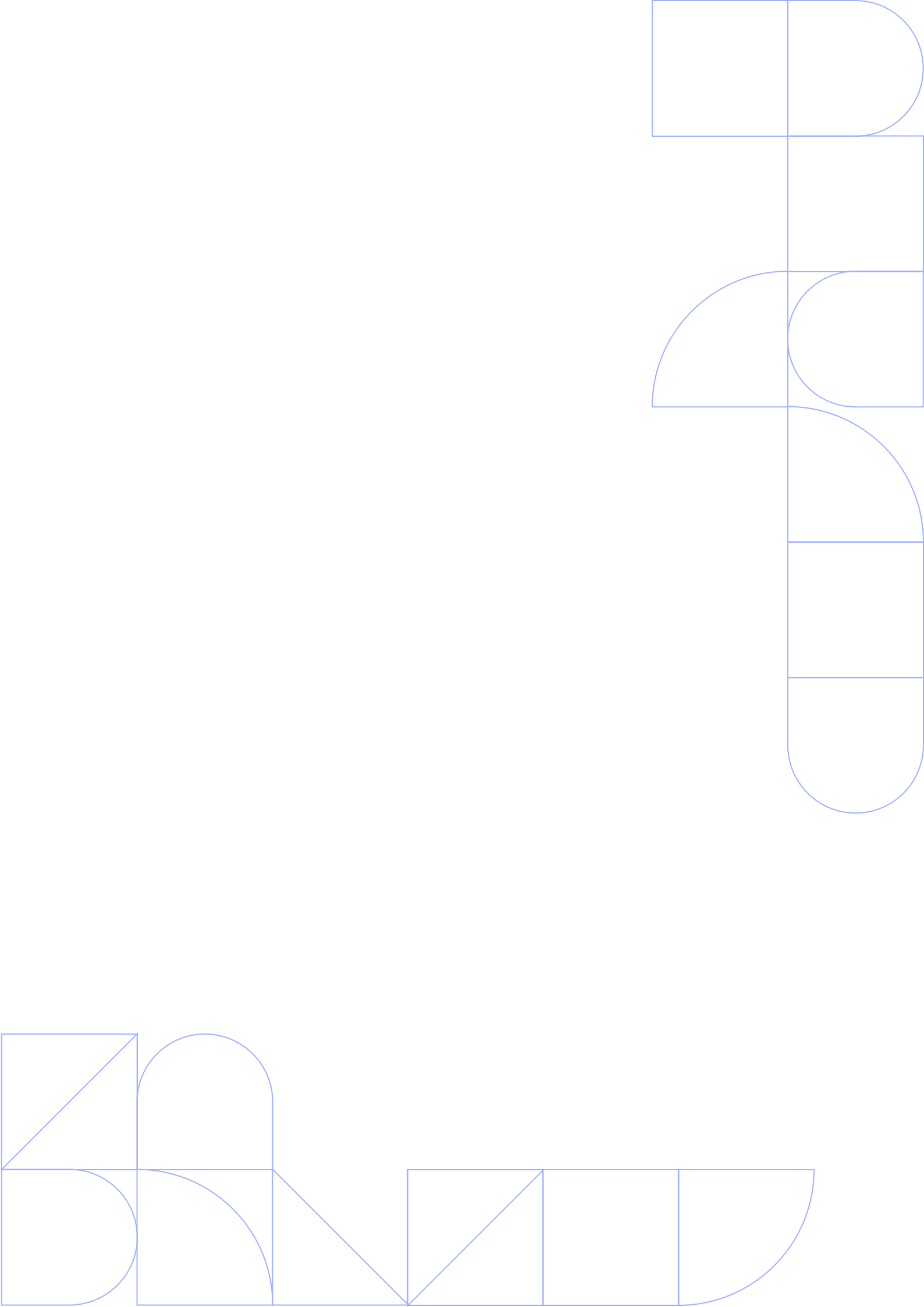


PLANO DE GESTÃO DE INCIDENTES COM DADOS PESSOAIS

MINISTÉRIO DA
GESTÃO E DA INOVAÇÃO
EM SERVIÇOS PÚBLICOS



PLANO DE GESTÃO DE INCIDENTES COM DADOS PESSOAIS

Julho de 2025

FICHA TÉCNICA

Ministra da Gestão e da Inovação em Serviços Públicos
Esther Dweck

Secretária Executiva
Cristina Kiomi Mori

Secretaria de Serviços Compartilhados
Cilair Rodrigues de Abreu

Diretoria de Gestão Estratégica
Wanessa Queiroz de Souza Oliveira

Coordenação-Geral de Proteção de Dados Pessoais
Luiz Fernando Bastos Coura
Maria Clara Souza Caribé Frutuoso
Andreia Queiroz Correia Dummar
Lucilene Ferreira da Silva Lopes
Julierme Rodrigues da Silva
Mário Jorge Pereira
Sheila Cristina Soares Vieira

Comitê de Privacidade e Proteção de Dados Pessoais

Titulares
Cristina Kiomi Mori
Luiz Fernando Bastos Coura
Fernanda Tsunematsu
Kimberly Coutinho Paes Leme de Castro
Rodrigo Morais Lima Delgado
Leonardo Rodrigo Ferreira
Antonio Fiuza de Sousa Landim
Lair Maria de Oliveira
Gustavo Fernando Frohlich
Clauber Teixeira Rodrigues
Fabio Valotto
Alex Pereira de Holanda
Francisco Eduardo de Holanda Bessa
Ana Carolina Quintanilha dos Santos Loriato
Érica Bezerra Queiroz

Substitutos
Adauto Modesto Júnior
Maria Clara Souza Caribé Frutuoso e
Andreia Queiroz Correia Dummar
Miriam Barbuda Fernandes Chaves
Carlos Eduardo Portella Sturm
André Luiz Lara Resende Saraiva
Marta Juvina de Medeiros
Rogério Mendes Meneguim
Edi Damasceno Maciel
Luciana de Almeida Toldo
Ronny Peterson Guimarães
Rudson Pereira Costa da Silva
Bruno de Freitas Tavares da Silva
Dilson Gonzaga Pereira Neto
Rildo Pereira Peixoto
Anderson Moreno Luz

Equipe Técnica de Elaboração
Coordenação-Geral de Proteção de Dados Pessoais – CGPDP/SSC/MGI

SUMÁRIO

1. INTRODUÇÃO 6

1.1 Motivações 7

1.2 Objetivos 8

2. DEFINIÇÕES 8

3. GESTÃO DE INCIDENTES COM DADOS PESSOAIS 10

3.1 Fase 1: Preparação 12

3.2 Fase 2: Detecção e Análise de Incidentes 15

3.3 Fase 3: Contenção, Erradicação e Recuperação 17

3.4 Fase 4: Atividades Pós-incidente 19

4. PRAZOS 21

5. CONSIDERAÇÕES FINAIS 22

REFERÊNCIAS 23

1. INTRODUÇÃO

Este Plano de Gestão de Incidentes com Dados Pessoais – PGI-DP é parte integrante **do Programa de Governança em Privacidade do Ministério da Gestão e Inovação em Serviços Púlbicos (PGP-MGI)**, estruturado em observância à Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e ao Programa de Privacidade e Segurança da Informação definido pela Secretaria de Governo Digital – SGD/MGI apoiado pelo Guia do Framework de Privacidade e Segurança da Informação.

