

# ANÁLISE-RESUMO

## Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais

No dia 02 de maio, foi publicada a minuta do Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais que busca estabelecer **regras para a comunicação de incidentes de segurança envolvendo dados pessoais** à ANPD e aos titulares. A minuta prevê aspectos relacionados ao prazo de notificação, estabelece aspectos processuais e providências para a salvaguarda dos direitos dos titulares.

O texto está aberto para recebimento de contribuições da sociedade, as quais podem ser feitas pela Plataforma Participe + Brasil, com encerramento previsto para **31/05/2023**.



## O QUE É CONSIDERADO UM INCIDENTE?

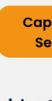
A ANPD define incidente de segurança como um evento adverso que comprometa a **confidencialidade, integridade ou disponibilidade** de dados pessoais, podendo decorrer de ações voluntárias ou acidentais que resultem na divulgação, alteração, perdas indevidas ou acessos não autorizados a dados pessoais, independentemente do meio em que estão armazenados. Exemplos:



Envio de informações para o destinatário incorreto



Furto de um dispositivo de armazenamento de dados



Invasão de um sistema de armazenamento de informações

## QUANDO OS INCIDENTES DEVEM SER COMUNICADOS?

Capítulo III  
Seção I

Devem ser comunicados à ANPD e aos titulares os incidentes de segurança com dados pessoais que tiverem as seguintes características:

### Causar risco ou danos relevantes aos titulares

têm o potencial de **afetar significativamente interesses e direitos fundamentais dos titulares** ao:

impedir ou limitar o exercício de direitos ou a utilização de um serviço

ou

ocasionar danos materiais ou morais aos titulares

ex. discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou uso indevido de identidade.



### Envolver pelo menos um dos seguintes critérios

Dados sensíveis

Dados Financeiros

Tratamento em larga escala

Dados de crianças e adolescentes ou idosos

Dados de autenticação em sistemas

## QUEM É O RESPONSÁVEL PELA COMUNICAÇÃO?

### O CONTROLADOR DOS DADOS PESSOAIS

É responsável pela comunicação do incidente de segurança envolvendo dados pessoais tanto para o titular quanto para a ANPD.



## QUAL O PRAZO DE COMUNICAÇÃO?

3 dias úteis

Para realizar a comunicação à ANPD e/ou aos titulares, contados a partir do conhecimento do incidente de segurança.

Para os agentes de tratamento de pequeno porte o prazo de comunicação é contado em dobro

As informações poderão ser complementadas, no prazo de 20 dias úteis, prorrogável uma vez, por igual período, mediante solicitação fundamentada a ser avaliada pela ANPD.

## QUAIS INFORMAÇÕES DEVERÃO CONSTAR NA COMUNICAÇÃO DO INCIDENTE PARA A ANPD?



descrição da **natureza** e da **categoria de dados pessoais afetados**



**número total de titulares afetados**, especificando o número de crianças, de adolescentes ou de idosos quando aplicável



**medidas de segurança** adotadas ou que serão adotadas para **reverter ou mitigar os efeitos do incidente**



**riscos** e os **possíveis impactos** aos titulares



os motivos da **comunicação não ter sido apresentada no prazo**, caso aplicável



**data** e a **hora do conhecimento do incidente** de segurança



**dados do encarregado**, quando aplicável, ou do **comunicante**



**dados de identificação do controlador**



informações sobre o **operador**, se houver



**descrição do incidente**



declaração de que foi realizada a **comunicação aos titulares**



o **número total** de titulares cujos dados são tratados pela organização e na atividade de tratamento afetada pelo incidente

## QUAIS INFORMAÇÕES DEVERÃO CONSTAR NA COMUNICAÇÃO DO INCIDENTE PARA OS TITULARES?



descrição da **natureza** e da **categoria de dados pessoais afetados**



**riscos** ou **impactos** ao titular



**medidas** que foram ou que serão adotadas para **reverter ou mitigar os efeitos do incidente**, se houver



**data do conhecimento** do incidente de segurança



**contato** para obtenção de informações e dados do encarregado, se houver



**uso de linguagem simples e de fácil entendimento**

**Ocorrer de forma direta e individualizada**

pode ser realizada pelos meios usualmente utilizados pelo controlador para contatar o titular, como telefone, e-mail, mensagem eletrônica ou carta.

**É necessário que a comunicação do incidente para os titulares siga os seguintes critérios:**

O controlador deverá comunicar o incidente pelos meios de divulgação disponíveis, como na sua página na Internet, em aplicativos, em suas mídias sociais e em canais de atendimento ao titular. A comunicação deverá ser de fácil visualização e ficar disponibilizada pelo período de, no mínimo, seis meses.



## O QUE FAZER SE NÃO FOR NECESSÁRIO COMUNICAR O INCIDENTE?

O controlador deverá manter o registro de incidentes de segurança, inclusive daqueles não comunicados à ANPD e aos titulares, pelo prazo mínimo de cinco anos, contados a partir da data do registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção.

