MINISTÉRIO DO TURISMO

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

MINISTÉRIO DO TURISMO

MODELO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

VERSÃO 1.0
2026

SUMÁRIO

1	**Contexto/Introdução**	4
2	**Base Legal e Normativa**	5
3	**Objetivo**	6
4	**Definições**	7
5	**Âmbito da Aplicação**	9
6	**Papéis e Responsabiliades**	10
	6.1 Unidades Organizacionais	10
	6.2 Área de Tecnologia da Informação	11
	6.3 Encarregado pelo Tratamento de Dados Pessoais	12
7	**Avaliação do Incidente de Risco**	13
8	**Comunicação do Incidente de Risco**	16
	8.1 Comunicação á Autoridade Nacional de Proteção de Dados	16
	8.2 Comunicação aos Titulares	17
9	**Registro e Documentação**	19
10	**Como Agir diante de um incidente de segurança (passo a passo)**	20
11	**O que é e o que não é incidente de segurança**	25
12	**Modelo orientativo de comunicação aos titulares (quando aplicável)**	26
13	**Guia rápido – incidente de segurança em dados pessoais**	27
14	**Disposições Finais**	28
	Anexos	29

MINISTÉRIO DO TURISMO

Esplanada dos Ministérios - Bloco U, Brasília/DF

GUSTAVO COSTA FELICIANO
Ministro do Estado de Turismo

GUSTAVO MACHADO PIRES
Chefe de Gabinete do Ministro de Estado do Turismo

FERNANDA CÂMARA NORAT
Secretária-Executiva

PAULA PAES MONTANDON VASCONCELOS
Encarregada pelo Tratamento de Dados

COMISSÃO INTERNA DA IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Ouvidor

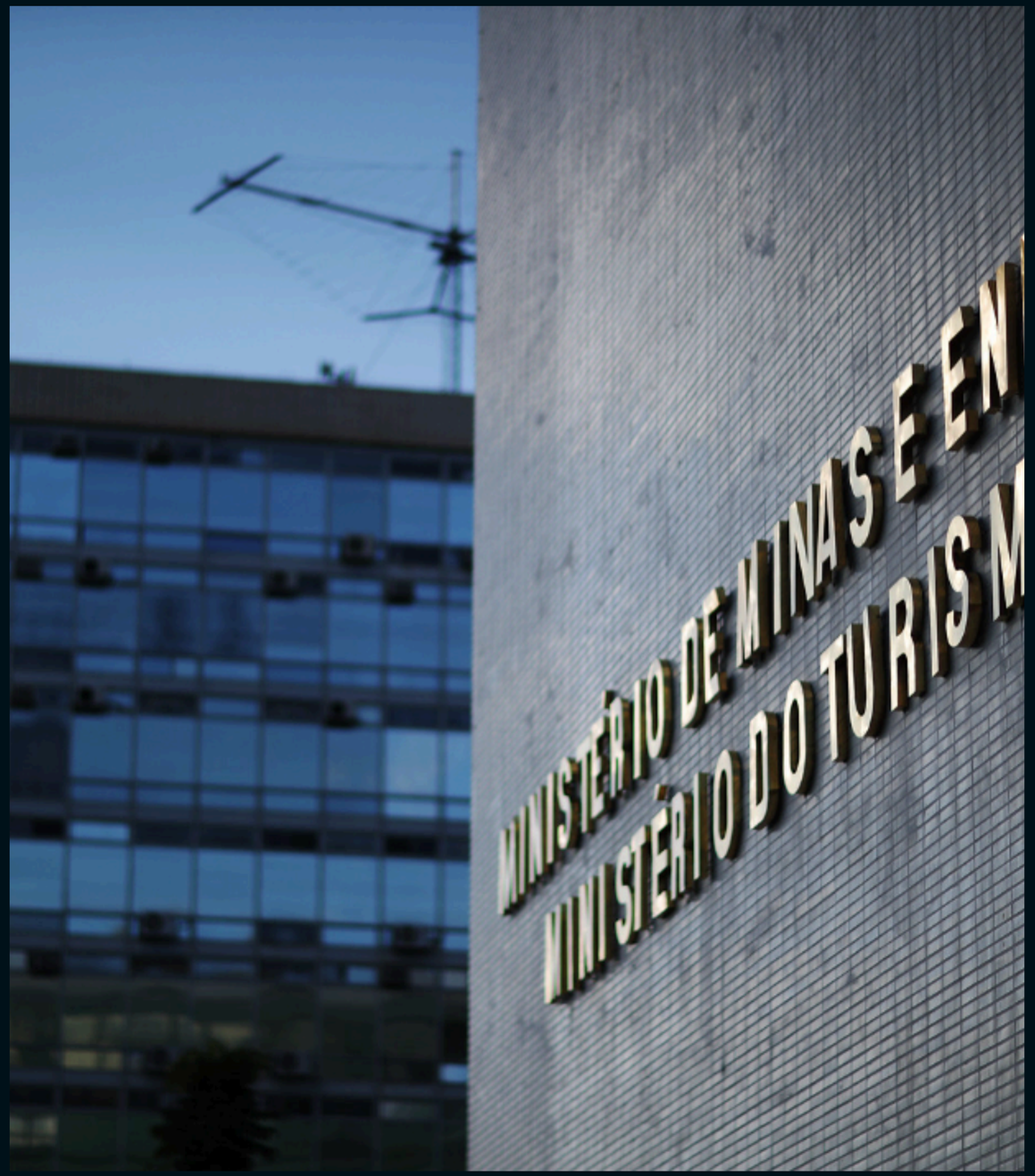
Coordenador - Geral da Tecnologia da Informação