O **PGI-DP** foi elaborado em atendimento à ação "**ID 18 – Elaborar Plano de Resposta a Incidentes com Dados Pessoais**" prevista no **Plano de Ações PGP-MGI 2024/2025**. Sua criação utilizou como base a antiga Resolução CEPPDP/ME 15/2022 (ME, 2022) e tem como objetivo atender ao **Controle 22** do **Guia do Framework de Privacidade e Segurança da Informação, que estabelece:**

Controle 22 – Políticas, Processos e Procedimentos: Definir, desenvolver, divulgar, implementar e atualizar políticas, processos e procedimentos operacionais, internos e externos que regem as ações relativas à proteção de dados pessoais e privacidade, e controles para programas, sistemas de informação ou tecnologias que envolvam o tratamento de dados pessoais.

O conteúdo deste Plano aborda procedimentos a serem executados quando da ocorrência de um incidente envolvendo dados pessoais, seja em meio digital ou não, suplementando orientações para gerenciamento de incidentes em redes computacionais da NC nº 08/IN01/DSIC/GSIPR e do Guia de Resposta a Incidentes de Segurança (DPSI/SGD, 2024), elaborado pela SGD/MGI.

Tendo em vista que a norma ABNT NBR ISO/IEC 29151:2020 faculta às organizações manterem, de forma separada ou integrada, planos de resposta a incidentes de privacidade e a incidentes de segurança da informação, este PGI-DP comporta possibilidade de integração futura com planos de resposta a incidente de segurança da informação, a serem eventualmente instituído pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, cujas atividades de estruturação estão em andamento.

A implementação de controles e procedimentos para resposta a incidentes de segurança da informação está prevista em diversas normas técnicas, tais como ABNT NBR ISO/IEC 27002:2022 (Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação), ABNT NBR ISO/IEC 27701:2020 (Requisitos e

diretrizes para gestão da privacidade da informação), ABNT NBR ISO/IEC 27035:2023 (Gerenciamento de incidentes de segurança da informação), NIST SP 800-61 Rev. 2 (Guia para incidentes de segurança em computadores), também usadas como referência neste PGI-DP.

Não é escopo deste Plano tratar sobre gestão de incidentes de segurança da informação. Orientações nesse sentido devem ser obtidas com a área responsável pela segurança da informação no MGI.

1.1 Motivações

A LGPD estabelece que os agentes de tratamento de dados devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais (art. 46). Nesse sentido, recomenda a implementação de programa de governança em privacidade que contemple planos de resposta a incidentes envolvendo dados pessoais (art. 50, § 2º, inciso I, alínea g).

Os tratamentos de dados pessoais estão sob constante ameaça de incidentes, fazendo-se necessária a adoção de medidas previamente planejadas que busquem tanto a prevenção da ocorrência ou recorrência de incidentes quanto a sua contenção a fim de minimizar seus impactos.

São inúmeras as consequências advindas de incidentes com dados pessoais, tanto para os titulares dos dados pessoais envolvidos quanto para o Ministério da Gestão e Inovação em Serviços Públicos – MGI. Limitando-se aos desdobramentos que tais eventos podem resultar ao Órgão, são elencadas a seguir algumas das adversidades que podem ser ocasionadas, e que motivam a elaboração deste PGI-DP:

- danos operacionais: incidentes podem resultar em impactos na operação governamental e na prestação de serviço aos cidadãos;
- danos reputacionais: dependendo da proporção do incidente, pode haver efeitos negativos na percepção que a sociedade e a comunidade internacional têm sobre o Ministério e seus agentes públicos;
- diminuição da eficiência e aumento dos custos: ocorrências de incidentes com dados pessoais, dependendo do volume ou proporção, podem gerar redução da confiança dos usuários dos serviços públicos digitais, além do aumento do trabalho manual e da diminuição da celeridade dos serviços oferecidos pelo Órgão e o consequente acréscimo dos custos da máquina pública.

Além disso, sanções administrativas poderão ser aplicadas pela Agência Nacional de Proteção de Dados (ANPD), assim como eventual assunção de custos pela Pasta com o pagamento de possíveis indenizações judiciais aos titulares impactados.

1.2 Objetivos

O objetivo principal deste PGI-DP é identificar atores, papéis, responsabilidades e estabelecer os procedimentos para o adequado tratamento dos incidentes com dados pessoais no âmbito do MGI, viabilizando respostas rápidas e efetivas quando concretizado um incidente.

Este Plano apresenta como objetivos específicos:

- comunicar incidentes à ANPD sempre que necessário, evitando comunicações paralelas com a Agência;
- primar pela adequada comunicação com os titulares, quando necessário;
- criar um fluxo de tratamento eficaz de incidentes que envolvam dados pessoais;
- manter atualizado o registro dos incidentes comunicados ao encarregado; e
- possibilitar que lições aprendidas com o tratamento de incidentes gerem subsídios para o aprimoramento deste Plano.

2. DEFINIÇÕES

A fim de proporcionar a adequada compreensão de todo o processo de gerenciamento de incidentes com dados pessoais descrito por este documento, é imprescindível destacar algumas definições inerentes ao tema. Portanto, no âmbito deste PGI-DP, além dos conceitos contidos na LGPD, considera-se:

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;

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.

Comunicado de Incidente de Segurança (CIS): documento sigiloso registrado no processo SEI, utilizando o tipo de documento de mesmo nome, que reúne informações sobre o incidente envolvendo dados pessoais para envio à Agência Nacional de Proteção de Dados (ANPD).

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

Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD) (Lei nº 13.709/2018).

Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR): Grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade. Anteriormente era chamada de Equipe de Tratamento de Incidentes de Rede (Portaria GSI/PR nº 93, de 18 de outubro de 2021 – Glossário de Segurança da Informação).

