Lobo de Rizzo

# Resolução CD/ANPD nº 15, de 24 de abril de 2024

## Regulamento de Comunicação de Incidente de Segurança

Na última sexta-feira (26), **a ANPD publicou** a **Resolução nº 15**, com entrada em vigor imediata, que aprova o Regulamento de Comunicação de Incidente de Segurança.

A Resolução aplica-se aos processos de comunicação de incidentes de segurança em curso, respeitados os atos processuais praticados e consolidados.

Destacamos, a seguir, os principais pontos trazidos pela nova resolução:

# Resolução CD/ANPD nº 15, de 24 de abril de 2024

## Regulamento de Comunicação de Incidente de Segurança

### Aspectos Gerais

**Definição de incidente de segurança**:

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

**Agente de tratamento responsável pela comunicação à ANPD e aos titulares:**

Controlador, representado pelo encarregado e/ou representante legal.

**Hipóteses de comunicação:**

Sempre que houver possibilidade de risco ou dano relevante aos titulares e, cumulativamente, envolver dados (a) sensíveis; (b) de crianças, adolescentes ou idosos; (c) financeiros; (d) de autenticação em sistemas; (e) protegidos por sigilo legal, judicial ou profissional e/ou (f) em larga escala.

### Comunicação de Incidente de Segurança à ANPD

**Prazo para a comunicação:**

**3 (três) dias úteis**, contados do conhecimento pelo controlador.
**Exceção:** agentes de pequeno porte (prazo em dobro).

**Comunicação complementar:**

**20 dias úteis**, a contar da data da comunicação.

**Informações obrigatórias:**

- Natureza e categoria de dados pessoais afetados;
- Número de titulares afetados, discriminando crianças, adolescentes e idosos;
- Medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, adotadas antes e após o incidente, observados os segredos comercial e industrial;
- Riscos e impactos aos titulares;
- Os motivos da demora, no caso de comunicação fora do prazo;
- Medidas que foram ou que serão adotadas para reverter ou mitigar riscos;
- Data do incidente, quando possível determinar;
- Data do conhecimento do incidente pelo controlador;
- Dados do encarregado ou representante legal;
- Identificação do controlador e, se for o caso, declaração confirmando se tratar de agente de pequeno porte;
- Identificação do operador, quando aplicável;
- Descrição do incidente, incluindo a causa principal, caso seja possível identificá-la;
- Total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente;
- Indicação sobre comunicação aos titulares (constando meios e conteúdo), quando cabível.

**Canal:** Super ANPD (atualmente).

**Sigilo do comunicado:**

**Público**, em regra, podendo ser solicitado sigilo de forma fundamentada.

### Comunicação de Incidente de Segurança ao Titular

**Prazo: 3 (três) dias úteis**, contados do conhecimento pelo controlador.
**Exceção:** agentes de pequeno porte (prazo em dobro).

**Informações obrigatórias:**

- Natureza e categoria de dados pessoais afetados;
- Medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- Riscos relacionados e impactos aos titulares;
- Motivos da demora, no caso de comunicação fora do prazo;
- As medidas que foram ou que serão adotadas para reverter ou mitigar riscos;
- A data do conhecimento; e
- Contato para mais informações e indicação de encarregado.

**Meio:**

Contato do titular a que tiver acesso. Quando **não for possível a comunicação direta e individualizada**, a comunicação deverá ocorrer via comunicado ostensivo em meios de divulgação disponíveis, tais como o site, aplicativos e mídias sociais do controlador, pelo período de, no mínimo, três meses.

**Atenção!**
Será considerada boa-prática a inclusão, na comunicação ao titular, de recomendações aptas a reverter ou mitigar os efeitos do incidente.

### Possíveis consequências da comunicação à ANPD

**Solicitação de informações adicionais:**

A **ANPD poderá solicitar informações adicionais** referentes ao incidente, tais como o registro das operações de tratamento dos dados pessoais (o "**ROPA**") afetados pelo incidente, relatório de impacto à proteção de dados pessoais (**RIPD**) e relatório de tratamento do incidente, estabelecendo prazo para o envio das informações.

**Determinação de medidas preventivas:**

A **ANPD poderá determinar a adoção imediata de medidas preventivas**, independente de prévia manifestação do controlador. Por exemplo, poderá requerer a ampla divulgação do incidente em meios de comunicação.

**Multas:**

Sem prejuízo de a sanção a ser imposta, a **ANPD poderá fixar multa diária para assegurar o cumprimento de medida preventiva**, conforme regulamento de dosimetria e aplicação de sanções administrativas.

**Hipóteses de declaração de extinção do processo:**

- Evidências insuficientes da ocorrência do incidente, ressalvada a possibilidade de reabertura caso surjam fatos novos;
- Não identificação de risco ou dano relevante aos titulares;
- Não envolvimento de dados pessoais;
- Reversão ou mitigação suficiente dos efeitos gerados; ou
- Realização da comunicação aos titulares e adoção das providências pertinentes pelo controlador.

**Processo administrativo sancionador:**

A **ANPD pode instaurá-lo caso o controlador não adote medidas para reverter ou mitigar** os efeitos no prazo e nas condições determinadas.

### Registro do incidente de segurança

**Obrigatoriedade:**

Ainda que não haja necessidade de comunicação à ANPD e aos titulares, o **controlador é obrigado a manter o registro** do incidente.

**Prazo de guarda: 5 anos**, contados a partir da data do registro, **exceto se constatadas obrigações adicionais** que demandem maior prazo de manutenção.

**Conteúdo obrigatório do registro do incidente:**

- Data de conhecimento do incidente;
- Descrição geral das circunstâncias em que o incidente ocorreu;
- Natureza e categoria de dados afetados;
- Número de titulares afetados;
- Avaliação do risco e possíveis danos;
- Medidas de correção e mitigação dos efeitos do incidente;
- Forma e conteúdo de eventual comunicação;
- Motivos da ausência de comunicação, quando for o caso.