POLÍCIA MILITAR
DISTRITO FEDERAL

SEGURANÇA DA INFORMAÇÃO · PROTEÇÃO DE DADOS PESSOAIS

PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

Conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD)
Lei Federal nº 13.709, de 14 de agosto de 2018

1ª EDIÇÃO
BRASÍLIA – DISTRITO FEDERAL · 2026

FICHA TÉCNICA

Identificação do Documento

Documento	**Plano de Resposta a Incidentes de Segurança com Dados Pessoais**
Órgão	Polícia Militar do Distrito Federal (PMDF)
Finalidade	Estabelecer diretrizes e procedimentos para identificação, contenção, tratamento, mitigação, registro e comunicação de incidentes de segurança envolvendo dados pessoais.
Base legal	Lei Federal nº 13.709/2018 (LGPD) Decreto Distrital nº 45.771/2024 Portaria PMDF nº 1.279/2022 Resolução CD/ANPD nº 15/2024 · ABNT NBR ISO/IEC 27001 e 27002
Controlador	Comandante-Geral da PMDF
Encarregado Setorial	Auditor da PMDF (PMDF/DCC/AUD)
Classificação	Documento institucional — observância obrigatória
Versão	**1ª Edição — Brasília/DF, 2026**

> Este Plano observa as diretrizes técnicas do **Guia de Gerenciamento de Vulnerabilidades** da Secretaria de Governo Digital (SGD) — Programa de Privacidade e Segurança da Informação (PPSI), versão 2.0 — especialmente quanto à criação de trilhas de auditoria, documentação de eventos, preservação de evidências, responsabilização, gestão contínua de vulnerabilidades e comunicação estruturada de incidentes.

APROVAÇÃO

Documento aprovado no âmbito da Polícia Militar do Distrito Federal

Rômulo Flávio Mendonça Palhares CEL QOPM
Comandante-Geral da PMDF
Representante do Controlador

Jean Araújo Santana do Vale CEL QOPM
Auditor da PMDF
Encarregado Setorial

ÍNDICE

Sumário

1 INTRODUÇÃO

A conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei Federal nº 13.709, de 14 de agosto de 2018, no âmbito da Polícia Militar do Distrito Federal — PMDF, visa garantir a proteção dos dados pessoais físicos e digitais custodiados pela Corporação, assegurando a privacidade, a segurança da informação e os direitos fundamentais dos titulares de dados.

Este Plano de Resposta a Incidentes de Segurança com Dados Pessoais estabelece diretrizes e procedimentos para identificação, contenção, tratamento, mitigação, registro e comunicação de incidentes envolvendo dados pessoais tratados pela PMDF.

O documento orienta militares, servidores civis, terceirizados, estagiários e colaboradores quanto às providências imediatas a serem adotadas diante de situações que possam comprometer a confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais.

Nos termos do art. 46 da LGPD, 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.

Além disso, a Portaria PMDF nº 1.279/2022 reforça que os operadores internos devem comunicar ao Encarregado Setorial a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, adotando imediatamente medidas cabíveis para cessar violações à LGPD.

O presente Plano também observa as diretrizes técnicas do Guia de Gerenciamento de Vulnerabilidades da Secretaria de Governo Digital — SGD, especialmente quanto à necessidade de:

- criação de trilhas de auditoria;
- documentação de eventos;
- preservação de evidências;
- responsabilização;
- gestão contínua de vulnerabilidades;
- comunicação estruturada de incidentes.

2 OBJETIVO

Este Plano tem por objetivo:

I – estabelecer procedimentos padronizados para resposta a incidentes de segurança envolvendo dados pessoais;

II – definir responsabilidades dos agentes envolvidos;

III – reduzir impactos operacionais, institucionais, reputacionais e legais;

IV – assegurar rastreabilidade e trilha de auditoria das ações adotadas;

V – garantir conformidade com:

- Lei Federal nº 13.709/2018 (LGPD);
- Decreto Distrital nº 45.771/2024;
- Portaria PMDF nº 1.279/2022;
- Normas e boas práticas de segurança da informação.

3 TERMOS E DEFINIÇÕES

Para fins deste Plano, aplicam-se os conceitos previstos na LGPD, no Decreto Distrital nº 45.771/2024 e na Política de Proteção de Dados Pessoais da PMDF.

