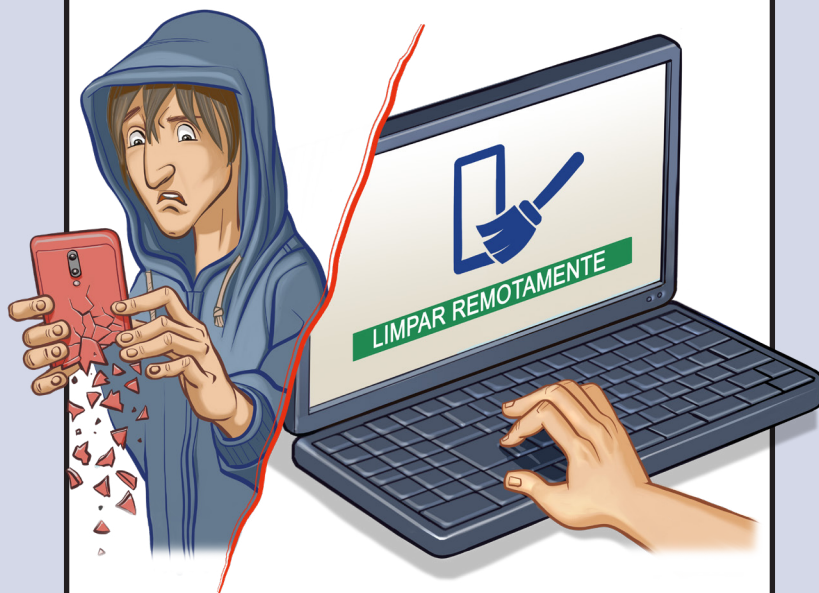
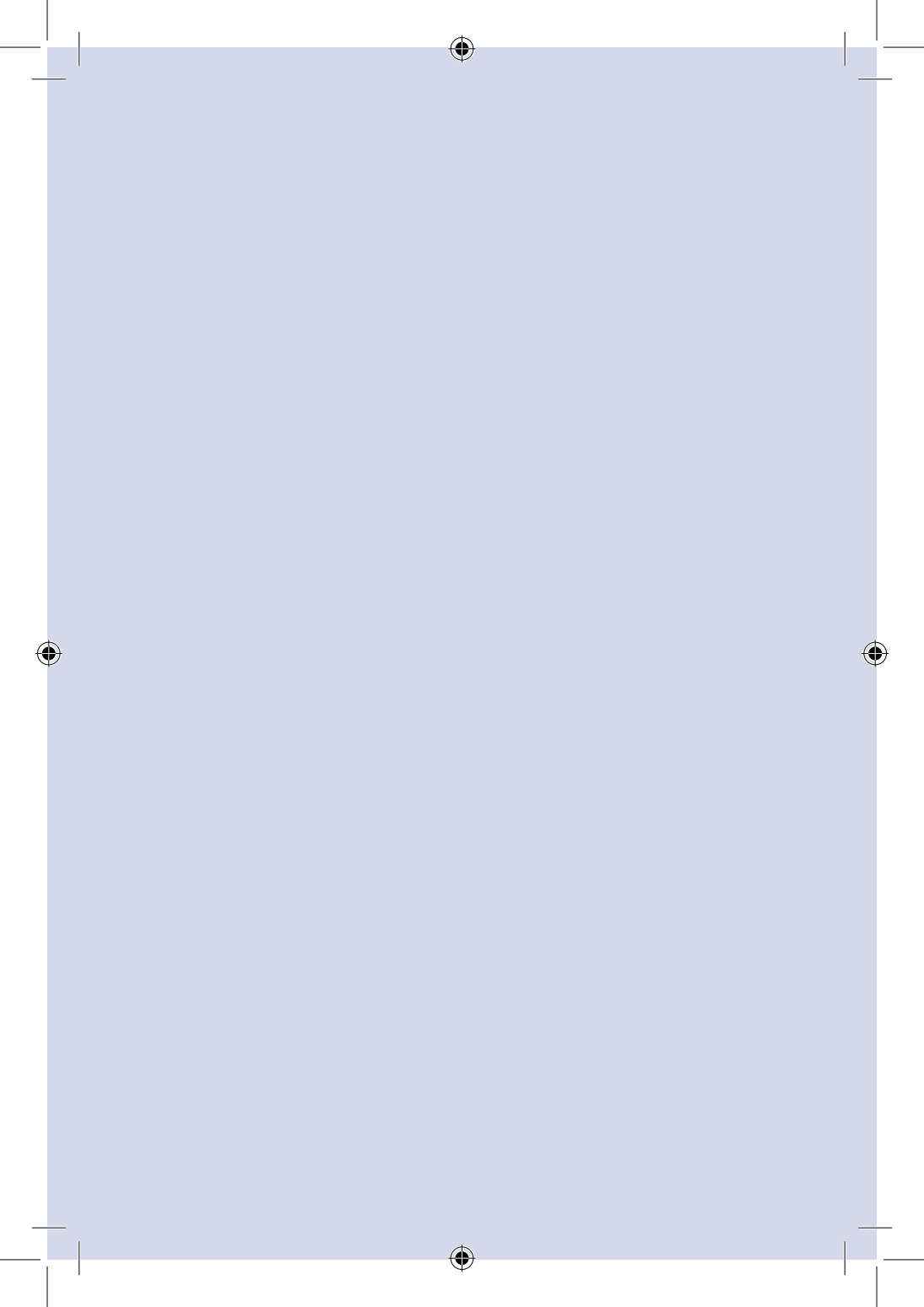


