

# Modelo de Comunicação Incidente de Segurança

Dados Pessoais



# Sumário

<b>1. Contexto</b>	<b>3</b>	<b>11. Comunicação aos Titulares</b>	<b>9</b>
<b>2. Base Legal</b>	<b>3</b>	<b>12. Competências</b>	<b>10</b>
<b>3. Objetivos</b>	<b>4</b>	<b>13. Registro, Documentação e Retenção</b>	<b>11</b>
<b>4. Conceituação</b>	<b>4</b>	<b>14. Governança e Accountability</b>	<b>12</b>
<b>5. Âmbito de Aplicação</b>	<b>5</b>	<b>15. DISPOSIÇÕES FINAIS</b>	<b>13</b>
<b>6. Diretrizes</b>	<b>5</b>	<b>ANEXO I – FORMULÁRIO INTERNO DE NOTIFICAÇÃO DE INCIDENTE DE SEGURANÇA</b>	<b>14</b>
<b>7. Identificação e Comunicação Interna</b>	<b>6</b>		
<b>8. Avaliação do Incidente e do Risco</b>	<b>6</b>		
<b>9. Contenção, Tratamento e Mitigação</b>	<b>8</b>		
<b>10. Comunicação à Autoridade Nacional de Proteção de Dados – ANPD</b>	<b>8</b>		



## 1. Contexto

O presente Modelo de Comunicação de Incidente de Segurança com Dados Pessoais estabelece diretrizes, responsabilidades, critérios e procedimentos a serem observados para identificação, avaliação, registro, tratamento e comunicação de incidentes de segurança envolvendo dados pessoais no âmbito da Empresa Brasil de Comunicação – EBC.

O documento tem por finalidade assegurar a adequada governança dos incidentes de segurança com dados pessoais, em conformidade com a Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente o disposto no art. 48, bem como com a Resolução CD/ANPD nº 15, de 24 de abril de 2024, que aprova o Regulamento de Comunicação de Incidente de Segurança.

O dever de prevenir, identificar, registrar, mitigar e responder aos incidentes de segurança deve integrar a estrutura de governança, segurança da informação, integridade e proteção de dados pessoais da EBC, observando-se os princípios da prevenção, responsabilização, prestação de contas, transparência e segurança.

Este procedimento deverá ser observado por todas as unidades organizacionais, empregados, colaboradores, estagiários, terceirizados, prestadores de serviço, operadores contratados e demais agentes que realizem atividades de tratamento de dados pessoais sob responsabilidade da EBC.

## 2. Base Legal

Este modelo observa, especialmente:

- [Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais \(LGPD\)](#);
- [Resolução CD/ANPD nº 15/2024, que aprova o Regulamento de Comunicação de Incidente de Segurança](#)
- [NOR 705 - Norma de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos](#);
- [PO 900/10 - Política de Proteção de Dados Pessoais](#);
- Demais orientações expedidas pela ANPD.



### 3. Objetivos

O presente modelo tem como objetivos:

- i. padronizar os procedimentos internos relacionados à identificação, análise, avaliação, tratamento e comunicação de incidentes de segurança envolvendo dados pessoais;
- ii. assegurar resposta tempestiva, coordenada e transparente aos incidentes de segurança;
- iii. reduzir riscos institucionais, operacionais, jurídicos, reputacionais e financeiros decorrentes de incidentes de segurança;
- iv. assegurar a adequada comunicação à Autoridade Nacional de Proteção de Dados – ANPD e aos titulares dos dados pessoais, quando aplicável;
- v. promover a rastreabilidade, documentação e accountability das decisões adotadas;
- vi. fortalecer a governança em proteção de dados pessoais e segurança da informação;
- vii. assegurar conformidade com a legislação aplicável.

### 4. Conceituação

Para os fins deste modelo, considera-se:

#### **Autoridade Nacional de Proteção de Dados (ANPD)**

Órgão da Administração Pública Federal responsável por zelar pela proteção dos dados pessoais, assim como por implementar e fiscalizar o cumprimento da legislação nacional de proteção de dados pessoais

#### **Dados Pessoais**

Informação relacionada à pessoa natural identificada ou identificável, inclusive o dado pessoal sensível, tal como definido na Lei Geral de Proteção de Dados Pessoais (LGPD).

#### **Dados Pessoais Sensíveis**

Dado pessoal sobre 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.



