Cartilha de

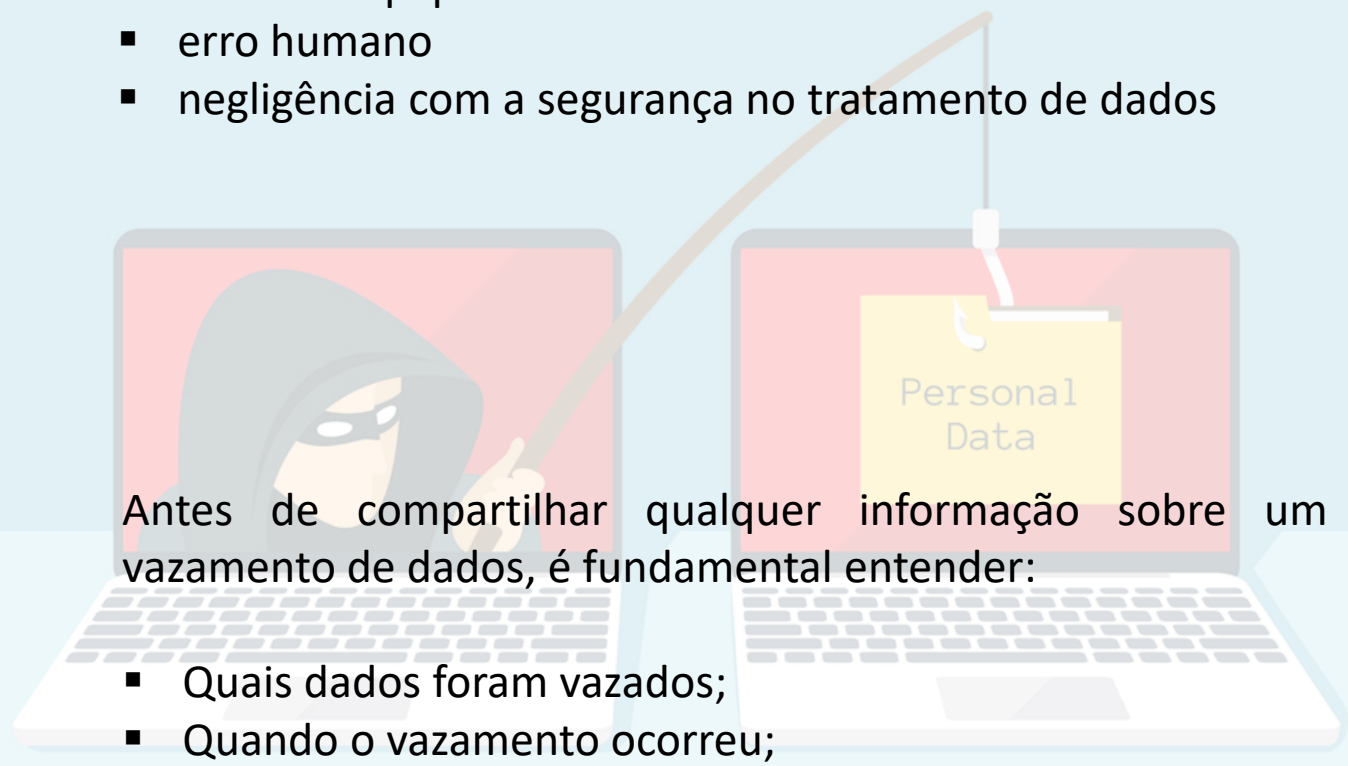
VAZAMENTO DE DADOS

Medidas para diminuir os riscos e danos

PREFEITURA DE niterói
TEMPO DE AVANÇAR
CONTROLADORIA GERAL DO MUNICÍPIO - CGM

O vazamento de dados ocorre quando informações são acessadas, coletadas ou divulgadas **indevidamente** na Internet. Isso pode acontecer por diferentes razões, como por exemplo:

- invasão de contas
- ação de atacantes ou malware
- furto de equipamentos
- erro humano
- negligência com a segurança no tratamento de dados



Antes de compartilhar qualquer informação sobre um vazamento de dados, é fundamental entender:

- Quais dados foram vazados;
- Quando o vazamento ocorreu;
- Quais medidas de contenção e mitigação já foram adotadas ou estão sendo planejadas.

Confirmar essas informações ajuda a evitar a disseminação de boatos e a garantir uma resposta mais eficiente e responsável.

