PROTOCOLO DE GESTÃO E RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS (PRI-PGFN)

PGAGOV **PGAGE**

CGCI **CGTI**

DIRIS **DGG**

Procuradoria-Geral da Fazenda Nacional

PROTOCOLO DE GESTÃO E RESPOSTA A INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

Brasília

Novembro/2025

Sumário

Histórico de versões

Data	versão	Descrição das Alterações	Responsável
14/11/2025	1.0	Elaboração inicial	DIRIS/PGAGOV
18/11/2025	1.0	Estruturação	DIRIS/PGAGOV
26/11/2025	1.1	Revisão CGTI	CGTI/PGAGE

01 Introdução

A promulgação da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) tornou imperativa a adequação das instituições da Administração Pública, como a Procuradoria-Geral da Fazenda Nacional (PGFN), às diretrizes de tutela de dados pessoais. Adicionalmente, a legislação exige a implementação, por parte dos agentes de tratamento, de salvaguardas técnicas e mecanismos administrativos de segurança, assim como a instituição de um arcabouço de boas práticas e princípios de governança (arts. 46 a 51).

Em estrito atendimento ao comando legal, a PGFN, em sua atuação como controladora de dados pessoais, reconhece a importância de instituir mecanismos formais de segurança e transparência. De forma específica, o **Artigo 48 da LGPD** estabelece a obrigatoriedade da comunicação de incidentes de segurança, afirmando que:

> *Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.*
> *§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:*
> *I - a descrição da natureza dos dados pessoais afetados;*
> *II - as informações sobre os titulares envolvidos;*
> *III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;*
> *IV - os riscos relacionados ao incidente;*
> *V - os motivos da demora, no caso de a comunicação não ter sido imediata; e*
> *VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.*

É importante ainda mencionar que a Autoridade Nacional de Proteção de Dados Pessoais (ANPD), no exercício de sua competência regulatória, estipulou o procedimento para

a comunicação de incidentes, que deverá ser realizada em **até 3 dias úteis (artigo 6.º da Resolução CD/ANPD nº 15, de 24 de abril de 2024)** da notícia do incidente – em consonância com o disposto no § 1º do art. 48 da LGPD, que determina a comunicação em prazo razoável.

A fim de garantir o cumprimento tempestivo e adequado destas e de outras obrigações decorrentes da lei, as áreas responsáveis pela governança e segurança da informação na PGFN elaboraram este **Protocolo de Resposta a Incidentes com Dados Pessoais**. O protocolo dispõe sobre as medidas que devem ser adotadas no caso de um evento de risco que possa ocasionar dano relevante aos titulares de dados pessoais, sensíveis ou não, viabilizando, inclusive, a comunicação apropriada e tempestiva à ANPD e aos titulares, quando for o caso. O conhecimento e a aplicação deste protocolo são essenciais para todos os servidores e colaboradores da PGFN.

02. Objetivos

A eficácia na proteção de dados e a resposta a crises dependem de um plano claro. Assim, após a implementação e difusão deste protocolo, a PGFN visa alcançar o seguinte

Objetivo Geral:

- Prover uma estrutura diretiva e processual para todas as unidades da PGFN, estabelecendo métodos documentados, formalizados, rápidos e confiáveis para a reação a incidentes de segurança. Isso inclui a preservação metódica de evidências para análise forense e a minimização da exposição legal e reputacional, assegurando o cumprimento integral das exigências de comunicação e transparência da LGPD.

Como desdobramento prático, este Protocolo visa alcançar os seguintes Objetivos Específicos:

a. **Clareza Processual:** Estruturar e disseminar o fluxo de procedimentos adequados, detalhando as etapas críticas de contenção, análise, erradicação da causa-raiz e recuperação dos sistemas afetados;

b. **Definição de Responsabilidades:** Designar de maneira inequívoca os papéis, as competências e as responsabilidades dos agentes envolvidos na gestão de incidentes com dados pessoais;

c. **Mitigação Reputacional:** Atuar de forma coordenada e transparente para resguardar a credibilidade e a imagem institucional da PGFN perante a sociedade, a mídia e os órgãos de fiscalização;

d. **Efetividade da Resposta:** Assegurar a capacidade da PGFN de propiciar respostas imediatas, coordenadas e tecnicamente eficazes, reduzindo o tempo de inatividade e mitigando o dano potencial aos titulares de dados e à própria infraestrutura da instituição.

