



Banpará

# USO DOS CANAIS DIGITAIS

## Cartilha educativa

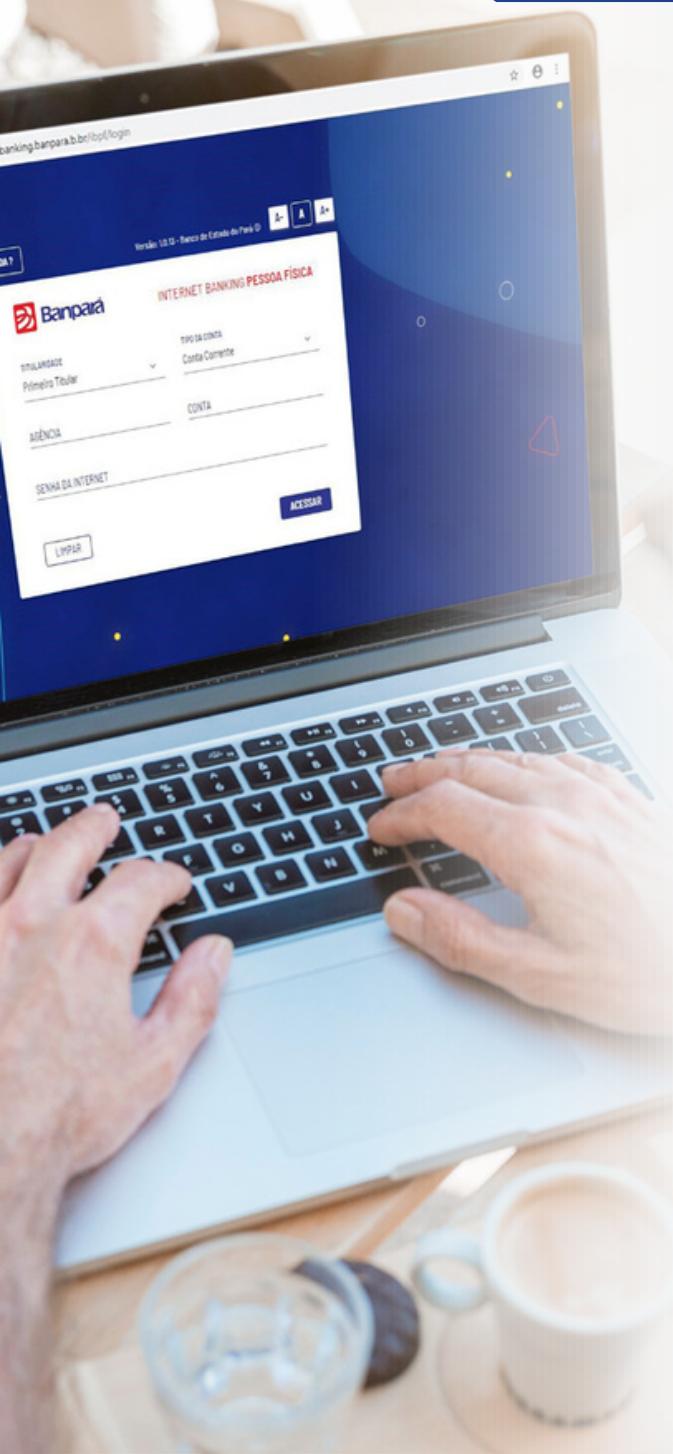
Dicas para tornar sua navegação mais fácil e segura

# Mobile Banking

O Mobile Banking é um canal que o Banpará coloca à disposição de seus clientes para realização de consultas e transações financeiras por meio de dispositivos móveis, com praticidade e segurança, agilizando o seu dia a dia. Para acessar este serviço é necessário que já você tenha cadastrado sua senha do Internet Banking de 8 dígitos no autoatendimento Banpará, e realizado seu primeiro acesso. A utilização deste serviço segue a tabela de pacotes e tarifas praticados no Banpará disponíveis nas agências e no site do Banco. É importante que cada cliente se atente as recomendações de segurança para utilização do aplicativo.



# Internet Banking



O Internet Banking é um Canal Digital na web onde você tem acesso aos produtos e serviços do Banpará por meio da internet sem precisar enfrentar filas ou ficar restrito aos horários de atendimento das Agências. É possível realizar transações financeiras, como pagamento de boletos, transferências, PIX, consultas empréstimos, investimentos e até recargas de celular. Além de transações não financeiras, como consulta de saldo/extrato, e 2<sup>a</sup> via de comprovantes. Para acessar o Internet Banking é necessário cadastrar uma senha de 8 dígitos em qualquer Caixa Eletrônico Banpará, na opção “Outros Serviços > Senha de Internet”. É necessário também realizar a habilitação do BPToken no seu celular para realizar transações financeiras, o passo a passo estará melhor detalhado na proxima página. Após o cadastro da senha, basta acessar o portal [www.banpara.b.br](http://www.banpara.b.br), clicar em “**Acesse sua conta**” e escolher o seu perfil. Lembrando que para realizar transações financeiras, o cliente deve primeiro habilitar o seu BPToken no aplicativo Mobile Banking, sendo a única forma de autenticação das transações em canais digitais.



