MINISTÉRIO DO MEIO AMBIENTE
E MUDANÇA DO CLIMA

# PLANO DE RESPOSTA A INCIDENTES COM DADOS PESSOAIS

**República Federativa do Brasil**

**Presidente:** Luiz Inácio Lula da Silva

**Vice-Presidente:** Geraldo José Rodrigues Alckmin Filho

**Ministério do Meio Ambiente e Mudança do Clima**
**Ministra:** Marina Silva

**Secretaria-Executiva**
**Secretário-Executivo:** João Paulo Ribeiro Capobianco

**Gabinete da Ministra**
**Chefe de Gabinete:** Daniel Pinheiro Viegas

**Ouvidoria**
**Ouvidor:** Leonardo Margonato Ribeiro Lima

**Encarregado pelo Tratamento de Dados Pessoais:** Marcelo Fontana da Silveira

Ministério do Meio Ambiente e Mudança do Clima
**Gabinete da Ministra**

# PLANO DE RESPOSTA A INCIDENTES COM DADOS PESSOAIS

**Brasília/DF**
**MMA**
**2025**

**Elaboração**
Marcelo Fontana da Silveira

**Coordenação**
Leonardo Margonato Ribeiro Lima

**Revisão**
Leonardo Margonato Ribeiro Lima
Humberto Luciano Schloegl
Edgard Augusto de Oliveira
Érika Rosa Pereira
Sílvio de Alvarenga Souza

**Arte e Diagramação**
Marcelo Fontana da Silveira

# PREFÁCIO

A proteção de dados pessoais é, hoje, um dos pilares essenciais da boa governança pública, da transparência administrativa e da preservação dos direitos fundamentais dos cidadãos. Em um contexto de transformação digital e crescente utilização de tecnologias da informação na gestão pública, torna-se imperativo que os órgãos da Administração Pública adotem mecanismos eficazes para prevenir, detectar e responder, de forma tempestiva e adequada, a incidentes que possam comprometer a segurança e a privacidade dos dados pessoais sob sua custódia.

Nesse cenário, o **Plano de Resposta a Incidentes com Dados Pessoais (PRIDP)** consolida diretrizes, responsabilidades e procedimentos voltados ao tratamento estruturado de incidentes que envolvam dados pessoais, garantindo conformidade com a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), as orientações da Autoridade Nacional de Proteção de Dados (ANPD) e as diretrizes do Programa de Privacidade e Segurança da Informação (PPSI) da Secretaria de Governo Digital do Ministério da Gestão e Inovação em Serviços Públicos (SGD/MGI).

O PRIDP foi concebido como um guia prático e orientador, promovendo a atuação coordenada entre a Alta Administração, o Encarregado pelo Tratamento de Dados Pessoais, as áreas técnicas, jurídicas, de tecnologia da informação e comunicação. Este instrumento normativo reafirma o compromisso institucional com a ética, a segurança jurídica e a confiança da sociedade na atuação do Estado ao estabelecer fluxos claros para avaliação, comunicação, contenção, mitigação e registro de incidentes, o Plano contribui para fortalecer a cultura organizacional de proteção de dados pessoais e para assegurar respostas proporcionais ao risco, fundamentadas em critérios técnicos e alinhadas aos princípios da responsabilização e da prestação de contas (*accountability*).

Mais do que atender a exigências legais, este Plano representa um compromisso institucional com a governança, a integridade e a melhoria

contínua das práticas de privacidade e segurança da informação no serviço público. Sua efetividade depende do engajamento de todas as unidades e agentes envolvidos, bem como da atualização constante frente à evolução normativa, tecnológica e aos riscos emergentes.

Assim, o **Plano de Resposta a Incidentes com Dados Pessoais** consolida-se como um instrumento dinâmico de governança, destinado a apoiar a atuação responsável do Ministério, proteger os titulares de dados e promover a confiança da sociedade na Administração Pública.

# SUMÁRIO

# 1. INTRODUÇÃO

O Ministério do Meio Ambiente e Mudança do Clima (MMA), em conformidade com a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), reconhece a importância da proteção de dados pessoais tratados em suas atividades institucionais e estabelece nesse documento o Plano de Resposta a Incidentes com Dados Pessoais. A adoção deste Plano se insere no escopo das ações de governança e gestão de riscos relacionadas à proteção de dados pessoais no setor público, fortalecendo os mecanismos de transparência, segurança jurídica e conformidade normativa no âmbito do Ministério.

O Plano de Resposta a Incidentes com Dados Pessoais - PRIDP tem por finalidade estabelecer os procedimentos técnicos e administrativos a serem observados no tratamento de incidentes que envolvam dados pessoais, garantir a segurança da informação, preservar os direitos dos titulares de dados e assegurar a adequada resposta a eventos que comprometam a integridade, confidencialidade ou disponibilidade desses dados, nos termos da LGPD, e demais normativos correlatos.

A elaboração e implementação deste Plano está alinhada ao *Guia de Resposta a Incidentes de Segurança* (SGD/MGI, 2024) e às diretrizes da Autoridade Nacional de Proteção de Dados (ANPD), bem como às boas práticas estabelecidas na Resolução CD/ANPD nº 15, de 24 de abril de 2024, que aprova o Regulamento de Comunicação de Incidente de Segurança. Nestes normativos, são definidas as competências dos agentes de tratamento no contexto institucional do MMA, as etapas do processo de resposta a incidentes, bem como os fluxos de comunicação interna e externa, inclusive com a ANPD, quando cabível.

A instituição deste Plano atende ao princípio da responsabilização e prestação de contas (*accountability*), previsto no art. 6º, inciso X, da LGPD,

e visa assegurar a adoção de medidas adequadas e eficazes para a identificação, contenção, resposta, registro e comunicação de incidentes de segurança com dados pessoais que possam acarretar risco ou dano relevante aos titulares dos dados.