Além de prover uma estrutura diretiva e processual, este protocolo visa especificamente:

- **Tempestividade Regulatória:** Assegurar o cumprimento do prazo de comunicação de **3 dias úteis** à ANPD, conforme Artigo 6º da Resolução CD/ANPD nº 15/2024.
- **Resiliência Operacional:** Minimizar o tempo de inatividade de sistemas críticos (ex: Dívida Ativa) através de contenção rápida.
- **Preservação Forense:** Garantir a cadeia de custódia das evidências digitais para fins de responsabilização e defesa institucional.
- **Proteção Reputacional:** Gerenciar a comunicação com transparência para resguardar a credibilidade da PGFN.

03. Abrangência e Prazo de Vigência

O presente Protocolo de Resposta a Incidentes estabelece um conjunto de diretrizes e procedimentos mandatórios, e sua aplicação se estende a todo o perímetro de atuação da Procuradoria-Geral da Fazenda Nacional (PGFN).

O escopo de aplicação engloba:

- **Ativos de Informação:** A totalidade dos recursos computacionais e tecnológicos pertencentes, operados, mantidos ou controlados pela PGFN, incluindo sistemas, redes de comunicação, aplicações *web*, servidores, estações de trabalho, dispositivos móveis e bases de dados e toda a infraestrutura física e documental que possa conter dados pessoais ou sensíveis, independentemente do formato (digital ou impresso).
- **Agentes de Tratamento:** A observância destas normas é compulsória para todos os servidores, colaboradores, estagiários, terceirizados e quaisquer agentes que, a serviço ou sob supervisão da PGFN, realizem operações de tratamento de dados pessoais. O protocolo se aplica a incidentes que afetem dados sob custódia da PGFN, em qualquer fase do ciclo de vida do tratamento.

A vigência deste Protocolo será iniciada na data de sua **homologação formal** pelas unidades ou autoridades competentes da PGFN, e permanecerá em efeito por tempo indeterminado, servindo como o documento normativo padrão (NOP) para a gestão de incidentes.

Não obstante sua vigência por prazo indeterminado, o documento será submetido a um ciclo de **revisão periódica obrigatória** ordinária, em caráter anual, ou extraordinária, sempre que identificada uma não-conformidade ou uma melhoria processual necessária. Essa revisão visa garantir a aderência contínua às melhores práticas de segurança da informação, bem como a adequação a eventuais alterações na arquitetura tecnológica da PGFN ou no panorama regulatório, notadamente novas regulamentações e orientações emitidas pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD). Alterações pontuais podem ser implementadas a qualquer tempo.

04. Termos e Definições

LGPD	**Lei Geral de Proteção de Dados Pessoais.** Acrônimo que identifica a Lei nº 13.709/2018. Esta é a norma jurídica brasileira que disciplina o uso, coleta, armazenamento e compartilhamento de dados pessoais, tanto no setor privado quanto no público, estabelecendo as bases para a segurança e a privacidade.

Controlador	Pessoa natural ou jurídica, de direito público ou privado, que detém a prerrogativa e a responsabilidade de tomar as decisões fundamentais relativas ao tratamento dos dados pessoais. No contexto deste manual, o **Controlador** é a **Procuradoria-Geral da Fazenda Nacional (PGFN)**.
Operador	Pessoa natural ou jurídica, de direito público ou privado, que efetua o tratamento de dados pessoais em nome e por conta do Controlador (PGFN), seguindo estritamente as instruções e finalidades por ele estabelecidas.
Dados Pessoais	Toda e qualquer informação que, isoladamente ou em conjunto, esteja vinculada a uma pessoa natural identificada ou que possa levar à sua identificação. Exemplos incluem nome, CPF, endereço, e-mail e registros de acesso.
Dados Pessoais Sensíveis	Categoria especial de dados que demanda proteção ainda mais rigorosa devido ao seu potencial discriminatório. Envolvem informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindical ou a organizações de caráter religioso/filosófico/político, dado referente à saúde, vida sexual, dado genético ou dado biométrico, quando estes estiverem relacionados a um indivíduo específico.
Tratamento	Qualquer operação ou sequência de operações executadas com dados pessoais, por meios automatizados ou não. Inclui, de maneira exemplificativa, a coleta, o registro, a organização, a estruturação, a adaptação, a modificação, o uso, a consulta, a disseminação, a cópia, a transferência, a guarda, a eliminação, o agrupamento, a restrição, a recuperação, a consulta, a destruição ou a anonimização de informações.
Agente de Tratamento	Termo que abrange o Controlador (PGFN) e o Operador, designando as entidades ou indivíduos que realizam o tratamento de dados pessoais em conformidade com as diretrizes legais e regulamentares.
Incidente de Segurança	Qualquer evento, ação, suspeita ou ameaça que comprometa de modo acidental ou ilícito a **confidencialidade**, a **integridade** ou a **disponibilidade** dos dados pessoais sob custódia da PGFN, seja em seus sistemas de informação ou em quaisquer meios físicos.

