Información y Condiciones del servicio BN Internet Banking y APPS del BNCR

Protección de cuentas y transacciones bancarias

El Banco Nacional de Costa Rica no tiene como política solicitar a sus clientes información confidencial tal como pero no limitada a claves de acceso a internet, número de identificación personal (PIN), los números de tarjetas de crédito o débito, sea a través de correos electrónicos, llamadas telefónica, servicios de mensajería de texto u otros. Si recibe una llamada telefónica, un correo electrónico o mensaje de texto donde se le solicite revelar información personal, le recomendamos borrarlo de inmediato y no ingresar a los sitios (links) que aparecen en el correo o mensaje. En caso de recibir alguna llamada telefónica, no brinde ninguna información y consulte inmediatamente con el Banco acerca de la veracidad de cualquier tipo de campaña, trámite o promoción que se le ofrezca.

Recuerde que la seguridad en el manejo de sus claves y dispositivos proveídos por el BNCR son su responsabilidad, por eso:

- *Evite acceder hipervínculos o ejecutar archivos adjuntos en mensajes de correo electrónico. No proporcione información personal o referente a sus claves de acceso o Tokens cuando es solicitada por medio de correo electrónico, teléfono o cualquier otro medio.*
- *Nunca ingrese información en un sitio sin haber verificado que el ambiente es seguro, esto se puede reconocer buscando "https://" en la barra de dirección, junto con un candado en la parte inferior derecha de su buscador.*
- *Realice sus transacciones únicamente en sitios seguros o aplicaciones oficiales, asegúrese que cuenta con los requerimientos de seguridad necesarios, de lo contrario no proceda a realizar sus transacciones desde ahí. Les recordamos que el Banco Nacional tiene a su disposición, en las agencias y sucursales, equipos con la seguridad adecuada para el uso de BN Internet Banking Personal.*
- *Utilice siempre las opciones tecnológicas para la generación de claves aleatorias (OTP), seguros, biometría y firma digital que le brinde el Banco Nacional. Para conocer más sobre la disponibilidad, puede encontrar la información en nuestro sitio web o en nuestras agencias y sucursales.*
- *Mantenga actualizado los sistemas operativos de sus Computadores y Dispositivos móviles (aplique los parches y recomendaciones del proveedor), el software antivirus, el antispyware y active las funcionalidades de seguridad de su sistema operativo.*
- *Reporte a cualquiera de nuestras oficinas o a la cuenta de correo bnseg@bncr.fi.cr todo correo sospechoso. Recuerde que en el Banco Nacional estamos más cerca de usted.*
- *Elimine correos sospechosos o que no conoce su procedencia. Sospeche de direcciones numéricas o vínculos desconocidos que se presenten visualmente parecidos a su Banco Nacional.*
- *Sospeche de llamadas telefónicas mediante las cuales se ofrezcan negocios fáciles, premios o se realicen promociones donde medie la entrega de información confidencial, como claves, correos electrónicos o números de tarjetas de crédito o débito.*

- *NUNCA brinde sus claves o accesos de servicios electrónicos a otras personas.*

- *Tenga presente que para realizar sus transacciones debe ingresar únicamente al sitio web www.bncr.fi.cr o a la aplicación BN Móvil (o cualquier app que la sustituya en el futuro) que deberá descargar desde las tiendas oficiales: Apple Store (https://itunes.apple.com) Google Play (https://play.google.com) y Appgallery (https://appgallery.huawei.com)*

Reserva de Derechos para los Sistemas de BN Internet Banking y APPS

El sistema Internet Banking, BN Móvil (o cualquier app que la sustituya en el futuro) y las aplicaciones dispuestas por el BNCR para el servicio son para los fines propios de la persona física o jurídica que acepta sus condiciones; por ello, de conformidad con lo establecido en los artículos 613, 614 y 616 del Código de Comercio, el Banco se reserva el derecho de restringir su uso o deshabilitar el servicio a aquellos clientes que utilicen esta herramienta con fines comerciales o de lucro propio sin la debida autorización del Banco, incluyendo el cobro de tarifas a terceros por la realización de transacciones, la venta de los bienes otorgados mediante el esquema de promociones o la utilización del nombre del Banco Nacional como un socio comercial sin los debidos permisos. Para conocer más sobre las aplicaciones y disponibilidad del servicio ver: www.bncr.fi.cr

Términos y Condiciones

1. El presente documento regula los términos y condiciones de uso de las Plataformas de Internet Banking Personal (Banca en línea) y APPS del BNCR, y las transacciones que se realicen a través de estas, y forma parte integral del Contrato suscrito por el (la) cliente para la Apertura de Servicios Bancarios.