A Proteção de Dados na Prática: Medidas Simples e Eficazes

PREFEITURA DE niterói
TEMPO DE AVANÇAR
CONTROLADORIA GERAL DO MUNICÍPIO - CGM

NAVEGAÇÃO SEGURA

Além de verificar se o site utiliza HTTPS e exibe o cadeado de segurança, é fundamental prestar atenção ao endereço (URL) acessado. Atualmente, é comum o uso de endereços muito semelhantes aos de sites legítimos com a intenção de enganar usuários. Fique atento para não cair em golpes ao acessar páginas falsas

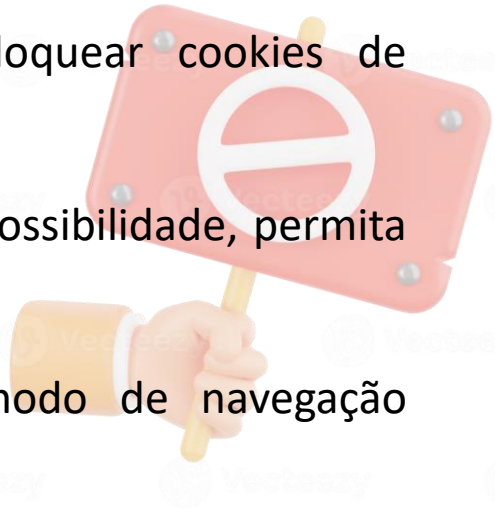
MONITORE

Dados vazados podem levar ao furto da sua identidade e trazer diversos prejuízos com isso. Para se proteger contra essas ações, aqui estão algumas medidas que podem ser tomadas:

- Ative alertas e monitore periodicamente extratos de cartões e contas bancárias
- Acompanhe seus registros financeiros no Banco Central, via sistema “Registrato” https://registrato.bcb.gov.br/
- Consulte no “Cadastro Pré-Pago” se alguma linha de celular foi ativada em seu CPF https://cadastropre.com.br/
- Em caso de qualquer suspeita, contate as instituições envolvidas

COLETA DE INFORMAÇÕES DE NAVEGAÇÃO

Os sites que você acessa podem coletar dados do seu navegador para identificar e acompanhar sua atividade online, incluindo os sites visitados, suas buscas e preferências. Com essas informações, é possível traçar um perfil detalhado sobre você, o que pode ser usado para oferecer conteúdos personalizados com o objetivo de influenciar decisões ou até restringir opções disponíveis. Para proteger sua privacidade, siga estas orientações:



- Configure seu navegador para bloquear cookies de terceiros;
- Ao visitar sites que oferecem essa possibilidade, permita apenas os cookies essenciais;
- Sempre que possível, utilize o modo de navegação anônima.

LINKS “ESTRANHOS”

Se você receber um SMS informando sobre uma transação que não realizou, não responda à mensagem. Evite clicar em links enviados por SMS, WhatsApp ou outros aplicativos, especialmente se o conteúdo parecer suspeito ou inesperado. Mensagens como “você ganhou um prêmio” ou “você está sendo notificado de uma multa” costumam conter links maliciosos que infectam seu celular/computador.

QUESTIONE

Ao preencher formulários e cadastros, é comum que sejam solicitadas mais informações do que o necessário. Muitas vezes, esses dados são usados para traçar perfis de consumo e direcionar anúncios personalizados — ou até mesmo vendidos a terceiros. Um exemplo bastante recorrente e atual são as farmácias.

Para se proteger, adote os seguintes cuidados:

Questione a real necessidade de fornecer determinados dados e se é mesmo indispensável que a instituição os armazene, especialmente quando considerar a solicitação excessiva;

Reflita se vale a pena trocar seus dados por descontos e se esses benefícios são realmente vantajosos ou apenas uma forma de coletar informações pessoais.

POLÍTICAS DE PRIVACIDADE

Antes de fornecer seus dados em sites e aplicativos, é importante saber como eles serão tratados. Isso ajuda a identificar práticas abusivas de coleta e compartilhamento de dados. Entenda: quais dados são coletados; para quais finalidades serão utilizados e com quem podem ser compartilhados.