Sistemas	Compreende o conjunto de recursos e equipamentos de tecnologia da informação (TI) utilizados pela PGFN para o exercício de suas competências. Engloba hardware, software, infraestrutura de rede, mídias de armazenamento, e quaisquer outras plataformas, sejam elas adquiridas, desenvolvidas, controladas ou operadas pela instituição para o suporte e execução de suas atividades-fim.
Vazamento de Dados	Caracteriza-se como qualquer divulgação, acesso, transmissão ou compartilhamento não autorizado de dados pessoais, que possa resultar, de forma acidental ou intencional, em perda, modificação ou desvio de finalidade das informações.
Violação de Privacidade	Refere-se a qualquer transgressão da legislação vigente (LGPD) ou evento que ocasione a destruição fortuita ou ilícita, perda, furto, alteração, divulgação ou acesso não autorizado aos dados pessoais, resultando em dano ou risco relevante aos seus titulares.
ANPD	**Autoridade Nacional de Proteção de Dados Pessoais.** Órgão da administração pública federal responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.
Titular	A pessoa natural a quem se referem os dados pessoais que são objeto de tratamento pela PGFN.

05. Tabela de Responsabilidades (Matriz RACI Adaptada)

Ator	Sigla	Responsabilidades no Incidente
Comitê de Estratégia de TI	**CETI**	Órgão colegiado composto por representantes de diversas áreas da PGFN. Poderá atuar como **Comitê de Crise**. Órgão deliberativo responsável por autorizar medidas de alto impacto (ex: desligamento total de sistemas) e aprovar a estratégia de comunicação externa.
Encarregado de Dados	**DPO**	Ponto focal com a ANPD e Titulares. Realiza a avaliação jurídica do risco ("Dano Relevante") e decide sobre a necessidade de notificação externa.
Coordenação-Geral de Tecnologia da Informação	**CGTI**	Unidade executora técnica. Responsável pela detecção, triagem, contenção técnica e erradicação da ameaça.
Procuradoria-Geral Adjunta de Governança	**PGAGOV**	Suporte administrativo e logístico. Atua na interface institucional e facilita a alocação de recursos emergenciais.
Notificador	-	Qualquer agente público ou cidadão que reporte uma anomalia. Deve agir com boa-fé e celeridade, preferencialmente via Fala.BR.
Autoridade Nacional de Proteção de Dados	**ANPD**	Autarquia federal de natureza especial responsável por fiscalizar e zelar pelo cumprimento da Lei Geral de Proteção de Dados (LGPD) em todo o território nacional.

06 Fluxo do Processo

O objetivo deste processo é estabelecer as diretrizes para a detecção, notificação e tratamento de prováveis incidentes de segurança envolvendo dados pessoais na Procuradoria-Geral da Fazenda Nacional.

O procedimento é conduzido em duas frentes simultâneas (Dupla Faixa): ações técnicas (como contenção do incidente) e ações de conformidade (avaliação legal), visando o cumprimento dos prazos estabelecidos na legislação.

6.1 Detecção e Notificação

O incidente pode ser identificado por alertas automáticos ou por meio de reporte humano.

Canais de Comunicação:

- **Externo:** Preferencialmente utilizando a plataforma Fala.BR.
- **Interno:** Reporte direto à Central de Serviços da CGTI.

Princípio Fundamental do Reporte:

- Na dúvida, o reporte deve ser feito. O notificador tem apenas a responsabilidade de relatar o ocorrido, sem a necessidade de realizar investigação prévia.

6.2 Triagem e Classificação (CGTI)

Após a notificação do incidente, a CGTI deve realizar a validação do alerta e classificar sua severidade. Esta classificação é crucial para determinar o escalonamento imediato necessário.

Matriz de Severidade e Ações Correspondentes:

Nível de Severidade	Descrição do Incidente	Ações Imediatas
1 (Baixo)	Incidente contido e sem vazamento externo.	A CGTI trata e registra o incidente.
2 (Médio)	Risco de acesso não autorizado ou envolvimento de dados cadastrais simples.	Acionamento imediato da Equipe de Tratamento de Incidentes de Resposta (ETIR) e do Encarregado pelo Tratamento de Dados Pessoais (DPO).

