

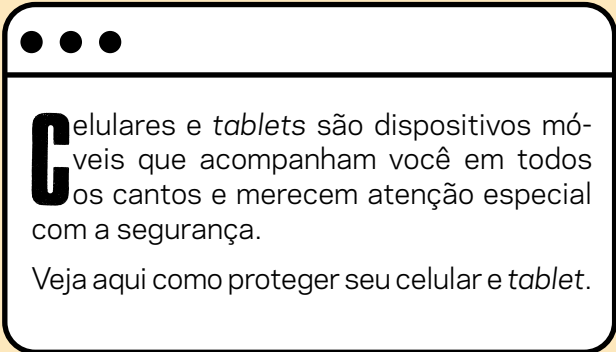
# *Celulares e Tablets*



Produção:

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

# PROTEÇÃO E SEGURANÇA ONDE VOCÊ ESTIVER



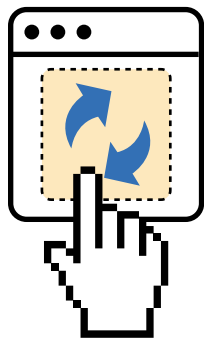
**C**elulares e *tablets* são dispositivos móveis que acompanham você em todos os cantos e merecem atenção especial com a segurança.

Veja aqui como proteger seu celular e *tablet*.

---

***CUIDADOS  
QUE VOCÊ DEVE  
TOMAR AO  
USAR O SEU  
DISPOSITIVO***

---



## INSTALE ATUALIZAÇÕES E EVITE APLICATIVOS DESNECESSÁRIOS

**S**istemas e aplicativos possuem falhas (vulnerabilidades) que podem ser exploradas para invadir o dispositivo, capturar dados ou instalar *malware*. Aplicar atualizações evita que você se torne vítima ou parte de ataques.

- » Mantenha o sistema e os aplicativos atualizados
  - ative a atualização automática, sempre que possível
  - aceite sempre as atualizações de segurança
  - atualize também relógios, fones e demais acessórios “inteligentes” conectados ao dispositivo
- » Mantenha instalados apenas aplicativos que você realmente usa





## **BAIKE APLICATIVOS SOMENTE DE LOJAS OFICIAIS**

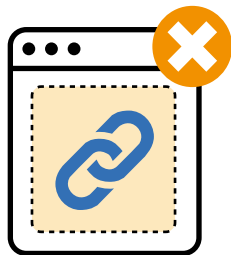
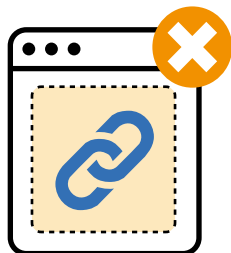
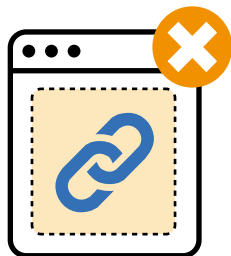
Infelizmente existem aplicativos criados com fins maliciosos e as lojas oficiais costumam ter políticas mais rígidas e mecanismos mais rápidos de exclusão destes aplicativos, quando detectados.

- » Use apenas a loja oficial do sistema ou do fabricante do dispositivo
  - nunca instale aplicativos recebidos via mensagens ou *links*
- » Mesmo assim, cuidado com aplicativos falsos
  - antes de instalar, confirme o nome do aplicativo e se o desenvolvedor é mesmo quem deveria ser

# NÃO CLIQUE EM TODOS OS LINKS QUE RECEBE

**L**inks maliciosos são usados para direcionar usuários para páginas falsas ou com *malware*. Atacantes tentam induzir os usuários a clicar nestes links usando truques como enviá-los de contas falsas ou invadidas, explorando a confiança entre pessoas conhecidas.