No Internet Banking as transações não financeiras estão disponíveis 24h por dia e 7 dias por semana. Algumas das transações financeiras têm horários e limites pré-estabelecidos. O acesso ao Internet Banking é gratuito, a utilização dos serviços segue a tabela de pacotes de tarifas praticados disponíveis nas agências e no Site do Banpará.

# Processo de habilitação



## Criação de apelido

Para realizar transações financeiras no aplicativo é necessário que o cliente habilite seu dispositivo móvel. Para tanto, o cliente deve, primeiramente, fazer o download do aplicativo nas lojas oficiais de aplicativos mobile: Google Play Store (ANDROID) ou App Store (IOS). Depois de instalado, será necessário realizar o cadastro do apelido, como exemplificado nas imagens abaixo, para posterior habilitação. Logo após o login, você deve realizar o cadastro do apelido do dispositivo. **Ex: iPhone de Jose.**

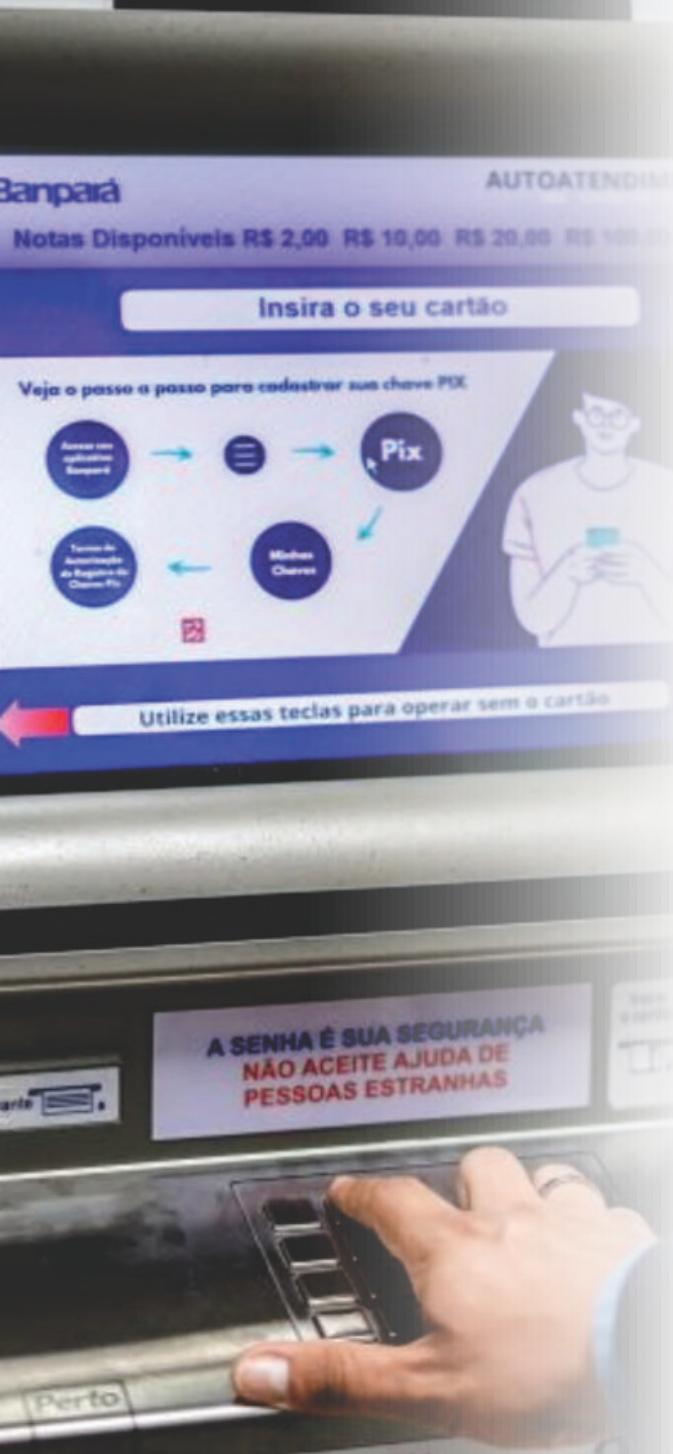


## Processo de habilitação

### CAIXA ELETRÔNICO



# Processo de habilitação



## Passo a Passo no Caixa Eletrônico

Para realizar a habilitação, procure um caixa eletrônico Banpará. Lembrando que é possível ter apenas 1 dispositivo habilitado por vez, por isso, caso o cliente já tenha outro token habilitado em outro aparelho, deve seguir primeiramente com o processo de desabilitação, no mesmo menu do caixa eletrônico.