Coordenador Geral de Gestão Estratégica de Pessoas

Coordenador Geral de Licitações e Contratos

Coordenador Geral de Recursos Logísticos

Encarregado pelo Tratamento de Dados Pessoais



1. CONTEXTO/INTRODUÇÃO

O presente Modelo de Comunicação de Incidente de Segurança estabelece diretrizes, procedimentos e responsabilidades a serem observados para a identificação, análise, avaliação, registro e comunicação de incidentes de segurança da informação envolvendo dados pessoais que possam acarretar risco ou dano relevante aos titulares.

Este documento atende às disposições da Lei nº 13.709, de 14 de agosto de 2018 — Lei Geral de Proteção de Dados Pessoais (LGPD) —, bem como às orientações, normativos e ao 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.

O dever de prevenir, identificar e mitigar riscos relacionados a incidentes de segurança deve estar integrado à estrutura de governança de segurança da informação e de proteção de dados pessoais, em alinhamento com a Política de Segurança da Informação (PSI), com as diretrizes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) e com as orientações dos órgãos centrais de governança digital e segurança da informação da Administração Pública Federal.

2. BASE LEGAL E NORMATIVA

I Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);

II Art. 48 da LGPD, que dispõe sobre a comunicação de incidentes de segurança;

III Normativos, guias e orientações expedidos pela Autoridade Nacional de Proteção de Dados (ANPD);

IV Resolução CD/ANPD nº 15, de 24 de abril de 2024, que aprova o Regulamento de Comunicação de Incidente de Segurança; e

V Demais normas aplicáveis à Administração Pública Federal relacionadas à segurança da informação, governança digital e proteção de dados pessoais

3. OBJETIVOS

O presente Modelo tem como objetivo:

Padronizar os procedimentos internos para a comunicação de incidentes de segurança envolvendo dados pessoais;

Assegurar a adequada, tempestiva e transparente comunicação à ANPD e, quando cabível, aos titulares dos dados pessoais;

Reduzir riscos institucionais, jurídicos, operacionais e reputacionais decorrentes de incidentes de segurança; e

Reduzir riscos institucionais, jurídicos, operacionais e reputacionais decorrentes de incidentes de segurança.

