Cartilha de **Segurança Digital**

Dicas Rápidas

Prevenção contra golpes e fraudes.

Juntos pela sua proteção no ambiente digital.

Sicredi

Nos dias de hoje, é frequente utilizarmos serviços financeiros via smartphone. Por isso, é importante ter boas práticas com os dados armazenados no celular. Assim você evita o uso indevido de sua conta bancária diante de casos de roubo, furto ou perda do aparelho.

Siga as dicas abaixo para aumentar a sua segurança.

Como se proteger:

- **Sempre utilize o bloqueio da tela de início do celular.** Opte pela opção de bloqueio automático mais rápida (30 segundos, por exemplo).

- **Utilize senhas fortes** e não repita o código de acesso ao Sicredi em outros aplicativos, e-mail ou sites de compras.

- **Jamais anote senhas em blocos de notas, e-mails, mensagens de WhatsApp** e outros locais ou arquivos do celular.

- **Apague conversas que contenham senhas** e/ou dados pessoais em e-mail, SMS, redes sociais ou aplicativos como WhatsApp.

- **Evite andar na rua usando o celular.** E redobre a atenção ao volante, especialmente ao usar apps de navegação como Waze ou Google Maps.

- **Coloque uma senha PIN no chip do celular.** Assim, caso o aparelho seja reiniciado, será necessário inserir o código pessoal para uso da linha e envio e recebimento de SMS.

- Nas configurações do aparelho, **desative notificações** e funções exibidas independentemente do bloqueio de tela inicial.

- **Nunca utilize o recurso de “lembrar/salvar senha”** em navegadores e sites.

Dicas rápidas

• **Utilize ferramentas de segurança adicionais,** como biometria, reconhecimento facial e dupla autenticação
(a segunda senha) em apps e no e-mail.

• **Mantenha o sistema operacional do celular atualizado** e sempre verifique se há atualizações de aplicativos pendentes.

→ Caso o seu celular seja roubado:

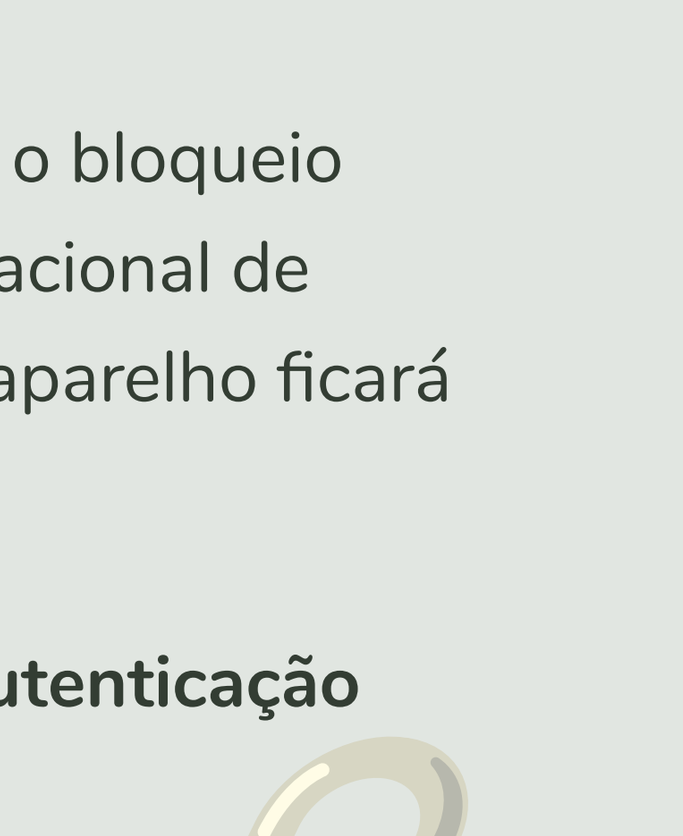
• **Notifique imediatamente o Sicredi** para que medidas de segurança sejam adotadas, como bloqueio do app, da senha de acesso e da própria conta.

• **Acesse as páginas criadas pela Apple** (no caso do iPhone www.icloud.com) **ou pelo Google** (para celulares Android www.android.com/find) para limpar todo o conteúdo do aparelho de maneira remota.

• **Avise sua operadora de telefonia** e solicite o bloqueio imediato do chip e do IMEI (Identidade Internacional de Equipamento Móvel). A partir do bloqueio, o aparelho ficará impedido de se conectar a redes de dados.

• **Troque as senhas e as configurações de autenticação das contas** e dos aplicativos instalados no smartphone, incluindo redes sociais e e-mail.

• **Acesse a ferramenta Registrato do Banco Central** para verificar se os seus dados não foram utilizados para abertura de contas ou empréstimos.