Incidente de segurança: qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais (Resolução CD/ANPD Nº 15/2024, Art. 3º, XII). Pode decorrer de ações voluntárias ou acidentais que resultem em divulgação, alteração, perda ou acesso não autorizado a dados pessoais, independentemente do meio em que estão armazenados (ANPD)[1]

Indício de Incidente de Segurança (IIS): notificação registrada em processo SEI sigiloso, criada com base em modelo de documento de mesmo nome, contendo informações relativas ao indício de incidente de segurança de evento adverso confirmado ou sob suspeita.

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

Notificação de Incidente de Segurança (NIS): notificação registrada em processo SEI sigiloso, criada com base em modelo de documento de mesmo nome, contendo informações relativas ao incidente de segurança.

1. Disponível em https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em 28/04/2025.

Notificador: qualquer pessoa física, jurídica ou área que comunique, mesmo que anonimamente, um evento adverso incidente de segurança com dados pessoais. Também pode ser representado por tecnologias de detecção de incidentes, como sistema de detecção de intrusão, soluções de *Security Informantion and Event Management* (SIEM), *Data Loss Prevention* (DLP), entre outras.

Processo SEI: processo sigiloso, disponível apenas para usuários previamente credenciados, no qual estarão registradas as informações acerca de um incidente de segurança com dados pessoais.

Registro Geral de Incidentes e Ações com Dados Pessoais (RG-IASDP): banco de dados que reúne informações sobre todos os incidentes de segurança envolvendo dados pessoais, incluindo as ações e medidas adotadas para mitigação, prevenção ou tratamento. Abrange os casos ocorridos no âmbito deste Ministério e comunicados ao encarregado.

Relatório Final de Tratamento de Incidente com Dados Pessoais: documento elaborado após o término do tratamento do incidente com dados pessoais, contendo todas as informações relativas ao incidente. Segundo definido na Resolução CD/ANPD nº 15/2024, Art. 3º, XIX, deve conter cópias, em meio físico ou digital, de dados e informações relevantes para descrever o incidente e as providências adotadas para reverter ou mitigar os seus efeitos

Unidade responsável: unidade(s) organizacional(is) do Ministério da Gestão e Inovação em Serviços Públicos gestora(s) dos dados pessoais impactados pelo incidente.

3. GESTÃO DE INCIDENTES COM DADOS PESSOAIS

A gestão de incidentes com dados pessoais deve ser considerada para incidentes em meios digitais e não digitais, uma vez que dados pessoais podem estar registrados em meio não digital (formulários, documentos impressos) ou digital (disco rígido, pen drive, cartão de memória, CD). Independente do meio, um evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, que possa ocasionar risco para os direitos e liberdades do titular dos dados pessoais, é um incidente de segurança com dados pessoais e, portanto, exige o adequado tratamento.

Como exemplos, citam-se alguns incidentes de segurança com dados pessoais: (i) publicação de documentos contento dados pessoais sem uma justificativa legal; (ii) compartilhamento com um terceiro, não autorizado, de dados pessoais de um indivíduo; (iii) brecha de segurança em um aplicativo que resulte no acesso de pessoas não autorizadas a dados pessoais de cidadãos que solicitaram um determinado serviço público; (iv) arrombamento de

uma sala de acesso restrito, resultando em acesso não autorizado às informações médicas, ou sensíveis, de servidores de uma determinada unidade.

Um processo clássico de gerenciamento de incidentes de segurança da informação é proposto em quatro fases pela publicação NIST 800-61 R2[2] (Figura 1), utilizada como referência pelo Guia de Resposta a Incidentes de Segurança (DPSI/SGD, 2024) — cujas recomendações são estendidas para gerenciar também os incidentes com dados pessoais.

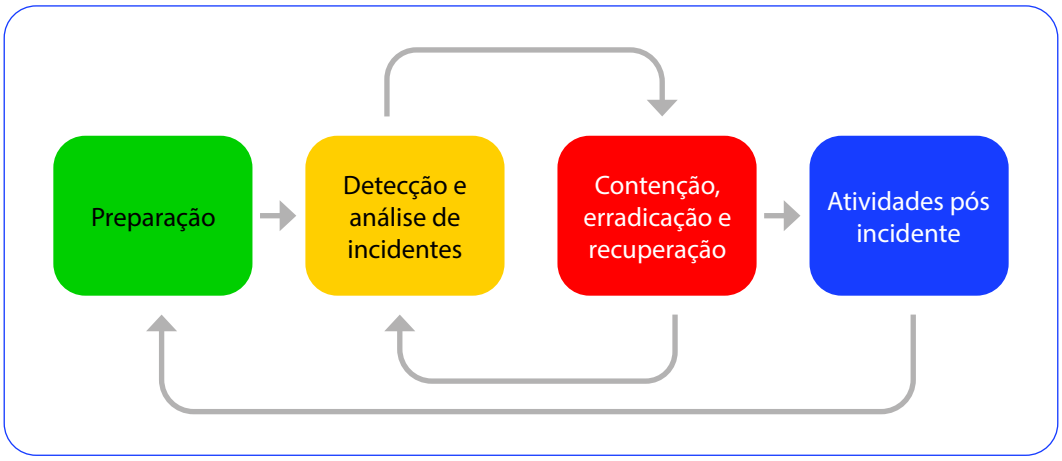


Figura 1 – Ciclo de resposta a incidentes (Fonte: Guia de Resposta a Incidentes de Segurança).

Os processos e documentos detalhados neste Plano registram os procedimentos a serem observados quando o incidente envolver dados pessoais, de acordo com o disposto na LGPD.

As atividades desenvolvidas durante o tratamento do incidente com dados pessoais devem ser documentadas. Essas atividades são consideradas imprescindíveis à segurança da sociedade e do Estado, pois contém detalhes técnicos de segurança que poderiam facilitar uma invasão, caso revelados. Dada essa criticidade, os registros somente devem ser acessados por profissionais autorizados, conforme definido no Art. 15 do Decreto nº 10.748/2021.

Antes de apresentar as fases de gestão de incidentes com dados pessoais, cumpre destacar que a ETIR mencionada neste PGI-DP não se confunde com a Equipe de Resposta a Incidentes – ERI prevista pelo Plano de Continuidade de Negócios do ColaboraGov.[3]

2. Disponível em https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf. Acesso em 28/04/2025.

3. Disponível em https://www.gov.br/gestao/pt-br/acesso-a-informacao/acoes-e-programas/programas-projetos-acoes-obras-e-atividades/PlanodeContinuidadedeNegcioSSC_v1.0.pdf. Acesso em 02/06/2025.