## Encarregado

Pessoa indicada pelo Diretor-Presidente para atuar como canal de comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

## Incidente de Segurança

Qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais

## Titular de Dados Pessoais

Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

## 5. Âmbito de Aplicação

Este modelo aplica-se:

- i. a todas as unidades organizacionais da EBC;
- ii. aos empregados públicos, colaboradores, estagiários e terceirizados;
- iii. aos prestadores de serviço e operadores contratados;
- iv. a quaisquer terceiros que realizem tratamento de dados pessoais sob responsabilidade da EBC.

## 6. Diretrizes

Constituem diretrizes gerais:

- I. atuação tempestiva na identificação e tratamento de incidentes;
- II. preservação da confidencialidade, integridade, disponibilidade e autenticidade dos dados pessoais;
- III. adoção de medidas preventivas, corretivas e mitigatórias;
- IV. observância dos princípios da necessidade, adequação, segurança, prevenção e responsabilização;
- V. transparência na comunicação com a ANPD e com os titulares;
- VI. manutenção de registros e evidências relacionados aos incidentes;
- VII. cooperação entre as unidades organizacionais envolvidas;
- VIII. melhoria contínua dos controles de segurança da informação e proteção de dados pessoais.



## 7. Identificação e Comunicação Interna

Qualquer empregado, colaborador, prestador de serviço, operador ou unidade organizacional que identificar ou suspeitar da ocorrência de incidente de segurança envolvendo dados pessoais deverá comunicar imediatamente:

- à área responsável pela Segurança da Informação;
- ao Encarregado pelo Tratamento de Dados Pessoais.

A suspeita razoável é suficiente para acionamento do fluxo interno de resposta ao incidente, independentemente de confirmação técnica prévia.

Deverão ser registrados, sempre que possível:

- I. data e hora da ciência do incidente;
- II. unidade ou pessoa que identificou o evento;
- III. descrição preliminar do ocorrido;
- IV. sistemas, bases ou documentos potencialmente afetados;
- V. medidas emergenciais já adotadas.

## 8. Avaliação do Incidente e do Risco

### Conceito e finalidade

A avaliação do incidente de segurança constitui etapa obrigatória do processo de resposta a incidentes e tem por finalidade verificar:

- I. a gravidade do evento;
- II. a extensão do incidente;
- III. a existência de risco ou dano relevante aos titulares;
- IV. a necessidade de comunicação à ANPD;
- V. a necessidade de comunicação aos titulares;
- VI. as medidas de contenção, mitigação e remediação aplicáveis.



## Responsáveis pela avaliação

A avaliação do incidente deverá ser conduzida pelo Encarregado pelo Tratamento de Dados Pessoais, com apoio técnico da área de Segurança da Informação e da Gerência Executiva de Governança Corporativa e Correição.

## Elementos mínimos da avaliação

Para fins da avaliação do incidente e do risco, deverão ser considerados, no mínimo:

- a natureza e categoria e volume dos dados pessoais afetados;
- a existência de dados pessoais sensíveis;
- o número estimado de titulares afetados;
- a possibilidade de identificação direta ou indireta dos titulares;
- a abrangência temporal e geográfica do incidente;
- a origem e causa do incidente, como a existência de falha humana, técnica, operacional ou ação maliciosa;
- os impactos potenciais aos titulares;
- as medidas técnicas e administrativas de segurança existentes;

- as medidas de mitigação adotadas;
- a possibilidade de contenção, reversão ou mitigação dos efeitos do incidente;
- a existência de indícios de uso indevido dos dados pessoais.

## Manifestação técnica fundamentada

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

- I. caracterização ou não do incidente de segurança com dados pessoais;
- II. avaliação sobre risco ou dano relevante aos titulares;
- III. necessidade de comunicação à ANPD;
- IV. necessidade de comunicação aos titulares;
- V. medidas corretivas e preventivas recomendadas;
- VI. justificativa das medidas a serem adotadas.

A avaliação deverá integrar o processo formal de registro do incidente.



## 9. Contenção, Tratamento e Mitigação

Após a identificação do incidente, deverão ser adotadas medidas destinadas à contenção, tratamento e mitigação dos riscos.