- » Antes de clicar, analise o contexto e observe os detalhes
  - na dúvida, não clique
- » Desconfie de mensagens recebidas, mesmo vindas de conhecidos
  - se necessário, contate quem supostamente a enviou usando outro meio de comunicação
- » Só leia códigos QR se confiar na fonte





## BLOQUEIE A TELA DE INÍCIO DO SEU DISPOSITIVO

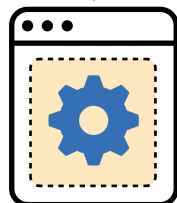
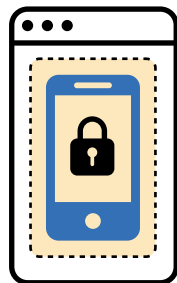
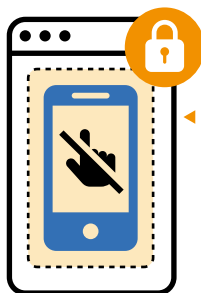
**S**e alguém pegar seu dispositivo desbloqueado, poderá acessar o conteúdo e usar os aplicativos se passando por você, para enviar mensagens, postar em redes sociais ou fazer transações em aplicativos de comércio eletrônico e bancos.

- » Configure um método de autenticação na tela inicial
  - use senhas longas, se possível alfanuméricas
  - evite usar padrão de desbloqueio com poucos pontos ou desenhos muito simples, como letras
- » Ative o bloqueio de tela automático com o menor tempo disponível

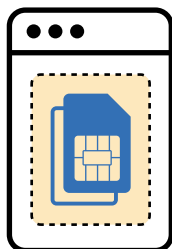
# DESABILITE FUNÇÕES EM TELA BLOQUEADA

**M**esmo com a tela bloqueada os sistemas permitem facilidades, como leitura de mensagens e atalhos para alterar configurações. Isso pode expor sua privacidade, ser usado 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



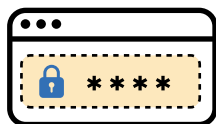




## PROTEJA O CHIP SIM COM UMA SENHA

O *chip* SIM conecta seu dispositivo à rede de telefonia móvel. Proteger o *chip* com senha evita o uso indevido em outro aparelho, impedindo que outra pessoa receba mensagens SMS com códigos de verificação usados para acessar contas e/ou redefinir senhas.

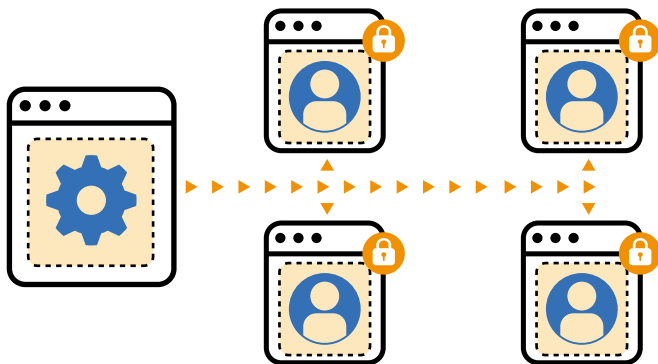
- » Ative o bloqueio do *chip* SIM
- » Altere o código PIN padrão
  - verifique o da sua operadora

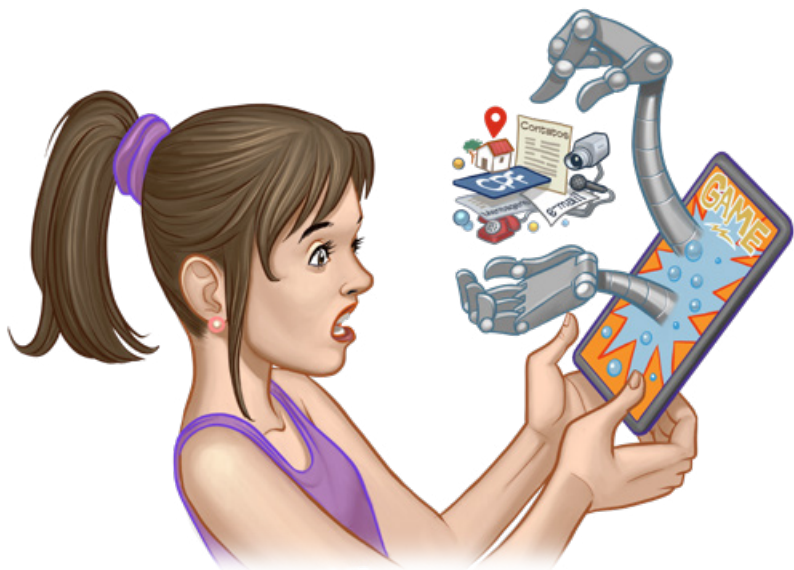


# LIMITE O ACESSO CASO OUTRA PESSOA USE SEU DISPOSITIVO

**C**ompartilhar ou emprestar um dispositivo pode expor sua privacidade ou trazer consequências indesejáveis, ainda que acidentais.