# *Furto de Celular*



Produção:

**cert.br nic.br cgi.br**



# ***SEU CELULAR É SUA CARTEIRA: CUIDE DA SUA VIDA DIGITAL***



**T**oda praticidade que o celular traz pode rapidamente se tornar um pesadelo se ele cair nas mãos erradas.

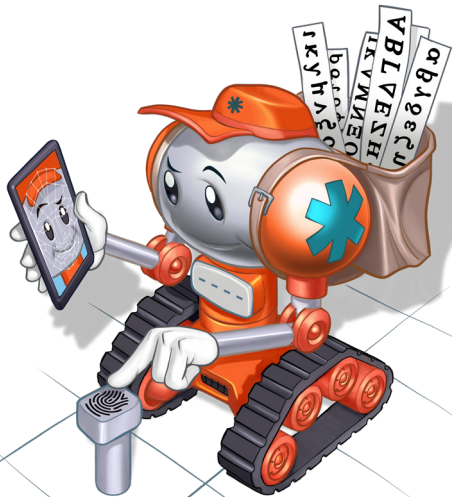
Veja aqui como se preparar antecipadamente para reduzir os danos e o que fazer se um furto ocorrer.

---

***COMO SE  
PREVENIR  
E REDUZIR  
PREJUÍZOS***

---

# **BLOQUEIE SEMPRE A TELA DO CELULAR COM UMA SENHA FORTE**



**S**e o ladrão pegar o celular desbloqueado ou se a senha de desbloqueio for fácil de adivinhar, ele consegue acessar aplicativos instalados, fazer buscas por senhas, alterar configurações e ler mensagens.

- » Configure um método de autenticação para a tela inicial
- » Defina uma senha longa, se possível, alfanumérica
- » Se usar padrão de desbloqueio:
  - utilize o maior número de pontos possíveis
  - evite desenhos simples, como letras
- » Ative o bloqueio de tela automático com o menor tempo disponível

# DESABILITE FUNÇÕES EM TELA BLOQUEADA

**M**esmo com a tela bloqueada os sistemas oferecem facilidades, como leitura de mensagens e atalhos para alterar configurações. Os ladrões fazem uso dessas facilidades para ganhar acesso às suas contas e dificultar a localização remota do aparelho.