Tais incidentes, acidentais ou intencionais, podem comprometer direitos fundamentais dos titulares de dados. Portanto, é essencial que haja preparo institucional para responder de maneira adequada e tempestiva, visando mitigar impactos, preservar a confiança pública e atender às obrigações legais previstas na Lei Geral de Proteção de Dados Pessoais.

A adoção deste Plano reforça o compromisso do MMA com a governança de dados pessoais, o cumprimento da legislação vigente e a promoção da confiança da sociedade na atuação ética e responsável do Estado.

# 2. OBJETIVOS

## 2.1. GERAL

Estabelecer diretrizes, procedimentos e responsabilidades institucionais para a prevenção, detecção, avaliação, comunicação, contenção, erradicação, recuperação, mitigação e documentação de incidentes de segurança envolvendo dados pessoais tratados no âmbito do Ministério do Meio Ambiente e Mudança do Clima (MMA), em conformidade com a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) e orientações da Autoridade Nacional de Proteção de Dados (ANPD).

## 2.2. ESPECÍFICOS

- Definir os fluxos e protocolos institucionais para resposta a incidentes de segurança com dados pessoais, incluindo etapas de identificação, notificação, contenção, erradicação, recuperação, investigação, investigação, mitigação e encerramento.

- Estabelecer os critérios e responsabilidades para a comunicação de incidentes à ANPD e aos titulares dos dados, nos termos do art. 48 da LGPD e dos guias técnicos expedidos pela ANPD.

- Padronizar procedimentos para registro e documentação dos incidentes de segurança, com vistas à análise posterior, à prestação de contas e à melhoria contínua dos controles internos.

- Promover a atuação coordenada entre as unidades organizacionais competentes, especialmente o Encarregado pelo Tratamento de Dados Pessoais, a Alta Administração/Controlador, a Subsecretaria de Planejamento, Orçamento e Administração (SPOA), a Coordenação-Geral de Tecnologia da Informação (CGTI/ETIR), a Assessoria de Comunicação Social (ASCOM), a Consultoria Jurídica (CONJUR) e as demais áreas envolvidas no incidente.

# 3. TERMOS E DEFINIÇÕES

**Agentes de Tratamento:** Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais, sendo classificada como Controlador ou Operador, nos termos do art. 5º, incisos IX e X, da LGPD.

**Anonimização:** processo que emprega meios técnicos razoáveis e disponíveis no momento do tratamento, com o objetivo de tornar os dados incapazes de serem associados, direta ou indiretamente, a uma pessoa natural.

**Ataque:** ação que explora vulnerabilidades com a finalidade de executar atividades maliciosas, como a invasão de sistemas, o acesso indevido a informações sigilosas ou a interrupção de serviços.

**Autoridade Nacional de Proteção de Dados (ANPD):** Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

**Consentimento:** uma das bases legais previstas pela LGPD para o tratamento de dados pessoais. Sua obtenção deve ocorrer mediante manifestação livre, informada e inequívoca do titular, atendendo aos requisitos legais estabelecidos.

**Controlador:** Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, nos termos do art. 5º, inciso VI, da LGPD.

**Dados Pessoais:** qualquer informação relativa à pessoa natural identificada ou identificável, seja isoladamente ou em combinação com outros dados.

**Dados que Identificam uma Pessoa Natural:** informações que permitem identificar diretamente um indivíduo, como nome completo (quando não houver homônimo), número do CPF, RG, passaporte, entre outros.

**Dados que Possam Identificar uma Pessoa Natural:** informações que, isoladamente, não identificam o titular, mas que, quando combinadas com outras, possibilitam sua identificação, como primeiro nome, endereço, ou características físicas.

**Dados Pessoais Sensíveis:** dados que dizem respeito à origem racial ou étnica, convicção religiosa, opinião política, filiação sindical ou a organização de caráter religioso, filosófico ou político, bem como dados referentes à saúde, à vida sexual, genéticos ou biométricos, nos termos do art. 5º, inciso II, da LGPD.

**Encarregado pelo Tratamento de Dados Pessoais:** Pessoa indicada pelo controlador para atuar como canal de comunicação entre o Controlador, os titulares dos dados pessoais e a ANPD, conforme art. 5º, inciso VIII, da LGPD.

**Engenharia Social:** método utilizado por agentes mal-intencionados para manipular usuários, levando-os a fornecer informações confidenciais, instalar malwares em seus dispositivos ou acessar links maliciosos.

**Hackers:** indivíduos que possuem conhecimento avançado em informática e sistemas computacionais, especialmente em áreas como programação, redes e segurança digital. Podem explorar, modificar ou manipular sistemas computacionais, muitas vezes ultrapassando barreiras tecnológicas que limitam o acesso comum.

**Incidente de Segurança com Dados Pessoais:** ocorrência, ação ou omissão que tenha possibilitado ou possa vir a possibilitar acesso não autorizado, interrupção ou modificação de operações (inclusive por meio de controle indevido), destruição, dano, exclusão ou alteração de informação protegida; bem como remoção, restrição de uso, apropriação indevida, divulgação ou publicação não autorizada de informação sensível vinculada a ativo crítico de informação ou a atividade essencial, ainda que por período inferior ao tempo previsto para recuperação.

**Malware:** termo genérico que designa qualquer tipo de software malicioso (*malicious software*) criado com a finalidade de infiltrar-se em dispositivos eletrônicos sem o conhecimento ou consentimento do usuário. Pode assumir diversas formas, com modos de ação variados, dependendo dos objetivos do agente malicioso.

**Manifestação Inequívoca:** expressão de vontade do titular sem qualquer ambiguidade, de modo que fique claramente evidenciado que ele consentiu com o tratamento de seus dados pessoais.