- » Crie perfis separados para cada usuário ou convidado, sempre que possível
- » Para deixar alguém usar um aplicativo específico, trave-o na tela
  - recurso chamado “Fixação de Tela” no Android e “Acesso Guiado” no iOS
- » Use controle parental, caso o dispositivo seja usado por crianças
  - lembre-se de conversar com elas sobre o uso seguro e responsável da Internet





## **AJUSTE AS PERMISSÕES DOS APLICATIVOS CONFORME O USO**

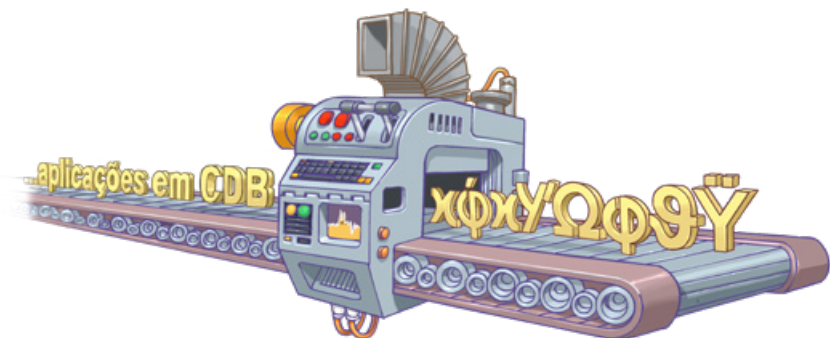
**P**ara funcionar, muitos aplicativos solicitam permissões, como acesso a câmera, microfone, geolocalização e lista de contatos. Alguns acessos são essenciais, mas há outros que são abusivos e podem comprometer a sua privacidade e segurança.

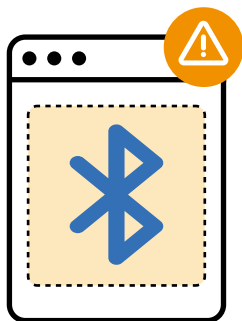
- » Ao instalar e usar um aplicativo, autorize apenas acessos que façam sentido com o seu uso

# SEJA CUIDADOSO AO USAR REDES WI-FI PÚBLICAS

**R**edes Wi-Fi públicas podem representar riscos, como expor a sua privacidade ou redirecionar suas conexões para *sites* maliciosos. Apesar de bastante práticas não há como garantir que estejam devidamente configuradas e protegidas.

- » Antes de se conectar, verifique se a rede é legítima
  - procure indicação da rede disponível, como placas e cartazes
  - confirme com o estabelecimento, caso tenha dúvida
- » Use conexões seguras, como https para acessar *sites*
- » Considere usar uma rede virtual privada (VPN)
- » Para fazer transações financeiras, prefira uma rede em que você confie

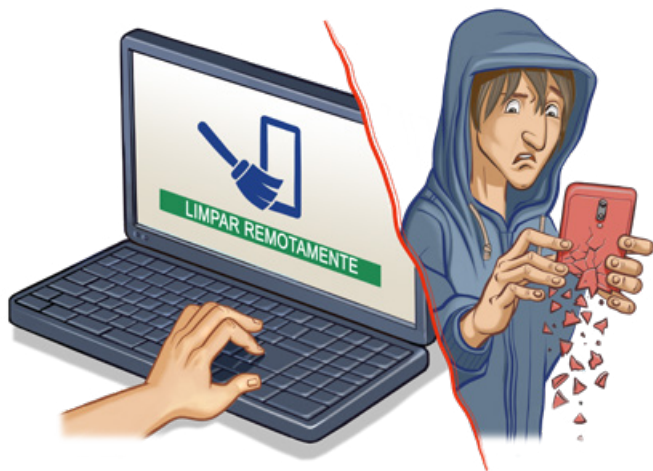




# TENHA CUIDADO AO USAR COMUNICAÇÃO POR PROXIMIDADE

**D**ispositivos móveis possuem recursos de conexão por proximidade, como *bluetooth* e NFC, para conectar acessórios, transferir e compartilhar dados e fazer pagamentos. Atacantes podem abusar de tais recursos para furtar dados, fazer pagamentos fraudulentos e invadir o dispositivo.