3.1 Dado Pessoal
Informação relacionada à pessoa natural identificada ou identificável.

3.2 Dado Pessoal Sensível
Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, dado referente à saúde, vida sexual, dado genético ou biométrico.

3.3 Tratamento de Dados
Toda operação realizada com dados pessoais, incluindo coleta, acesso, utilização, armazenamento, compartilhamento, transmissão e eliminação.

3.4 Incidente de Segurança com Dados Pessoais
Evento adverso confirmado ou suspeito relacionado à violação da segurança de dados pessoais, capaz de ocasionar: destruição; perda; alteração; vazamento; acesso não autorizado; indisponibilidade; tratamento inadequado ou ilícito.

3.5 Controlador
Pessoa jurídica responsável pelas decisões referentes ao tratamento dos dados pessoais.

3.6 Operador
Pessoa que realiza o tratamento de dados pessoais em nome do controlador.

3.7 Encarregado Setorial
Pessoa indicada pelo Controlador para atuar como canal de comunicação entre o controlador, titulares e o Encarregado Governamental.

3.8 Trilha de Auditoria
Logs, registros e evidências documentais cronológicas referentes às ações executadas durante o tratamento do incidente.

4 INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

O que constitui um incidente de segurança com dados pessoais? Segundo a ANPD, um incidente de segurança com dados pessoais é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita, que possa ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

Constituem exemplos de incidentes:

I – envio equivocado de documentos contendo dados pessoais;

II – vazamento de informações em grupos de mensagens ou sistemas;

III – acesso indevido a assentamentos funcionais;

IV – compartilhamento indevido de dados sensíveis;

V – perda, furto ou roubo de equipamentos institucionais;

VI – descarte inadequado de documentos;

VII – infecção por malware ou ransomware;

VIII – exposição indevida de informações em sistemas;

IX – acessos não autorizados a bancos de dados;

X – utilização indevida de credenciais institucionais;

XI – vulnerabilidades críticas em sistemas informatizados.

> **Nem todo problema de segurança da informação envolve dados pessoais.** Incidentes que envolvam somente dados anonimizados ou que não permitam identificar indivíduos específicos não geram a necessidade de comunicação à ANPD. A mera existência de uma vulnerabilidade também não constitui, por si só, um incidente — embora sua exploração possa resultar em um.

5 DIRETRIZES GERAIS

A resposta a incidentes deverá observar os seguintes princípios:

I – atuação imediata;

II – minimização dos danos;

III – preservação das evidências;

IV – confidencialidade das informações;

V – necessidade de rastreabilidade;

VI – responsabilização;

VII – melhoria contínua dos controles de segurança;

VIII – manutenção de trilha de auditoria.

Conforme o Guia de Gerenciamento de Vulnerabilidades da SGD, é fundamental que os processos de segurança da informação possuam responsáveis definidos, documentação adequada e mecanismos contínuos de monitoramento e remediação.

6 RESPONSABILIDADES

6.1 Dos Usuários de Dados

Compete aos usuários de dados:

I – comunicar imediatamente qualquer incidente ou suspeita;

II – preservar evidências;

III – não ocultar falhas;

IV – colaborar com a apuração;

V – comunicar formalmente o incidente via Sistema Eletrônico de Informações — SEI.

A comunicação deverá:

- ser direcionada à chefia imediata;
- ser encaminhada à Auditoria da PMDF (PMDF/DCC/AUD), na qualidade de unidade responsável pela atuação do Encarregado Setorial de Dados Pessoais.

6.2 Da Chefia Imediata

Compete à chefia:

I – adotar medidas iniciais de contenção;

II – garantir a preservação das evidências;

III – encaminhar imediatamente o processo à PMDF/DCC/AUD;

IV – acompanhar a adoção das medidas corretivas.