- » Desabilite opções em tela bloqueada, como:
- visualização de mensagens
  - acessos rápidos (atalhos) a configurações

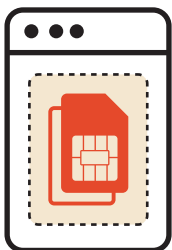




## **TRAVE O APLICATIVO NA TELA SE PRECISAR DEIXAR ABERTO**

**L**adrões costumam furtrar celulares desbloqueados. Fixar um aplicativo na tela permite mantê-lo aberto e impede o acesso a outras funções do celular. Use quando for navegar com o GPS, solicitar transporte ou trocar mensagens, por exemplo.

- » Configure a opção de fixar a tela em uma aplicação
  - recurso chamado “Fixação de Tela” no Android e “Acesso Guiado” no iOS
- » Acione sempre que usar um aplicativo em vias públicas



## PROTEJA O CHIP SIM COM UMA SENHA

Um *chip* SIM protegido por senha impede o ladrão de ativá-lo em outro aparelho. Evita que o ladrão receba mensagens SMS com códigos de verificação que permitem acessar suas contas e/ou redefinir suas senhas.

- » Ative o bloqueio do *chip* SIM
- » Altere o código PIN padrão
  - verifique o da sua operadora





# ANOTE O IMEI DO APARELHO CELULAR

**O** IMEI, código identificador do aparelho, é necessário para solicitar bloqueio na operadora e fazer boletim de ocorrência. Com o IMEI bloqueado o aparelho não pode ser usado na rede de telefonia móvel.

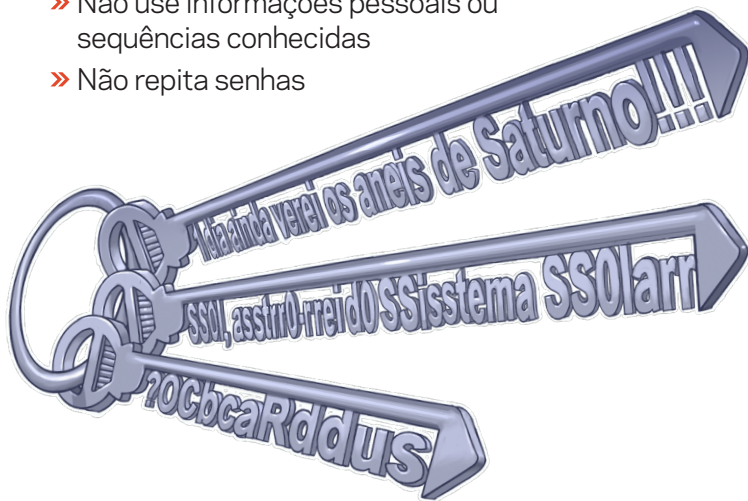
- » Anote o IMEI e guarde-o em local seguro. Você pode encontrá-lo:
- na nota fiscal
  - na caixa do equipamento
  - nas configurações do sistema
  - digitando **\*#06#** diretamente no aparelho



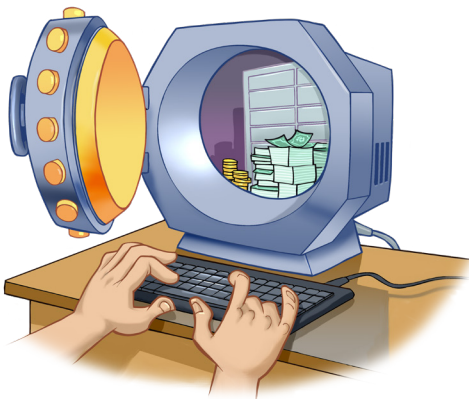
# USE SENHAS FORTES PARA EVITAR FRAUDES

**S**equências conhecidas ou baseadas em informações pessoais, como datas, são fáceis de adivinhar. **Reutilizar senhas também facilita a vida do ladrão**, pois dá acesso a todas as contas onde a mesma senha é usada.