4. DEFINIÇÕES

INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS	Evento adverso confirmado, decorrente de ação voluntária ou acidental, que comprometa as propriedades de confidencialidade, integridade, disponibilidade ou autenticidade da segurança de dados pessoais, podendo resultar em acesso não autorizado, divulgação, alteração, perda, indisponibilidade ou qualquer forma de tratamento inadequado ou ilícito de dados pessoais, independentemente do meio em que estejam armazenados.
DADOS PESSOAIS	Informação relacionada a pessoa natural identificada ou identificável, nos termos da LGPD.
DADOS PESSOAIS SENSÍVEIS	Dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos.
TITULAR	Pessoa natural a quem se referem os dados pessoais objeto de tratamento.
ANPD	Autoridade Nacional de Proteção de Dados.
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.

INTEGRIDADE	Propriedade pela qual se assegura que o dado pessoal não foi modificado ou destruído de maneira não autorizada ou acidental.
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
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.
TITULAR	Pessoa natural a quem se referem os dados pessoais objeto de tratamento.
COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA	Ato do controlador que comunica à ANPD e ao titular de dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
DADOS EM LARGA ESCALA	Aquele que abranger número significativo de titulares, considerando, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica de localização dos titulares.

5. ÂMBITO DA APLICAÇÃO

Este Modelo aplica-se a todas as unidades organizacionais do Ministério do Turismo, abrangendo servidores públicos, colaboradores, estagiários, prestadores de serviço, operadores contratados e quaisquer terceiros que realizem atividades de tratamento de dados pessoais sob responsabilidade do MTur.

6. PAPÉIS E RESPONSABILIDADES

6.1 Unidades Organizacionais

Compete às unidades organizacionais do Ministério do Turismo:

Cooperar com as atividades de apuração, contenção, mitigação e resposta ao incidente; e

Comunicar imediatamente à área responsável e ao Encarregado pelo Tratamento de Dados Pessoais a ocorrência ou suspeita de incidente de segurança.

6.2 Área da Tecnologia da Informação

Compete à área de Tecnologia da Informação:

Apoiar tecnicamente a identificação, contenção, análise e tratamento do incidente;

Fornecer informações técnicas necessárias para a avaliação do impacto e do risco do incidente; e

Implementar medidas corretivas e preventivas para mitigar vulnerabilidades identificadas.

6.3 Encarregado pelo Tratamento de Dados Pessoais (DPO)

Compete ao Encarregado:

Avaliar a gravidade do incidente e o potencial risco ou dano relevante aos titulares;

Coordenar a elaboração e o envio da comunicação à ANPD e aos titulares, quando aplicável;

Manter registro atualizado e documentado dos incidentes de segurança; e

Atuar como ponto de contato institucional junto à ANPD.

7. AVALIAÇÃO DO INCIDENTE E DE RISCO

A avaliação do incidente de segurança com dados pessoais constitui etapa obrigatória do processo de resposta a incidentes e tem por finalidade verificar a gravidade do evento, sua extensão e a existência de risco ou dano relevante aos titulares dos dados pessoais, de modo a subsidiar a adoção de medidas de mitigação e a decisão acerca da necessidade de comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares.

A avaliação será conduzida pelo Encarregado pelo Tratamento de Dados Pessoais (DPO), com apoio técnico da Área de Tecnologia da Informação e das unidades organizacionais envolvidas, imediatamente após o conhecimento da ocorrência ou da suspeita do incidente.

Para fins da avaliação do incidente e de risco, deverão ser considerados, no mínimo, os seguintes elementos:

I - A natureza e as categorias dos dados pessoais afetados, inclusive a existência de dados pessoais sensíveis;

II - O volume de dados pessoais envolvidos e o número estimado de titulares afetados;

III - O grau de identificabilidade dos titulares, direta ou indireta;

IV - A extensão temporal, a duração e o alcance do incidente;

V - A origem e a causa do incidente, inclusive se decorrente de falha humana, técnica, operacional ou de ação maliciosa;

VI - A probabilidade de ocorrência de danos aos titulares, tais como prejuízos financeiros, discriminação, violação de direitos fundamentais, danos morais ou reputacionais;

VII - A adoção de medidas técnicas e administrativas de segurança, tais como criptografia, anonimização, controle de acesso e registro de logs; e

VIII - A possibilidade de contenção, mitigação, reversão ou eliminação dos efeitos do incidente.