6.3 Do Encarregado Setorial

Compete ao Encarregado Setorial:

I – receber comunicações de incidentes;

II – avaliar riscos e impactos;

III – coordenar resposta institucional;

IV – comunicar o Representante do Controlador sobre incidentes reportados pelos operadores internos;

V – avaliar necessidade de comunicação à ANPD;

VI – manter registro dos incidentes;

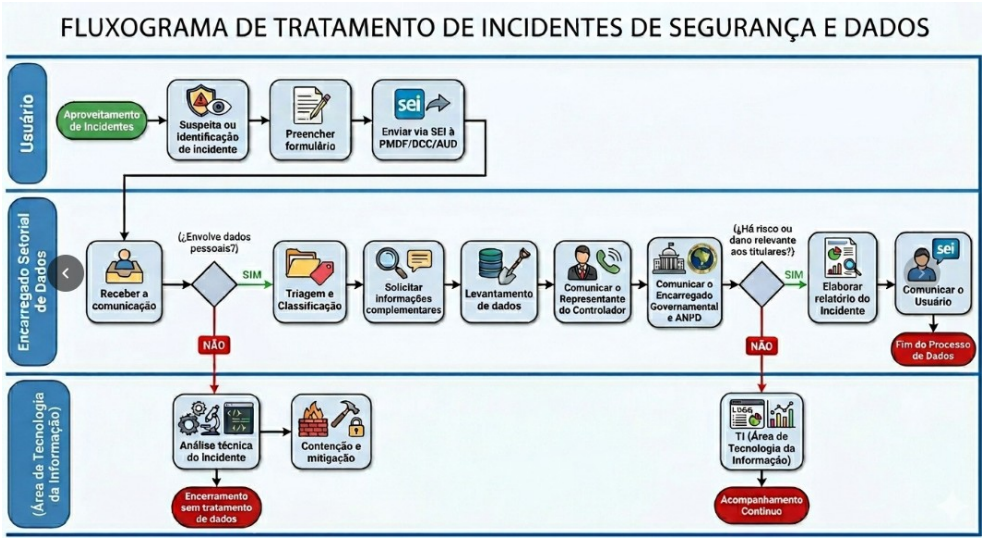
VII – propor medidas preventivas e corretivas.

Quadro-resumo de responsabilidades

Ator	Principais responsabilidades
Usuários de Dados	▪ Comunicar imediatamente incidentes ou suspeitas; ▪ Preservar evidências e não ocultar falhas; ▪ Colaborar com a apuração; ▪ Comunicar formalmente via SEI à chefia imediata e à PMDF/DCC/AUD.
Chefia Imediata	▪ Adotar medidas iniciais de contenção; ▪ Garantir a preservação das evidências; ▪ Encaminhar imediatamente o processo à PMDF/DCC/AUD; ▪ Acompanhar a adoção das medidas corretivas.
Encarregado Setorial	▪ Receber comunicações e avaliar riscos e impactos; ▪ Coordenar a resposta institucional; ▪ Comunicar o Representante do Controlador; ▪ Avaliar a necessidade de comunicação à ANPD; ▪ Manter registro dos incidentes e propor medidas preventivas e corretivas.

7 FLUXO DE RESPOSTA A INCIDENTES

O fluxo de resposta a incidentes de segurança com dados pessoais observa sete etapas encadeadas, da identificação ao encerramento, conforme síntese abaixo. As ações de cada etapa estão detalhadas na sequência.



Etapa 1 — Identificação

Ao identificar incidente ou suspeita, o usuário deverá:

I – interromper imediatamente a ação que possa ampliar o dano;

II – preservar documentos, prints, e-mails e logs;

III – comunicar imediatamente à chefia imediata;

IV – registrar comunicação formal via SEI;

V – encaminhar o processo à PMDF/DCC/AUD.

Etapa 2 — Registro

O registro deverá conter:

I – data e horário;

II – unidade envolvida;

III – descrição detalhada;

IV – categoria dos dados afetados;

V – quantidade estimada de titulares;

VI – medidas iniciais adotadas;

VII – evidências preservadas.

Etapa 3 — Contenção

Poderão ser adotadas:

I – suspensão de acessos;

II – redefinição de credenciais;

III – bloqueio de contas;

IV – isolamento de sistemas;

V – recolhimento de documentos;

VI – interrupção de compartilhamentos indevidos.

Etapa 4 — Análise

A análise deverá verificar:

I – causa raiz do incidente;

II – extensão do comprometimento;

III – vulnerabilidades exploradas;

IV – impacto aos titulares;

V – riscos institucionais.