- » Não use informações pessoais ou sequências conhecidas
- » Não repita senhas



# GUARDE SUAS SENHAS DE FORMA SEGURA



**S**enhas guardadas no celular podem ser encontradas pelos ladrões usando mecanismos de buscas. Não guarde senhas, especialmente de instituições financeiras, em aplicativos de *e-mail*, anotações, mensagens, contatos e fotos.

- » Utilize um aplicativo gerenciador de senhas
  - configure uma senha forte para acessar o gerenciador
- » Caso prefira, use outras opções:
  - grave as senhas em um arquivo criptografado, ou
  - anote as senhas em papel e guarde-o em local seguro



# REDUZA OS LIMITES DE TRANSAÇÕES PARA MINIMIZAR PREJUÍZOS

Uma prática bastante comum dos ladrões é a fraude via transferências bancárias.

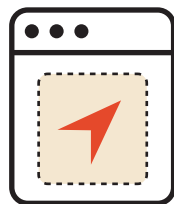
- » Reduza os limites de transferência entre contas, PIX e TED
- » Reavalie limites de créditos pré-aprovados



# PREPARE-SE PARA APAGAR O APARELHO REMOTAMENTE

**A**pagar o conteúdo do aparelho remotamente depende de ativar previamente a sua localização.

- » Ative a localização remota do aparelho
  - recurso chamado "Encontre Meu Dispositivo" no Android e "Buscar iPhone" no iOS



**C**onsidere cadastrar-se no serviço "Celular Seguro", que avisa algumas instituições financeiras e operadoras de telefonia em caso de furto. <https://celularseguro.mj.gov.br/>

# ATIVE A “PROTEÇÃO DE DISPOSITIVO ROUBADO” SE TIVER IPHONE

**C**om a proteção ativa, o sistema requer sua biometria e adiciona um tempo de espera para realizar algumas operações críticas, sempre que o aparelho estiver longe de locais como casa ou trabalho. Este tempo de espera pode ser suficiente para apagar o dispositivo remotamente.

- » Habilite a opção "Proteção de Dispositivo Roubado"
  - em ajustes "Face ID e Código" ou "Touch ID e Código"
- » Veja adiante o que fazer em caso de furto
  - aja rapidamente, nem todos os aplicativos ficam protegidos

**A**s operações críticas protegidas incluem acessar e trocar senhas, incluir nova biometria e desativar o recurso "Buscar".



## PLANEJE-SE PARA RECUPERAR SUAS CONTAS E DADOS DEPOIS

**P**ara recuperar suas contas e dados em outro aparelho, algumas ações e configurações devem ser feitas antes que o furto ocorra.

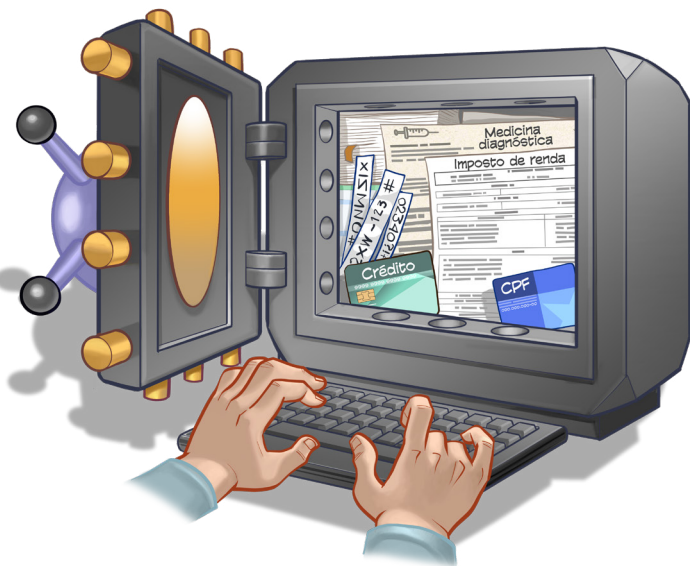
- » Defina um número de celular alternativo para recuperação de contas, como a do Apple ID
- » Gere e tenha em fácil acesso códigos de *backup* para contas que usem verificação em duas etapas
- » Faça *backups*

**C**ódigos de *backup* são gerados pela função de verificação em duas etapas para serem usados quando outros métodos de autenticação não estiverem disponíveis.

