do cidadão, ações judiciais, danos à imagem da instituição em âmbito nacional e internacional, prejuízo à entidade em contratos com fornecedores e clientes, e impacto total ou parcial nas atividades desenvolvidas pela entidade.

Devem ser preservados o máximo de evidências do incidente e de todas as medidas adotadas a partir da sua ciência, a fim de que se demonstre, para eventuais autoridades que posteriormente vierem a apurar os fatos, toda a cadeia de diligências realizadas para entendimento do evento e mitigação dos seus efeitos.

Nesse cenário, todos os passos devem ser devidamente documentados no Relatório de Tratamento de Incidentes (preliminar), desde o momento inicial de atuação até a contenção e os efeitos.

Caso o incidente não seja confirmado, o processo é encerrado com a respectiva comunicação ao notificador do incidente.

ENTENDA:

Imediatamente após o conhecimento do incidente, a ETIR ou o Gestor da Base de Dados deverá iniciar as medidas de segurança necessárias para conter e erradicar o incidente.

6.3. RELATÓRIO DE IMPACTO

Em seguida, o Gestor da Base de Dados ou a ETIR, juntamente com o encarregado pelo tratamento de dados pessoais, 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 ICMBio evolua em relação às boas práticas de governança em privacidade.

Conforme o art. 8º da Resolução CD/ANPD nº 15/2024, a ANPD pode solicitar, a qualquer tempo, o RIPD e/ou o Relatório de Tratamento do Incidente com as informações adicionais, referentes ao incidente de segurança, inclusive com o registro das operações de tratamento dos dados pessoais afetados pelo incidente.

6.4. PROCEDIMENTOS DE COMUNICAÇÕES DO INCIDENTE

Concluida a análise prévia e definido que o incidente pode acarretar risco ou dano relevante aos titulares de dados pessoais, deverão ser realizadas as **comunicações obrigatórias por Lei.**

1 AO ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

O Gestor da Base de Dados ou a ETIR encaminha o Relatório de Tratamento de Incidente, mesmo que em fase preliminar, para conhecimento do encarregado, **o mais breve possível**, para as providências previstas na LGPD sobre comunicação de incidentes de segurança.

2 AO CONTROLADOR

O encarregado deve comunicar o incidente com dados pessoais ao Controlador **o mais breve possível**, a fim de viabilizar que este exerça o seu papel tempestivamente. A comunicação deve ocorrer mesmo nos casos em que houver dúvidas sobre a relevância dos riscos e danos envolvidos.

3 À ANPD

O Encarregado comunica à ANPD, com a anuência da autoridade máxima da instituição, a existência do incidente e encaminha o relatório inicial, no prazo de **três dias úteis** contados do conhecimento pelo controlador.

Quando o incidente atender aos critérios cumulativos para comunicação à ANPD, o Encarregado, com o apoio do Gestor da Base de Dados ou da ETIR, deverá preencher o Requerimento relacionado à LGPD, disponível no sítio eletrônico da ANPD (https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/denuncia-peticao-de-titular).

A comunicação de incidente de segurança deverá conter as seguintes informações, conforme o § 2°do art. 6° da Resolução CD/ANPD n° 15/2024:

I - a descrição da natureza e da categoria de dados pessoais afetados;
II - o número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;
III - as medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, adotadas antes e após o incidente, observados os segredos comercial e industrial;
IV - os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;
V - os motivos da demora, no caso de a comunicação não ter sido realizada no prazo previsto no caput deste artigo;
VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;
VII - a data da ocorrência do incidente, quando possível determina-la, e a de seu conhecimento pelo controlador;
VIII - os dados do encarregado ou de quem represente o controlador;
IX - a identificação do controlador e, se for o caso, declaração de que se trata de agente de tratamento de pequeno porte;
X - a identificação do operador, quando aplicável;
XI - a descrição do incidente, incluindo a causa principal, caso seja possível identificá-la; e
XII - o total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente.

ENTENDA:

Conforme o § 5º do artigo 6º da Resolução CD/ANPD nº 15/2024, o responsável por comunicar um incidente de segurança à ANPD é o controlador dos dados, que pode agir por meio de seu **encarregado de tratamento de dados pessoais** ou outro representante legalmente constituído.

A comunicação deve ocorrer em até **três dias úteis após o controlador tomar conhecimento do incidente** que possa gerar risco ou dano relevante aos titulares.

A ANPD esclarece que, caso não seja possível disponibilizar todas as informações no momento da comunicação preliminar, será admitido o **envio de complementações** posteriormente, no prazo de **vinte dias úteis**, a contar da data da comunicação.