Dicas rápidas

Dicas Rápidas

Pix

- **Ative a chave Pix somente nos nossos canais oficiais.** Se receber e-mails, mensagens ou ligações solicitando o cadastro da chave, não passe nenhuma informação.
- Não realize nenhuma “transação de teste”. Isso não existe.
- Ao realizar um Pix, confirme os dados do recebedor, inclusive quando o pagamento for via QR Code.

WhatsApp

- **Evite que seu WhatsApp seja clonado, habilite a verificação em duas etapas.**

iOS: no WhatsApp, acesse Ajustes > Conta > Confirmação em duas etapas > Ativar.

Android: no WhatsApp, acesse Menu > Configurações > Conta > Confirmação em duas etapas > Ativar.

- **Exiba sua foto apenas para os contatos de confiança, para que ela não seja usada indevidamente.**

iOS: no WhatsApp, acesse Ajustes > Conta > Privacidade > Foto de Perfil > Meus contatos.

Android: no WhatsApp, acesse Menu > Configurações > Conta > Privacidade > Foto de perfil > Meus contatos.

WhatsApp

• **Sempre encerre sessões ativas no WhatsApp Web. Faça o seguinte:**

iOS: no WhatsApp, acesse Ajustes > WhatsApp Web/ Computador > Desconectar de todos os aparelhos.

Android: no WhatsApp, acesse Menu > WhatsApp Web > Sair de todas as sessões.

• Atenção! Não realize nenhuma transação antes de **confirmar a legitimidade do pedido.** Mesmo que a foto seja de alguém que você conhece, ligue para a pessoa e faça perguntas pessoais.

Leilão Virtual e Promoções Tentadoras

• Atenção aos sites que possuem domínio**.com** e produtos com **valores muito abaixo do praticado.**

• Ao realizar uma compra on-line, consulte as páginas oficiais das lojas e verifique a sua reputação.

• No caso de Leilão Virtual, desconfie de sites que exijam que o pagamento seja feito em contas de pessoas físicas. Ele deve ser feito em contas judiciais ou em nome do próprio leiloeiro oficial.

• Se sua intenção for a de adquirir um veículo, verifique a possibilidade de analisá-lo pessoalmente. Por lógica, toda empresa de leilão virtual deve ter um pátio onde os veículos são armazenados.

Dicas rápidas

Sites Falsos/Links Falsos

- Evite clicar em links, procure sempre digitar o endereço no navegador.
- Verifique se o endereço do site em que você compra contém um cadeado à esquerda. Sites falsos possuem domínios bastante similares aos verdadeiros. Dê preferência aos que terminam em **.com.br**, pois eles indicam que são hospedados em servidores no Brasil.
- Desconsidere mensagens de instituições financeiras com as quais você não tem relação, especialmente quando solicitarem seus dados pessoais e senhas.
- Não abra arquivos de fontes desconhecidas.
- Evite se conectar por redes Wi-Fi públicas.

Ligações Falsas

- **Nunca forneça senha ou dados pessoais a terceiros,** principalmente por telefone.
- Não ligamos para você solicitando atualização do **módulo de segurança ou atualização cadastral.**
- Em nossos contatos, nunca pediremos sua senha ou código token. Essas informações são exclusivamente para você realizar suas operações em nossos canais. **Jamais** repasse essas informações ou digite em sites que não sejam os canais oficiais.

Compra e Venda em sites de negociação

- Ao fazer uma negociação, confirme o efetivo recebimento do dinheiro em sua conta antes de entregar a mercadoria. Tenha atenção a comprovantes falsos, comprovantes de agendamento ou comprovantes de depósito feitos em caixa eletrônico utilizando um envelope vazio.

Dicas rápidas

Pagamento de Boleto

Ao realizar um pagamento de boleto, certifique-se de que a linha digitável está de acordo com o logo da instituição financeira, além do Beneficiário – Cedente e Pagador – Sacado.

Golpe do Motoboy

- **Nunca entregue seu cartão a outra pessoa.**

Nenhuma instituição financeira faz coleta de cartões.