2. El ingreso a la plataforma de Banca en línea se realiza accediendo a la página electrónica del Banco en internet www.bncr.fi.cr. El acceso se debe realizar a través de una microcomputadora con acceso a internet. El ingreso a través de las aplicaciones oficiales del Banco se realiza mediante el software que puede ser descargado en las tiendas oficiales tanto en Apple Store como en Google Play y en App Gallery.

El cliente en su calidad de tarjetahabiente, poseedor de una clave de acceso y tecnologías de protección que el BNCR dispone para el servicio, se compromete a suministrar su información bajo las más estrictas normas de confidencialidad, incluyendo la no divulgación a terceros ajenos a la contratación.

3. Para el uso tanto de Banca en línea como de Internet Banking, el (la) cliente debe poseer al menos una tarjeta de débito, crédito o una tarjeta especial de afiliación del Banco, en estado activo. Al momento de registrarse en el servicio el (la) cliente debe verificar que la computadora o dispositivo móvil cuente con la versión más reciente del APP, navegador o "browser, en caso de no ser así debe realizar la actualización en el sitio de internet de la empresa que desarrolló el navegador o revisar las nuevas versiones dispuestas en las Tiendas oficiales para los APPS. El certificado digital de Symantec es el mecanismo de seguridad para garantizar la confidencialidad e integridad de la información, el BNCR dispondrá de la más alta tecnología de encriptación disponible comercialmente. Posterior a esto puede ser requerido digitar su número de tarjeta, cédula de identidad, código CVC (incluido en el reverso de la tarjeta), clave de la tarjeta o cualquier otro elemento que por seguridad haya sido implementado y pueda ser requerido por el Banco, incluyendo, pero no limitado a biometría, códigos OTP y certificados digitales, lo cual le dará acceso a una página de aprobación de las nuevas cláusulas del contrato y a la definición de su clave de acceso y parámetros especiales.

4. El (La) cliente se obliga a elegir una clave que contenga entre 6 y 12 caracteres, que incluya al menos cuatro caracteres alfabéticos y cuatro numéricos y que no sea de reconocimiento obvio, tales como pero no limitados a fechas de cumpleaños,

números de cédula, nombres propios o textos de fácil identificación. El Banco se reserva la facultad de establecer los requerimientos y restricciones para la definición de claves de acceso, los cuales deberán ser observadas por el (la) cliente.

5. El Banco se reserva la facultad de aceptar o rechazar la afiliación al sistema de Banca en línea o el uso de sus APPS. En caso de aceptar la afiliación, la clave designada por el (la) cliente será registrada electrónicamente y será asociada a la identidad del (la) cliente junto con cualquier otra tecnología de seguridad o método de autenticación que se encuentre implementado. El (la) cliente acepta que los elementos de autenticación y seguridad tales como pero no limitados a las claves de acceso, tokens, certificados digitales, biometría, son confidenciales, de uso personal e intransferible, indelegables y sustituyen su firma autógrafa dado que no es posible consignarla en medios electrónicos, surte los mismos efectos que las leyes le otorgan a la firma, teniendo el mismo valor probatorio sin lugar a repudio de las gestiones hechas por el sistema, las cuales se consideran reales por el concepto de autenticación por algo que el cliente "sabe" o sea su clave, generado o almacenado en un dispositivo Token o tarjeta, algo que el cliente "posee" o aspectos biométricos, algo que el cliente "es", por lo que el (la) cliente es responsable único y exclusivo por su uso.

6. Toda persona autorizada por el (la) cliente para el uso y gestión de los productos o servicios que mantenga con el Banco, deberá utilizar sus propias claves de acceso y elementos de autenticación y seguridad para el acceso a Banca en línea o las apps del Banco, por lo que en ningún caso el cliente deberá compartir con dichas personas su información confidencial ni los elementos de seguridad de uso personal e intransferible.

7. El Banco prestará el Servicio Banca en Línea y BN Móvil (o cualquier app que la sustituya en el futuro) en el tanto cuente con las condiciones tecnológicas y operativas para hacerlo. Banca en línea y las APPS del Banco son canales alternos por lo que el (la) cliente no debe considerarlos como una vía única y exclusiva para la atención de sus necesidades bancarias. En caso de que el (la) cliente no pueda acceder a estas plataformas por causa de inconvenientes tecnológicos o de otra índole, puede acudir a cualquiera de las oficinas del Banco para atender sus requerimientos.