As medidas poderão incluir:

- I. bloqueio de acessos indevidos;
- II. isolamento de sistemas ou ambientes comprometidos;
- III. redefinição de credenciais;
- IV. correção de vulnerabilidades;
- V. restauração de backups;
- VI. suspensão temporária de operações;
- VII. monitoramento reforçado;
- VIII. preservação de evidências e logs;
- IX. adoção de medidas preventivas adicionais.

A preservação de evidências deverá observar boas práticas de segurança da informação e possibilitar eventual auditoria, apuração ou fiscalização.

## 10. Comunicação à Autoridade Nacional de Proteção de Dados – ANPD

### Hipóteses de comunicação

A comunicação à ANPD deverá ocorrer quando houver, cumulativamente:

- I. incidente confirmado;
- II. envolvimento de dados pessoais;
- III. risco ou dano relevante aos titulares.

### Prazo para comunicação

A comunicação deverá ser realizada em até 3 (três) dias úteis contados do conhecimento do incidente.

Quando não for possível apresentar todas as informações no momento inicial da comunicação, poderá ser realizada comunicação preliminar, com complementação posterior das informações em até 20 (vinte) dias úteis, mediante justificativa técnica.

### Responsável pela comunicação

A comunicação à ANPD deverá ser realizada pelo Encarregado pelo Tratamento de Dados Pessoais ou por representante formalmente designado pela EBC, exclusivamente por meio do sistema eletrônico



disponibilizado pela Autoridade em seu portal institucional, observando-se os formulários, procedimentos e orientações vigentes.

### **Conteúdo mínimo da comunicação**

A comunicação à ANPD deverá conter, sempre que possível:

- I. descrição da natureza do incidente;
- II. data e hora da ocorrência e da ciência do incidente;
- III. categorias de dados pessoais afetados;
- IV. quantidade aproximada de titulares envolvidos;
- V. indicação da existência de dados pessoais sensíveis;
- VI. descrição das medidas técnicas e administrativas utilizadas para proteção dos dados;
- VII. riscos relacionados ao incidente;
- VIII. medidas de contenção, mitigação e remediação adotadas;
- IX. possíveis impactos aos titulares;
- X. justificativa para eventual atraso na comunicação;

XI. identificação e contato do Encarregado;

XII. informações sobre comunicação aos titulares, quando aplicável.

### **Comunicação complementar**

Sempre que houver atualização relevante das informações inicialmente comunicadas, a EBC deverá complementar a comunicação junto à ANPD.

## **11. Comunicação aos Titulares**

### **Hipóteses de comunicação**

Os titulares dos dados pessoais deverão ser comunicados quando o incidente puder acarretar risco ou dano relevante.

### **Forma da comunicação**

A comunicação aos titulares deverá ocorrer de forma:

- I. clara;
- II. adequada;
- III. transparente;



IV. objetiva;

V. proporcional à gravidade do incidente.

Preferencialmente, deverá ser realizada comunicação individualizada e direta.

Excepcionalmente, quando não for possível identificar ou individualizar os titulares afetados, poderá ser realizada comunicação pública, devidamente justificada.

### **Conteúdo mínimo da comunicação aos titulares**

A comunicação deverá conter, no mínimo:

I. descrição do incidente;

II. categorias de dados afetados;

III. data do conhecimento do incidente;

IV. riscos e impactos potenciais;

V. medidas técnicas e administrativas adotadas;

VI. orientações aos titulares;

VII. canais de contato do Encarregado pelo Tratamento de Dados Pessoais.

### **Recomendações aos titulares**

Sempre que aplicável, deverão ser fornecidas orientações aos titulares para redução dos riscos decorrentes do incidente, incluindo:

I. alteração de senhas;

II. monitoramento de movimentações financeiras;

III. atenção a tentativas de fraude ou phishing;

IV. atualização de credenciais;

V. contato com instituições financeiras ou autoridades competentes.

## **12. Competências**

### **Unidades organizacionais**

I. comunicar imediatamente incidentes ou suspeitas;

II. cooperar com as atividades de apuração, contenção e mitigação;

III. disponibilizar informações necessárias à avaliação do incidente;

IV. apoiar a implementação de medidas corretivas.



## **Gerência Executiva de Tecnologia da Informação**

- I. apoiar tecnicamente a identificação, contenção e tratamento do incidente;
- II. fornecer informações técnicas necessárias à avaliação do risco;
- III. implementar medidas corretivas e preventivas;
- IV. preservar evidências e registros técnicos;
- V. apoiar a recuperação dos ambientes afetados.
- VI. monitorar vulnerabilidades e ameaças;

