GUIA PRÁTICO PARA *USO SEGURO* DE SERVIÇOS E APLICATIVOS DIGITAIS

Versão 2.0 dez/2025

Gerência de Segurança Cibernética

GRUPO energisa 120

Guia para Uso Seguro de Serviços e Aplicativos Digitais

01 - Vazamento e Super Exposição de Dados e Privacidade

02 – Engenharia Social, Fraudes Digitais e IA

03 - Roubo de Identidade Digital

04 - Malware e Ataques Cibernéticos

05 – Golpes Financeiros e Falsos Investimentos

06 - Impacto Reputacional e Assédio

07 - Perda, Furto ou Roubo do Celular

08 - O Que Fazer em Caso de Incidentes

Anexos

Atenção: O Grupo Energisa não se responsabiliza pela perda de dados pessoais após a execução por parte do usuário nas orientações relacionadas neste guia.

Prefácio

Hoje, nossa rotina digital envolve praticamente tudo: comunicação, trabalho, transações financeiras, autenticação de serviços e acesso a informações pessoais.

Com esse avanço, cresceram também as ameaças: **golpes impulsionados por inteligência artificial, fraudes em meios de pagamento instantâneo, uso indevido de dados, manipulação de identidade e crimes que exploram distração, confiança e urgência**.

Esta nova versão do guia reúne orientações claras e práticas para ajudar você a navegar com **mais segurança nesse ambiente em constante transformação.**

Aqui, apresentamos **medidas essenciais de proteção e passos objetivos para agir em situações de risco**.

Nos anexos, você encontra instruções detalhadas para configurar recursos de segurança em aplicativos, serviços digitais e dispositivos pessoais.

Vazamento e Super Exposição de Dados e Privacidade

Ocorre quando informações pessoais (nome, CPF, telefone, endereço, fotos, localização, hábitos, perfis sociais) tornam-se acessíveis a pessoas não autorizadas ou ficam excessivamente expostas em ambientes públicos.

O QUE FAZER?

- ✓ Use **senhas seguras** e únicas para cada conta
- ✓ Mantenha seus **perfis restritos** para amigos ou contatos conhecidos
- ✓ Atualize regularmente os **contatos de recuperação**
- ✓ Revise **permissões de apps** regularmente.
- ✓ Verifique periodicamente os **dispositivos vinculados**.

O QUE NÃO FAZER?

- ○ **Não salve** informações sensíveis permanentemente
- ○ **Não divulgue** sua localização nas redes sociais
- ○ **Não manter** aplicativos não utilizados instalados.
- ○ **Não permitir** que informações privadas apareçam nas notificações.
- ○ **Não interagir** com desconhecidos ou sem verificação.

Principais Controles Tecnológicos Associados

- Ativar login biométrico (impressão digital/Face ID)
- Desativar compartilhamento de localização em tempo real e em fotos
- Cadastrar um canal seguro para recuperação de senhas

Consulte **"Mais Controles"** clicando nos links abaixo e saiba **"Como Aplicá-los"** na prática em:

REDES SOCIAIS | **APPS DE MENSAGENS** | **APPS BANCÁRIOS** | **CONTAS DE E-MAIL** | **SISTEMAS OPERACIONAIS**

Engenharia Social, Fraudes Digitais e Inteligência Artificial

Com o uso da IA, os golpes ficaram mais convincentes: áudios clonados, vídeos manipulados e mensagens extremamente personalizadas. Apesar disso, os princípios de defesa continuam os mesmos: **desconfiar**, **validar por canais confiáveis e não tomar decisões sensíveis sem verificação**.

O que fazer

- ✓ Revisar os dados antes de confirmar qualquer transação.
- ✓ Relatar tentativas de golpes às plataformas.
- ✓ Evitar responder números desconhecidos.

O que NÃO fazer

- ✗ Não clicar em links suspeitos recebidos por e-mail ou mensagens.
- ✗ Não fornecer informações pessoais em chamadas ou mensagens suspeitas.

Como me Proteger?

Proteção contra E-mails Indesejados
Ativar filtros para bloquear mensagens de spam e phishing

Alertas Suspeitos
Ativar alerta de atividade suspeita na conta

Confirmação de Pagamento
Ativar "confirmação antes de envio" de pagamentos

Bloqueio Preventivo
Habilitar o bloqueio de chamadas e mensagens desconhecidas

Consulte **"Mais Controles"** clicando nos links abaixo e saiba **"Como Aplicá-los"** na prática em:

REDES SOCIAIS | **APPS DE MENSAGENS** | **APPS BANCÁRIOS** | **CONTAS DE E-MAIL**

Roubo de Identidade Digital

Roubo de identidade acontece quando alguém não autorizado usa suas informações para abrir contas, fazer compras ou cometer fraudes em seu nome. Isso pode acontecer através de vazamentos de dados ou uso de informações pessoais suas quando compartilhadas online.