Concluída a avaliação, o Encarregado deverá emitir manifestação técnica fundamentada quanto:

- I - À caracterização do incidente de segurança com dados pessoais;
- II - À existência ou não de risco ou dano relevante aos titulares;
- III - À obrigatoriedade de comunicação do incidente à ANPD, nos termos da legislação vigente;
- IV - À necessidade de comunicação aos titulares dos dados pessoais; e
- V - Às medidas corretivas, preventivas e de mitigação a serem adotadas.

A avaliação do incidente e de risco deverá ser formalmente registrada e mantida atualizada, integrando o processo de registro do incidente de segurança, para fins de comprovação de conformidade, rastreabilidade das decisões adotadas e atendimento aos princípios da responsabilização e da prestação de contas previstos na Lei nº 13.709, de 14 de agosto de 2018.

8. COMUNICAÇÃO DO INCIDENTE

8.1 Comunicação à Autoridade Nacional de Proteção de Dados (ANPD)

Quando aplicável, a comunicação à ANPD deverá ser realizada pelo DPO ou representante legal do Ministério do Turismo nos seguintes casos:

- Incidente confirmado;
- Dados pessoais envolvidos; e
- Risco ou dano relevante aos titulares.

A comunicação deverá ser realizada no prazo de 3 dias úteis a partir do conhecimento do incidente, por meio de peticionamento eletrônico no SEI da ANPD.

Admite-se comunicação em etapas, com complementação em até 20 dias úteis, quando tecnicamente justificado.

8.2 Comunicação aos Titulares

Quando aplicável, os titulares dos dados deverão ser comunicados o mais rapidamente possível, de forma clara, adequada e transparente, preferencialmente por meio de comunicação individual e direta, utilizando-se os canais habitualmente empregados pelo Ministério do Turismo.

Excepcionalmente, quando não for possível identificar ou individualizar os titulares afetados, poderá ser adotada comunicação indireta, mediante divulgação pública, devidamente justificada e com destaque adequado.

A comunicação aos titulares deverá conter, no mínimo:

- A descrição da natureza e das categorias de dados pessoais afetados;
- As medidas técnicas e de segurança utilizadas para a proteção dos dados;
- Os riscos e impactos potenciais aos titulares;
- As medidas adotadas ou planejadas para mitigar os efeitos do incidente;
- A data do conhecimento do incidente; e
- Os dados de contato do Encarregado.

Fluxo de Resposta a Incidente

1 Identificação

2 Comunicação Interna

3 Contenção e Análise Técnica

4 Avaliação de Risco

5 Comunicação à ANPD

6 Comunicação aos Tiulares

7 Registro e Melhoria Contínua

9. REGISTRO E DOCUMENTAÇÃO

Todos os incidentes de segurança, independentemente da obrigatoriedade de comunicação à ANPD, deverão ser formalmente registrados e documentados pelo Ministério do Turismo, com vistas a:

- Assegurar a rastreabilidade das decisões e ações adotadas;
- Subsidiar auditorias internas, externas e fiscalizações; e
- Apoiar a melhoria contínua dos controles de segurança da informação e proteção de dados pessoais.

10. COMO AGIR DIANTE DE UM INCIDENTE DE SEGURANÇA

Passo a passo para Ouvidoria, Áreas Técnicas e DPO.

Este capítulo apresenta, de forma objetiva e operacional, o fluxo de atuação diante da ocorrência ou suspeita de incidente de segurança envolvendo dados pessoais, observando as responsabilidades de cada ator institucional e os prazos previstos na legislação vigente.