O Guia de Gerenciamento de Vulnerabilidades recomenda análise contínua de vulnerabilidades, classificação de criticidade, rastreamento e remediação estruturada.

Etapa 5 — Comunicação

Quando aplicável, o incidente deverá ser comunicado:

I – ao Operador Interno;

II – ao Encarregado Setorial;

III – ao Comandante-Geral;

IV – ao Encarregado Governamental;

V – à ANPD;

VI – aos titulares afetados.

A comunicação deverá considerar a natureza dos dados, o volume de titulares, a gravidade e o risco de dano relevante.

A comunicação de incidente de segurança à ANPD, bem como ao titular, deverá ser realizada pelo controlador no prazo de três dias úteis contados do conhecimento pelo controlador de que o incidente afetou dados pessoais.

Etapa 6 — Remediação

As ações de remediação poderão incluir:

I – atualização de sistemas;

II – aplicação de patches;

III – correção de vulnerabilidades;

IV – revisão de permissões;

V – reforço de controles;

VI – treinamento de usuários.

O Guia da SGD recomenda o estabelecimento de ciclos contínuos de detecção, relatórios, remediação, controle de exceções e auditoria.

Etapa 7 — Encerramento

O incidente será encerrado após:

I – mitigação dos riscos;

II – elaboração de relatório conclusivo;

III – documentação das medidas adotadas;

IV – registro das lições aprendidas;

V – atualização de controles internos.

8 TRILHA DE AUDITORIA E PRESERVAÇÃO DE EVIDÊNCIAS

Toda resposta a incidente deverá possuir trilha de auditoria contendo:

I – registros SEI;

II – logs de acesso;

III – prints;

IV – e-mails;

V – relatórios técnicos;

VI – registros de comunicação.

O Guia de Gerenciamento de Vulnerabilidades destaca a necessidade de manutenção de trilha de auditoria e armazenamento seguro dos registros para auditorias internas e externas.

9 MEDIDAS PREVENTIVAS

A PMDF adotará medidas preventivas como:

I – capacitação periódica;

II – controle de acessos;

III – gestão de perfis;

IV – testes de vulnerabilidade;

V – monitoramento contínuo;

VI – atualização de sistemas;

VII – descarte seguro de documentos;

VIII – campanhas de conscientização;

IX – auditorias periódicas.

Conforme o Guia de Gerenciamento de Vulnerabilidades, recomenda-se gestão contínua de vulnerabilidades, testes periódicos e monitoramento constante de ameaças e exposições.

10 REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Lei Federal nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais.

DISTRITO FEDERAL. Decreto Distrital nº 45.771/2024, de 27 de abril de 2021.

POLÍCIA MILITAR DO DISTRITO FEDERAL. Portaria PMDF nº 1.279/2022.

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. Guia de Gerenciamento de Vulnerabilidades — Programa de Privacidade e Segurança da Informação (PPSI), versão 2.0, março de 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS — ANPD. Regulamento de Comunicação de Incidente de Segurança aprovado pela Autoridade Nacional de Proteção de Dados (ANPD), por meio da Resolução CD/ANPD nº 15, de 24 de abril de 2024.

ABNT NBR ISO/IEC 27001.

ABNT NBR ISO/IEC 27002.

FORMULÁRIOS

Anexos

Integram este Plano os formulários a seguir, a serem instruídos no Sistema Eletrônico de Informações (SEI) e classificados como restritos (informação pessoal):

Anexo I – Formulário de Notificação de Incidente de Segurança — utilizado para a comunicação inicial do incidente pelo militar, servidor ou colaborador que o identificar.

Anexo II – Formulário de Registro de Incidente de Segurança — utilizado para o registro do incidente pela Auditoria da PMDF (PMDF/DCC/AUD), em conjunto com o gestor da base de dados afetada.

ANEXO I

Formulário de Notificação de Incidente de Segurança

Processo SEI nº _____ / _____ - ____

Preenchido pelo militar, servidor ou colaborador que identificar o incidente, e encaminhado, via SEI, à Auditoria da PMDF (PMDF/DCC/AUD), na qualidade de Encarregado Setorial pelo Tratamento de Dados Pessoais.