A ERI é responsável por gerenciar incidentes críticos que possam comprometer a continuidade dos serviços prestados pela Secretaria de Serviços Compartilhados e a ETIR atua no tratamento de incidentes específicos de segurança em redes de computadores.

Nos casos em que a ETIR não for encontrada ou estiver indisponível, a equipe técnica da área de tecnologia da informação do MGI assumirá suas responsabilidades.

3.1 Fase 1: Preparação

Nesta fase, o MGI deve realizar o planejamento para tratar os incidentes que envolvem dados pessoais, estando pronto para ação quando de sua concretização. Para tanto, deverão ser disponibilizados mecanismos objetivando a notificação dos incidentes, consignando informações e meios para contato com os responsáveis e as partes interessadas, assim como os procedimentos a serem executados para o adequado tratamento do incidente.

O tratamento de incidentes de segurança deve seguir as políticas, procedimentos e normas de segurança da informação. Caso o incidente envolva dados pessoais, os atores indicados na Tabela 1 devem ser acionados para garantir o cumprimento da LGPD.

Atores e respectivas responsabilidades na governança e gestão de incidentes com dados pessoais	
Atores	**Responsabilidades**
Alta Administração	• Fornecer recursos humanos, operacionais e técnicos para habilitar o MGI à adequada gestão de incidentes com dados pessoais. • Assegurar que a unidade responsável execute as medidas necessárias para recuperar as atividades e continuar as operações após a detecção de um incidente com dados pessoais.
CPDP	• Formular, aprovar e monitorar diretrizes sobre gestão de incidentes com dados pessoais no âmbito do MGI. • Promover os conhecimentos relativos à gestão de incidentes com dados pessoais no MGI. • Apoiar e incentivar práticas que levem à conscientização e à melhoria contínua da gestão de incidentes com dados pessoais.

→

Atores e respectivas responsabilidades na governança e gestão de incidentes com dados pessoais	
Atores	**Responsabilidades**
Encarregado pelo tratamento de dados pessoais	• Atuar como Notificador quando tiver conhecimento de qualquer indício ou incidente de segurança de dados pessoais. • Disponibilizar e manter atualizado no SEI o formulário para comunicação de incidentes adotado pela ANPD, para acesso da equipe técnica/ETIR e da unidade responsável pelo tratamento de dados pessoais envolvidos em incidente. • Se necessário, solicitar à equipe técnica/ETIR e à unidade responsável a complementação de informações sobre o incidente. • Registrar o incidente no Registro Geral de Incidentes e Ações com Dados Pessoais (RG-IASDP), mantendo-o atualizado com as informações acerca do incidente. • Efetuar comunicações parciais, complementares e completas à ANPD, além de qualquer contato necessário com o órgão. • Encaminhar determinações da ANPD para a unidade responsável e à equipe técnica/ETIR. • Apoiar a unidade responsável quanto às informações necessárias à comunicação com os titulares de dados pessoais. • Orientar as unidades organizacionais quanto às informações necessárias à eventual ampla divulgação do incidente em meios de comunicação. • Manter-se atualizado quanto aos requisitos regulamentares relativos à comunicação de incidentes, além dos procedimentos relacionados.
Equipe Técnica / ETIR	• Atuar como Notificador quando tiver conhecimento de qualquer indício ou incidente de segurança de dados pessoais. • Receber a notificação de incidente por meio dos canais definidos pelas normas de segurança. • Realizar a triagem – identificando se há ou não dados pessoais envolvidos – e a priorização do incidente. • Solicitar mais informações da Unidade Responsável, quando necessário. • Realizar o processo de Contenção, Erradicação e Recuperação, definido pela ETIR. • Criar processo SEI sigiloso e encaminhar à unidade responsável pelo tratamento dos dados pessoais e ao encarregado (documento do tipo “Informações de Incidente com Dados Pessoais”). • Realizar interlocução com a unidade responsável pelo tratamento dos dados pessoais envolvidos visando a melhor resposta ao incidente. • Adotar providências adicionais eventualmente determinadas, registrando-as no processo SEI. • Registrar no SEI o documento do tipo “Relatório Final de Tratamento de Incidente com Dados Pessoais”.

→

Atores e respectivas responsabilidades na governança e gestão de incidentes com dados pessoais	
Atores	**Responsabilidades**
Notificador	• Notificar a ocorrência, fornecendo à ETIR todas as informações das quais dispuser acerca do incidente com dados pessoais.

Unidade responsável	• Atuar como Notificador quando tiver conhecimento de qualquer indício ou incidente de segurança de dados pessoais.
	• Receber a notificação de incidente por meio dos canais definidos pelas normas de segurança.
	• Solicitar mais informações do Notificador, quando possível e necessário.
	• Avaliar, com o apoio do encarregado, a gravidade do incidente.
	• Atualizar processo SEI com o resultado da avaliação realizada.
	• Se o incidente puder acarretar risco ou dano relevante ou titular:
	  ○ comunicar os titulares de dados pessoais afetados no incidente;
	  ○ informar a Ouvidoria;
	  ○ atualizar o processo SEI; e
	  ○ adotar, se necessário, providências adicionais acerca do incidente.
	• Colaborar com a equipe técnica/ETIR e com o encarregado na fase de Contenção, Erradicação e Recuperação do incidente.
	• Disponibilizar ao encarregado os dados exigidos pela ANPD, observando formulário para comunicação de incidentes disponibilizado no SEI.

Agentes públicos	• Atuar como Notificador quando tiver conhecimento de qualquer indício ou incidente de segurança de dados pessoais. • Saber reconhecer incidentes com dados pessoais. • Manter seus dados de contato atualizados para que possam ser contatados durante o horário de expediente ou em horário extraordinário no caso de emergências.

Tabela 1 – Atores e respectivas responsabilidades na gestão de incidentes com dados pessoais

Outro aspecto de extrema relevância na fase de preparação refere-se à conscientização dos agentes públicos do MGI para que estejam aptos a identificar e atuar no reporte dos incidentes, representando fator determinante para o sucesso deste Plano.

Assim, serão desenvolvidas ações de comunicação e conscientização acerca da importância de se reconhecer um incidente que envolva dados pessoais, assim como as medidas a serem adotadas pelos agentes públicos quando do conhecimento de evento que implique violação na segurança de dados pessoais.