1 IDENTIFICAÇÃO DO INCIDENTE

Quem pode Identificar: qualquer servidor, colaborador, prestador de serviço ou operador.

O que caracteriza a identificação:

- acesso não autorizado a dados pessoais
- vazamento, extravio ou perda de dados;
- indisponibilidade de sistemas com dados pessoais;
- envio indevido de informações; e
- falhas de segurança que possam comprometer dados pessoais.

⚠ **Atenção: a suspeita razoável já é suficiente para acionar o fluxo. Não é necessário aguardar confirmação técnica.**

2 COMUNICAÇÃO IMEDIATA INTERNA

Responsável: Unidade Organizacional que tomou conhecimento do fato

Providência → **Comunicar Imediatamente**

- Área de Tecnologia da Informação
- Encarregado pelo Tratamento de Dados Pessoais (DPO).

Forma: Canais institucionais definidos: (e-mail funcional, sistema interno ou outro meio formal)

Boa prática: registrar a data e a hora exatas do conhecimento do incidente.

3 CONTENÇÃO E ANÁLISE TÉCNICA

Responsável: Área da Tecnologia da Informação

Atividades Principais:

- Conter o incidente (bloqueio de acesso, isolamento de sistemas, correção de falhas);
- Preservar evidências;
- Identificar a causa e a extensão do incidente; e
- Produzir informações técnicas preliminares.

4 AVALIAÇÃO DE RISCO E DECISÃO SOBRE COMUNICAÇÃO

Responsável: Encarregado pelo Tratamento de Dados Pessoaos - DPO, com apoio técnico

Aspectos Avaliados:

- Natureza e volume dos dados pessoais;
- Envolvimento de dados sensíveis;
- Número de titulares afetados;
- Possibilidade de identificação dos titulares; e
- Potenciais danos aos direitos e liberdades.

Resultado Esperado:

- definição fundamentada sobre a necessidade de comunicação à ANPD;
- a necessidade de comunicação aos titulares; e
- a forma e o prazo dessas comunicações.

5 COMUNICAÇÃO À ANPD

Responsável: DPO ou representante legal do MTur.

Quando comunicar:

- Incidente confirmado
- Dados pessoais envolvidos
- Risco ou dano relevante aos titulares

Prazo: até 3 dias úteis a partir do conhecimento do incidente

Forma: peticionamento eletrônico do SEI da ANPD

6 COMUNICAÇÃO AOS TITULARES (QUANDO APLICÁVEL)

Responsável: DPO, com apoio das áreas competentes.

Forma preferencial: comunicação direta e individualizada

Forma excepcional: comunicação pública, quando a identificação individual for inviável, mediante justificativa.

A comunicação deve ser:
clara
transparente
proporcional ao risco

7

REGISTRO, DOCUMENTAÇÃO E MELHORIA CONTÍNUA

Responsável: DPO, com apoio das áreas envolvidas.

Providências:

- Registro formal do incidente;
- Arquivamento das decisões e comunicações;
- Análise de lições aprendidas; e
- Proposição de medidas preventivas.

CHECKLIST RÁPIDO

- O incidente foi comunicado imediatamente?
- O DPO foi acionado?
- Houve avaliação de risco documentada?
- A decisão sobre comunicar à ANPD está fundamentada?
- O incidente foi registrado formalmente?

11. O QUE É E O QUE NÃO É INCIDENTE DE SEGURANÇA

QUADRO ORIENTATIVO PARA AS UNIDADES

É considerado incidente de segurança com dados pessoais:	Não é considerado incidente de segurança (em regra):
vazamento ou divulgação não autorizada de dados pessoais	falhas operacionais sem envolvimento de dados pessoais
acesso indevido a sistemas ou bases de dados	solicitações de titulares sobre seus direitos (acesso, correção etc)
perda ou extravio de documentos físicos ou mídias com dados pessoais	reclamações administrativas comuns
envio de e-mail com dados pessoais a destinatário incorreto	incidentes puramente técnicos que não afetem dados pessoais
indisponibilidade de sistemas que comprometa dados pessoais	
falhas de segurança exploradas ou potencialmente exploráveis	

⚠️ Importante: em caso de dúvida, o evento deve ser tratado inicialmente como incidente, até avaliação técnica e de risco pelo DPO.