# PROTEJA SEUS DADOS PARA NÃO SEREM USADOS EM FRAUDES

**D**ados armazenados sem proteção podem ser facilmente acessados pelos ladrões e usados para fraudes.

» Não armazene fotos de documentos, cartões e senhas





---

***O QUE  
FAZER SE  
OCORRER  
O FURTO***

---



## NOTIFIQUE AS INSTITUIÇÕES FINANCEIRAS

Ladrões podem usar aplicativos de instituições financeiras e de comércio eletrônico para cometer fraudes, como transferências bancárias, empréstimos, pagamentos de boletos e compras *online*.

- » Notifique as instituições financeiras que você acessa via aplicativos e solicite:
  - o bloqueio do acesso às contas pelo aplicativo
  - o bloqueio dos cartões usados no celular furtado

**S**e tiver cadastro no serviço "Celular Seguro" faça a notificação de furto ou peça para a pessoa de confiança cadastrada fazer por você. <https://celularseguro.mj.gov.br/>



## CONTATE A OPERADORA DE CELULAR

A operadora de celular pode desativar o *chip* SIM e bloquear o IMEI do aparelho para impedir a conexão à rede de telefonia móvel. Sem poder fazer ou receber chamadas e mensagens SMS, as chances de fraudes, inclusive contra seus contatos, são reduzidas.

- » Solicite à operadora a desativação do *chip* SIM e o bloqueio do código IMEI do aparelho



# FAÇA UM BOLETIM DE OCORRÊNCIA

**O** boletim de ocorrência é o registro policial que ajuda você a se defender, em especial se o ladrão tentar se passar por você. Geralmente é exigido para contestar fraudes e acionar seguros.

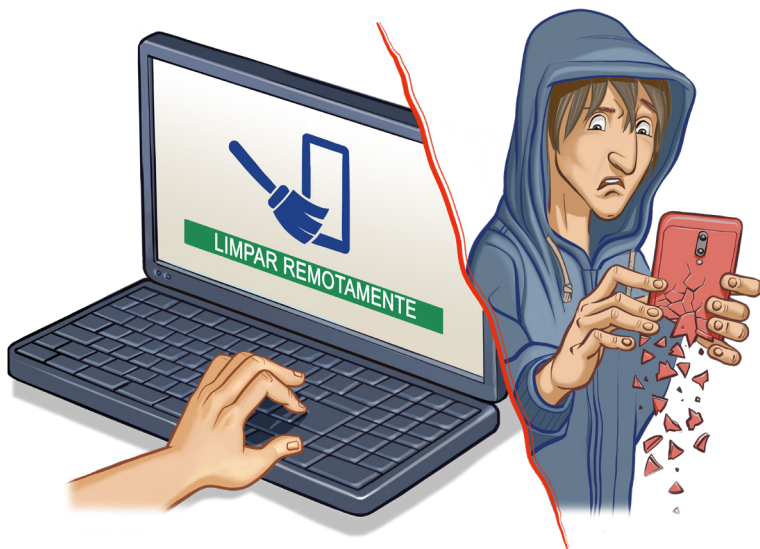
» Declare o código IMEI e o número de série do aparelho no boletim de ocorrência



# APAGUE REMOTAMENTE O APARELHO

**U**m celular furtado dificilmente é recuperado. Para evitar o uso indevido do seu celular e de seus dados, apague remotamente todo o conteúdo.