8. El (La) cliente podrá definir un límite máximo para las transacciones de transferencia de fondos, así como definir las cuentas a las cuales se pueden realizar dichas transferencias, las cuales se denominan cuentas favoritas. El (La) cliente declara conocer y aceptar que si la cuenta de débito, de la cual se toma el dinero para la transferencia, y la cuenta de crédito, a la cual se transfieren los fondos, están relacionadas al (la) cliente sea como titular o autorizado, las transferencias pueden realizarse por cualquier valor sin sujeción al límite máximo definido por el (la) cliente. Asimismo, el (La) cliente declara conocer y aceptar que podrá realizar transferencias de fondos a cuentas corrientes, de ahorros o electrónicas únicamente si éstas se encuentran en estado activo y sin restricciones. Los débitos por las transacciones se realizan en línea en tiempo real, sin embargo, el Banco se reserva el derecho de procesar las transacciones de acuerdo con sus posibilidades tecnológicas.

9. El Banco emitirá un comprobante electrónico por cada transacción realizada. El cliente declara conocer y aceptar que el Banco no proveerá el comprobante en formato impreso, por lo que de requerirlo es responsabilidad exclusiva proceder a su impresión.

10. El Banco no será responsable cuando el cliente no pueda realizar transacciones a través de Banca en Línea o las APPS del Banco, debido a insuficiencia de fondos, cualquier causa atribuible al (la) cliente, inconvenientes tecnológicos tales como pero no limitados a dificultades en las líneas de comunicación, en los sistemas del proveedor de servicios de

internet, en los servicios de tecnología y/o infraestructura del Banco o de terceros contratados, o de socios tecnológicos. El (La) cliente deberá verificar la correcta ejecución de sus transacciones, y corroborar las mismas en caso de recibir algún mensaje o alerta del sistema que advierta problemas en la transacción debido a alguna de las circunstancias mencionadas. El (la) cliente es responsable único y exclusivo de cualquier error en que incurra al momento de realizar las transacciones, tales como pero no limitados a errores en el monto o moneda de la transacción, en la cuenta destino, duplicidad de transacciones, y deberá gestionar por su propia cuneta la recuperación de los fondos, ya que las transacciones realizadas en estos canales no pueden ser reversadas.

11. El cliente acepta y reconoce que el Banco brindará los servicios de Banca en Línea y BN Móvil (o cualquier app que la sustituya en el futuro) en horarios permitidos por los sistemas centrales. Algunos servicios tienen horario de tramitación 24 o 48 horas después. El servicio podrá suspenderse sin previo aviso en los casos que se considere que el cliente está operando de manera inadecuada o dolosa el sistema o cuando se identifiquen riesgos en los esquemas de seguridad.

12. El cliente se compromete en forma expresa e irrevocable a asumir el pago de cualquier comisión o cargo asociado a la prestación de los servicios aquí regulados, así como aquellos derivados de la implementación de esquemas de seguridad tales como Token, códigos OTP, certificados digitales, seguros, o biometría de huella dactilar o de reconocimiento facial, para lo cual autoriza expresamente al Banco a debitar los cargos o comisiones de cualquiera de las cuentas que el cliente mantenga con el Banco, o bien realizar el cargo a cualquier tarjeta de crédito a nombre del cliente en el Banco. El Banco se reserva la facultad de fijar el importe de las anteriores comisiones y cargos, así como de establecer nuevos cargos por la prestación de los servicios aquí regulados. Los costos, comisiones o gastos relacionados con los servicios, se mantienen publicados y están a disposición del cliente en el sitio https://www.bncr.fi.cr/requisitos-de-servicios, en la ruta Personas/Requisitos de Servicios/Comisiones.

13. El cliente se compromete a acatar las recomendaciones que en materia de seguridad emita el Banco y su incumplimiento será motivo de suspensión del servicio. Además, se compromete a acceder el servicio únicamente en el sitio oficial del Banco www.bncr.fi.cr o a través del software dispuesto por el BNCR en las Tiendas oficiales en Apple Store, AppGallery y Google Play. El uso de Token, códigos OTP, certificados digitales, seguros y biometría de huella dactilar o de registro facial es opcional, pero el banco restringirá algunas transacciones que considere de riesgo cuando el cliente no cuente con este mecanismo de seguridad según la disponibilidad y requerimiento del Banco.