Entretanto, nessa fase inicial, o Encarregado deverá informar à ANPD se haverá fornecimento futuro de novos elementos, bem como os meios utilizados para sua obtenção.

A ANPD poderá, ainda, solicitar informações adicionais a qualquer momento, conforme a necessidade de apuração do incidente.

4 AOS TITULARES DE DADOS

Nos termos da LGPD, cabe ao controlador comunicar aos titulares de dados pessoais, no prazo de **três dias úteis contados do conhecimento pelo controlador** de que o incidente afetou dados pessoais, a ocorrência de incidente que possa lhes acarretar riscos ou danos relevantes.

Essa comunicação deve ser redigida em linguagem clara e acessível e incluir, sempre que aplicável, os elementos previstos no art. 9º da Resolução CD/ANPD nº 15/2024, tais como:

> I - a descrição da natureza e da categoria de dados pessoais afetados;
> II - as medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
> III - os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;
> IV - os motivos da demora, no caso de a comunicação não ter sido feita no prazo do caput deste artigo;
> V - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis;
> VI - a data do conhecimento do incidente de segurança; e
> VII - o contato para obtenção de informações e, quando aplicável, os dados de contato do encarregado.

A comunicação deve ser realizada, sempre que possível, de forma individual e direta aos titulares, utilizando-se meios como telefone, e-mail, mensagem eletrônica ou correspondência.

Quando, em razão da natureza do incidente, não for possível identificar individualmente os titulares afetados, a notificação deverá ser estendida a todos os titulares cujos dados constem na base comprometida. Nesses casos, a divulgação deverá ocorrer por meio do sítio eletrônico institucional, aplicativos, mídias sociais e demais canais de atendimento ao titular, de forma a assegurar ampla divulgação e fácil visualização, pelo período mínimo de três meses.

Por fim, o controlador deverá anexar ao processo de comunicação do incidente uma declaração que comprove a realização da comunicação aos titulares, informando os meios utilizados para sua divulgação. Essa declaração deverá ser apresentada no prazo máximo de **três dias úteis após o envio das comunicações aos titulares**.

7. RELATÓRIO FINAL DO INCIDENTE

Após a coleta de todas as informações e evidências, o Encarregado, com o apoio do Gestor da Base de Dados ou da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), deverá concluir o Relatório Final do Incidente.

Esse relatório será produzido com base em todas as evidências reunidas desde a identificação até a conclusão das apurações, contendo a descrição detalhada do incidente, as medidas adotadas durante o processo de resposta e as propostas de aprimoramento ou aquisições necessárias para reduzir o risco de novas ocorrências.

Além de servir como comprovação formal das ações implementadas pelo ICMBio perante as autoridades competentes, o relatório tem também caráter educativo e preventivo, permitindo que servidores e equipes envolvidas analisem as causas do incidente, avaliem a efetividade dos procedimentos adotados e identifiquem oportunidades de melhoria no Plano de Resposta a Incidentes.

O Relatório Final do Incidente deverá ser assinado pelo Encarregado e mantido disponível para consulta, especialmente em casos de atualização do Relatório de Impacto à Proteção de Dados (RIPD). Quando necessário, poderá ainda ser apresentado a autoridades policiais, órgãos reguladores ou demais partes interessadas.

8. REGISTRAR INCIDENTE DE SEGURANÇA

É indispensável que o controlador mantenha o registro detalhado das informações relativas ao incidente de segurança, ainda que o incidente não tenha sido comunicado à ANPD ou aos titulares. Tais informações deverão ser preservadas por, no mínimo, **cinco anos**, contados a partir da data do registro, salvo se houver obrigações adicionais que demandem um prazo maior de manutenção.

Tal registro deverá conter minimamente os seguintes itens:

I. a data de conhecimento do incidente;
II. a descrição geral das circunstâncias em que o incidente ocorreu;
III. a natureza e a categoria de dados afetados;
IV. o número de titulares afetados;
V. a avaliação do risco e os possíveis danos aos titulares;
VI. as medidas de correção e mitigação dos efeitos do incidente, quando aplicável;
VII. a forma e o conteúdo da comunicação, se o incidente tiver sido comunicado; e
VIII. os motivos da ausência de comunicação, quando for o caso.