Controles Comportamentais Importantes

Não compartilhar credenciais de acesso com terceiros

Alterar senhas regularmente para evitar acessos indevidos

Evitar a reutilização de credenciais

Revisar dispositivos conectados regularmente

Utilizar diferentes senhas para cada conta

Ativar a verificação de identidade em plataformas bancárias

Utilizar gerenciadores de senhas confiáveis

Revisar notificações de transações bancárias

Como me proteger?

Login MFA
Habilitar autenticação multifator para login seguro

PIN do eSIM
Configurar um PIN para seu cartão eSIM ou chip

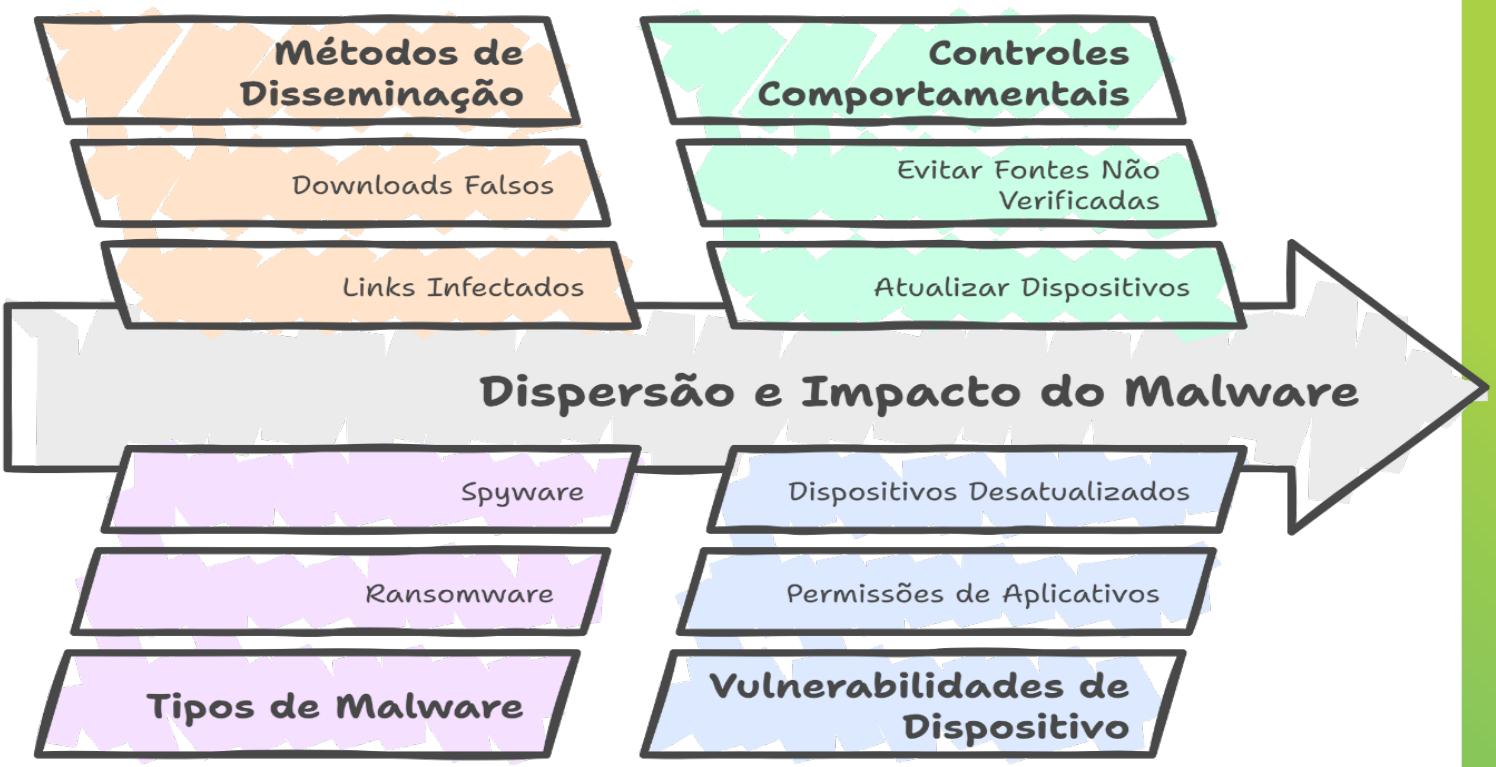
Consulte **"Mais Controles"** clicando nos links abaixo e saiba **"Como Aplicá-los"** na prática em:

REDES SOCIAIS | **APPS DE MENSAGENS** | **APPS BANCÁRIOS** | **CONTAS DE E-MAIL** | **SISTEMAS OPERACIONAIS**

GRUPO energisa 120

Malware e Ataques Cibernéticos

Malwares são programas maliciosos que podem roubar informações, travar seu dispositivo ou até pedir resgate pelos seus dados. Eles são disseminados através de links infectados, downloads falsos e anexos suspeitos.