3.2 Fase 2: Detecção e análise de incidentes

Nesta fase, o MGI deverá adotar meios para detecção de incidentes e analisar tais eventos, buscando documentar, priorizar e notificar — Guia de Resposta a Incidentes de Segurança (DPSI/SGD, 2024, p. 36) — conforme fluxo para tratamento de incidentes com dados pessoais descrito na Figura 2.

A detecção poderá ocorrer a partir da notificação promovida por qualquer pessoa física, jurídica ou área acerca do evento adverso. Também poderá ser conhecida por tecnologias de detecção de incidentes, como sistema de detecção de intrusão, soluções de *Security Informantion and Event Management (SIEM), Data Loss Prevention (DLP), entre outras.*

Recebida a notificação sobre o possível o incidente de segurança da informação, a Unidade Responsável deverá avaliar se o indício pode ter alguma relação com a violação da confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais. Caso entenda que pode haver essa relação, a Unidade Responsável deverá preencher o documento Indício de Incidente de Segurança (IIS) com as informações gerais sobre o incidente e sobre os dados pessoais afetados — em processo SEI cujo nível de acesso deve ser sigiloso. Em seguida, o processo deverá ser encaminhado para o Encarregado.

Após o envio do processo ao Encarregado, a Unidade Responsável deverá analisar a notificação com objetivo de confirmar a ocorrência do evento adverso informado. Caso necessite de apoio técnico para a realizar essa tarefa, a Unidade Responsável deverá solicitar que a confirmação seja realizada pela equipe técnica ou ETIR. Ao estar certa de que a notificação de incidente trata-se de um caso confirmado que envolve dados pessoais, a Unidade Responsável deve preencher o documento Notificação de Incidente de Segurança (NIS) com as informações gerais sobre o incidente, bem como com informações técnicas que confirmem o incidente e seus impactos.

O Recebimento do NIS pelo Encarregado marca o início do prazo de 3 dias úteis para a necessária a comunicação do incidente aos titulares e à ANPD.

De posse das informações encaminhadas no NIS, o Encarregado elaborará o Comunicado de Incidente de Segurança (CIS) e o encaminhará à ANPD.

Em razão da autonomia e independência da ETIR do MGI, o processo denominado "Detecção de incidente", indicado no Fluxo de Tratamento de Incidente com Dados Pessoais (Figura 2), não é detalhado neste Plano, pois tal especificação compete à área de segurança da Pasta.

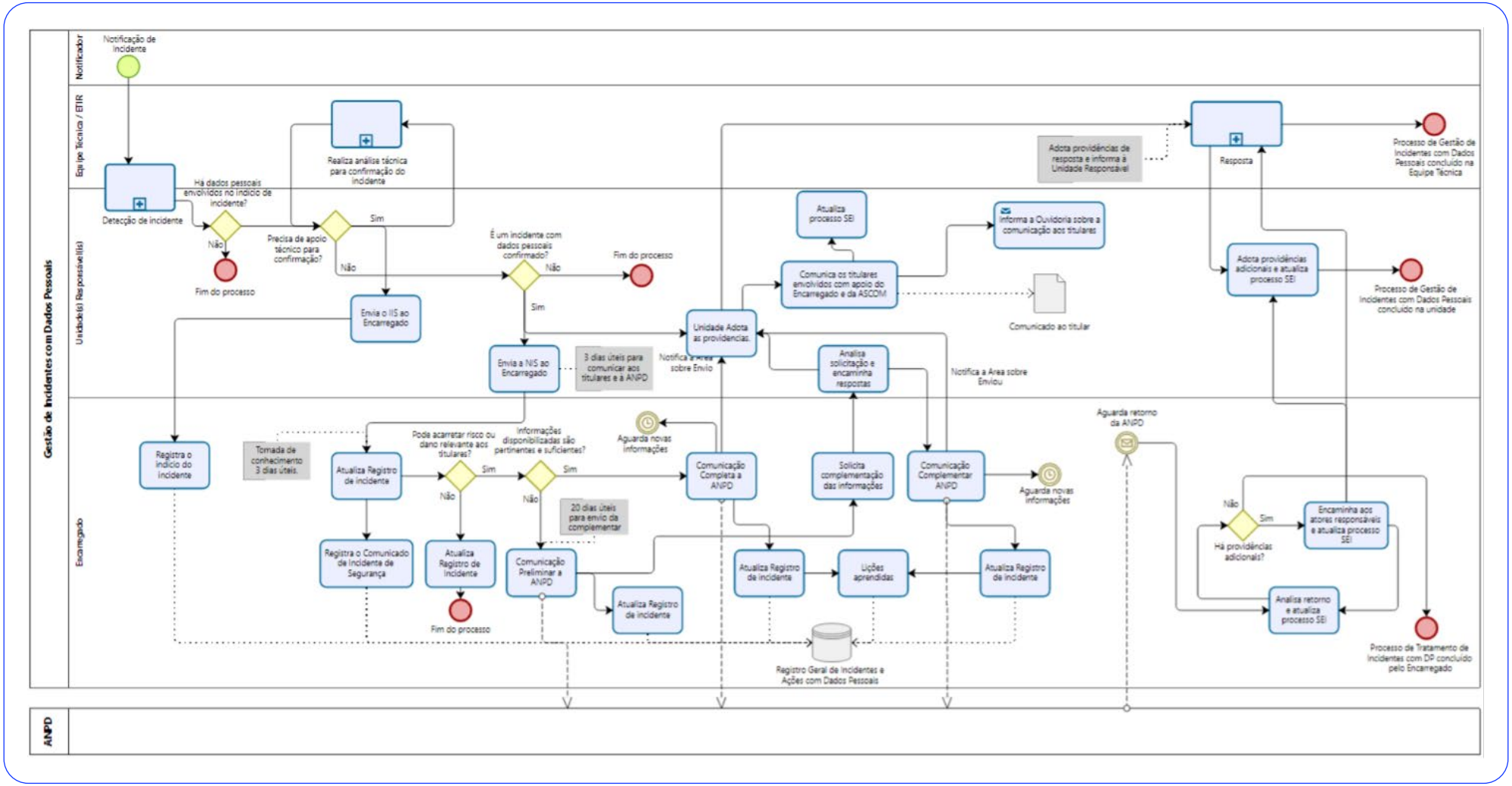


Figura 2 – Fluxo para Tratamento de Incidentes com Dados Pessoais

3.3 Fase 3: Contenção, erradicação e recuperação

Após a detecção e a análise do incidente, deverão ser realizadas ações buscando a remediação ou a restauração dos recursos comprometidos e, quando possível, a recuperação de tais recursos ao estado anterior ao incidente. Para isso, deverão ser seguidos os procedimentos já estabelecidos internamente para resposta a incidentes (DPSI/SGD, 2024, p. 46).