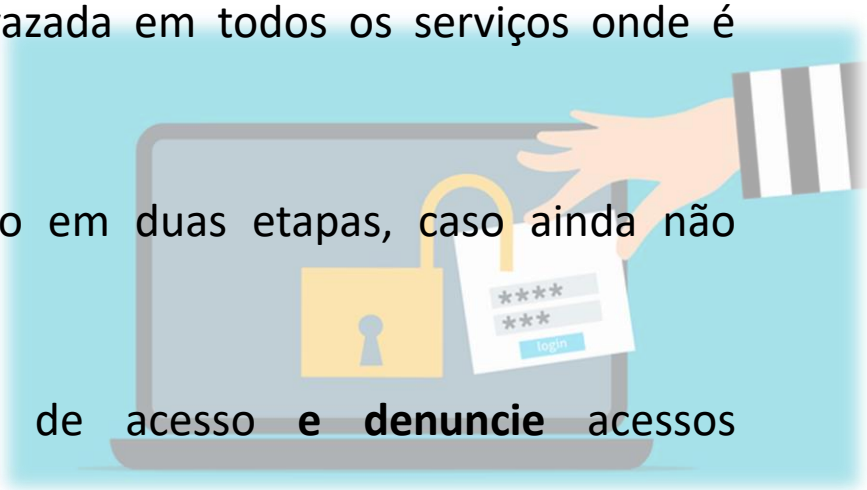
Não aceite e não use o serviço se não concordar com os termos

SENHA VAZADA. O QUE FAZER?

Troque a senha vazada em todos os serviços onde é usada

Ative a verificação em duas etapas, caso ainda não tenha feito

Analise registros de acesso **e denuncie** acessos indevidos



COMO CRIAR UMA SENHA FORTE?

Seja cuidadoso ao criar suas senhas. **Evite** utilizar dados pessoais que possam ser obtidos em redes sociais e páginas Web como uma data de aniversário, seu sobrenome ou a clássica sequência de teclado "123456".

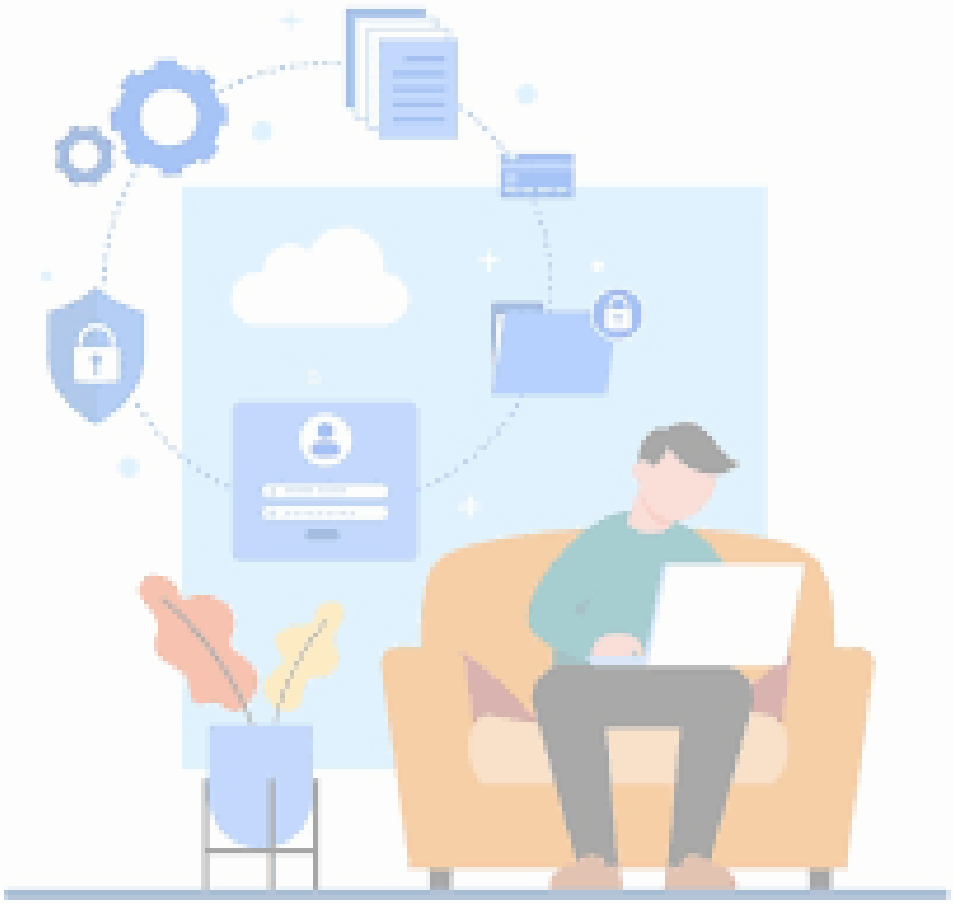
Além disso, utilizar a mesma senha em vários locais é como ter uma chave só que serve para todas as portas da sua casa, carro, escritório, etc. **O trabalho do ladrão fica bem mais fácil assim!**

Dessa forma, recomendamos que cada aplicativo, *site* ou serviço diferente que você usa **tenha sua própria senha**. Apesar de trabalhoso, é a melhor alternativa para se proteger.