Controles Tecnológicos

Saiba "Como Aplicar" mais controles aqui:

CONTAS DE E-MAIL

SISTEMAS OPERACIONAIS

Golpes Financeiros e Falsos Investimentos

Golpes financeiros hoje combinam fraudes bancárias, falsas ofertas de investimento e o uso indevido do sistema de pagamento instantâneo, aplicado com engenharia social em redes sociais, e-mails e sites falsos.

Cuidados com Informações Financeiras

Nunca compartilhe dados financeiros em mensagens privadas, ligações recebidas ou redes sociais.

Use cartões virtuais para compras online

Ative alertas de todas as transações. Via app + SMS + e-mail, se disponível

Tenha notificação de transações enviadas a um terceiro de confiança (quando o banco permitir)

O Pix tornou-se um dos canais mais explorados em golpes financeiros no Brasil.

⚠ Lembre-se

Pix é rápido, prático e seguro,
mas irreversível na maioria dos casos

O BC aprimorou o MED, aumentando a rastreabilidade de transferências usadas em golpes. Com a medida, haverá mais chances de recuperação dos valores. A medida passa a ser obrigatória para todos os bancos em fevereiro de 2026.

CLIQUE AQUI E SAIBA MAIS

Saiba **"Como Aplicar"** mais controles aqui:

APPS BANCÁRIOS

GRUPO energisa12

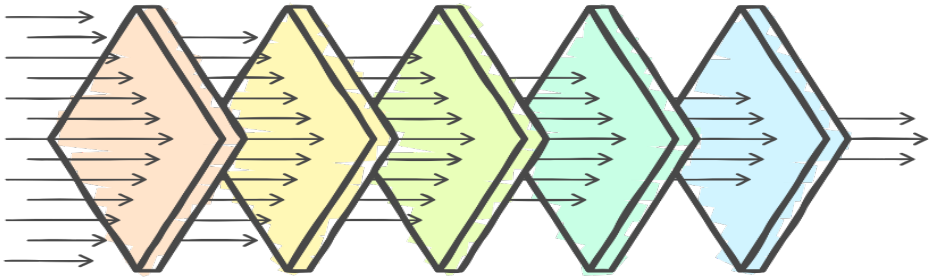
Impacto Reputacional e Assédio

Postagens e mensagens inadequadas podem afetar sua reputação profissional e pessoal. Além disso, o assédio online também é um problema crescente e necessitam de prevenção e denúncia.

Boas Práticas de Comportamento Online

Configurar alertas de menção

Denunciar assédio e abuso



Ambiente Online Seguro

Ativar restrições de comentários ofensivos

Controlar permissões de marcação de fotos e postagens

Proteja-se!

Bloqueie usuários com comportamento inadequado

Não participe de discussões ofensivas

Denuncie conteúdos ofensivos nas redes sociais

Pense antes de postar algo que pode comprometer sua imagem

Consulte **"Mais Controles"** clicando nos links abaixo e saiba **"Como Aplicá-los"** na prática em:

REDES SOCIAIS

APPS DE MENSAGENS

Perda, Furto ou Roubo do Celular

Perder o celular, ou tê-lo roubado, é um dos incidentes mais graves atualmente, pois pode permitir o acesso às suas contas de e-mail, bancárias, redes sociais, armazenamento de arquivos e mensageiros.

Medidas preventivas: **configurações essenciais**

Use uma senha adicional no app de e-mail.

O e-mail é a porta de recuperação de contas e precisa de uma camada adicional de segurança. Clique **AQUI** e saiba como aplicar.