**Manifestação Informada:** ocorre quando o titular, antes de fornecer o consentimento, recebe de forma clara, prévia e suficiente todas as informações relevantes sobre o tratamento de seus dados pessoais, incluindo sua natureza, finalidades, métodos, duração, fundamentos legais, riscos envolvidos, responsabilidades dos agentes de tratamento e eventuais benefícios.

**Manifestação Livre:** o consentimento deve ser dado espontaneamente pelo titular, sem qualquer tipo de coação, induzimento ou condicionamento que possa comprometer sua liberdade de escolha.

**Mitigação:** Conjunto de ações destinadas a reduzir os danos ou prejuízos decorrentes de um incidente de segurança com dados pessoais.

**Notificação de Incidente:** Comunicação formal do incidente à Autoridade Nacional de Proteção de Dados (ANPD) e, quando necessário, aos titulares afetados, conforme previsto no art. 48 da LGPD.

**Operador:** Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador, conforme art. 5º, inciso VII, da LGPD.

**Phishing:** técnica de engenharia social utilizada para enganar usuários por meio de fraude eletrônica, com o objetivo de obter informações sensíveis, como nomes de usuário, senhas e dados bancários ou de cartões de crédito.

**Plano de Resposta a Incidentes:** Instrumento normativo que define os procedimentos e medidas organizacionais e técnicas a serem adotadas para o tratamento de incidentes de segurança com dados pessoais.

**Pseudonimização:** processo pelo qual informações identificáveis são substituídas por identificadores artificiais, códigos ou chaves criptográficas, mantendo os dados identificadores armazenados separadamente, sob controle exclusivo do Controlador.

***Privacy by Default* (Privacidade por Padrão):** princípio segundo o qual devem ser implementados mecanismos que assegurem, por padrão, a coleta e o uso mínimo necessário de dados pessoais, limitados à finalidade específica de cada operação de tratamento.

***Privacy by Design* (Privacidade desde a Concepção):** abordagem que prevê a incorporação de medidas de proteção de dados pessoais, desde as fases iniciais de concepção de produtos, serviços ou sistemas, considerando os riscos à privacidade ao longo de todo o seu ciclo de vida.

**Ransomware:** tipo de malware que realiza o sequestro de dados por meio de criptografia, bloqueando o acesso da vítima a seus próprios arquivos e exigindo pagamento de resgate, geralmente em criptomoedas, como condição para a liberação dos dados.

**Relatório de Impacto à Proteção de Dados Pessoais (RIPD):** documento elaborado pelo Controlador nos casos em que o tratamento de dados pessoais possa representar riscos relevantes aos direitos e liberdades fundamentais do titular, contendo a descrição dos processos de tratamento e as medidas adotadas para mitigar tais riscos.

**Resposta a Incidente:** Processo estruturado que compreende as etapas de identificação, análise, contenção, erradicação, recuperação, comunicação e documentação de um incidente de segurança.

**Risco:** Possibilidade da ocorrência de um evento que possa comprometer a integridade, confidencialidade ou disponibilidade de dados pessoais, bem como a conformidade com a legislação aplicável.

**Segurança da Informação:** Conjunto de medidas técnicas e administrativas destinadas a proteger as informações contra acessos não autorizados e garantir sua integridade, confidencialidade e disponibilidade.

**Sistemas:** conjunto integrado de hardware, software, redes, dispositivos de armazenamento e demais recursos tecnológicos utilizados, gerenciados, desenvolvidos, acessados ou operados pelo MMA para suporte às suas atividades institucionais.

**Titular de Dados Pessoais:** Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, nos termos do art. 5º, inciso V, da LGPD.

**Transferência Internacional:** envio de dados pessoais para país estrangeiro ou para organismo internacional do qual o Brasil seja membro, conforme previsto na LGPD.

**Tratamento de Dados Pessoais:** 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, controle, modificação, comunicação, transferência, difusão ou extração, conforme art. 5º, inciso X, da LGPD.

**Vazamento de Dados:** exposição indevida de dados pessoais que resulte, de forma acidental ou intencional, na sua perda, alteração, divulgação, acesso, transmissão, armazenamento ou tratamento não autorizado.

**Violação de Privacidade:** qualquer ação, omissão ou evento que contrarie as normas legais ou princípios da LGPD, resultando na destruição, perda, acesso não autorizado, uso indevido ou qualquer outra forma de comprometimento de dados pessoais.

# 4. ATORES E RESPONSABILIDADES

## 4.1. Governança mínima do PRIDP

Para fins de governança, adota-se a estrutura mínima prevista no art. 7º da Portaria SGD/MGI nº 9.511/2025 (PPSI), composta por:

- A alta administração nos termos do art. 2º, caput, inciso III, do Decreto nº 9.203/2017 compreende os Ministros de Estado, ocupantes de cargos de natureza especial, ocupantes de cargo de nível 6 do Grupo-Direção e Assessoramento Superiores - DAS: compete gerir os riscos no âmbito organizacional, fornecer os recursos necessários para assegurar a gestão da privacidade e da segurança da informação, viabilizar a implementação da estrutura de governança do PPSI e adotar decisões sobre privacidade e segurança da informação em um nível de relevância e prioridade adequadas e alinhadas com a estratégia e com a consecução dos objetivos do órgão ou entidade no cumprimento da sua missão institucional.;

- Gestor de Tecnologia da Informação e Comunicação (TIC): responsável por planejar, desenvolver, executar e monitorar as medidas de privacidade e segurança da informação em soluções de tecnologia da informação e comunicação (TIC), considerando inclusive a cadeia de suprimentos relacionada à solução pelo planejamento, desenvolvimento, execução e monitoramento das atividades de TIC, por assegurar recursos para resposta técnica;

- Gestor de Segurança da Informação: deve conduzir o diagnóstico de segurança da informação, bem como orientar, planejar e monitorar as medidas de segurança da informação;

- Encarregado pelo Tratamento de Dados Pessoais: atuar como ponto focal do PRIDP e canal com titulares e ANPD; compete conduzir o diagnóstico de privacidade, bem como orientar os agentes de tratamento no planejamento, implementação e monitoramento das

medidas de privacidade; coordenar a avaliação de risco e reportar à alta Administração; e

- Responsável setorial pela gestão da integridade: compete o diagnóstico das medidas relativas à estruturação básica e instrumentos fundamentais de governança do PPSI, além da coordenação e gestão dos riscos para a integridade relacionados aos temas.