- » Acesse o serviço de localização remota
  - serviço <https://android.com/find/> para Android e <https://icloud.com/find/> para iOS
  - lembre-se de ativar previamente
- » Apague remotamente todos os dados do dispositivo





## **DESCONECTE APLICATIVOS E TROQUE AS SENHAS DE SUAS CONTAS**

Vários aplicativos, como *e-mail* e redes sociais, permanecem autenticados no seu aparelho sem que você precise digitar a senha a cada uso. Desconectar os aplicativos e trocar as senhas fará com que o ladrão perca o acesso a eles.

- » Desconecte as contas de aplicativos instalados no celular (*logout*)
- » Troque as senhas das contas usadas no celular, em especial:
  - *e-mail*
  - *login* social (conta de rede social usada para autenticar em outros aplicativos)
  - instituições financeiras
  - ID de sistema, como Apple ID e Google ID



## **CONTESTE FRAUDES E MONITORE SUA VIDA FINANCEIRA**

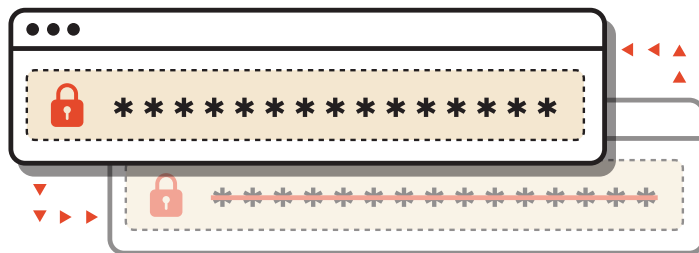
**M**esmo depois do susto inicial ter passado, os problemas podem continuar se seus dados e contas forem usados indevidamente.

- » Revise os extratos de seus cartões e contas em instituições financeiras e de telefonia
- » Conteste transações fraudulentas, como transferências, empréstimos, pagamentos e compras
  - registre reclamação no Banco Central, se necessário