As ações do processo "Resposta", detalhadas pela ETIR, ocorrerão em paralelo aos procedimentos indicados na Figura 2 e objetivam a contenção, erradicação e recuperação do incidente com dados pessoais. Os procedimentos de tratamento do incidente perante a LGPD deverão ser executados pelo encarregado e pela unidade responsável, além da própria ETIR.

A unidade responsável deverá avaliar a gravidade do incidente, indicando se pode acarretar risco ou dano relevante aos titulares de dados pessoais. Caso haja tal possibilidade, deverá comunicar aos titulares afetados no incidente, contando com o apoio do encarregado e, no que couber, da ASCOM; a Ouvidoria também deverá ser informada acerca do comunicado emitido aos titulares, pois é o canal adequado para o recebimento de manifestações dos cidadãos, que podem necessitar de esclarecimentos adicionais acerca do ocorrido.

O processo SEI deverá ser atualizado pela unidade responsável com as providências adotadas, sendo necessário também registrar ocorrência se o incidente não terá possibilidade de gerar dano aos titulares.

Conforme o Guia de Resposta a Incidentes de Segurança (DPSI/SGD, 2024, p. 25), a comunicação aos titulares deverá ser feita em linguagem clara e simplificada 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:

- descrição geral do incidente e a data da ocorrência;
- natureza dos dados pessoais afetados e os riscos relacionados ao incidente;
- medidas técnicas e de segurança atualmente utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- motivo da demora, no caso de a comunicação não ter sido feita no prazo determinado;
- medidas tomadas e recomendadas para reverter ou mitigar os efeitos do incidente;
- data do conhecimento do incidente de segurança;

- contato do encarregado ou o ponto de contato para que os titulares obtenham informações a respeito do incidente;
- motivo da demora, no caso de a comunicação não ter sido feita no prazo determinado; e
- outras informações que possam auxiliar os titulares a prevenirem possíveis danos.

O encarregado, por sua vez, registrará o incidente no RG-IASDP. Para análise do incidente, avaliará a documentação registrada pela unidade responsável e pela ETIR no processo SEI. Se entender necessário, prestará orientações a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

O encarregado avaliará sobre a necessidade de comunicar a ANPD; se necessário, o fará utilizando-se das informações fornecidas pela unidade responsável e pela ETIR. Na hipótese de tais informações serem incompletas, não estando disponíveis, portanto, todos os dados requeridos no formulário de comunicação de incidente da ANPD, o encarregado poderá realizar uma comunicação parcial à ANPD ou solicitar complementação de informações aos atores envolvidos. É importante ressaltar que a ANPD possibilita a comunicação parcial do incidente, para posterior complementação quando da coleta de mais informações pelo Órgão. Assim, ainda que seja feita a comunicação parcial, as informações prestadas pela ETIR e pela unidade responsável deverão ser pertinentes, de modo a viabilizar a comunicação pelo encarregado.

Se comunicada a ANPD, é possível que a Agência determine a ampla divulgação do fato em meios de comunicação, caso ainda não tenha sido feito, e a adoção de medidas para reverter ou mitigar os efeitos do incidente (LGPD, art. 48, § 2º).

Durante todo o tratamento do incidente, o encarregado manterá frequente comunicação com a unidade responsável e com a ETIR, avaliando o conteúdo dos documentos gerados no processo SEI e a existência de providências a serem adotadas, encaminhando-as aos atores responsáveis por meio do mesmo processo SEI.

Enquanto houver necessidade de complementação da comunicação realizada à ANPD, o encarregado acompanhará as ações referentes ao andamento do tratamento do incidente desenvolvido tanto pela ETIR quanto pela unidade responsável, realizando interlocuções com todos os atores envolvidos a fim de solicitar as informações pertinentes, até que a comunicação à ANPD seja concluída.

Após a conclusão das atividades do processo "Resposta", a ETIR encaminhará, por meio do processo SEI, o Relatório Final de Tratamento de Incidente com Dados Pessoais, composto por modelo determinado pela própria ETIR, acrescido da atualização do formulário do tipo Informações do Incidente com Dados Pessoais, que inclui os elementos necessários à conclusão do registro na ANPD. Importante destacar que no Relatório deverá ser evidenciada a causa raiz do incidente, a relação de medidas adotadas para contenção, erradicação e recuperação, bem como a pertinência de tais medidas considerando a causa raiz identificada.

Adotados todos os procedimentos para tratamento do incidente com dados pessoais, inclusive quanto ao registro das lições aprendidas pelo encarregado, o processo SEI deverá ser encerrado pela ETIR, pela unidade responsável e pelo encarregado.

As informações registradas no processo SEI pelos agentes envolvidos deverão ser pertinentes e suficientes para tratamento do incidente e registro das lições aprendidas, inclusive para que o encarregado possa registrar as ocorrências e evidências do tratamento do incidente no Registro Geral de Incidentes e Ações de Segurança com Dados Pessoais (RG-IASDP).

3.4 Fase 4: Atividades pós-incidente

Esta é uma das fases mais importantes do tratamento de incidentes, pois é muito útil para aprimorar as medidas de segurança e de proteção de dados pessoais, além do próprio processo de tratamento de incidentes, que deverá ser aperfeiçoado continuamente por meio de mecanismos que propiciem a melhoria contínua visando:

- menor tempo de resposta no tratamento do incidente;
- diminuição de falsos positivos e falsos negativos na avaliação de existência de dados pessoais no incidente;
- aumento da qualidade do tratamento, por exemplo, identificando claramente em relatório a relação das medidas realizadas com a causa-raiz do incidente; e
- prevenção de reincidências do mesmo caso ou de casos semelhantes.

O Guia de Resposta a Incidentes de Segurança (DPSI/SGD, 2024) apresenta importantes informações a serem consideradas também nas atividades pós-incidente, razão pela qual reitera-se a importância de sua leitura aos agentes envolvidos no tratamento do incidente com dados pessoais.

É esperado que os agentes públicos do MGI aprimorem os conhecimentos a partir dos incidentes com dados pessoais ocorridos, de modo a evitar a recorrência de situações similares. Assim, é imprescindível que, após relatado o incidente e adotadas as medidas de resposta e solução definitiva dos impactos gerados, possam ser oferecidas garantias de que o processo em que o incidente foi originado não possibilite sua recorrência – assim como processos similares.