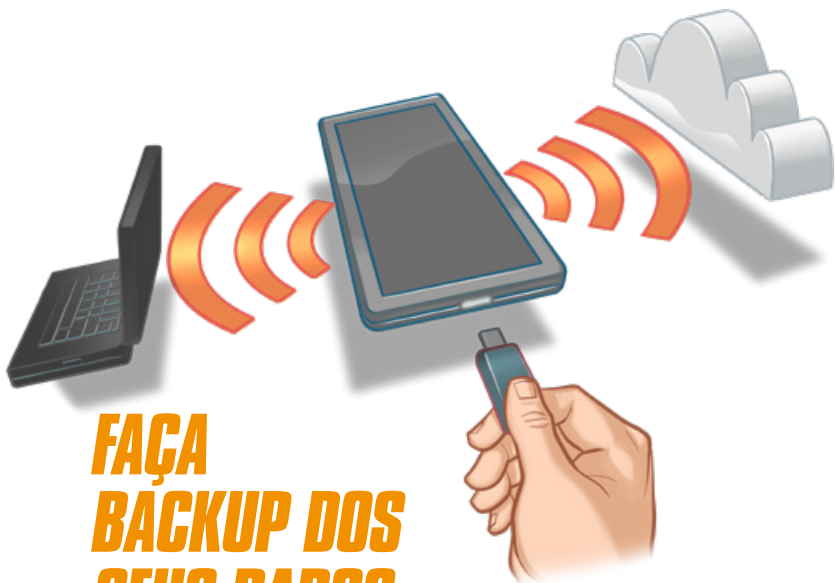
- » Fique atento a pedidos de pareamento
  - só permita se tiver certeza de que são seus próprios acessórios
- » Exija autenticação para autorizar pagamentos por aproximação (NFC)
- » Ative o recurso de compartilhamento somente quando necessário
  - recurso chamado “Compartilhar por proximidade” no Android e “AirDrop” no iOS
- » Reduza a exposição desligando recursos que normalmente não usa
  - atenção com *bluetooth* pois costuma vir ativo de fábrica



## **CUIDADO COM SEUS DISPOSITIVOS EM AMBIENTES PÚBLICOS**

**D**ispositivos móveis são pequenos, estão em uso constante e podem ser facilmente esquecidos e perdidos. Costumam ser objeto de desejo de ladrões, pelo preço do aparelho, pelas informações que carregam e pelos acessos que possibilitam.

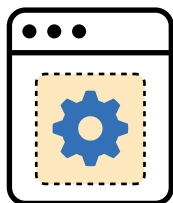
- » Ative a localização remota do aparelho
  - recurso chamado “Encontre Meu Dispositivo” no Android e “Buscar iPhone” no iOS
  - tente localizar, bloquear ou apagar o aparelho, conforme a necessidade
- » Anote o IMEI do celular e guarde-o em local seguro
- » Em caso de furto, veja o que fazer no fascículo “Furto de Celular”



## FAÇA BACKUP DOS SEUS DADOS

**O**s dados armazenados em seu dispositivo podem ser perdidos por falhas, perda ou furto do aparelho. Ter cópias dos dados permite recuperá-los.

- » Faça cópias periódicas de seus dados
  - selecione a opção mais conveniente, como nuvem, outro equipamento ou *pen drives* específicos
  - programe seus *backups* para serem feitos automaticamente



## **EXPLORE OS RECURSOS DE SEGURANÇA DO SEU DISPOSITIVO**

O sistema do seu dispositivo já possui diversas opções de segurança e privacidade que nem sempre vem ativadas ou configuradas de fábrica. Além disso, caso deseje recursos adicionais, há aplicativos de segurança que podem ser instalados.

- » Verifique as opções de segurança e privacidade oferecidas em seu dispositivo
  - ajuste-as às suas necessidades e boas práticas
- » Instale aplicativos extras de segurança, caso queira recursos adicionais



---

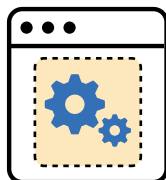
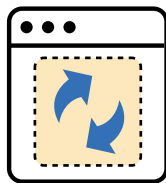
***CUIDADOS  
QUE VOCÊ DEVE  
TOMAR AO  
COMPRAR UM  
DISPOSITIVO***

---

# AVALIE A DISPONIBILIDADE DE ATUALIZAÇÕES

**O**s fabricantes fornecem atualizações e correções de falhas por prazo limitado. Celulares muito antigos ficam desprotegidos pois deixam de recebê-las.