12. MODELO ORIENTATIVO DE COMUNICAÇÃO AOS TITULARES (QUANDO APLICÁVEL)

Nota: o texto abaixo é apenas orientativo e deve ser adaptado ao caso concreto, considerando o princípio da transparência e da proporcionalidade.

Assunto: Comunicação sobre incidente de segurança envolvendo dados pessoais

O Ministério do Turismo informa que, em [data], tomou conhecimento de um incidente de segurança que envolveu dados pessoais sob sua responsabilidade.

O incidente consistiu em [descrição objetiva], tendo afetado as seguintes categorias de dados: [informar]. Até o momento, não há/foram identificados indícios de uso indevido dos dados.

Desde a identificação do incidente, o Ministério do Turismo adotou medidas técnicas e administrativas para contenção e mitigação dos riscos, incluindo [descrever de forma sucinta].

Os titulares podem, a qualquer tempo, entrar em contato com o Encarregado pelo Tratamento de Dados Pessoais por meio do e-mail [canal institucional], para esclarecimentos adicionais.

O Ministério do Turismo reafirma seu compromisso com a proteção dos dados pessoais e com a transparência no tratamento dessas informações.

Atenciosamente,
Ministério do Turismo

13. GUIA RÁPIDO – INCIDENTE DE SEGURANÇA EM DADOS PESSOAIS

Resumo executivo da cartilha

Identificou ou suspeitou de incidente? Comunique imediatamente a TI e o DPO.

Contenção: a TI atua para conter e analisar tecnicamente.

Avaliação: o DPO avalia risco ou dano relevante.

Prazos:
até 3 dias úteis → comunicação à ANPD;
até 20 dias úteis → comunicação complementar (se necessário).

Titulares: comunicar quando houver risco ou dano relevante

Registro: todo incidente deve ser documentado.

Regra de ouro: rapidez, documentação e proteção do titular são pilares da boa governança em proteção de dados.

14. DISPOSIÇÕES FINAIS

O presente Modelo deverá ser periodicamente revisado, considerando alterações normativas, atualizações das orientações da ANPD e mudanças nos processos internos do Ministério do Turismo.

Os casos omissos serão avaliados pelo Encarregado pelo Tratamento de Dados Pessoais, em conjunto com as áreas competentes.

ANEXO I -

Formulário de **Notificação** de Incidente de segurança.

Processo nº	XXXXX.XXXXX/XXXX-XX
1. **Identificação do Comunicante**	
Nome completo	
Unidade/Lotação	
E-mail de contato	
Telefone para contato	
Data da comunicação	Data da comunicação
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]
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 – conforme LGPD
Categoria dos Dados Pessoais	( ) Dados de crianças, adolescentes ou 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: [Especifique]

ANEXO II -

Formulário de **Registro** de Incidente de Segurança

Processo nº	XXXXX.XXXXX/XXXX-XX
1. **Descrição Geral do Incidente**	
Data do 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 dos Afetados**	
Natureza dos Afetados	( ) Dados pessoais gerais ( ) Dados pessoais sensíveis (detalhar, quando aplicável)
Categoria dos Afetados	( ) Dados de crianças, adolescentes ou idosos ( ) Dados financeiros ( ) Dados de autenticação em sistemas ( ) Dados protegidos por sigilo legal, judicial ou profissional ( ) Dados em larga escala
Avaliação do risco	[Descrição]
Possíveis danos aos titulares	[Descrição]
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]

MODELO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

2026

MINISTÉRIO DO TURISMO

GOVERNO FEDERAL

BRASIL

UNIÃO E RECONSTRUÇÃO