Senha forte de bloqueio, Face ID / Biometria ativada

iPhone: Ajustes → Face ID e Código → Alterar código

Android: Configurações → Segurança → Bloqueio de tela

Buscar dispositivo (Find My / Encontrar meu dispositivo)

iPhone: Ajustes → [Seu nome] → Buscar → Buscar iPhone
Android: Configurações → Google → Encontrar meu dispositivo

Bloqueio do SIM/eSIM (PIN)

iPhone: Ajustes → Celular → PIN do SIM
Android: Configurações → Segurança → Bloqueio do SIM

Oculte notificações na tela bloqueada

iPhone: Ajustes → Notificações → Pré-visualizações → “Quando desbloqueado”
Android: Configurações → Notificações → Tela bloqueada → “Ocultar conteúdo sensível”

Habilite backup automático

iPhone: Ajustes → [Seu nome] → iCloud → Backup do iCloud
Android: Configurações → Google → Backup

Perda, Furto ou Roubo do Celular

Perder o celular, ou tê-lo roubado, é um dos incidentes mais graves atualmente, pois pode permitir o acesso às suas contas de e-mail, bancárias, redes sociais, armazenamento de arquivos e mensageiros.

O que fazer **imediatamente após** o furto ou roubo. Execute as ações em ordem.

Atenção: Clique em cada item para acessar o passo a passo detalhado.

01. Bloqueie o aparelho remotamente

02. Bloqueie o SIM/eSIM imediatamente

03. Desconecte sessões de aplicativos críticos

04. Troque as senhas principais

05. Notifique o(s) banco(s) imediatamente

06. Registre Boletim de Ocorrência

07. Bloqueie o IMEI

Recuperando suas contas após o incidente (Clique Aqui)

Perda, Furto ou Roubo do Celular

Aplicativo Celular Seguro

O **Celular Seguro**, criado pelo Governo Federal, permite realizar **bloqueios emergenciais** para reduzir o risco de golpes após perda, furto ou roubo do aparelho. Ele integra serviços públicos e privados vinculados ao **gov.br**, facilitando a interrupção rápida de acesso a contas e aplicativos críticos.
O app é uma camada adicional de proteção, **não substitui as medidas preventivas listadas no guia**, mas funciona como uma resposta imediata que deve ser acionada em situações reais de risco

Clique AQUI para acessar o Guia Oficial do Aplicativo Celular Seguro

Cuidados importantes antes de usar o app

- ✓ Configurar contatos de confiança é obrigatório
- ✓ Ative a proteção biométrica no gov.br
- ✓ Mantenha o login do gov.br sempre atualizado.
- ✓ Saiba que acionar por engano gera impacto real:
  - Se você acionar o app sem necessidade, será desconectado de todas as suas contas.
  - Por isso, só acione o app em situações legítimas e comprovadas.

O Que Fazer em Caso de Incidentes 01

Golpes financeiros hoje combinam fraudes bancárias, falsas ofertas de investimento e o uso indevido do sistema de pagamento instantâneo, aplicado com engenharia social em redes sociais, e-mails e sites falsos.

Sua conta foi invadida?

1. **Tente recuperar o acesso** imediatamente redefinindo a senha:
- No **WhatsApp**: Vá para Configurações > Conta > Verificação em duas etapas e redefina o PIN.
- No **Instagram/Facebook**: Acesse a opção Esqueci minha senha na tela de login e siga as instruções.

2. **Revise e encerre sessões suspeitas**:
- No **Instagram/Facebook**: Vá para Configurações e privacidade > Segurança e login e remova dispositivos desconhecidos.
- No **WhatsApp**: Se notar acessos não autorizados, saia de todas as sessões do WhatsApp Web e reative a verificação em duas etapas.

3. **Ative a verificação em duas etapas (MFA)** caso ainda não tenha feito.
4. **Verifique e atualize suas informações de recuperação**, como e-mail e número de telefone, para evitar futuras invasões.
5. **Se não conseguir recuperar a conta**, entre em contato com o suporte da plataforma para solicitar a recuperação.

📌 **Lembre-se:** Quanto mais rápido agir, menor o impacto do incidente. Denunciar atividades suspeitas ajuda a tornar as redes sociais mais seguras para todos.

O Que Fazer em Caso de Incidentes 02

Golpes financeiros hoje combinam fraudes bancárias, falsas ofertas de investimento e o uso indevido do sistema de pagamento instantâneo, aplicado com engenharia social em redes sociais, e-mails e sites falsos.

Caiu em um golpe?

1. **Se fez um pagamento ou compartilhou dados bancários**, entre em contato com seu banco imediatamente para tentar reverter a transação e bloquear possíveis fraudes.
2. **Denuncie à plataforma** onde ocorreu o golpe:
   - No **Instagram/Facebook**: Acesse a postagem ou perfil fraudulento, toque nos três pontos ⋮ e selecione Denunciar.
   - No **WhatsApp**: Acesse a conversa do golpista, toque no nome e selecione Denunciar e bloquear.
3. **Registre um boletim de ocorrência online** no site da Polícia Civil do seu estado, especialmente se envolver transações financeiras ou roubo de identidade.
4. **Se forneceu informações sensíveis (CPF, RG, senhas),** monitore seu nome em serviços de proteção contra fraudes, como **Registrato (Banco Central)** e **Serasa**.