1. Identificação do Comunicante

Nome / Posto / Graduação	*[Nome completo e posto ou graduação]*
Quadro	*[Quadro / especialidade]*
Matrícula	*[Matrícula funcional]*
Unidade / Lotação	*[Unidade ou setor de lotação]*
E-mail de contato	*[E-mail institucional]*
Telefone para contato	*[Telefone / ramal]*
Data da comunicação	*[dd/mm/aaaa]*

2. Descrição Geral do Incidente

Data e hora da ocorrência (ou da suspeita)	*[dd/mm/aaaa hh:mm]*
Data e hora da ciência (quando você descobriu)	*[dd/mm/aaaa hh:mm]*
Local / Origem do incidente	*[Unidade, setor, sistema ou local físico/lógico onde se originou]*
Descrição do incidente	*[Descreva objetivamente o que aconteceu, como descobriu, em que meio, se há alguém envolvido e qual a localização física ou lógica dos dados afetados]*
Causa principal (se identificada)	*[Descrição]*

3. Dados Pessoais Afetados

Natureza dos dados pessoais	☐ Dados pessoais gerais ☐ Dados pessoais sensíveis — origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural
Categoria dos dados pessoais	☐ Dados de crianças, de adolescentes ou de idosos ☐ Dados financeiros ☐ Dados de autenticação em sistemas ☐ Dados protegidos por sigilo legal, judicial ou profissional ☐ Dados em larga escala
Número de titulares afetados	*[Total e, se aplicável, número de crianças, adolescentes ou idosos]*
Tipo de violação (marque a(s) principal(is) suspeita(s))	☐ Acesso não autorizado ☐ Vazamento / Comunicação indevida ☐ Alteração indevida ☐ Perda / Destruição ☐ Sequestro de dados (Ransomware) ☐ Roubo / Furto de equipamento ☐ Outra: _____

4. Medidas Iniciais e Evidências

Medidas iniciais de contenção adotadas	*[Ex.: suspensão de acessos, bloqueio de contas, recolhimento de documentos, isolamento de sistemas]*
Evidências preservadas	☐ Registros / processo SEI ☐ Logs de acesso ☐ Prints de tela ☐ E-mails ☐ Outras: _____
Chefia imediata cientificada	☐ Sim ☐ Não

ANEXO II

Formulário de Registro de Incidente de Segurança

Processo SEI nº _____ / _____ - ____

Preenchido pela Auditoria da PMDF (PMDF/DCC/AUD) em conjunto com o gestor da base de dados afetada, observadas as regras aplicáveis aos documentos de guarda permanente. Mantido inclusive para incidentes não comunicados à ANPD e aos titulares.

1. Descrição Geral do Incidente

Data de conhecimento do incidente	*[dd/mm/aaaa hh:mm]*
Descrição geral das circunstâncias em que o incidente ocorreu	*[Descrição]*
Outras informações relevantes	*[Descrição]*

2. Dados Pessoais Afetados

Natureza dos dados afetados	☐ Dados pessoais gerais ☐ Dados pessoais sensíveis: ☐ origem racial ou étnica ☐ convicção religiosa ☐ opinião política ☐ filiação a sindicato ou a organização de caráter religioso, filosófico ou político ☐ saúde ☐ vida sexual ☐ dado genético ou biométrico
Categoria dos dados pessoais afetados	☐ Dados de crianças, de adolescentes ou de idosos ☐ Dados financeiros ☐ Dados de autenticação em sistemas ☐ Dados protegidos por sigilo legal, judicial ou profissional ☐ Dados em larga escala
Avaliação do risco	*[Baixo / Médio / Alto / Crítico — com justificativa]*
Possíveis danos aos titulares	*[Ex.: discriminação, fraude financeira, roubo de identidade, violação à imagem e à reputação]*

3. Ações Corretivas e Mitigadoras (quando aplicável)

Medidas de correção	*[Descrição]*
Medidas de mitigação	*[Descrição]*

4. Comunicação do Incidente de Segurança

Forma e conteúdo da comunicação à ANPD	*[Descrição]*
Forma e conteúdo da comunicação aos titulares	*[Descrição]*
Motivos da ausência de comunicação (quando for o caso)	*[Descrição]*