As atividades pós-incidente relacionadas à proteção de dados pessoais dizem respeito, basicamente, ao registro de lições aprendidas pelo encarregado, que as utilizará para avaliação da necessidade de adoção de providências adicionais, incluindo a pertinência de ajustes neste Plano de Gestão de Incidentes com Dados Pessoais – situação em que submeterá à avaliação do Comitê de Proteção de Dados Pessoais deste Ministério.

Ademais, o encarregado manterá atualizadas as lições aprendidas no Registro Geral de Incidentes e Ações de Segurança com Dados Pessoais (RG-IASDP).

A autonomia e a independência da ETIR do MGI pressupõem a existência de ações a serem executadas após a fase de contenção, erradicação e recuperação dos incidentes de segurança da informação, que não são abordadas neste PGI-DP visto não estarem relacionadas à conformidade à LGPD.

4. PRAZOS

Tendo em vista que a ANPD determina o prazo de três dias úteis[4] para comunicação do incidente com dados pessoais, os prazos internos que viabilizam o atendimento dessa determinação estão apresentados na Tabela 2.

Ação	Prazo	Responsável
Reportar o incidente à Unidade Responsável	Imediato	Notificador
Submeter à unidade responsável e ao Encarregado o processo SEI contendo informações sobre o incidente	Até 3 horas (úteis) do recebimento da comunicação efetuada pelo notificador	ETIR/Unidade Responsável
Caso o incidente possa acarretar risco ou dano relevante aos titulares, comunicá-los e preencher o formulário no SEI com informações requeridas pela ANPD	Até 3 dias (úteis) do recebimento das informações preliminares do incidente	Unidade responsável
Submeter o formulário de comunicação de incidentes com dados pessoais à ANPD, caso o incidente possa acarretar risco ou dano relevante aos titulares	Até 3 dias (úteis) do conhecimento do incidente (recebimento do NIS)	Encarregado
Apresentar informações adicionais sobre o progresso do tratamento do incidente à ANPD, caso o incidente possa acarretar risco ou dano relevante aos titulares	Regularmente, à medida que houver informações substanciais acerca do incidente	Encarregado
Submeter o relatório final de tratamento de incidentes com dados pessoais	Até 3 dias (úteis) após a conclusão do tratamento do incidente pela ETIR	ETIR
Submeter informações para concluir a comunicação dos incidentes à ANPD, caso o incidente possa acarretar risco ou dano relevante aos titulares	Até 3 dias (úteis) após o recebimento de Relatório Final	Encarregado
Submeter informações complementares ao CIS Preliminar, caso emitido.	Até 20 dias (úteis) da data de envio do Comunicado de Incidente de Segurança (CIS) para a ANPD	Encarregado
Elaborar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) das atividades afetadas pelo incidente	Até 20 dias (úteis) da data de envio do Comunicado de Incidente de Segurança (CIS) para a ANPD	Unidade Responsável, Encarregado e ETIR
Efetuar o Registro Geral dos incidentes e Ações com Dados Pessoais (RG-IASDP)	Durante todo o tratamento. Conclusão em até 3 dias (úteis) após recebimento do Relatório Final. Caso haja ações de médio e longo prazo a serem adotadas pela unidade responsável, complementar o RG-IASDP após a conclusão de tais ações	Encarregado

4. https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca

5. CONSIDERAÇÕES FINAIS

A gestão de incidentes com dados pessoais no âmbito do MGI objetiva proteger os dados pessoais e a privacidade dos titulares.

Desse modo, deve observar normativos e melhores práticas na preparação das respostas a incidentes, assim como na execução dos procedimentos para detecção, análise, contenção, erradicação e recuperação dos incidentes – além do fundamental registro das lições aprendidas ao longo de todo o tratamento dos incidentes.

Como referência aos procedimentos contidos neste Plano, foi usado o Guia de Resposta a Incidentes de Segurança (DPSI/SGD, 2024), baseado em normas NIST, ISO e CIS, expedido com o objetivo de auxiliar entes da administração pública federal na resposta a incidentes de segurança e proteção de dados pessoais.

Estima-se que as lições aprendidas no decorrer do tratamento dos incidentes forneçam valiosas informações que possibilitem a atualização do PGI-DP, como melhoria contínua do processo de gestão de incidentes com dados pessoais. Assim, ajustes neste Plano poderão ser submetidos ao Comitê de Proteção de Dados Pessoais, para análise da conveniência e oportunidade da aplicação de medidas de melhorias no tratamento de incidentes com dados pessoais no âmbito da Pasta.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:2022**: Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação. Rio de Janeiro, 2022.

_____. **ABNT NBR ISO/IEC 27701:2020**: Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes. Rio de Janeiro, 2020.

_____. **ABNT NBR ISO/IEC 27035:2023**: Tecnologia da informação — Gestão de incidentes de segurança da informação Parte 1: Princípios e processo. Rio de Janeiro, 2023.

_____. **ABNT NBR ISO/IEC 27035:2023**: Tecnologia da informação — Gestão de incidentes de segurança da informação Parte 2: Diretrizes para planejar e preparar a resposta a incidentes. Rio de Janeiro, 2023.

BRASIL. Agência Nacional de Proteção de dados. **Comunicação de incidentes de segurança.** Disponível em: < https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca >. Acesso em: 28 de abril de 2025.

BRASIL. Agência Nacional de Proteção de dados. **Regulamento de Comunicação de incidentes 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: 28 de abril de 2025.

BRASIL. Ministério da Economia. **Resolução CEPPDP/ME nº 15, de 6 de dezembro de 2022. Plano de Gestão de Incidentes com Dados Pessoais.**