3 (Alto)	Vazamento confirmado, envolvimento de dados sensíveis/fiscais ou paralisação de sistemas.	Acionamento imediato da ETIR, DPO, Procuradora-Geral da Fazenda Nacional (PGFN), Comitê Estratégico de Tecnologia da Informação (CETI) e Gabinete do Procurador-Geral.

6.3 Contenção, Erradicação e Preservação (CGTI)

Esta etapa é executada pela CGTI/ETIR simultaneamente à Triagem e Classificação e compreende as seguintes etapas:

- **Contenção:** Ações imediatas, como bloqueio de acessos, isolamento de servidores ou suspensão de serviços, para interromper o incidente e estancar o vazamento.
- **Preservação Forense:** Realização da cópia forense (imagem de disco/memória) *antes* de qualquer alteração ou formatação, visando garantir a cadeia de custódia e fornecer provas para futuras investigações (Polícia Federal ou Ministério Público).
- **Erradicação:** Remoção completa do *malware* ou elemento causador e o fechamento das vulnerabilidades exploradas.

6.4 Avaliação de Risco e Comunicação

6.4.1 Ações da CGTI após a Confirmação do Incidente

Após confirmar a ocorrência do incidente, e mesmo antes de sua completa avaliação de extensão e danos, a Coordenação-Geral de Tecnologia da Informação (CGTI) deve tomar as seguintes providências:

- **Autuação de Processo SEI:** Iniciar um processo no SEI, anexando toda a documentação referente ao incidente.
- **Comunicação Formal:** Enviar os autos do processo, por meio de comunicação formal, tanto ao órgão/empresa responsável pelo tratamento do incidente quanto ao Encarregado pelo Tratamento de Dados Pessoais (DPO) da PGFN.

6.4.2 Comunicação do Incidente pelo Encarregado de Dados (DPO)

A responsabilidade pela comunicação formal do incidente é do Encarregado de Dados Pessoais (DPO) da PGFN. Essa comunicação deve ser finalizada no prazo máximo de **3 (três) dias úteis** a partir da data de confirmação do incidente.

Independentemente da gravidade do ocorrido, o DPO da PGFN tem o dever de notificar formalmente as seguintes instâncias:

- O Comitê Estratégico de Tecnologia da Informação (CETI).
- A Procuradoria-Geral Adjunta de Governança (PGAGOV).
- O Gabinete do(a) Procurador(a)-Geral da Fazenda Nacional.

6.4.3 Procedimentos de Notificação Externa (LGPD)

- **Critério de Avaliação:** O DPO deve avaliar a existência de *"risco ou dano relevante"* aos titulares (como danos financeiros, morais ou roubo de identidade).
- **Comunicação à ANPD (se houver risco ou dano relevante aos titulares):** Caso o risco ou dano grave aos titulares seja confirmado, deve ser enviado um comunicado à Autoridade Nacional de Proteção de Dados (ANPD) detalhando a natureza dos dados afetados, os riscos envolvidos e as medidas técnicas adotadas.
- **Comunicação ao Titular (se houver risco ou dano relevante):** A notificação direta ao titular dos dados é obrigatória quando houver risco ou dano relevante, devendo ser feita em linguagem clara e acessível.

6.5 Recuperação

Restauração segura dos serviços a partir de backups verificados, somente após a confirmação de erradicação da ameaça, com monitoramento assistido para evitar reincidência.

6.6 Registro e Memória

Para fins de auditoria e conformidade com o Art. 10 da Resolução CD/ANPD nº 15/2024:

- Todo incidente (notificado ou não à ANPD) deve ser registrado.
- **Prazo de Retenção:** Mínimo de **5 anos**.

- **Conteúdo:** Deve incluir a análise de risco detalhada do DPO (justificando a decisão de notificar ou não) e o relatório técnico da CGTI.

07. Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Disponível em: https:// www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf Acesso em: 17 nov. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público. Versão 1.0 jan. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf Acesso em: 10 out. 2022. 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/L13709compilado.htm. Acesso em: 17 nov. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Guia de resposta a incidentes de segurança**. Programa de Privacidade e Segurança da Informação (PPSI). Versão 3.3. Brasília, DF: Ministério da Gestão e da Inovação em Serviços Públicos, 2024. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_resposta_incidentes.pdf. Acesso em: 17 nov. 2025.

BRASIL. 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, ed. 79, seção 1, p. 114-115, 26 abr. 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em: 17 nov. 2025.