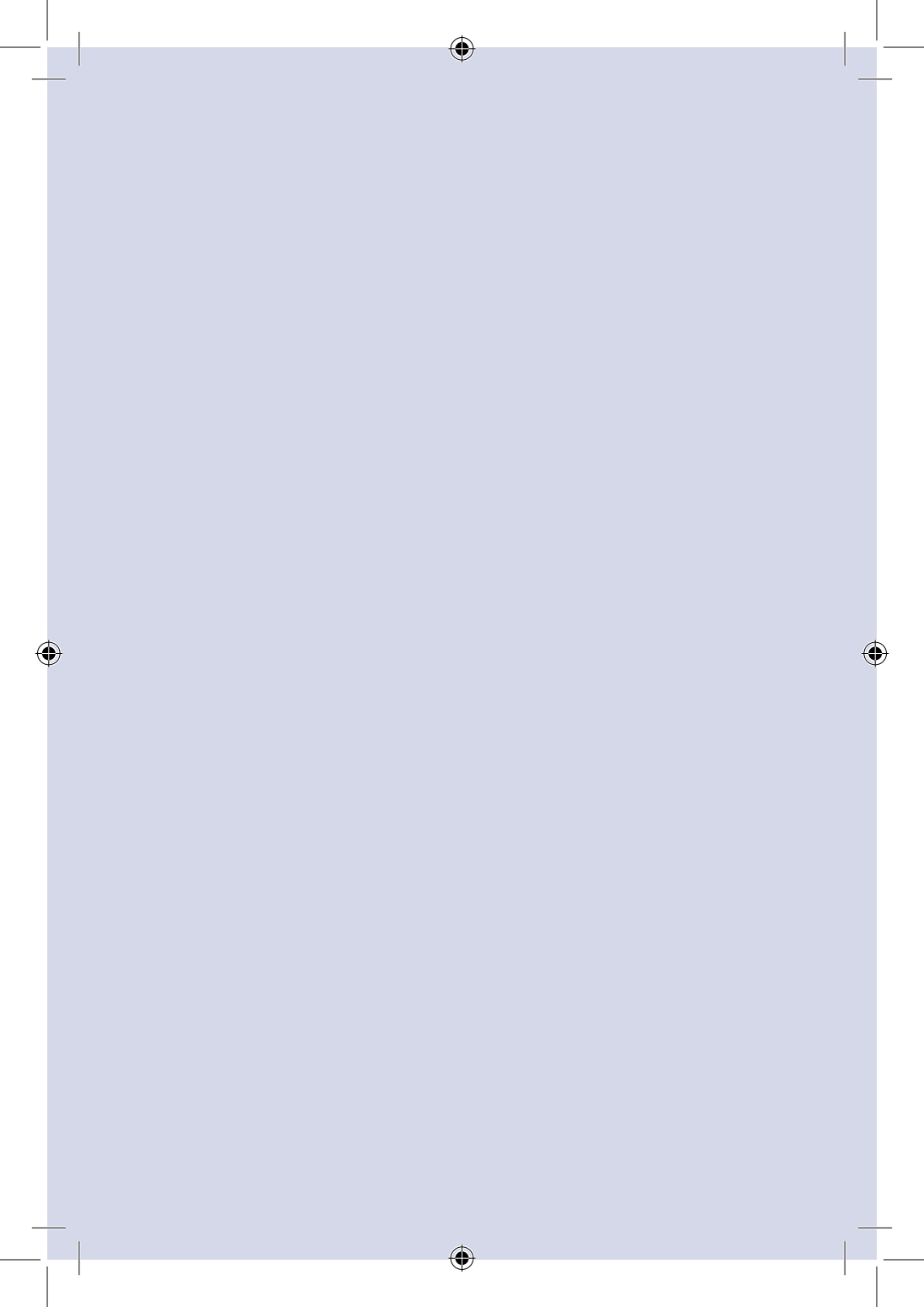
# TROQUE AS SENHAS USADAS EM DISPOSITIVOS DE TERCEIROS

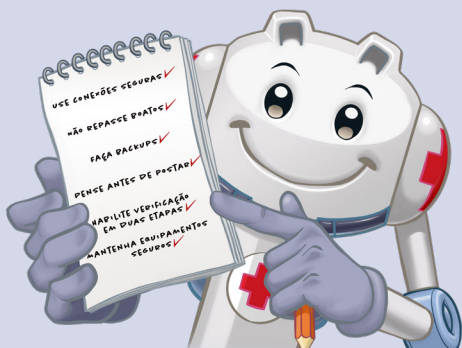
**A**ção rápida para conter prejuízos e acessos indevidos é fundamental. Na urgência, você pode ter usado suas senhas em algum dispositivo emprestado, cuja segurança não é garantida.

- » Redefina as senhas usadas no dispositivo emprestado, assim que estiver em um dispositivo confiável



