

Política de Estrutura de Segurança de Acesso ao Home Banking

Acesso Seguro

Disponibilizamos um conjunto de medidas de segurança para que todos os clientes do *Home Banking* do Banco de la Nación Argentina operem com total tranquilidade, sabendo que estão utilizando um sistema seguro.

A segurança é uma atividade multidisciplinar, além de fornecer um conjunto que estabelece um sistema seguro, também depende do usuário não revelar informações cruciais. O Banco de la Nación Argentina em nenhum momento lhe solicitará informações relativas às suas senhas, tanto do Home Banking como do seu e-mail. Em nenhum caso esta informação deve ser fornecida.

O usuário também deve certificar-se de que está acessando o portal Home Banking do Banco de la Nación Argentina e de que não está sendo enganado.

Acesso ao Home Banking

A experiência do usuário no Home Banking é especialmente projetada com os navegadores de última geração. O Home Banking pode ser acessado com todos os navegadores do mercado.

No caso de acesso com Internet Explorer, deve-se utilizar a partir versão 10.

Aspectos de segurança na comunicação

SSL (Criptografia 256 bits)

O SSL ou Secure Sockets Layer é a tecnologia utilizada para criptografar as informações trocadas entre o seu computador e o Home Banking. Todas as páginas que contêm informações de sua conta e/ou de suas aplicações financeiras, bem como as movimentações efetuadas, são criptografadas. Assim, caso um terceiro tente interceptá-las, essas informações estarão "embaralhadas", impossibilitando sua interpretação. Dessa forma, o site do Banco de la Nación Argentina garante total confidencialidade e segurança durante seu acesso.

O SSL de 256 bits, utilizado pelo Home Banking, é o protocolo de segurança mais eficiente no mercado. Essa tecnologia é considerada padrão internacional de segurança na transmissão de dados pela Internet.

Cadeado de Segurança

Ao acessar o Home Banking, você deve olhar a imagem do Cadeado de Segurança datado no seu navegador (localizada na barra superior do navegador). Isso indica que a conexão e o tráfego de informações estão sendo realizados com segurança. Clique duas vezes para que o certificado de autoridade, concedido pela VeriSign, seja exibido, confirmando a navegação em um ambiente seguro.

Se, por algum motivo o cadeado não estiver datado ou não estiver no local indicado acima, em hipótese alguma insira seus dados. Nesse caso, contacte-nos através dos e-mails do Banco de la Nación Argentina (ouvidoria@bnabr.com.br) ou pelo telefone 0800 773 3773, nos dias úteis, das 8h às 18h.

Aspectos de segurança do aplicativo

Pedido de Acesso

Todo usuário, seja PESSOA FÍSICA ou PESSOA JURÍDICA, faz um pedido digital de acesso ao Home Banking.

No processo de candidatura, é validado que são clientes reais, sendo o CPF registrado no caso de PESSOA FÍSICA, ou, CNPJ e CPF no caso de PESSOA JURÍDICA.

Além disso, o usuário insere a senha que será utilizada para acessar o Home Banking. Desta forma, a senha só é conhecida pelo usuário que inseriu a solicitação.

O candidato também registra seus dados de e-mail e seu número de telefone celular. Esses dados, e-mail e número de celular, são validados pelo aplicativo, de forma a confirmar que são dados confiáveis.

Com a aplicação introduzida digitalmente, e para completar o processo de registo, as pessoas devem apresentar-se fisicamente ao Banco de la Nación Argentina, onde os funcionários do Banco atestam a veracidade dos documentos e confirmam que a pessoa é quem dizem ser, permitindo assim aos utilizadores o acesso Home Banking.

Neste momento, os usuários podem entrar no Home Banking.

Teclado virtual

Cada vez que uma senha for solicitada, será forçado a fazê-lo por meio de um teclado virtual, que não permite que outros programas maliciosos acessem a senha.

Além disso, este teclado altera a posição dos valores, cada vez que é pressionado, de forma a dificultar a uma terceira pessoa presente no momento de digitar a senha a visualização da senha que está sendo digitada.



OTP transaccional

Cada transação realizada no Home Banking requer para sua confirmação a entrada de uma OTP (senha de uso único).

Este OTP é enviado por e-mail e SMS para o número de telefone celular cadastrado.

Assim, as transações só podem ser confirmadas inserindo informações (OTP) que são enviadas para canais de comunicação certificados com o cliente, funcionando como um segundo fator de autenticação (2FA).