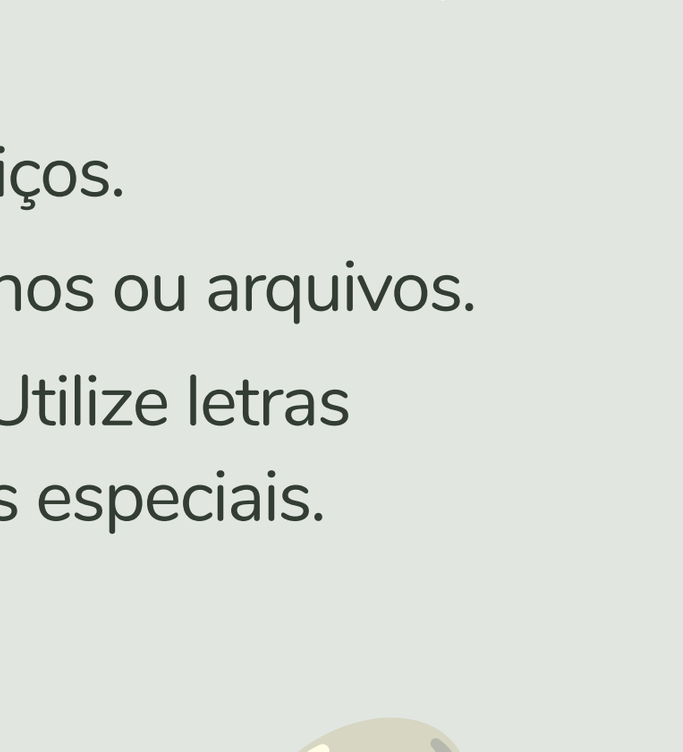
- Sempre corte o chip do cartão ao descartá-lo.
- Nunca digite sua senha em links recebidos por SMS ou WhatsApp.
- Se receber algum contato solicitando senha, desligue e informe sua Cooperativa.

Senhas e Autenticação

- Ao utilizar o recurso de login por biometria, esteja ciente de que toda biometria cadastrada em seu celular terá acesso aos aplicativos em que você utiliza essa funcionalidade.
- Em caso de perda ou roubo de celular, comunique imediatamente sua instituição financeira para solicitar o bloqueio da conta e do acesso ao aplicativo.
- Não utilize a mesma senha para vários serviços.
- Não salve senhas em bloco de notas, cadernos ou arquivos.
- Crie senhas difíceis de serem descobertas. Utilize letras maiúsculas, minúsculas, números e caracteres especiais.

Sua Conta, Sua Responsabilidade

- Lembre-se: você é responsável pela movimentação financeira de sua conta, por isso não a empreste a terceiros para receber valores que você desconheça a origem e não saiba a procedência.



Dicas rápidas

Conte conosco e, em caso de dúvidas, entre em contato pelos nossos canais digitais oficiais ou pelos nossos telefones:

SAC

Informações, elogios e reclamações

0800 724 7220

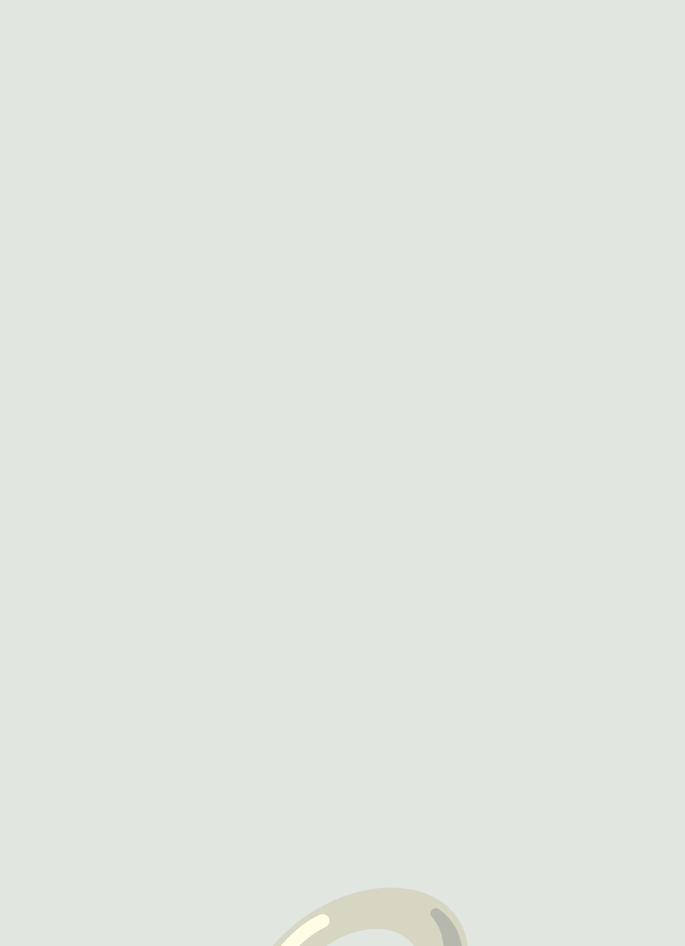
Atendimento aos Deficientes Auditivos ou de Fala

0800 724 0525

Ouvidoria e Denúncias

0800 646 2519

Confira mais informações em www.sicredi.com.br/seguranca



Dicas rápidas

Seguindo essas dicas e cuidados, você vai ficar muito mais protegido e pronto para orientar todos ao seu redor.

Sicredi