BRASIL. Ministério de Gestão e da Inovação em Serviços Públicos. **Norma Complementar nº 18, abril de 2013. Plano de Desenvolvimento de Pessoas 2023.** Disponível em: < https://www.gov.br/servidor/pt-br/acesso-a-informacao/servidor/carreiras/eppgg/sobre-a-carreira/desenvolvimento-profissional-1/arquivos/formularios/plano_de_desenvolvimento_de_pessoas_2023.pdf >. Acesso em: 30 de abril de 2025.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 8.112, de 11 de dezembro de 1990. **Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais)**. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/l8112cons.htm >. Acesso em: 30 de abril de 2025.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 12.527, de 18 de novembro de 2011. **Lei de Acesso à Informação (LAI)**. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm >. Acesso em: 30 de abril de 2025.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet**. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acesso em: 30 de abril de 2025.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm >. Acesso em: 30 de abril de 2025.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Decreto nº 9.637, de 26 de dezembro de 2018. **Política Nacional de Segurança da Informação – PNSI**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm >. Acesso em: 30 de abril de 2025.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Decreto nº 9.991, de 28 de agosto de 2019**. Dispõe sobre a Política Nacional de Desenvolvimento de Pessoas da Administração Pública Federal Direta, Autárquica e Fundacional.** Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9991.htm >. Acesso em: 30 de abril de 2025.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Decreto nº 10.222, de 5 de fevereiro de 2020. **Aprova a Estratégia Nacional de Segurança Cibernética**. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm >. Acesso em: 30 de abril de 2025.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Decreto nº 10.641, de 2 de março de 2021. **Altera a Política Nacional de Segurança da Informação – PNSI**. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10641.htm >. Acesso em: 30 de abril de 2025.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Decreto nº 10.748, de 16 de julho de 2021. **Institui a Rede Federal de Gestão de Incidentes Cibernéticos**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10748.htm >. Acesso em: 30 de abril de 2025.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Portaria GSI/PR nº 93, outubro de 2021**. Aprova o glossário de segurança da informação.** Disponível em: < https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370 >. Acesso em: 30 de abril de 2025.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Instrução Normativa nº 01, maio de 2020**. Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal.** Disponível em: <https://www.gov.br/gsi/pt-br/dsic/legislacao/copy_of_IN01_consolidada.pdf>. Acesso em: Acesso em: 30 de abril de 2025.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Instrução Normativa nº 03, maio de 2021. **Dispõe sobre os processos relacionados à Gestão de Segurança da Informação nos Órgãos e nas Entidades da Administração Pública Federal.** Disponível em: < https://www.gov.br/gsi/pt-br/dsic/legislacao/copy_of_IN03_consolidada.pdf >. Acesso em: 30 de abril de 2025.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Norma Complementar nº 8, agosto de 2010**. Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.** Disponível em: < https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/legislacao/NC08.pdf >. Acesso em: 30 abr. 2025.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Norma Complementar nº 17, abril de 2013**. Dispõe sobre a Atuação e Adequações para Profissionais a Área de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.** Disponível em: < https://www.gov.br/gsi/pt-br/dsic/legislacao/NC17.pdf >. Acesso em: 30 de abril de 2025.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Norma Complementar nº 18, abril de 2013**. Dispõe sobre as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.** Disponível em: < https://www.gov.br/gsi/pt-br/dsic/legislacao/NC18.pdf >. Acesso em: 30 de abril de 2025.

BRASIL. Secretaria de Governo Digital. Portaria SGD/MGI nº 852, março de 2023. Dispõe sobre o Programa de Privacidade e Segurança da Informação – PPSI. Disponível em: < https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908 >. Acesso em: 30 de abril de 2025.

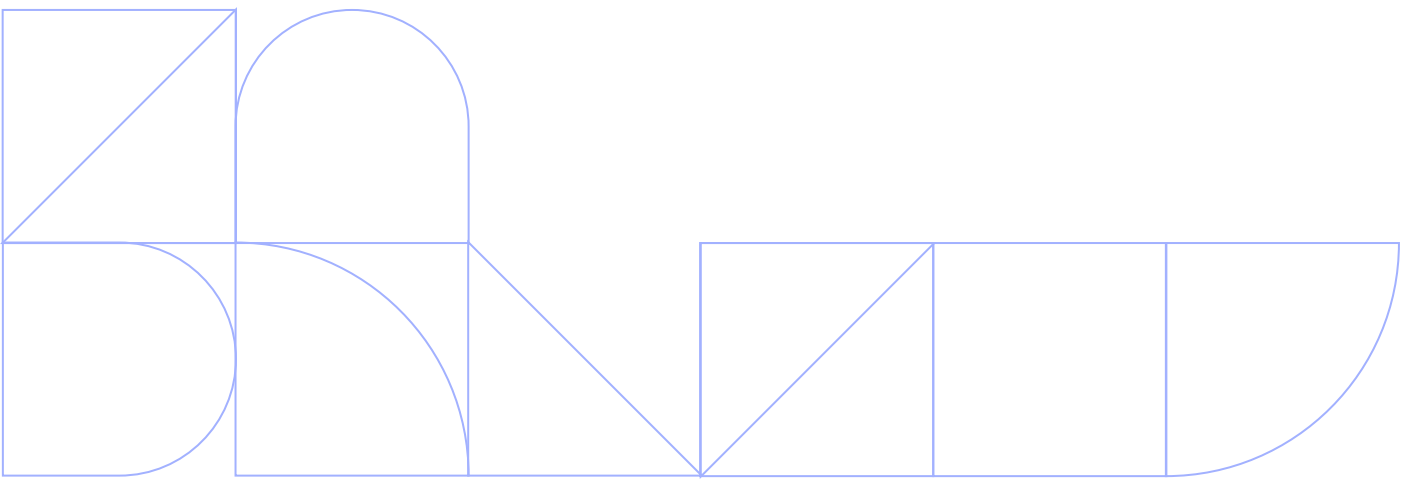
CENTER INTERNET SECURITY. **Security Awareness Skills Training Policy Template for CIS Control 14. março 2023. Disponível em: <** https://www.cisecurity.org/insights/white-papers/security-awareness-skills-training-policy-template-for-cis-control-14 > . Acesso em: 30 de abril de 2025.

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. **Guia do Framework de Privacidade e Segurança da Informação. Dezembro 2024**. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf>. Acesso em: 30 de abril de 2025.

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. **Guia de Resposta a Incidentes de Segurança. Julho 2024**. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_resposta_incidentes.pdf>. Acesso em: 30 de abril de 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST Special Publication 800-61 revisão 2: Computer Security Incident Handling Guide. Disponível em: < https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf >. Acesso em: 28 de abril de 2024.

UNIVERSIDADE DE FEDERAL DA BAHIA. SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO. **Plano de conscientização em segurança da informação. Março de 2023**. Disponível em: < https://sti.ufba.br/plano-de-conscientizacao-em-seguranca-da-informacao >. Acesso em: 30 de abril de 2025.



Este exemplar é parte do nosso compromisso com a responsabilidade ambiental.
Cada página foi impressa em papel proveniente de fontes responsáveis,
refletindo nosso cuidado em preservar os recursos naturais e minimizar
o impacto sobre o planeta. Edição limitada.

MINISTÉRIO DA
GESTÃO E DA INOVAÇÃO
EM SERVIÇOS PÚBLICOS