Após inserir o cartão, acesse as opções: Outros Serviços > Segurança e Acesso > BPToken > Habilitar dispositivo.

1



2



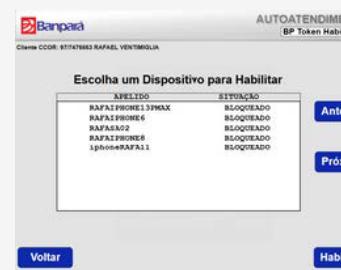
3



4



5

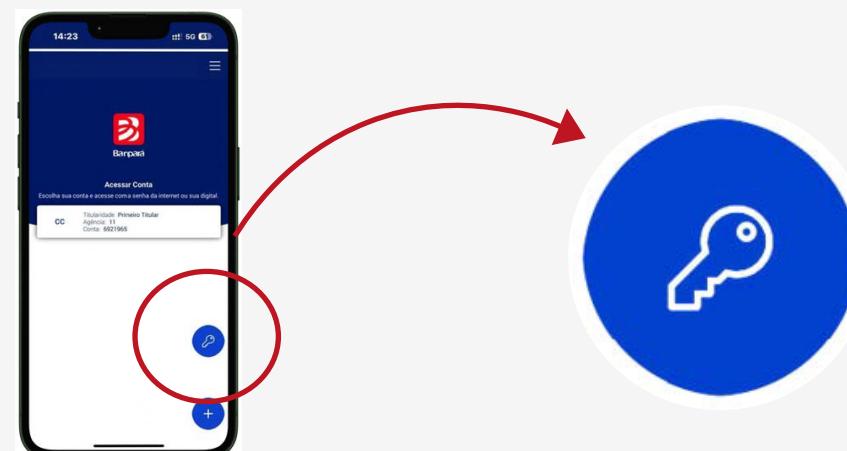


6



# Processo de habilitação

Após a habilitação do dispositivo, em sua próxima sessão no App, aparecerá um botão com o ícone de uma chave na tela inicial do aplicativo. As transações feitas no aplicativo Banpará serão autorizadas automaticamente no dispositivo habilitado, dispensando a inserção de código para validação. Caso deseje realizar transações pelo Internet Banking, deverá inserir o código gerado no dispositivo habilitado, clicando no ícone de uma chave na tela inicial para confirmação de cada transação feita no Internet Banking PF.



## RESUMO:



# Dicas de segurança

Com os investimentos em segurança e tecnologia, não é tão simples conseguir fraudar ou furtar dados diretamente de uma conta bancária. Sabendo disso, os golpistas procuram meios de enganar e persuadir você, buscando coletar informações e/ou convencê-lo a realizar ações como: executar códigos maliciosos nos seus dispositivos (computador, celulares, tablets), acessar páginas falsas e até mesmo efetuar transações financeiras. Para isso, é comum encontrar os seguintes temas usados por falsários, na tentativa de chamar a sua atenção:

- Solicitação para atualização do cadastro bancário, dos cartões e senhas via internet;
- Lançamentos e atualizações de sistemas de segurança bancária;
- Novas campanhas, como lançamento de produtos, novas linhas de crédito, unificação de bancos e contas;
- Comprovantes de transações e depósitos;
- Cadastros de computadores para acesso ao canal de Internet Banking;
- Suspensão de acesso.

Além disso, é comum que tentem coletar os seus dados utilizando outros meios, como por exemplo:

- Oferta e disponibilização de aplicativos maliciosos que podem coletar os dados do usuário;
- Ligações telefônicas se passando por funcionários do Banpará, como o Gerente da sua agência de relacionamento, e solicitar seus dados;
- Explorar possível vulnerabilidades no seu computador, tentando, por exemplo instalar vírus capazes de capturar os dados inseridos no acesso ao Internet Banking;
- Explorar possíveis falhas de segurança nos equipamentos de acesso à internet, como senhas fracas;
- Coleta de informações confidenciais que sejam enviadas à sites sem criptografia.