9. REVISÃO DO PLANO

A atualização do Plano de Resposta a Incidentes de Segurança de Dados Pessoais será realizada a cada 2 (dois) anos, ou em prazo inferior quando houver mudanças relevantes nos processos, tecnologias ou na legislação aplicável. O objetivo é assegurar a manutenção da eficácia do plano e seu alinhamento contínuo com a realidade institucional e com o cenário atualizado de riscos cibernéticos.

A revisão periódica bienal é fundamental para incorporar lições aprendidas de incidentes anteriores, adequar procedimentos às novas ameaças e vulnerabilidades, bem como garantir conformidade com a legislação vigente, em especial a Lei nº 13.709/2018 (LGPD), que determina a adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais e exige respostas tempestivas, transparentes e registradas em caso de incidente de segurança.

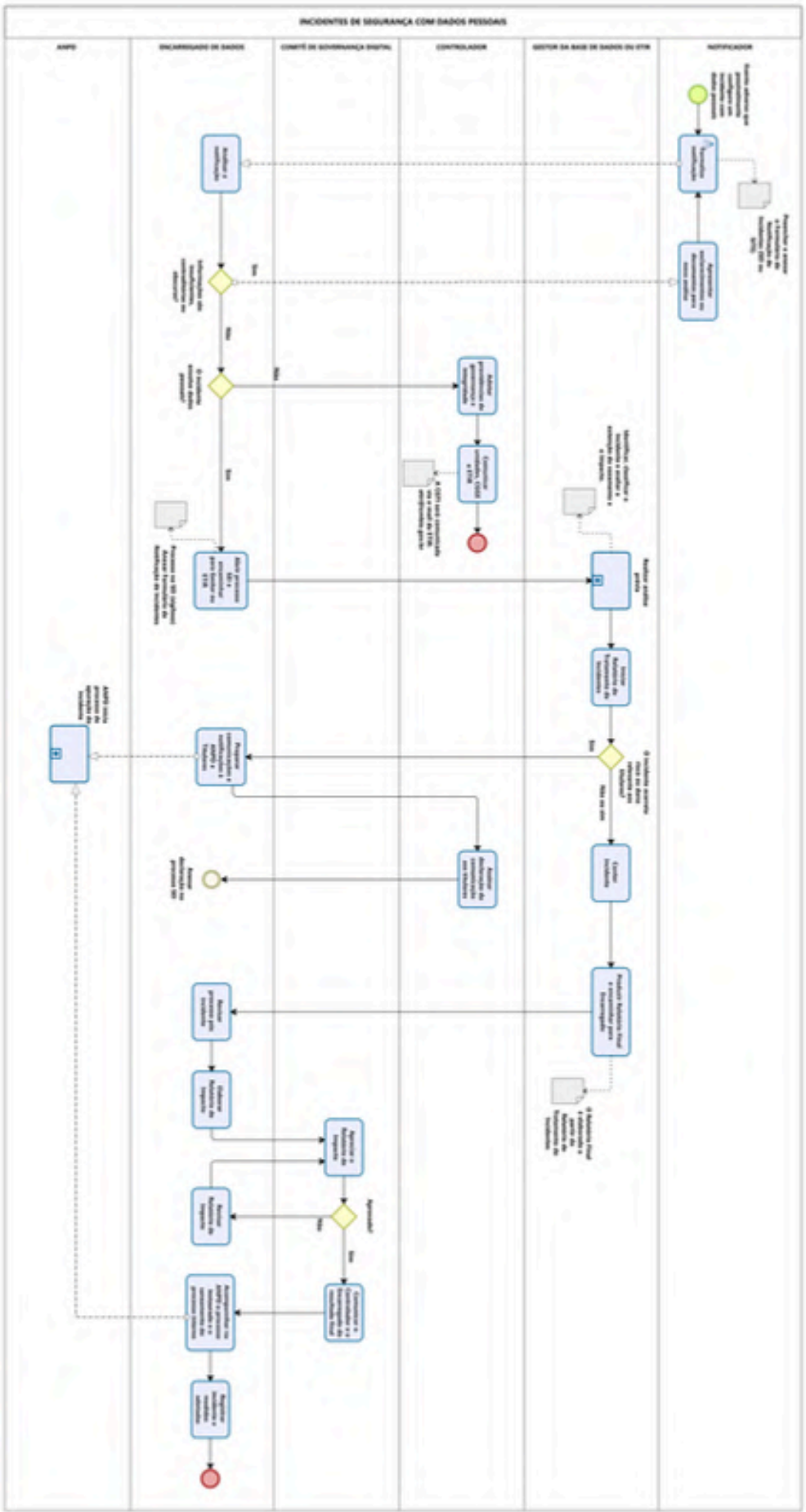
Além disso, a atualização regular possibilita ajustar o plano às eventuais alterações na infraestrutura de TI, na estrutura organizacional, nos processos de trabalho e nas responsabilidades das equipes envolvidas, de modo a assegurar clareza de papéis, coordenação eficiente e mitigação de impactos financeiros, operacionais, reputacionais e, sobretudo, sobre os titulares dos dados pessoais.