14. El (La) cliente entiende y acepta que las condiciones del servicio establecidas en el presente contrato corresponden a mejores prácticas, las cuales son mitigantes de los riesgos que presenta este servicio, y que por su naturaleza, corresponden ser ejecutadas por el (la) propio cliente en su beneficio, por lo que el (la) cliente se obliga a mantener sus equipos y dispositivos móviles en óptimas condiciones, libres de virus informáticos, programas espías o los conocidos "malware" que buscan adueñarse de la información confidencial del usuario. El cliente exime de responsabilidad al Banco por fallas que se presenten en el software o en el sistema operativo de sus equipos o dispositivo móvil, las cuales no pueden ser controladas por el Banco.

15. El Banco quedará exento de toda responsabilidad por la negligencia, imprudencia o dolo de alguno de los usuarios que le cause perjuicio a través de transacciones fraudulentas o erróneas. Ratificando y aceptando sin reservas el contenido total del presente convenio.

16. Este contrato es electrónico, la sola aceptación del cliente para continuar con el proceso de afiliación da prueba de que el cliente ha leído y aprobado las cláusulas adicionadas al Contrato de Servicios Bancarios. Para efectos fiscales, el presente adendum se considera inestimable.

17. El cliente autoriza al Banco Nacional de Costa Rica para tratar, recopilar, almacenar, ceder y transferir la información de sus datos personales, incluidos los de uso restringido. Esta autorización incluye:

a) *la posibilidad de compartir la información indicada con el Banco Nacional y las demás subsidiarias del Conglomerado Banco Nacional existentes o futuras, o a terceros subcontratados (dentro y fuera del territorio nacional) por el Banco Nacional y sus subsidiarias para el manejo y archivo de expedientes, envíos de estados de cuenta y para brindar servicios como cliente del conglomerado o de la subsidiaria, incluyendo pero no limitado a los contratos de tarjetas, infraestructura tecnológica, servicios de Call Center, servicios de venta o contratación de productos, mercadeo, promociones en general y de servicios bancarios y financieros, de cobro, servicios para la seguridad de las transacciones a efectuar u otros servicios a través de medios telefónicos, digitales, mensajes de texto, correo electrónico o cualquiera otras que ayude a llevar a cabo transacciones. Dichas comunicaciones podrán ser con fines informativos, de venta directa, de verificación de datos, de cobro, de promoción de productos y cualquier otro que se considere oportuno brindar por estos medios.*
b) *la posibilidad de compartir la información indicada con el Banco Nacional y las demás subsidiarias del Conglomerado Banco Nacional para efectos de verificar el cumplimiento de la Ley 8204 y otras regulaciones que apliquen en función de la operación del BNCR. Por otra parte, el cliente autoriza expresamente y en forma irrevocable al Banco Nacional para que como entidad supervisada acceda y consulte mi información en el Centro de Información Crediticia (CIC) de la Superintendencia General de Entidades Financieras. Asimismo, esta autorización permite el uso de la información que se acceda y que dicha información pueda ser compartida con BN Vital, BN Valores, BN SAFI y BN Corredora de Seguros para facilitar cualquier análisis de crédito o de negocios que vaya a ser realizado por las entidades indicadas, incluso para el ofrecimiento de servicios, productos comerciales y/o financieros. El cliente acepta que ha sido informado y acepta que la falta de entrega de la información solicitada puede provocar el rechazo de su solicitud o el no recibir los servicios prestados por el Banco y su conglomerado y que puede ejercer los derechos de acceso, rectificación y cancelación establecidos en la ley.*

18. El Banco pone a disposición del (la) cliente la posibilidad de autenticación a través de las funcionalidades de biometría como registro facial y de huellas dactilares, disponibles en los dispositivos móviles. Este método de autenticación está disponible únicamente para el ingreso a la aplicación BN Móvil (o cualquier app que la sustituya en el futuro) y no así para el ingreso a Banca en línea, que debe realizarse mediante el registro de usuario, contraseña y las demás medidas que el Banco disponga. El uso de las funcionalidades de biometría del dispositivo móvil, permitirá al (la) cliente únicamente autenticarse para el ingreso a la aplicación, pero no constituye un mecanismo de seguridad para la confirmación de transacciones, para lo cual el Banco mantiene implementados diferentes mecanismos de seguridad según el tipo de transacción.