  Nota: As demais unidades listadas a seguir atuam como interfaces operacionais do PRIDP, conforme suas competências.

### 4.2. Interfaces operacionais

- Coordenação-Geral de Tecnologia da Informação (CGTI) e Equipe de Tratamento de Incidentes (ETIR): identificação técnica, investigação, contenção, erradicação, recuperação e preservação de evidências; acionamento do CTIR Gov quando cabível;
- Assessoria de Comunicação Social (ASCOM): apoio e execução das comunicações aos titulares, quando determinadas pelo Controlador;
- Consultoria Jurídica (CONJUR): pareceres e revisão de comunicações sob o prisma jurídico;
- Unidades/Áreas proprietárias do processo/ativo: reporte tempestivo; apoio à apuração; implementação de correções;
- Comitê Gestor de Proteção de Dados Pessoais (CGPD): formulação de diretrizes, priorização e monitoramento de melhorias; e
- Comitê de Governança Digital (CGD): priorização de recursos de TIC e alinhamento estratégico.

# 5. INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

Segundo o Guia de Resposta a Incidentes de Segurança da Secretaria de Governo Digital (SGD/MGI) um incidente de segurança com dados pessoais pode ser definido como 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.

O art. 46 da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei n. 13.709/2018) estabelece que os agentes de tratamento devem 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, e que tais medidas de segurança deverão ser observadas desde a concepção do produto ou serviço (*Privacy by Design*) até a sua execução.

Nem todo incidente de segurança com dados pessoais deve ser comunicado à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados. Segundo o art. 48 da LGPD, o Controlador **deverá** comunicar a ocorrência de um incidente de segurança quando acarretar **risco ou dano relevante** aos titulares dos dados pessoais.

# 6. RISCO OU DANO RELEVANTE

A definição de risco ou dano relevante é trazida pela Resolução CD/ANPD n. 15, de 24 de abril de 2024, cujo art. 5º dispõe 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:

I. dados pessoais sensíveis;

II. dados de crianças, de adolescentes ou de idosos;

III. dados financeiros;

IV. dados de autenticação em sistemas;

V. dados protegidos por sigilo legal, judicial ou profissional; ou

VI. dados em larga escala.

Responde pelos danos decorrentes da violação da segurança dos dados o Controlador ou o Operador que, ao deixar de adotar as medidas de segurança der causa a dano ao titular do dado pessoal.

Qualquer colaborador, fornecedor ou parte interessada que tiver conhecimento de um incidente de segurança com dados pessoais deve comunicar o incidente ao Encarregado pelo Tratamento de Dados Pessoais, o mais rápido possível, por um dos seguintes meios:

**Sistema Eletrônico de Informações – SEI/MMA**

**Plataforma Integrada de Ouvidoria e Acesso à Informação – Fala.BR**

**e-mail: lgpd@mma.gov.br**

# 7. PROCEDIMENTOS ESPECÍFICOS PARA AVALIAÇÃO E TRATAMENTO DO INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

## 7.1. AVALIAÇÃO INTERNA DO INCIDENTE

O objetivo é obter informações iniciais sobre impacto do evento; natureza, categoria e quantidade de titulares de dados pessoais afetados; consequências do incidente para os titulares e a entidade, criticidade e probabilidade; além disso, é necessário preservar todas as evidências do incidente.

Quando a entidade tem conhecimento de um incidente de segurança com dados pessoais, deve ser realizada uma avaliação interna pelo Encarregado pelo Tratamento de Dados Pessoais, com o auxílio da Coordenação-Geral de Tecnologia da Informação e dos gestores dos sistemas afetados, sob a ótica da segurança e privacidade dos dados pessoais que estão sob a guarda do Ministério do Meio Ambiente e Mudança do Clima (MMA), para que sejam obtidas informações como:

I. **Vulnerabilidade explorada:** 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; entre outras;

II. **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;

III. **categoria de dados pessoais:** dados sensíveis, dados pessoais de crianças e adolescentes;

IV. **extensão do vazamento:** quantificar os titulares e os dados pessoais que tiveram a sua segurança violada neste evento;

V. **avaliação do impacto ao titular:** avaliar quais são os impactos que o incidente pode gerar aos titulares;

VI. **avaliação do impacto no serviço:** avaliar os impactos que o incidente pode gerar a 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.

**Figura 1: Atividades de avaliação interna do incidente com dados pessoais**


**Fonte: Guia de Resposta a Incidentes de Segurança (SGD/MGI).**

Ao tomar ciência do evento, abrir imediatamente a “Ficha de Registro do Incidente (FRI)” no SEI (modelo no ANEXO A), com carimbo temporal (data/hora), campos mínimos e anexação de evidências, de forma a preservar a cadeia de custódia e registrar integralmente decisões e ações e encaminhar para o Encarregado para ciência e demais providências.

Após avaliado o evento, se não for considerado um incidente à privacidade dos dados pessoais, a comunicação será devolvida àquele que notificou para que o notificante possa buscar outro canal para a solução do problema encontrado.