10. PRAZOS

Considerando que a ANPD estabelece o prazo de **três dias úteis** para a comunicação de incidentes envolvendo dados pessoais, os demais prazos necessários ao cumprimento dessa determinação estão dispostos na Tabela 1.

Ação	Prazo	Responsável
Reportar o incidente ao encarregado	**Imediato**	Notificador
Ações necessárias para comunicar à ANPD via peticionamento eletrônico por meio do sistema SEI! da ANPD	**até 3 (três) dias úteis a partir da ciência do incidente**	Encarregado, com apoio do Gestor e da ETIR
Encaminhamento de informações complementares à ANPD	**20 (vinte) dias úteis, a contar da data da comunicação**	Encarregado, com apoio do Gestor e da ETIR
Comunicar aos Titulares de Dados	**3 (três) dias úteis contados do conhecimento pelo controlador**	Controlador
Assinar declaração que comprove a realização da comunicação aos titulares	**3 (três) dias úteis, após comunicação aos titulares**	Controlador
Mantenha o registro detalhado das informações relativas ao incidente de segurança	**5 (cinco) anos, contado a partir da data do registro**	Controlador

11. FLUXO DO PROCESSO



12. GLOSSÁRIO

Definições extraídas da Resolução CD/ANPD nº 15, de 24 de abril de 2024, e do Guia de Avaliação de Riscos de Segurança e Privacidade da Controladoria-Geral da União (2021).

Acesso indevido a dados pessoais: entrada irregular em ambiente físico ou lógico. Agentes de tratamento: o(a) Controlador(a) e o Operador.

Ampla divulgação do incidente em meios de comunicação: providência que pode ser determinada pela ANPD ao(à) controlador(a), nos termos do art. 48, § 2º, I, da LGPD, no processo de comunicação de incidente de segurança, como a publicação no sítio eletrônico, nas redes sociais do(a) Controlador(a) ou em outros meios de comunicação.

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, que impossibilitem associar, direta ou indiretamente, a um indivíduo.

ANPD: Autoridade Nacional de Proteção de Dados, uma autarquia de natureza especial, responsável por zelar, implementar e fiscalizar o cumprimento da legislação de proteção de dados pessoais em território nacional.

Ataque cibernético: esforço intencional para tirar proveito das vulnerabilidades, com execução de ações maliciosas, visando roubar, expor, alterar ou destruir dados, por meio de acesso não autorizado a redes, sistemas de computador ou dispositivos digitais.

Autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.

Bot: um *bot* ou *botnet*, no contexto *hacker*, é um programa de computador utilizado para automatizar atividades maliciosas, como ataques cibernéticos, disseminação de spam, propagação de malware, ataques de negação de serviço distribuído (DDoS) ou roubo de dados.

Categoria de dados pessoais: classificação dos dados pessoais de acordo com o contexto e a utilização, como dados de identificação pessoal, dados de autenticação em sistemas, dados financeiros.

Comprometimento de senha: credenciais de acesso (login e senha de acesso pessoal) expostas a terceiros.

Comunicação de incidente de segurança: ato do(a) Controlador(a) que comunica à ANPD e ao titular de dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Confidencialidade: propriedade pela qual se assegura que o dado pessoal não esteja disponível ou não seja revelado a pessoas, empresas, sistemas, órgãos ou entidades não autorizados.

Controlador(a): pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Dado de autenticação em sistemas: qualquer dado pessoal utilizado como credencial para determinar o acesso a um sistema ou para confirmar a identificação de um usuário, como contas de login, tokens e senhas.

Dado financeiro: dado pessoal relacionado às transações financeiras do titular, inclusive para contratação de serviços e aquisição de produtos.

Dado pessoal: qualquer informação relativa à pessoa natural identificada ou identificável que permita identificar, direta ou indiretamente, um indivíduo, como: nome completo, números de documentos pessoais e profissionais, assinaturas, telefone, endereço, e-mail, dentre outros.

Dado pessoal afetado: dado pessoal cuja confidencialidade, integridade, disponibilidade ou autenticidade tenha sido comprometida em um incidente de segurança.