📌 **Lembre-se:** Quanto mais rápido agir, menor o impacto do incidente. Denunciar atividades suspeitas ajuda a tornar as redes sociais mais seguras para todos.

O Que Fazer em Caso de Incidentes 03

Golpes financeiros hoje combinam fraudes bancárias, falsas ofertas de investimento e o uso indevido do sistema de pagamento instantâneo, aplicado com engenharia social em redes sociais, e-mails e sites falsos.

Detectou um perfil falso?

1. **Denuncie diretamente na plataforma**:
   - No **Instagram/Facebook**: Acesse o perfil falso, toque em ⋮ e selecione Denunciar > Imitação de outra pessoa.
   - No **WhatsApp**: Informe aos seus contatos que alguém pode estar se passando por você e peça para que também denunciem.
2. **Avise seus amigos e familiares**, pois o perfil falso pode estar tentando enganar conhecidos.
3. **Se a conta falsa estiver se passando por uma empresa**, verifique se a empresa já possui um canal oficial para denúncias e faça um alerta público sobre perfis fraudulentos.

✅ **Dica Extra:** Se sua foto de perfil estiver sendo usada sem autorização, você pode reivindicar seus direitos sobre a imagem.

📌 **Lembre-se:** Quanto mais rápido agir, menor o impacto do incidente. Denunciar atividades suspeitas ajuda a tornar as redes sociais mais seguras para todos.

ANEXOS Redes Sociais

(Clique nas imagens de "👆" para acessar o passo a passo de como implementar o controle indicado em cada plataforma.)

Controles de Segurança	Tiktok	LinkedIn	Facebook	Instagram	Youtube
Cadastrar um canal seguro para recuperação de senhas.	👆	👆	👆	👆	👆
Habilitar o duplo fator de autenticação.	👆	👆	👆	👆	👆
Habilitar o modo privado para a rede social, sendo necessário aceitar seguidores ou amigos para visualizar informações do perfil.	👆	X	👆	👆	👆
Habilitar alertas para tentativas de login a partir de dispositivos ou locais desconhecidos.	👆	👆	👆	👆	👆
Remover acessos de aplicativos de terceiros que não são mais utilizados.	👆	👆	👆	👆	👆
Definir níveis adequados de privacidade para publicações e informações do perfil.	👆	👆	👆	👆	👆
Revisar e desconectar sessões ativas em dispositivos que não são mais utilizados ou que possam estar comprometidos.	👆	👆	👆	👆	👆

ANEXOS Apps de Mensagens

Controles de Segurança	WhatsApp	Telegram
Ativar as notificações de segurança no smartphone principal.	Acesse Configurações > Conta > Ative "Mostrar notificações de segurança"	Acesse Configurações > Notificações e Sons > Certifique-se de que as notificações relevantes estão ativadas
Crie uma chave de acesso para proteção da conta.	Acesse Configurações > Conta > Chave de Acesso > Definir uma senha	Acesse Configurações > Privacidade e Segurança > Senha de Bloqueio > Ativar e definir uma senha
Confirme o endereço de e-mail atribuído à sua conta.	Acesse Configurações > Conta > Endereço de email > Adicione ou atualize o e-mail cadastrado	Acesse Configurações > Privacidade e Segurança > Verificação em duas etapas >Verificar e-mail de recuperação
Habilite a confirmação em duas etapas para adicionar mais uma camada de segurança no acesso a conta.	Acesse Configurações > Conta > Verificação em duas etapas > Ativar e definir um código PIN	Acesse Configurações > Privacidade e Segurança > Verificação em duas etapas > Ativar e definir uma senha
Habilite o bloqueio do App para solicitar uma senha / biometria para abrir o aplicativo.	Acesse Configurações > Privacidade > Bloqueio do app > Ativar e configurar	Acesse Configurações > Privacidade e Segurança > Código de Bloqueio > Ativar e definir uma senha
Permita que somente contatos possam ver a sua foto do Perfil.	Acesse Configurações > Privacidade > Foto do perfil > Selecione "Meus contatos"	Acesse Configurações > Privacidade e Segurança > Foto do perfil > Escolha "Meus contatos
Permita que apenas seus contatos possam adiciona-lo em grupos.	Acesse Configurações > Privacidade > Grupos > Escolha "Meus contatos"	Acesse Configurações > Privacidade e Segurança > Convites > Selecione "Meus contatos"
Selecione "Ninguém" para que seus contatos não possam ver seus dados de Pix.	Acesse Configurações > Privacidade > Pix > Escolha "Ninguém"	X
Selecione "ninguém" ou "meus contatos" para que possam ver seu número de telefone	X	Acesse Configurações > Privacidade e Segurança > Número de telefone > Escolha "Meus contatos" ou "Ninguém"
Selecione "meus contatos" para garantir que somente seus contatos possam enviar convites.	X	Acesse Configurações > Privacidade e Segurança > Convites > Escolha "Meus contatos"
Verifique os dispositivos conectados à conta e mantenha somente os dispositivos confiáveis.	Clique nos três pontinhos no canto superior direito da tela > Dispositivos conectados > Remova dispositivos desconhecidos	Acesse Configurações > Dispositivos > Verifique e remova conexões suspeitas