Se o evento for relacionado a incidente de segurança da informação com reflexos na privacidade dos dados pessoais custodiados pelo MMA será acionada a ETIR. Serão levantadas as primeiras informações sobre o evento e sua abrangência, com o máximo de informações para prosseguir com o tratamento.

A ETIR, por meio da Coordenação-Geral de Tecnologia da Informação acionará o **Centro de Tratamento e Resposta a Incidentes Cibernéticos do Governo (CTIR Gov)** visando a realização de ações conjuntas durante o tratamento do incidente com dados pessoais para uma resolução mais célere, técnica e eficaz.

### 7.2. COMUNICAR O CONTROLADOR POR MEIO DE RELATÓRIO

O Encarregado pelo Tratamento de Dados Pessoais providenciará, na sequência, a elaboração de um relatório a ser encaminhado à alta gestão do MMA, destinado à coleta de evidências técnicas necessárias à constituição de prova sobre o possível incidente, a identificação de falhas de segurança que tenham permitido ou contribuído para sua ocorrência, e indicação das correções indispensáveis, essenciais para o aprimoramento do órgão quanto às boas práticas de governança em privacidade.

Neste documento, o incidente deverá ser avaliado quanto ao grau de risco ou danos a que foram expostos os titulares dos dados pessoais:

I. **se o risco ou dano não forem relevantes**, é feita a remediação do evento que causou o incidente e sugestão de melhorias nos processos e sistemas visando evitar nova ocorrência;

II. **Caso a avaliação técnica interna, conduzida pelo Encarregado com o apoio das áreas competentes, indique a possibilidade de risco ou dano relevante, o Encarregado encaminhará relatório ao Controlador para deliberação final.** Nesse caso, deve ser feita a comunicação ao Controlador, que tem a prerrogativa de realizar a comunicação do incidente de segurança à Autoridade Nacional de Proteção de Dados – ANPD, por meio do Encarregado pelo Tratamento de Dados Pessoais, conforme o art. 6º, §5º da Resolução CD/ANPD nº 15, de 24 de abril de 2024.

O Operador deve comunicar incidentes com dados pessoais ao Controlador o mais rápido possível, a fim de viabilizar que o Controlador exerça seu papel tempestivamente.

### 7.3. CONFECÇÃO DE RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

Diante de todas as evidências, é importante que a entidade avalie a necessidade de elaborar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), que poderá ser solicitado em casos específicos previstos na LGPD pela Autoridade Nacional de Proteção de Dados (ANPD). São eles:

- 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).

## 7.4. COMUNICAR À ANPD E AOS TITULARES DE DADOS PESSOAIS

Os arts. 6º e 9º, da Resolução CD/ANPD nº 15, de 24 de abril de 2024**,** exigem que a comunicação à ANPD e ao titular de dados pessoais seja feita em até 3 (três) dias úteis da ciência do incidente pelo Controlador, visando preservar os direitos dos titulares e diminuir os possíveis prejuízos que um incidente de segurança possa causar.

O processo de comunicação do incidente de segurança deverá ser realizado nos moldes do capítulo V da Resolução CD/ANPD nº 15/2024, por meio de formulário disponibilizado para ser protocolado por peticionamento eletrônico no sistema SUPER da ANPD (https://www.gov.br/anpd/pt-br/canais_atendimento/peticionamento-eletronico-anpd).

Conforme a LGPD, art. 48, cabe ao controlador comunicar ao titular dos dados pessoais a ocorrência de incidente de segurança que tenha potencial de lhe gerar riscos ou danos relevantes.

A comunicação do incidente aos titulares deve ser feita em linguagem clara, simplificada, de forma individual, e diretamente aos titulares, sempre que possível. Na impossibilidade de identificar individualmente os titulares afetados, a comunicação deverá ser direcionada a todos os indivíduos cujos dados constem na base de dados comprometida.

Se, pela natureza do incidente, não for possível identificar individualmente os titulares afetados, excepcionalmente, o Controlador deverá utilizar a comunicação indireta pelos meios de divulgação disponíveis, tais como seu sítio eletrônico, aplicativos, suas mídias sociais e canais de atendimento ao titular, de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização, pelo período mínimo de 3 (três) meses, conforme a Resolução CD/ANPD nº 15/2024.

A comunicação deve ser feita em linguagem clara e mencionar, no que couber, os elementos previstos no §1º do Art. 48 da LGPD, e do Art. 9º da Resolução CD/ANPD nº 15/2024, tais como:

- a descrição geral do incidente e a data da ocorrência;
- a natureza dos dados pessoais afetados e os riscos relacionados ao incidente com a identificação dos possíveis impactos aos titulares;
- as medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- o motivo da demora, no caso de a comunicação não ter sido feita no prazo determinado (3 dias úteis);
- as medidas tomadas e recomendadas para reverter ou mitigar os efeitos do incidente;
- a data do conhecimento do incidente de segurança;
- o contato do Encarregado ou o ponto de contato para que os titulares obtenham informações a respeito do incidente; e
- outras informações que possam auxiliar os titulares a prevenir possíveis danos.

O processo de comunicação de incidente será considerado extinto nas seguintes hipóteses:

- caso não sejam identificadas evidências suficientes da ocorrência do incidente;
- caso o problema tenha sido resolvido ou verificado que os dados pessoais não foram afetados;
- caso o incidente não envolva dados pessoais;
- caso tenham sido tomadas todas as medidas adicionais para mitigação ou reversão dos efeitos gerados;

- após comunicação aos titulares dos dados pessoais e adoção das providências pertinentes pelo controlador, em conformidade com a LGPD e as determinações da ANPD.

Ao término do tratamento do incidente pelas áreas responsáveis, o Encarregado realizará a consolidação das informações sobre o incidente por meio de um Relatório Final do Incidente.