Os principais riscos aos quais você está exposto ao não adotar as devidas medidas de segurança, durante a navegação na internet, são:

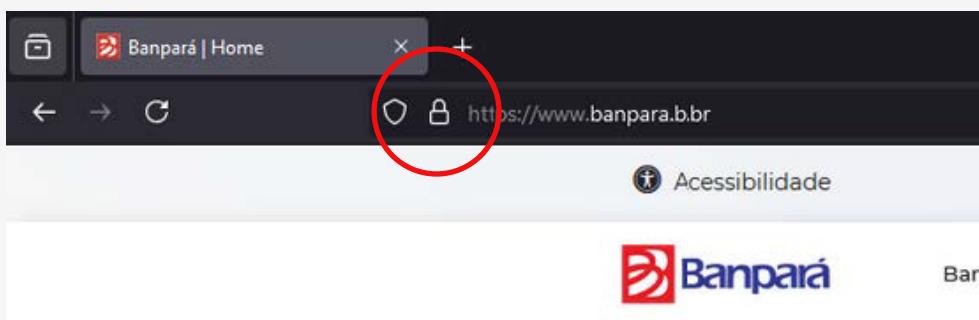
Utilização da conta de maneira indevida por golpistas, para ações maliciosas;

- Perdas financeiras;
- Invasão de privacidade, pois o golpista poderá ter acesso à suas informações pessoais e transações financeiras;
- Violação do sigilo bancário, que ocorre quando alguém não autorizado acessa sua conta;
- Participação de esquemas fraudulentos, os golpistas podem utilizar sua conta como intermediária para aplicar golpes a terceiros.

# Dicas de **segurança** para navegar na internet

## Certifique-se que está utilizando um dispositivo seguro:

- Digite o endereço do site Banpará ([www.banpara.b.br](https://www.banpara.b.br)) diretamente no navegador Web;
- Evite clicar em links recebidos via mensagens eletrônicas (SMS, e-mails e redes sociais);
- Evite utilizar sites de busca para acessar o site do Banpará;
- Evite utilizar dispositivos de terceiros, ou de uso coletivo, como em lan houses;
- Evite navegar em redes públicas de wi-fi, certifique-se de que sua conexão é segura. Os sites do Banpará começam com <https://> isto significa que o site possui um certificado de segurança e as informações inseridas trafegam de maneira criptografada;
- A barra de endereços dos sites do Banpará são apresentadas, com o desenho de um cadeado fechado, e o nome do banco ao lado, como mostra a imagem abaixo, isso sinaliza que o portal têm um certificado de segurança válido.



As características dos dispositivos móveis podem torná-los mais atraentes para pessoas mal-intencionadas. Dentre os riscos aos quais os usuários estão sujeitos, destacam-se:

- Vazamento das informações armazenadas no dispositivo, seja na instalação de aplicativos maliciosos, após perda ou furto do aparelho celular, assim como em uma eventual troca de aparelho, sem que tenham sido excluídas as informações pessoais de maneira correta;
- Maior vulnerabilidade à perda e furtos;
- Instalação e propagação de aplicativos e/ou códigos maliciosos através de e-mails, redes sociais, SMS e outros;
- Para se proteger dos riscos aos quais os dispositivos móveis estão sujeitos, você deve atentar para os seguintes cuidados:
- Não utilize um dispositivo móvel desbloqueado ilegalmente e, de fontes suspeitas ou que tenham suas permissões de acesso alteradas, assim como aparelhos com root ou jailbreak;
- Caso opte por adquirir um modelo usado, restaure o aparelho para suas configurações originais ou “de fábrica”;
- Observe os mecanismos de segurança disponibilizados pelo fabricante;
- Não clique em links recebidos por mensagens (SMS, e-mails, redes sociais, entre outros);
- Mantenha o controle físico sobre o seu dispositivo;
- Proteja suas senhas, crie senhas complexas (alfanuméricas);
- Proteja sua privacidade, tenha cuidado com aplicativos que acessem seus dados pessoais, assim como a publicação de informações como, por exemplo, a localização;
- Não baixe aplicativos fora das lojas oficiais do seu dispositivo;
- Mantenha a versão do seu aplicativo Banpará e Sistema Operacional vdo seu dispositivo sempre atualizados;

**Ao trocar de dispositivo, lembre-se de apagar todas as informações contidas nele e restaurar as configurações de fábrica.**

O Banpará não liga e nem envia SMS ou e-mail solicitando alteração de dados cadastrais, senhas ou informações do seu BPToken. Não clique em links recebidos por SMS ou e-mail. Lembre-se que a senha é a sua assinatura eletrônica para efetuar as suas transações.

Mais informações:

Central Banpará  
3004-4444 | 0800 285 8080

SAC  
0800 280 6605

Ouvidoria  
0800 280 9040