ANEXOS

Apps Bancários

(Clique nas imagens de "👆" para acessar o passo a passo de como implementar o controle indicado em cada plataforma.)

Controles de Segurança	Santander	Itaú	Nubank	Bradesco
Confirme as informações cadastradas no Perfil e verifique a existência de um canal seguro registrado para recuperação de senhas.	👆	👆	👆	👆
Ative os alertas e notificações de compras por cartão para receber avisos por push.	👆	👆	👆	👆
Altere o limite do seu pix para pagamentos e transferências, evitando que valores altos possam ser transferidos de uma única vez.	👆	👆	👆	👆
Ative o Alô Protegido, proteção para que o aplicativo ajude a evitar golpes de falsas centrais.	X	X	👆	X

ANEXOS

Contas de E-mail

(Clique nas imagens de "👆" para acessar o passo a passo de como implementar o controle indicado em cada plataforma.)

Controles de Segurança	Outlook	Gmail	Yahoo	iCloud
Cadastrar um canal seguro (e-mail secundário e telefone válido para SMS) para recuperação de senhas.	👆	👆	👆	👆
Habilitar o duplo fator de autenticação.	👆	👆	👆	👆
Utilizar um app Autenticador (ex.: Microsoft Authenticator, Google Authenticator) para iniciar sessão sem necessidade de senha	👆	👆	👆	👆
Garantir que somente dispositivos conhecidos estão vinculados à sua conta de e-mail	👆	👆	👆	👆
(!) Ativar a Proteção Avançada do Google	X	👆	X	X
(!!) Ativar Proteção Avançada de Dados do iCloud	X	X	X	👆
Garantir que apenas aplicações e serviços conhecidos têm acesso às informações de e-mail	👆	👆	👆	👆