### 7.5. ELABORAÇÃO DE RELATÓRIO FINAL DO INCIDENTE

É fundamental que todas as informações, evidências coletadas e ações realizadas durante o processo de tratamento de incidentes de segurança envolvendo dados pessoais sejam devidamente registradas, de forma a viabilizar a elaboração do Relatório Final sobre o incidente. Esse documento deverá incluir considerações relevantes para promover a melhoria contínua dos processos de tratamento de incidentes e permanecer acessível para consulta em eventuais atualizações do Relatório de Impacto à Proteção de Dados (RIPD).

Deve constar do referido Relatório no mínimo as seguintes informações:

1. atividades realizadas desde o recebimento da notificação do evento até sua completa resolução;
2. evidências coletadas;
3. falhas identificadas no tratamento de dados pessoais;
4. medidas implementadas para minimizar os danos ao titular;
5. partes interessadas;
6. recomendações da ETIR e do Encarregado para prevenção contra a ocorrência de novas falhas de violação de privacidade.

O Relatório Final deverá ser encaminhado às partes envolvidas (Controlador, ANPD e Titulares) para conhecimento das ações realizadas, com o objetivo de dar transparência ao processo e possibilitar ações de melhoria contínua no tratamento dos dados pessoais.

Caso o evento tenha ocorrido por processamento de dados pelo Operador, cabe ao Controlador por meio da Coordenação-Geral de Tecnologia da Informação do MMA solicitar que o Operador elabore também um Relatório de Incidentes.

### 7.6. ENCERRAMENTO DO PROCESSO

O processo de comunicação de incidente será considerado extinto nas seguintes hipóteses:

**I.** caso não sejam identificadas evidências suficientes da ocorrência do incidente;

**II.** caso o problema tenha sido resolvido ou verificado que os dados pessoais não foram afetados;

**III.** caso o incidente não envolva dados pessoais;

**IV.** caso tenham sido tomadas todas as medidas adicionais para mitigação ou reversão dos efeitos gerados;

**V.** após comunicação aos titulares dos dados pessoais e adoção das providências pertinentes pelo controlador, em conformidade com a LGPD e as determinações da ANPD.

O Plano de Resposta a Incidentes de Segurança com Dados Pessoais poderá ser revisitado para contemplar orientações específicas da ANPD ou quaisquer instruções normativas.

O Plano deverá ser atualizado sempre que necessário, para fazer frente aos desafios relacionados à segurança com dados pessoais.

# 8. REVISÃO PERIÓDICA

Este Plano será revisado a cada dois anos ou sempre que houver alteração normativa, mudança tecnológica relevante ou incidente significativo que recomende ajustes.

# REFERÊNCIAS

**AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)**. Resolução CD/ANPD nº 15, de 24 de abril de 2024. Aprova o Regulamento de Comunicação de Incidente de Segurança. Diário Oficial da União, Brasília, DF, 26 abr. 2024.

**BRASIL**. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

**MINISTÉRIO DA ECONOMIA (ME)**. Secretaria de Governo Digital (SGD). Instrução Normativa SGD/ME nº 117, de 19 de novembro de 2020. Dispõe sobre a indicação do Encarregado pelo Tratamento dos Dados Pessoais. Diário Oficial da União, Brasília, DF, 20 nov. 2020.

**MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS (MGI)**. Secretaria de Governo Digital (SGD). Guia de Resposta a Incidentes de Segurança. Versão 3.3, Brasília, DF: MGI, 2024.

**MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS (MGI)**. Secretaria de Governo Digital (SGD). Portaria SGD/MGI nº 852, de 28 de março de 2023. Dispõe sobre o Programa de Privacidade e Segurança da Informação (PPSI). Diário Oficial da União, Brasília, DF, 29 mar. 2023.

**MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS (MGI)**. Secretaria de Governo Digital (SGD). Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025. Institui o Programa de Privacidade e Segurança da Informação no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional, que possuem unidades que integram o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo federal. Diário Oficial da União, Brasília, DF, 31 out. 2025.

**MINISTÉRIO DO MEIO AMBIENTE (MMA)**. Gabinete do Ministro. Portaria GM/MMA nº 132, de 18 de maio de 2022. Designa o Encarregado pelo Tratamento de Dados Pessoais do Ministério do Meio Ambiente. Diário Oficial da União, Brasília, DF, 19 maio 2022.

# 10. ANEXO A – Modelo da Ficha de Registro do Incidente (FRI)

1. Identificação do Processo (SEI):_____
2. Carimbo Temporal (data/hora da ciência): ___/___/_____ __:__
3. Origem do Reporte: ( ) Unidade/Servidor(a) ( ) ETIR/CGTI ( )

Terceiro/Operador ( ) Outro: _____

4. Descrição preliminar do evento:_____
5. Sistemas/ativos afetados: _____
6. Categorias de dados pessoais envolvidas: ( ) Pessoais comuns ( )

Sensíveis ( ) Crianças/Adolescentes ( ) Idosos ( ) Financeiros ( ) Autenticação ( )

Sigilo legal/judicial/profissional ( ) Larga escala ( ) Outros: _____

7. Estimativa de titulares potencialmente afetados: _____
8. Análise inicial de risco/dano (resumo): _____
9. Medidas de contenção iniciais adotadas: _____
10. Responsáveis (RACI) nesta etapa:

Responsável (R): _____
Aprovador (A): _____
Consultados (C): _____
Informados (I): _____

11. Comunicações realizadas até o momento: ( ) Unidade reportante ( )

Gestor de SI ( ) CGTI/ETIR ( ) Encarregado ( ) Controlador ( ) CTIR Gov ( )

ASCOM ( ) CONJUR ( ) Operador ( ) Outras: _____

12. Evidências anexadas (hash/descrição): _____
13. Observações adicionais: _____

Assinatura/Identificação do responsável pelo registro:

_____ Data: ___/___/_____

# 11. ANEXO B – RACI Sintético do Processo

**Legenda RACI:**

- **R (Responsável):** Quem executa a atividade. Pode haver mais de um.
- **A (Aprovador/Autoridade):** Quem decide e responde pelo resultado. Idealmente, apenas um por atividade.
- **C (Consultado):** Quem contribui com conhecimento técnico ou jurídico. A interação é bidirecional.
- **I (Informado):** Quem recebe comunicação sobre o andamento ou resultado. A interação é unidirecional.