## **Encarregado pelo Tratamento de Dados Pessoais**

- I. coordenar a avaliação do incidente;
- II. atuar como ponto de contato junto à ANPD;
- III. coordenar a elaboração e envio das comunicações à ANPD e aos titulares;
- IV. manter registro atualizado dos incidentes;
- V. emitir manifestação técnica fundamentada;

VI. orientar as unidades organizacionais quanto às medidas necessárias;

VII. apoiar ações de conscientização e governança em proteção de dados.

## **Alta Administração**

I. assegurar recursos necessários à gestão de incidentes;

II. apoiar ações de governança e conformidade;

III. promover cultura institucional de proteção de dados e segurança da informação.

## **13. Registro, Documentação e Retenção**

Todos os incidentes de segurança envolvendo dados pessoais, independentemente da obrigatoriedade de comunicação à ANPD, deverão ser formalmente registrados e documentados.

Os registros deverão conter, sempre que possível:

I. descrição do incidente;

II. data da ocorrência e da ciência;

III. unidades envolvidas;



- IV. dados afetados;
- V. avaliação de risco;
- VI. decisões adotadas;
- VII. medidas implementadas;
- VIII. comunicações realizadas;
- IX. evidências e documentos relacionados.

Os registros deverão ser mantidos pelo prazo mínimo definido na regulamentação aplicável e nas normas internas da EBC.

### **Medidas Corretivas, Preventivas e Melhoria Contínua**

Após o encerramento do tratamento do incidente, deverão ser avaliadas medidas destinadas à prevenção de recorrências.

As medidas poderão incluir:

- I. revisão de controles internos;
- II. atualização de políticas e procedimentos;
- III. reforço de mecanismos de autenticação e controle de acesso;
- IV. atualização tecnológica;

- V. capacitação e conscientização de empregados;
- VI. revisão contratual com operadores e fornecedores;
- VII. realização de auditorias e testes de segurança.

A EBC deverá promover melhoria contínua de seus controles de segurança da informação e proteção de dados pessoais.

## **14. Governança e Accountability**

A gestão de incidentes de segurança com dados pessoais deverá observar os princípios da responsabilização e prestação de contas.

A EBC deverá manter evidências capazes de demonstrar:

- I. adoção de medidas preventivas e corretivas;
- II. atuação diligente na resposta aos incidentes;
- III. conformidade com a legislação aplicável;
- IV. rastreabilidade das decisões adotadas;
- V. efetividade das medidas implementadas.

A gestão de incidentes deverá integrar as práticas institucionais de governança, gestão de riscos, integridade, segurança da informação e proteção de dados pessoais.



## 15. DISPOSIÇÕES FINAIS

Este modelo deverá ser revisado periodicamente, considerando:

- I. alterações normativas;
- II. orientações expedidas pela ANPD;
- III. evolução dos riscos tecnológicos;
- IV. alterações nos processos internos;
- V. resultados de auditorias, avaliações e lições aprendidas.

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



## ANEXO I – FORMULÁRIO INTERNO DE NOTIFICAÇÃO DE INCIDENTE DE SEGURANÇA

Este formulário destina-se ao registro e à comunicação interna preliminar de incidentes de segurança envolvendo dados pessoais, devendo ser preenchido pela unidade organizacional, empregado, colaborador, operador ou prestador de serviço que identificar ou suspeitar da ocorrência do incidente.

### 1. Identificação do comunicante

Nome:

Unidade/Lotação:

E-mail:

Telefone:

Data da comunicação:

### 2. Descrição geral do incidente

Data e hora da ocorrência:

Data e hora da ciência:

Descrição objetiva do incidente:

Sistemas ou bases afetadas:

Causa provável:

### 3. Dados pessoais afetados

Dados pessoais gerais

Dados pessoais sensíveis

Dados financeiros

Dados de autenticação

Dados de crianças, adolescentes ou idosos

Dados protegidos por sigilo legal

Quantidade aproximada de titulares afetados:

### 4. Tipo de violação

Acesso não autorizado

Vazamento

Alteração indevida

Perda ou destruição

Indisponibilidade

Roubo ou furto de equipamento

Ransomware

Outro

### 5. Medidas adotadas

Descrever as medidas de contenção e mitigação já implementadas.