ANEXOS

Sistemas Operacionais

Controles de Segurança	Android	iOS
Habilite o bloqueio de tela e defina um código de acesso para criar uma barreira de segurança que impeça uma pessoa não autorizada de acessar seu smartphone.	Abra o aplicativo "Configurações" > "Segurança" > "Bloqueio de tela". Escolha o tipo de bloqueio desejado (PIN, padrão, senha) e siga as instruções para configurá-lo.	Acesse "Ajustes" > "Face ID e Código" (ou "Touch ID e Código" em modelos anteriores) > "Ativar Código". Siga as instruções para definir um código de acesso.
Use o Reconhecimento Facial para desbloquear o smartphone, autorizar compras e pagamentos e, iniciar uma sessão em vários apps de terceiros com segurança	A disponibilidade do reconhecimento facial varia conforme o dispositivo. Em dispositivos compatíveis, vá para "Configurações" > "Segurança" > "Desbloqueio facial" e siga as instruções para configurar.	Acesse "Ajustes" > "Face ID e Código" > "Configurar Face ID". Siga as instruções para configurar o Face ID. Para autorizar compras, ative "iTunes e App Store" na mesma seção.
Ative a função de Buscar Dispositivo para ajudar a encontrar o seu aparelho e impedir que outra pessoa ative ou use o smartphone.	Abra "Configurações" > "Segurança" > "Encontrar Meu Dispositivo" e ative a opção.	Acesse "Ajustes" > toque no seu nome > "Buscar" > "Buscar iPhone" e ative a opção.
Desative o conteúdo de notificações na tela de bloqueio, para que não sejam exibidas publicamente informações de recuperação de senha, tokens e códigos de validação	Vá para "Configurações" > "Aplicativos e notificações" > "Notificações" > "Na tela de bloqueio" e escolha "Não mostrar notificações" ou "Ocultar conteúdo confidencial".	Acesse "Ajustes" > "Notificações" > "Mostrar Pré-visualizações" e selecione "Quando Desbloqueado" ou "Nunca".
Controle o acesso a informações em apps e as informações de localização compartilhadas.	Vá para "Configurações" > "Privacidade" > "Gerenciador de permissões" e selecione categorias como "Localização", "Contatos", "Câmera" etc., para ajustar as permissões dos aplicativos.	Acesse "Ajustes" > "Privacidade" e selecione categorias como "Serviços de Localização", "Contatos", "Fotos" etc., para gerenciar as permissões de cada aplicativo.
Crie senhas fortes e proteja a conta com multifator de autenticação (MFA) para manter a sua conta segura	Utilize aplicativos de autenticação, como o Google Authenticator ou o Microsoft Authenticator, disponíveis na App Store e Google Play Store, para configurar a autenticação de dois fatores em suas contas.	
Proteja os seu dados caso ocorra perda ou roubo do seu smartphone utilizando o Modo Perdido (iOS) / Bloqueio Remoto (Android): Permite bloquear o dispositivo remotamente e exibir uma mensagem de contato caso o aparelho seja perdido.	Acesse "android.com/find", faça login com sua conta Google, selecione o dispositivo perdido e escolha a opção "Bloquear" para bloquear remotamente e adicionar uma mensagem de contato.	Acesse o site "iCloud.com" ou use o app "Buscar" em outro dispositivo Apple, selecione seu iPhone perdido e ative o "Modo Perdido".
Utilize o recurso "Bloqueio de Aplicativos" para bloquear os aplicativos indesejados.	Como configurar a Pasta Segura no Samsung > Abra o app “Configurações” > Toque em “Biometria e Segurança” > Selecione “Private Share” > Faça login com a sua conta Samsung > Siga as instruções e defina um tipo de bloqueio para a Pasta Segura.	X
Configure um PIN no cartão eSIM / chip do celular para exigir que um código de identificação seja inserido em um novo aparelho ou para fazer ligações e usar os dados celulares	Vá para "Configurações" > "Segurança" > "Configurações do SIM" > "Bloqueio do cartão SIM" e ative a opção, inserindo um código PIN.	Acesse "Ajustes" > "Celular" > "PIN do SIM" e ative a opção, inserindo um código PIN.
Tenha uma cópia de segurança das suas informações para restaurar em outro smartphone em caso de perda ou roubo.	Ative o backup do Google. Vá para "Configurações" > "Sistema" > "Backup" e ative a opção "Fazer backup no Google Drive".	Utilize o iCloud para backups automáticos. Acesse "Ajustes" > toque no seu nome > "iCloud" > "Backup do iCloud" e ative a opção.
Utilize o recurso "Recurso de Tempo de Uso" para impedir o acesso ao Icloud e bloquear os aplicativos indesejados, após determinado limite de tempo definido pelo usuário.	X	Use o recurso "Tempo de Uso" para definir limites de uso para aplicativos específicos. Acesse "Ajustes" > "Tempo de Uso" > "Limites de Apps" e configure os limites desejados.
Mantenha o seu dispositivo atualizado com as últimas versões do sistema operacional.	Use o recurso "Bem-estar digital" para definir limites de uso de aplicativos. Vá para "Configurações"	Acesse "Ajustes" > "Tempo de Uso" e configure os limites desejados para aplicativos específicos ou categorias de aplicativos.

ANEXOS Perda, Furto ou Roubo do Celular

Medidas preventivas

Use uma senha adicional no app de e-mail

iPhone (Tempo de Uso / Screen Time)
Ajustes → Tempo de Uso → Ativar Tempo de Uso
→ Usar Código do Tempo de Uso → Defina um PIN diferente do código do iPhone
→ Limites de Apps → Adicionar Limite
→ Categoria: Criatividade (ou escolha o app Mail)
→ Defina 1 minuto → Ative **Bloquear ao Término do Limite**
Resultado: o app de e-mail só abre após digitar o PIN extra do Tempo de Uso.

Android (Bloqueio de Aplicativos / Secure Folder)
Configurações → Segurança / Privacidade / Aplicativos (varia por fabricante)
→ “Bloqueio de Aplicativos”, “Bloquear Apps”, “Proteção de Apps” ou “Pasta Segura”
→ Defina um PIN ou biometria diferente
→ Selecione o app de e-mail (Gmail, Outlook, etc)
Resultado: o app de e-mail fica protegido mesmo se o celular estiver desbloqueado.