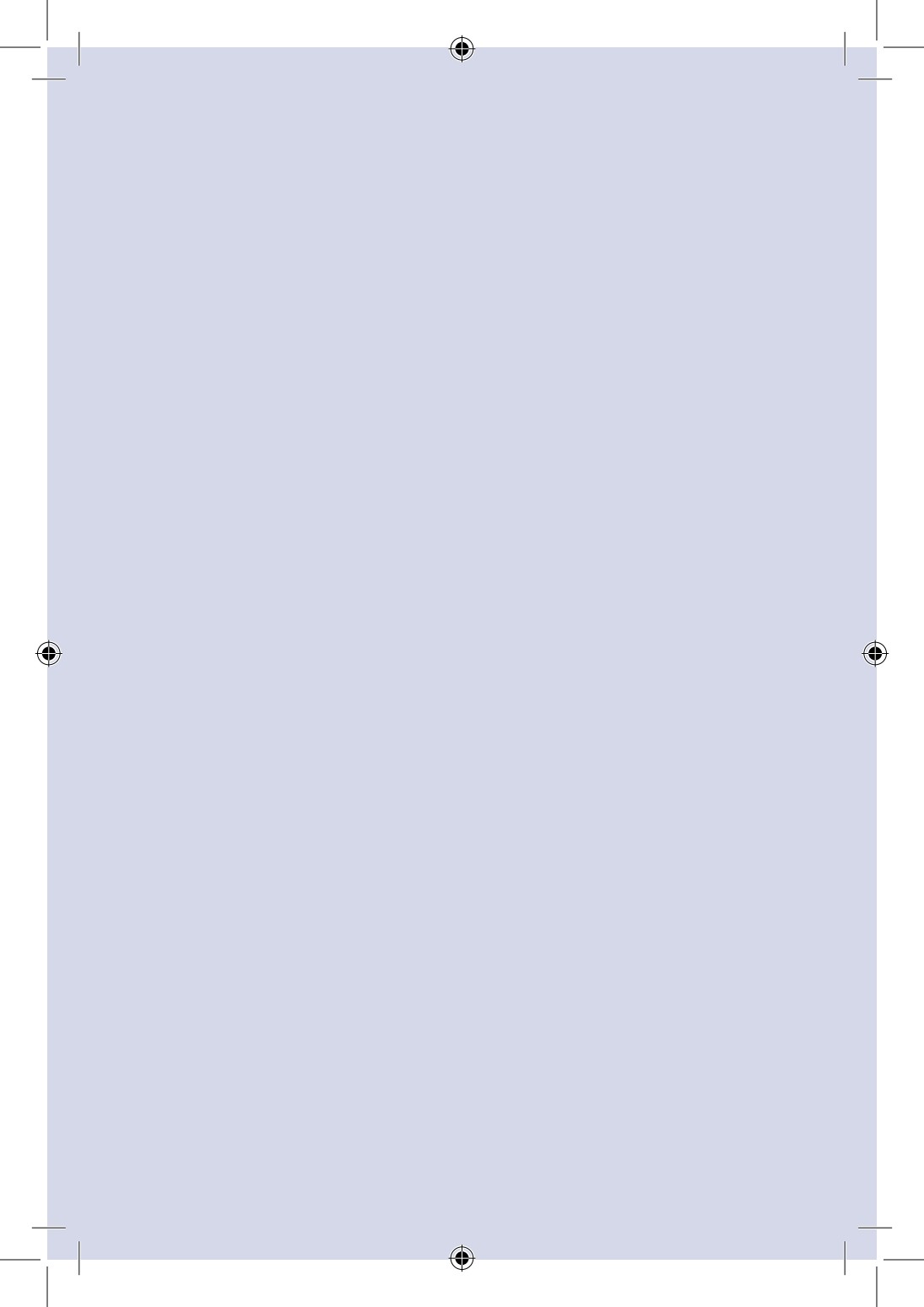






## SAIBA MAIS

- » Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança para Internet, disponíveis em: <https://cartilha.cert.br/>
- » Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: <https://internetsegura.br/>



## cert.br

O CERT.br (<https://cert.br/>) é um Grupo de Resposta a Incidentes de Segurança (CSIRT) de responsabilidade nacional de último recurso, mantido pelo NIC.br. Além da gestão de incidentes, também atua na conscientização sobre os problemas de segurança, na consciência situacional e transferência de conhecimento, sempre respaldado por forte integração com as comunidades nacional e internacional de CSIRTs.

## nic.br

O Núcleo de Informação e Coordenação do Ponto BR - NIC.br (<https://nic.br/>) é uma entidade civil de direito privado e sem fins de lucro, encarregada da operação do domínio .br, bem como da distribuição de números IP e do registro de Sistemas Autônomos no País. Conduz ações e projetos que trazem benefícios à infraestrutura da Internet no Brasil.

## cgi.br

O Comitê Gestor da Internet no Brasil (<https://cgi.br/>), responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados.