Guia de segurança do Digitech/Firjan SENAI para aparelhos celulares

⇨ Principais configurações de Cibersegurança

*Além de anotar o IMEI (*Identificação Internacional de Equipamento Móvel*) e das cautelas com a exposição pública do celular – especialmente em eventos de grande aglomeração –, é importante adotar algumas das principais configurações de segurança. Elas podem ser acessadas por meio da aba de pesquisa em "Configurações" do aparelho.*

1. **Ative os serviços nativos de segurança**, como rastreamento, bloqueio remoto, apagamento de dados à distância e bloqueio automático por senha ou biometria (como o *Modo Ladrão*, no Android).

2. Instale o aplicativo Celular Seguro, do Governo Federal. A ferramenta permite o bloqueio remoto da linha telefônica, de aplicativos e do **IMEI** do aparelho por meio da plataforma Gov.br, inclusive por pessoas de confiança previamente cadastradas. O aplicativo também notifica o usuário quando um novo chip é habilitado, reduzindo o risco de fraudes e auxiliando na recuperação do dispositivo.

3. Ative a autenticação por senha ou biometria em todos os aplicativos bancários e autenticação em dois fatores (2FA) nos aplicativos **de e-mail, redes sociais, mensageiros e serviços em nuvem**.

4. Segundo a Federação Brasileira de Bancos (Febraban), muitas pessoas anotam senhas em blocos de notas, mensagens de WhatsApp ou e-mails.

É recomendável utilizar **gerenciadores de senha** como **Bitwarden**, **1Password**, **LastPass** **ou** **KeePass**.

5. Em grandes eventos, desative **pagamentos por aproximação** ou **remova cartões que não serão utilizados** de carteiras digitais (Apple Pay, Google Wallet e Samsung Pay). O importante é não ter vários cartões cadastrados, principalmente aqueles com limites ou valores altos. Opte por um cartão com limite ou valor reduzido somente para o evento.

6. Realize **backup** completo antes de sair de casa (nuvem ou computador). O ideal é configurar um backup automático para que seja feito regularmente ao acessar o Wi-Fi de sua residência.

7. Proteja fotos, documentos e aplicativos sensíveis com senha adicional ou biometria. Para isso, o usuário deve utilizar **cofres de aplicativos** e **pastas seguras,** ou os recursos nativos de proteção por senha/biometria disponíveis no sistema operacional do aparelho. No Android há a Pasta Segura, e no iPhone existem recursos de ocultar aplicativos por Face ID/Touch ID.

8. Antes de ir a grandes eventos, faça **logoff de redes sociais** que não serão usadas, incluindo os e-mails principais, pois permitem redefinir senhas.

9. Evite **QR Codes aleatórios** e Wi-Fi público ao acessar bancos ou dados sensíveis.

10. Habilite o **apagamento automático** após várias tentativas incorretas de senha. No Android, acesse: Configurações → Segurança e privacidade → Mais configurações de segurança → Apagar após tentativas incorretas; no iPhone, acesse: Ajustes → Face ID/Touch ID e Código → Apagar Dados.

⇨ O que fazer após ter o celular furtado ou roubado

Nesta situação, cada minuto é importante para evitar maiores transtornos.

1. **Apague os dados (prioritário):** no Android, acesse **https://www.google.com/android/find; no iPhone, acesse** **https://www.icloud.com/find**.

2. **Celular Seguro:** contacte a pessoa de confiança cadastrada para desabilitar a linha e os principais aplicativos vinculados ao aparelho.

3. **Resete o aparelho:** realize o apagamento completo para impedir a reutilização das suas informações pessoais. Seus dados poderão ser recuperados posteriormente em outro aparelho, caso o backup esteja atualizado.

4. **Desabilite o chip:** entre em contato com a operadora para bloquear o SIM/eSIM e solicitar uma segunda via.

5. **Alerte seus contatos:** avise aos amigos e familiares sobre eventuais tentativas de golpe, pois criminosos podem se passar por você para pedir **senhas, códigos de verificação (SMS/WhatsApp), links de recuperação ou transferências financeiras**.

6. **Boletim de Ocorrência:** faça o registro on-line pelo site da Polícia Civil do Estado do Rio de Janeiro.