Dado pessoal sensível: dado pessoal sobre 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.

Dado protegido por sigilo legal ou judicial: dado pessoal cujo sigilo decorra de norma jurídica ou decisão judicial.

Dado protegido por sigilo profissional: dado pessoal cujo sigilo decorra do exercício de função, ministério, ofício ou profissão, cuja revelação possa produzir dano a outrem.

Disponibilidade: propriedade pela qual se assegura que o dado pessoal esteja acessível e utilizável, sob demanda, por uma pessoa natural ou por determinado sistema, órgão ou entidade devidamente autorizados.

Encarregado(a) ou Data Privacy Officer (DPO): pessoa indicada pelo(a) Controlador(a) e pelo Operador para atuar como canal de comunicação entre o(a) Controlador(a), os titulares de dados e a ANPD.

Engenharia Social: técnica utilizada por golpistas para manipular usuários, explorando erros humanos para obter dados pessoais sigilosos, além de induzir o acesso a *links* infectados e/ou espalhar infecções por *malware*.

Falha ou erro de processamento: dados de entrada que não são corretamente validados e/ou operações de tratamento automatizadas de sistema que alteram de maneira indevida a composição do dado armazenado.

Firewall: ato, ameaça ou circunstância que comprometa a confidencialidade, a integridade ou a disponibilidade de dados pessoais e dados pessoais sensíveis, sob custódia da PGE/MS.

Incidente: é um dispositivo de segurança que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.

Incidente de segurança com dados pessoais: evento inadequado, relacionado à violação de dados pessoais, sendo acesso não autorizado, acidental ou não, resultando na perda, alteração, vazamento ou qualquer forma ilícita de tratamento de dados.

Integridade: propriedade pela qual se assegura que o dado pessoal não foi modificado ou destruído de maneira não autorizada ou acidental.

Inventário de Dados Pessoais (IDP): representa um artefato primordial para documentar o tratamento de dados pessoais realizados pela Autarquia.

LGPD: Lei Geral de Proteção de Dados Pessoais nº 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais, em meios físicos e digitais, realizado por pessoa natural ou jurídica de direito público ou privado, com o objetivo de proteger os dados pessoais dos titulares.

Log: processo de registro de eventos relevantes em sistema computacional.

Malware: software malicioso concebido para se infiltrar em dispositivos eletrônicos à revelia do usuário.

Medidas de segurança: medidas técnicas e/ou administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Natureza dos dados pessoais: classificação de dados pessoais em gerais ou sensíveis.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do(a) Controlador(a). O servidor não é operador.

Phishing: ataque cibernético por meio de tentativas de fraude para obter ilegalmente informações como número da identidade, senhas bancárias, número de cartão de crédito, entre outras, por meio de e-mail com conteúdo duvidoso.

Procedimento de apuração de incidente de segurança: procedimento instaurado pela ANPD para apurar a ocorrência de incidente de segurança não comunicado pelo(a) Controlador(a).

Procedimento de comunicação de incidente de segurança: procedimento instaurado pela ANPD após o recebimento de comunicação de incidente de segurança.

Processo de comunicação de incidente de segurança: processo administrativo instaurado pela ANPD do procedimento de apuração incidente de segurança e do procedimento de comunicação de incidente de segurança.

Pseudonimização: tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo(a) Controlador(a) em ambiente controlado e seguro.

Ransomware: é um tipo de malware que sequestra dados confidenciais ou dispositivos da vítima e ameaça mantê-los bloqueados – ou até pior – a menos que a vítima pague um resgate ao invasor.

Relatório de Impacto à Proteção de Dados Pessoais (RIPD): documentação do Controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Relatório final: documento que contém todas as evidências e ações realizadas para tratamento do incidente e que deve ser emitido ao final das tratavas.

Repasse indevido de dados pessoais: instituição não atende sua finalidade legal e compartilha os dados sem consentimento do titular dos dados pessoais.

Roubo de dados pessoais: dados pessoais apropriados irregularmente nas dependências do(a) Controlador(a), falhas nos controles de segurança dos sistemas.

Sistemas: hardware, software, armazenador de mídias e demais recursos computacionais utilizados, desenvolvidos, adquiridos, acessados ou operados pela PGE/MS para apoio na execução de suas atividades.

Titular: pessoa natural a quem se referem os dados pessoais que são objeto do tratamento.