Anexo 1

Checklist de Triagem e Decisão

Este instrumento deve ser anexado ao Processo SEI de gestão do incidente para documentar a tomada de decisão inicial.

Critério de Avaliação	Sim / Não	Ação Necessária
1. Confirmação: O evento é um incidente real (não é falso positivo)?	[ ]	Se NÃO, encerrar como "Evento de Segurança".
2. Dados Pessoais: Envolve dados pessoais sob custódia da PGFN?	[ ]	Se SIM, acionar DPO obrigatoriamente.
3. Risco Relevante: Há potencial de dano material/moral ao titular?	[ ]	Critério decisivo para notificação à ANPD (3 dias).
4. Sigilo Fiscal: Há dados protegidos pelo CTN?	[ ]	Se SIM, alertar as áreas envolvidas e o Gabinete da PGFN.
5. Amplitude: Afeta serviços externos ao cidadão?	[ ]	Se SIM, alertar as áreas envolvidas e o Gabinete da PGFN, sugerindo o envolvimento da ACOM.

Anexo 2

Minuta de Comunicado de Incidente à ANPD (Modelo Padrão)

Instrução: *Este modelo é de uso exclusivo do* ***Encarregado de Dados (DPO)****. Sua estrutura visa a notificação preliminar tempestiva (em até 72 horas) mesmo que a investigação técnica conduzida pela CGTI ainda esteja em andamento, seguindo o princípio da "Resposta em Dupla Faixa".-----****DESTINATÁRIO:*** *Autoridade Nacional de Proteção de Dados (ANPD)*

ASSUNTO: Comunicação de Incidente de Segurança com Dados Pessoais
FUNDAMENTO LEGAL: Art. 48 da Lei nº 13.709/2018 (LGPD) e Resolução CD/ANPD nº 15/20241. Identificação do Controlador
Controlador: Procuradoria-Geral da Fazenda Nacional (PGFN).

1. Detecção e Tempestividade da Notificação

Em observância ao Artigo 6º da Resolução CD/ANPD nº 15/2024, comunicamos a ocorrência de um evento adverso detectado em **[DATA/HORA]**.
A presente notificação é realizada dentro do prazo regulamentar de 3 dias úteis, contado a partir da confirmação de risco relevante pelo nosso Encarregado.

2. Natureza e Volume dos Dados Afetados (Triagem Preliminar)
Conforme avaliação inicial, o incidente envolve as seguintes categorias de dados:

- **Dados Comuns/Cadastrais:** *(Selecionar: Nome, CPF, Endereço, etc.)*
- **Dados Sensíveis ou Sujeitos a Sigilo:** *(Selecionar: Débitos, Patrimônio, Saúde de Servidores – com implicações de Sigilo Fiscal)*
- **Volume Estimado: [INSERIR QUANTIDADE APROXIMADA DE REGISTROS]** titulares afetados.

3. Riscos e Consequências Prováveis para os Titulares
A exposição destes dados pode resultar nas seguintes consequências:

- Risco de fraude ou roubo de identidade.

- Danos à imagem ou reputação financeira dos titulares (devido à natureza fiscal dos dados).
- Violação do sigilo fiscal (em conformidade com o Código Tributário Nacional – CTN).

4. Medidas de Segurança Preexistentes

Informamos que, previamente ao incidente, a PGFN mantinha as seguintes salvaguardas preventivas em uso: **[EX: FIREWALL, CRIPTOGRAFIA, CONTROLE DE ACESSO]**. Salienta-se que o incidente ocorreu apesar destas medidas de segurança, sendo a provável causa: **[EX: VULNERABILIDADE ZERO-DAY / ENGENHARIA SOCIAL / FALHA HUMANA]**.6. Medidas de Mitigação e Resposta Adotadas
Após a detecção, o Comitê de Estratégia de TI (CETI) e a CGTI ativaram imediatamente o Protocolo de Resposta a Incidentes, executando as seguintes ações:

- **Contenção:** Isolamento dos sistemas atingidos.
- **Perícia Forense:** Preservação de *logs* e evidências para análise técnica.
- **Erradicação:** Correção das vulnerabilidades exploradas.

5. Justificativa para Eventual Demora na Notificação

(Preencher apenas se a notificação ultrapassar o prazo de 3 dias úteis, detalhando a complexidade técnica ou a excepcionalidade do caso que levou à prorrogação do prazo, conforme Art. 48, § 1º, V da LGPD.)

Atenciosamente,

[NOME DO ENCARREGADO/DPO]
Procuradoria-Geral da Fazenda Nacional