## O QUE ACONTECE COM OS INCIDENTES NÃO COMUNICADOS PELO CONTROLADOR QUE A ANPD VENHA A TOMAR CONHECIMENTO?

Caso o incidente possa **ocasionar risco ou dano relevante** aos titulares, e o controlador não tenha comunicado o incidente, a Autoridade poderá investigar a situação por meio do **procedimento de apuração de incidente**.

### SANÇÕES



A ANPD poderá **fixar multa diária** para assegurar o cumprimento do envio da comunicação do incidente à Autoridade e aos titulares:



O limite da multa diária a ser estabelecida pela ANPD é de **R\$ 50.000.000,00 (cinquenta milhões de reais)**

conforme disposto no [Regulamento de Dosimetria e Aplicação de Sanções Administrativas](#)



A ANPD poderá **instaurar processo administrativo sancionador** para apurar o descumprimento da obrigação de comunicação dos dados pessoais do incidente, podendo resultar na aplicação de demais sanções previstas na legislação.

## APÓS A COMUNICAÇÃO, QUAL SERÁ O PROCEDIMENTO SEGUIDO PELA ANPD?

**1** Recebimento da comunicação do incidente pela ANPD

**2** Realização de auditorias ou inspeções

A ANPD poderá, a **qualquer momento**, determinar ou realizar auditorias ou inspeções junto aos agentes de um controlador para coletar informações complementares ou validar as informações recebidas.

**3** Avaliação da gravidade do incidente

Com as informações fornecidas pelo controlador ou coletadas durante as auditorias e inspeções, a ANPD avaliará a gravidade do incidente.

**4** Determinação de providência de salvaguardas

Após a avaliação da gravidade do incidente, a ANPD poderá determinar ao controlador:

### Ampla divulgação do incidente



**Em meios de comunicação** como a publicação em sites e nas redes sociais do controlador ou em outros meios de grande alcance.



quando a comunicação realizada pelo controlador se mostrar insuficiente para alcançar os titulares afetados.

### Medidas de mitigação

Que garantam a confidencialidade, a integridade, a disponibilidade e a autenticidade dos dados pessoais afetados, bem como medidas capazes de minimizar os efeitos do incidente para os titulares de dados.



**DIVULGAÇÃO NO SITE DA ANPD**

ANPD poderá divulgar em seu site informações relativas a incidentes de segurança com dados pessoais, com o objetivo de trazer maior transparência, segurança e orientações aos titulares afetados, observados os segredos comercial e industrial.

Obs: Cabe ao controlador solicitar à ANPD, de maneira fundamentada, o sigilo de informações protegidas por lei.

**5** Monitoramento do cumprimento das determinações e da implantação das medidas

A ANPD realizará o monitoramento do cumprimento das determinações e da implantação das medidas, com base em critérios de priorização.

**6** Instauração de processo administrativo sancionador

Caso o controlador não adote as medidas solicitadas, a ANPD poderá instaurar processo administrativo sancionador, podendo resultar na aplicação de multas e outras sanções descritas na lei.

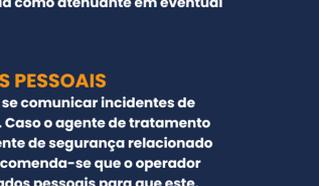
**7** Fim do processo de comunicação de incidente

Ocorrerá a extinção do processo de comunicação se, durante o procedimento de comunicação, a ANPD considerar:

1) que o incidente não possui potencial para acarretar risco ou dano relevante aos titulares de dados; ou

2) que não sejam necessárias medidas adicionais para mitigação ou reversão dos efeitos gerados

## PONTOS IMPORTANTES SOBRE A COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA



### NEM TODO INCIDENTE DEVE SER COMUNICADO À ANPD

Existe a obrigação legal de comunicar à ANPD apenas os incidentes que possam causar riscos ou danos relevantes aos titulares. É papel do controlador dos dados pessoais realizar uma avaliação cuidadosa sobre os riscos e impactos aos titulares decorrentes do incidente, verificando se existe a necessidade de comunicar a Autoridade.

### INDICAÇÃO DE BOA-FÉ

A comunicação voluntária do incidente pelo controlador reforça a transparência, cooperação e boa-fé do agente e poderá ser considerada como atenuante em eventual ação fiscalizatória da ANPD.

### CASO ATUE COMO OPERADOR DOS DADOS PESSOAIS

O artigo 48 da LGPD determina que a obrigação legal de se comunicar incidentes de segurança à ANPD é do controlador dos dados pessoais. Caso o agente de tratamento atue como operador e tome conhecimento de um incidente de segurança relacionado aos dados tratados sob as ordens de um controlador, recomenda-se que o operador envie as informações necessárias ao controlador dos dados pessoais para que este, caso deseje, realize a devida comunicação.