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Vazamento de dados: quebra de sigilo e/ou divulgação de dados, intencional ou não, que resulte em perda, alteração, compartilhamento, acesso, transmissão, armazenamento ou processamento de dados não autorizados.

Violação (privacidade/segurança): conduta e evento que resulte em destruição, perda, roubo, alteração, divulgação dos dados pessoais ou acesso não autorizado, danos ou desvio de finalidade em seu tratamento.

13. BIBLIOGRAFIA

ANPD, Autoridade Nacional de Proteção de Dados. Comunicação de incidente de segurança. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 13 nov. 2025.

ANPD, Autoridade Nacional de Proteção de Dados. Denúncias ou Petições de titular. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/denuncia-peticao-de-titular. Acesso em: 13 nov. 2025.

_____, Autoridade Nacional de Proteção de Dados. Guia Segurança da Informação para agentes de tratamento de pequeno porte. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-sobre-seguranca-da-informacao-para-agentes-de-tratamento-de-pequeno-porte. Acesso em: 13 nov. 2024.

_____, Autoridade Nacional de Proteção de Dados. Resolução da ANPD n° 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: 10 nov. 2025.

_____, Autoridade Nacional de Proteção de Dados. Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_orientativo_tratamento_de_dados_pessoais_pelo_poder_publico. Acesso em: 13 nov. 2025.

BRASIL. Lei n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 nov. 2025.

CERT. Vazamento de dados. Cartilha. Disponível em: https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf. Acesso em: 10 nov. 2025.

GOVBR. Guia de Boas Práticas: Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf. Acesso em: 10 nov. 2025.

14. ANEXO

FORMULÁRIO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA E VAZAMENTO DE DADOS PESSOAIS

Dados do Notificante / Representante Legal	
□ O próprio encarregado pela proteção de dados.	
□ Outros (especifique):	
Nome:	
CNPJ/CPF:	
Telefone:	
E-mail:	

Detalhes sobre a Denúncia	
Sobre o que trata sua denúncia? (Marque apenas a opção PRINCIPAL, caso haja mais de uma)	
□ Ausência de encarregado pelo tratamento de dados pessoais	□ Ausência de canal de comunicação com o agente de tratamento
□ Ausência de medidas de segurança adequada	□ Ausência de política de privacidade/Política de cookies
□ Exposição indevida de dados pessoais	□ Uso de dados pessoais para fins discriminatórios
□ Coleta excessiva de dados pessoais.	□ Acesso indevido a dados pessoais
□ Venda de dados Pessoais	□ Vazamento de dados/Incidente de segurança
□ Compartilhamento indevido de dados pessoais	
Descrição da denúncia Descreva, detalhadamente, a situação que motivou a denúncia, ou seja, a situação de violação à LGPD:	

O tratamento de dados em questão envolve dados de crianças e/ou adolescentes?	
□ Sim.	□ Não.

Informe as seguintes datas, sobre o incidente:	
Quando ocorreu	
Quando tomou ciência	

Se aplicável, quais ostipos de dados pessoais sensíveis foram violados? (admite mais de uma marcação)		
□ Origem racial ou étnica.	□ Convicção religiosa.	□Opinião política.
□ Referente à saúde.	□ Biométrico.	□Genético.
□ Referente à vida sexual.	□ Filiação a organização sindical, religiosa, filosófica ou política.	

Se aplicável, descreva os tipos de dados pessoais sensíveis violados:

14. ANEXO

Se aplicável, quais os tipos de dados pessoais violados? (admite mais de uma marcação)		
☐ Dados básicos de identificação (ex:nome,sobrenome,datadenascimento, matrícula)	☐ Número de documentos de identificação oficial. (ex:RG, CPF, CNH, passaporte)	☐ Dados de contato. (ex:telefone,endereço, e-mail)
☐ Dados de meios de pagamento. (ex:cartão de crédito/débito)	☐ Cópias de documentos de identificação oficial.	☐ Dados protegidos por sigilo profissional/legal.
☐ Dado financeiro ou econômico.	☐ Nomes de usuário de sistemas de informação.	☐ Dado de autenticação de sistema. (ex: senhas, PIN ou tokens)
☐ Imagens / Áudio / Vídeo	☐ Dado de geolocalização. (ex:coordenadasgeográficas)	☐ Outros (especifique abaixo)
Descreva os tipos de dados pessoais violados:		

Declaro, sob as penas da lei, serem verdadeiras as informações prestadas acima.

<ASSINATURA>


Ouvidoria
ICMBio - MMA


ICMBio
INSTITUTO CHICO MENDES
MMA