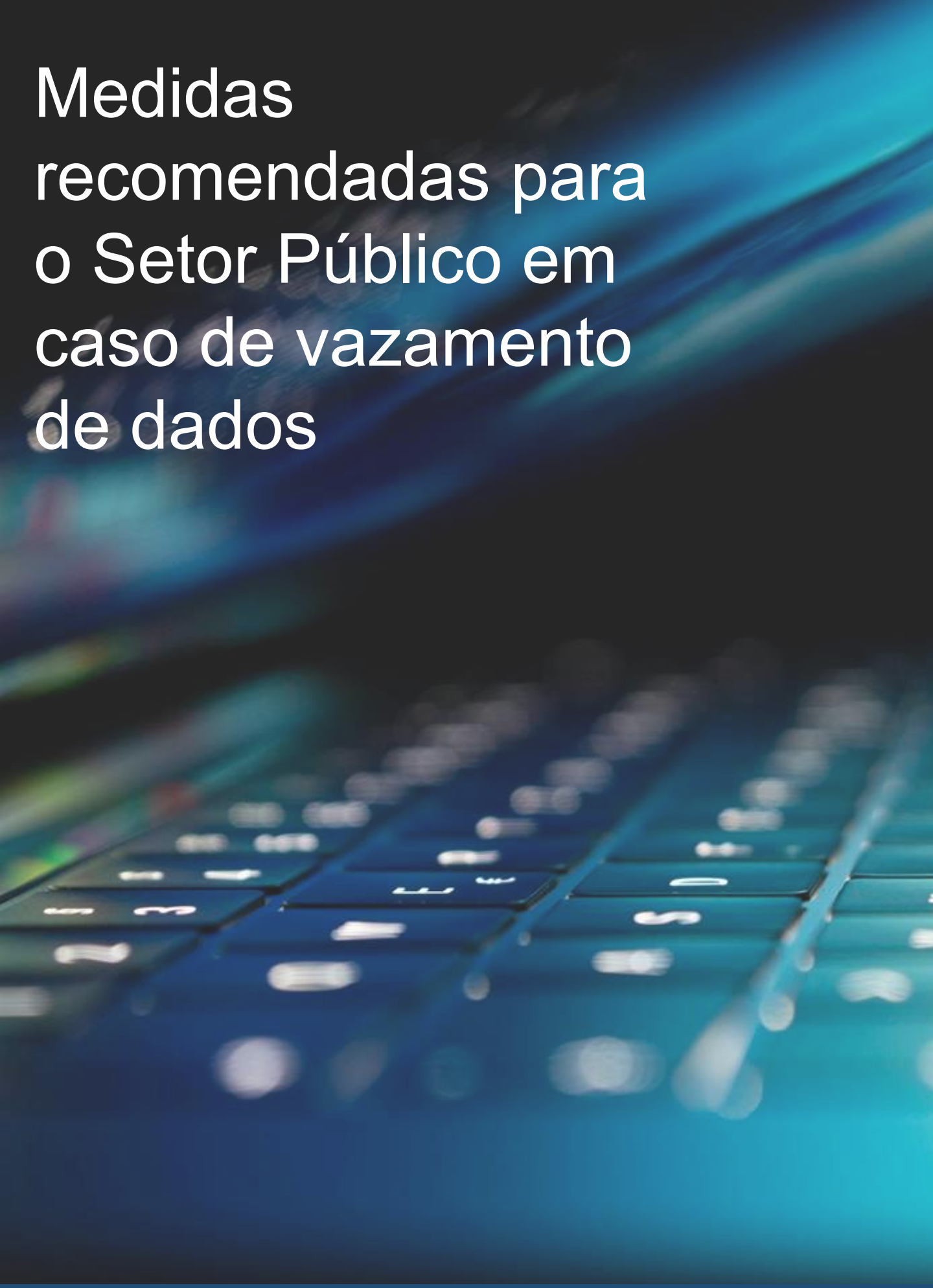
HOUVE VAZAMENTO. A QUEM RECORRER

Denuncie rapidamente no site da **ANPD:** [Denúncia/Petição de Titular — Autoridade Nacional de Proteção de Dados]