Quadro B.1 - RACI Sintético do Processo

| Macroatividade | Controlador | Encarregado | CGTI/ETIR | ASCOM | CONJUR | Unidade/Área |
|---|---|---|---|---|---|---|
| Detecção / Notificação | I | R | I | I | I | R |
| Avaliação Interna | A | R | R | I | C | C |
| Contenção / Erradicação / Recuperação | I | C | R | I | C | C |
| Decisão de Comunicar (ANPD/Titulares | A | R | C | C | C | I |
| Comunicação à ANPD | I | R | C | I | C | I |
| Comunicação a Titulares | I | C | C | R | C | I |
| Relatório Final / Lições Aprendidas | A | R | R | I | C | C |
| Encerramento do Processo | A | R | C | I | C | I |

**Observações:** O quadro é orientativo. Em contratos com **Operadores**, devem ser refletidas as obrigações contratuais e os Acordos de Nível de Serviço (SLAs). Quando houver **comitês** (ex.: CGPD), usualmente atuam como **Consultados (C)** em ajustes de política/processo.

# 12. ANEXO C – Sensibilização sobre vazamento de dados pessoais (onde, quando e como acontecem)

## 📍 ONDE PODEM OCORRER?

Quadro C.1 – Local de ocorrência

| Ambiente | Exemplos |
|---|---|
| Físico | Documentos impressos esquecidos, lixo sem trituração, estações desbloqueadas |
| Digital | Bancos de dados, sistemas internos, armazenamento em nuvem |
| Redes Conexões | Wi-Fi públicas, conexões sem criptografia, transferências inseguras |

## ⏰ QUANDO PODEM OCORRER?

Quadro C.2 – momento da ocorrência

| Momento | Exemplos |
|---|---|
| Durante o Tratamento | Coleta, transmissão, armazenamento, compartilhamento, descarte |
| Falhas Técnicas | Erros em backups, atualizações, interrupções de energia |
| Ataques Cibernéticos | Phishing, ransomware, malware, invasões externas |
| Ações Inadequadas | Envio errado de e-mails, uso indevido de sistemas, má conduta de pessoal |