- » Prefira modelos atuais, com suporte a atualizações
  - observe o ano de lançamento ou de fabricação
  - avalie a versão do sistema operacional

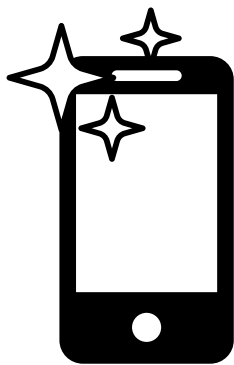


# AVALIE OS RECURSOS DE SEGURANÇA

Diferentes fabricantes, sistemas e modelos oferecem diferentes recursos de segurança, como biometria, opção de múltiplos perfis de usuários, autenticação para autorizar pagamentos e política da loja de aplicativos.

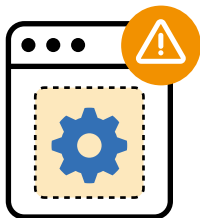
- » Pesquise sobre os recursos de segurança oferecidos
  - escolha o modelo que melhor atenda às suas necessidades





## EVITE PROBLEMAS AO COMPRAR UM CELULAR USADO

É preciso tomar cuidados extras ao comprar um celular usado, pois nem sempre é possível garantir a sua procedência. Ele pode estar em situação irregular (IMEI bloqueado), vinculado à conta do dono anterior ou infectado com *malware*.



- » Verifique a situação do aparelho
  - tenha certeza que o aparelho está desvinculado da conta do dono anterior
  - solicite o código IMEI do aparelho ao vendedor, e consulte sua situação em: <https://www.gov.br/anatel/pt-br/assuntos/celular-legal/>
- » Restaure as configurações originais (“de fábrica”), antes de começar a usá-lo

---

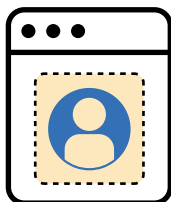
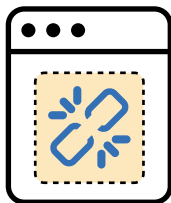
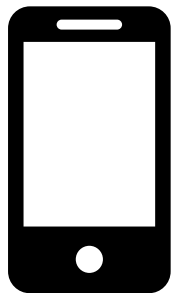
***CUIDADOS  
QUE VOCÊ DEVE  
TOMAR AO  
DESCARTAR OU  
REPASSAR UM  
DISPOSITIVO***

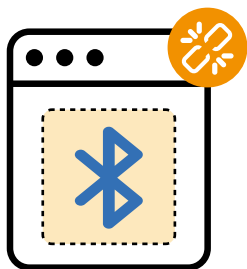
---

# APAGUE OS DADOS DO DISPOSITIVO E DESVINCULE-O DA SUA CONTA

**O**s dados do seu dispositivo podem ser acessados por outros, caso não sejam excluídos. O ID de sistema precisa ser desconectado para que o aparelho seja desvinculado da sua conta e o próximo dono possa usá-lo.

- » Desconecte sua conta ID de sistema
  - opção chamada “Remover conta” no Android e “Finalizar Sessão” no iOS
- » Restaure as configurações originais (“de fábrica”)
  - tenha certeza de apagar todo conteúdo e configurações
- » Remova o dispositivo da lista de dispositivos confiáveis em sua conta ID de sistema

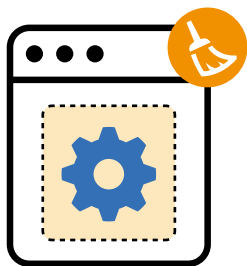




## REMOVA ASSOCIAÇÕES AO CELULAR ANTIGO



Você pode ter várias contas de aplicativos e acessórios conectados, por exemplo via *bluetooth*, que ficavam permanentemente autenticados no celular. É preciso remover das contas e dos acessórios as autorizações relacionadas ao celular antigo.



- » Remova das suas contas de aplicativos os acessos concedidos ao celular
- » Remova de seus acessórios as autorizações ou pareamentos associados ao celular



## **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.