Faça um **Boletim de ocorrência** caso seja vítima de um golpe ou uma fraude



Medidas recomendadas para o Setor Público em caso de vazamento de dados



PREFEITURA DE niterói TEMPO DE AVANÇAR
CONTROLADORIA GERAL DO MUNICÍPIO - CGM

O INCIDENTE DE SEGURANÇA

A resolução **CD/ANPD nº 15/24** afirma que o incidente de segurança pode **acarretar risco ou dano relevante** aos titulares quando puder afetar significativamente interesses e direitos fundamentais dos titulares e, cumulativamente, envolver, pelo menos, **um dos seguintes critérios**:

I - dados pessoais sensíveis;

II - dados de crianças, de adolescentes ou de idosos;

III - dados financeiros;

IV - dados de autenticação em sistemas;

V - dados protegidos por sigilo legal, judicial ou profissional; ou

VI - dados em larga escala.

Após avaliar a gravidade do incidente de segurança, a ANPD poderá determinar a adoção de providências como:

- ampla divulgação do incidente em meios de comunicação e
- medidas para reverter ou mitigar os efeitos do incidente.

O QUE UMA ORGANIZAÇÃO DEVE FAZER

Segundo a ANPD as seguintes medidas devem ser tomadas:

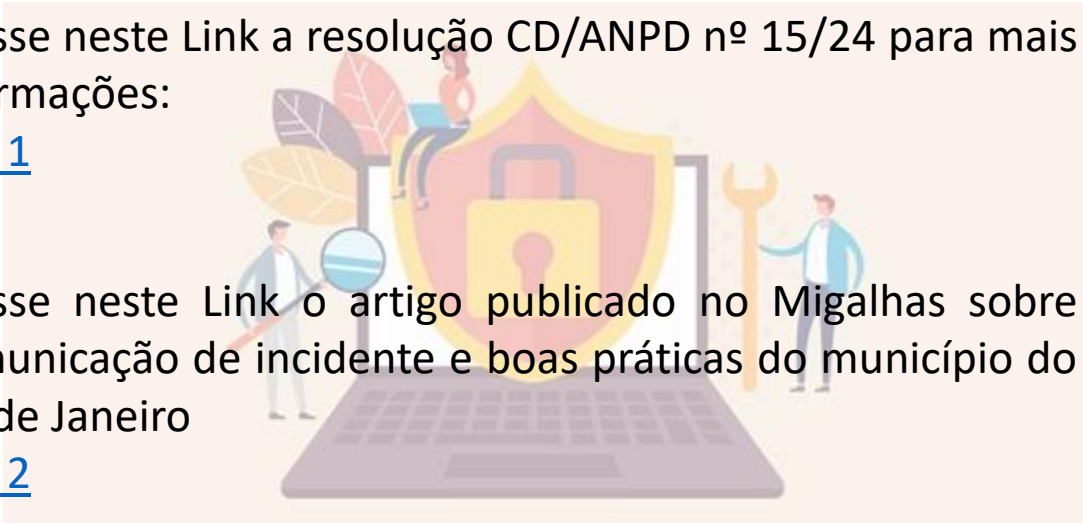
- Realizar uma **avaliação interna** para identificar a natureza do incidente, a categoria e a quantidade de titulares afetados, bem como o **tipo e volume de dados** comprometidos, considerando também as consequências concretas e potenciais;
- **Informar** o Encarregado de Dados;
- Caso atue como operador, **comunicar o incidente** ao Controlador;
- Comunicar **à ANPD** e aos **titulares de dados**, em caso de risco ou dano relevante aos titulares; e
- **Registrar** formalmente a avaliação interna do acidente, as medidas adotadas e a análise dos riscos.

A comunicação precisa ser bastante **detalhada**, acompanhada de documentos, como o relatório do incidente de segurança, que auxilia a ANPD a avaliar o incidente, os riscos e as medidas tomadas. Tal comunicação deve ser feita no prazo de **três dias úteis**, ressalvada a existência de prazo para comunicação previsto em legislação específica.

A ANPD disponibiliza neste link um formulário para **comunicação de incidentes.**

O controlador deverá manter o registro do incidente de segurança, inclusive daquele não comunicado à ANPD e aos titulares, pelo **prazo mínimo de cinco anos.**

INFORMAÇÕES ADICIONAIS



Acesse neste Link a resolução CD/ANPD nº 15/24 para mais informações:
Link 1

Acesse neste Link o artigo publicado no Migalhas sobre Comunicação de incidente e boas práticas do município do Rio de Janeiro
Link 2

BIBLIOGRAFIA

BRASIL. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Comunicação de incidente de segurança. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis .

Cartilha de Segurança para Internet, autor CERT.br/NIC.br - https://cartilha.cert.br/