ANEXOS Perda, Furto ou Roubo do Celular

O que fazer imediatamente após o furto ou roubo (passo a passo)

Passo 1 — Bloqueie o aparelho remotamente

Isso impede acesso ao conteúdo e, se necessário,

permite apagar tudo.

- **Android:** https://www.google.com/android/find/
  → Selecione *Bloquear* e depois *Apagar dispositivo* (se necessário)
- **iPhone:** https://www.icloud.com/find
  → Acione *Modo Perdido* e, se necessário, *Apagar iPhone*

Passo 2 — Bloqueie o SIM/eSIM imediatamente

Entre em contato com sua operadora e solicite:

- Bloqueio do chip
- Bloqueio do eSIM
- Cancelamento temporário da linha
- Registro de fraude (se aplicável)

Operadoras: Vivo (10315), Claro (1052), TIM (*144).

O que fazer imediatamente após o furto ou roubo (passo a passo)

Passo 3 — Desconecte sessões de aplicativos críticos

WhatsApp

Configurações → Dispositivos conectados → *Desconectar de todos os dispositivos*

Instagram / Facebook

Configurações → Segurança e login → *Encerrar sessões desconhecidas*

Gmail / Google

myaccount.google.com → Segurança → Seus dispositivos → *Encerrar sessão*

Outlook / Microsoft

account.microsoft.com → Segurança → Revisar atividade → *Encerrar sessões*

Bancos

Acesse via navegador → Configurações → "Encerrar todas as sessões"
(Disponível nos principais bancos brasileiros)

O que fazer imediatamente após o furto ou roubo (passo a passo)

Passo 4 — Troque imediatamente as senhas principais

Ordem sugerida:

1. **E-mail** (Gmail, Outlook, iCloud)
2. **WhatsApp**
3. **Aplicativos bancários**
4. **Redes sociais**
5. **Serviços críticos (Google, Apple, Microsoft)**

Use senhas novas, longas e exclusivas.

Passo 5 — Notifique o(s) banco(s) imediatamente

Peça:

- bloqueio preventivo
- análise de movimentações recentes
- contestação de transações suspeitas
- bloqueio de cartão
- novo dispositivo seguro para acessar o app

ANEXOS Perda, Furto ou Roubo do Celular

O que fazer imediatamente após o furto ou roubo (passo a passo)

Passo 6 — Registre Boletim de Ocorrência

Sempre utilize a **Delegacia Virtual do seu estado** (Polícia Civil).

É rápido, gratuito e necessário para:

- contestar transações
- bloquear IMEI
- acionar garantias e seguros
- comprovar fraude

Passo 7 — Bloqueie o IMEI

IMEI = identidade do aparelho.
Mesmo apagado, ainda pode ser bloqueado.

Como fazer:

- Pela operadora (Vivo, TIM, Claro etc.)
- Pelo sistema da **Anatel** (via operadora)

Tenha o IMEI anotado em local seguro antes do incidente:

- Dial: *#06# para exibir
- Anote no gerenciador de senhas

ANEXOS

Recuperando suas contas após o incidente - 01

Google, Apple e Microsoft

Se a conta estiver comprometida:

- **Google** → https://g.co/recover
- **Apple** → https://iforgot.apple.com
- **Microsoft** → https://account.live.com/acsr

Esses serviços possuem fluxos robustos de recuperação e validação de identidade.

Redes sociais

Procedimentos variam por plataforma:

- **Instagram / Facebook:**
  → Recuperação pela tela de login (“Obter ajuda para entrar”)
- **X (Twitter):**
  → Suporte via help center
- **LinkedIn:**
  → Recuperação por e-mail ou verificação adicional

Nunca confie em “suporte por WhatsApp”, “perfil verificado”, “agente terceirizado” ou “técnico remoto”.

ANEXOS

Recuperando suas contas após o incidente - 02

WhatsApp

Se o ladrão tentar usar seu número:

1. Envie um e-mail para **support@whatsapp.com**
2. Assunto: **“Desativar conta por perda/roubo”**
3. No corpo do e-mail, escreva:

“Solicito desativação do WhatsApp associado ao número +55 XX XXXXX-XXXX devido a perda/roubo.”

A conta será desativada imediatamente.

Depois, quando recuperar sua linha:

- Reinstale o WhatsApp
- Faça login pelo seu número
- Confirme o PIN do WhatsApp (que você já deve ter configurado)

E-mail

Siga os passos e valide sua identidade.

Gmail → https://accounts.google.com/signin/recovery
Outlook / Hotmail → https://account.live.com/acsr
Apple ID → https://iforgot.apple.com