## ⚠️ COMO ACONTECEM?

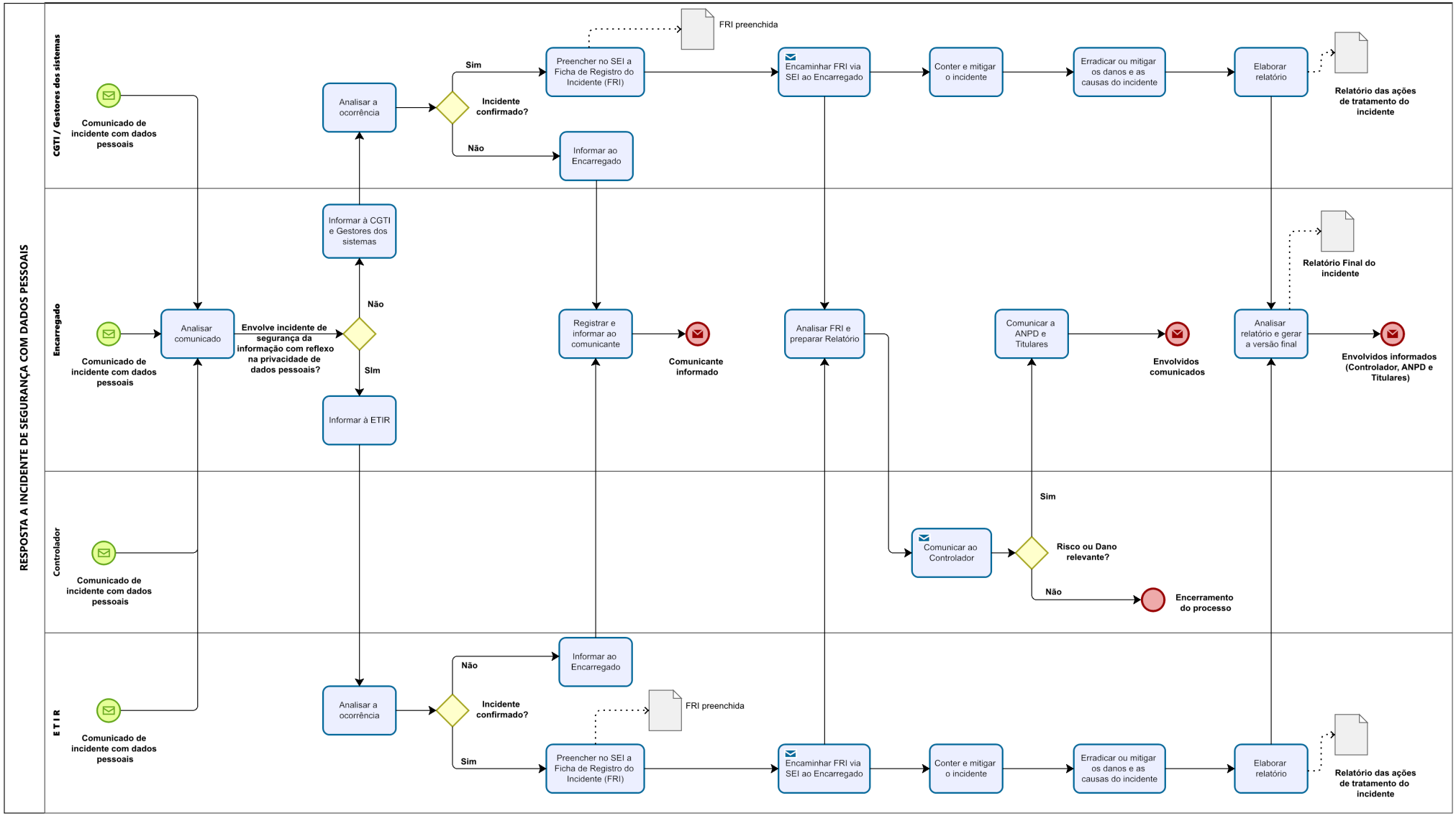
Quadro C.3 – Causas de ocorrência

| Causa | Detalhes |
|---|---|
| Erro Humano | Falta de capacitação, descuido, envio de dados ao destinatário errado |
| Falha Técnica | Configurações inseguras, sistemas desatualizados ou sem suporte |
| Ataques Maliciosos | Hackers explorando brechas, engenharia social, roubo de credenciais |
| Negligência em Segurança | Ausência de políticas, controle de acesso, monitoramento ou criptografia |

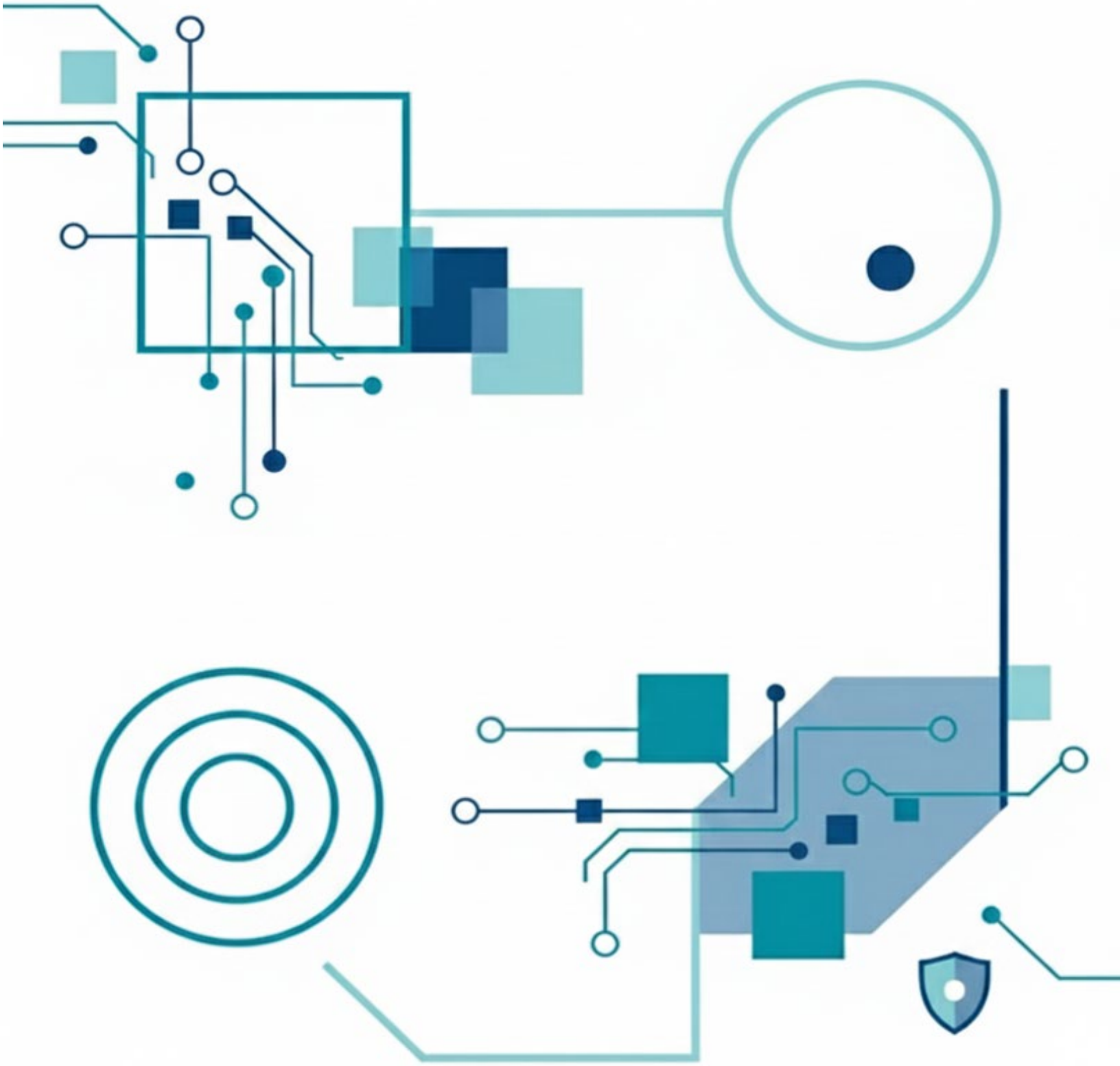
✅ **Dica:**
Implemente **medidas técnicas e organizacionais** eficazes, **treine equipes** e **revise políticas** para reduzir os riscos!

# 13. ANEXO D – Fluxograma do Processo de Resposta a Incidentes

Fluxograma D.1 - Processo de Resposta a Incidentes




Fonte: Autor



MINISTÉRIO DO
**MEIO AMBIENTE E**
**MUDANÇA DO CLIMA**

GOVERNO DO
BRASIL
DO LADO DO POVO BRASILEIRO