19. Para poder habilitar el acceso con huella digital o reconocimiento facial en su dispositivo móvil, el cliente debe contar con un teléfono inteligente o una tableta electrónica que disponga de:

a) lector de huella digital o de reconocimiento facial,

b) haber registrado sus huellas digitales o sus registros faciales en su dispositivo móvil,

c) mantener un factor de seguridad de bloqueo/desbloqueo de su dispositivo móvil como por ejemplo: patrón, pin, huella digital o registro facial,

d) haber realizado el registro de dispositivo móvil en el Banco, según se menciona en la cláusula 20,

d) mantener actualizadas las versiones del sistema operativo y los programas (software) que el fabricante del dispositivo móvil pone a disposición, para su adecuado funcionamiento,

e) memoria de almacenamiento y capacidad de procesamiento en el dispositivo móvil, que permita el adecuado funcionamiento de la aplicación,

f) conexión a internet mediante redes inalámbricas o de datos que permita que permita el adecuado funcionamiento de la aplicación.

20. Como requisito de seguridad para la activación del acceso a la aplicación BN Móvil (o cualquier app que la sustituya en el futuro) con huella dactilar o reconocimiento facial, el usuario debe realizar previamente el registro de su dispositivo móvil en el Banco, según se describe en el documento ubicado en www.bncr.fi.cr, mediante la siguiente ruta: Personas/Requisitos de servicios/Servicios digitales/Términos y Condiciones – Uso de Registro de Dispositivos Móviles en Banco Nacional. Si el cliente no realiza el registro de su dispositivo móvil, no podrá habilitar el acceso a BN Móvil (o cualquier app que la sustituya en el futuro) a través de la funcionalidad de biometría. Asimismo, el cliente solo podrá accesar a BN Móvil (o cualquier app que la sustituya en el futuro) a través de biometría en aquellos dispositivos que tenga registrados; para dispositivos no registrados deberá utilizar el método de ingreso por usuario y contraseña.

21. El acceso a BN Móvil (o cualquier app que la sustituya en el futuro) por medio de biometría consiste en el ingreso a la aplicación utilizando la funcionalidad de huella dactilar o de reconocimiento facial del dispositivo móvil. Previamente el cliente debe tener almacenadas sus huellas dactilares o sus registros faciales en el dispositivo móvil, realizar el registro de dispositivo, activar el icono de huella dactilar o de reconocimiento facial que se le muestra en la ventana inicial de la aplicación y aceptar estos términos y condiciones que se le presentan en una nueva ventana en el mismo dispositivo móvil. Una vez realizado ese proceso, el cliente podrá ingresar a BN Móvil (o cualquier app que la sustituya en el futuro) cada vez que lo requiera, activando el icono de huella dactilar o reconocimiento facial para que se valide que su huella o registro facial es la que se encuentra previamente registrada en el dispositivo.

Es responsabilidad del cliente asegurarse que las huellas dactilares o los registros faciales almacenados en el dispositivo móvil pertenecen únicamente a su persona, ya que de encontrarse almacenadas huellas dactilares o registros faciales de terceras personas en el dispositivo móvil podrían ser utilizadas para el acceso a la aplicación BN Móvil (o cualquier app que la sustituya en el futuro) y realizar transacciones que comprometan la seguridad del cliente.

El Banco no almacenará dentro de sus sistemas ninguna imagen o archivo electrónico de las huellas dactilares o de los registros faciales de los clientes que activen esta funcionalidad.

22. Dado que la funcionalidad de uso de huella dactilar o reconocimiento facial son facilitadas por el fabricante del dispositivo/sistema operativo del cliente, el Banco no puede validar que las huellas o registros faciales almacenados en el dispositivo del cliente, efectivamente pertenezcan a éste, por lo que es responsabilidad única y exclusiva del cliente asegurarse de que en su dispositivo únicamente se encuentren almacenadas dactilares y/o su registro facial.

23. El Banco se reserva la facultad de implementar diferentes mecanismos de seguridad según el nivel de riesgo de las transacciones, de acuerdo con los parámetros establecidos por el Banco, entre los cuales se cuentan, pero no se limitan a el uso de firma digital, registro de dispositivo, software token, hardware token y códigos de verificación por mensaje de texto SMS o por correo electrónico, así como aquellos mecanismos de seguridad que el Banco llegue a implementar en el futuro.

25. El cliente exime de responsabilidad al Banco por fallas que se presenten en el software o en el sistema operativo del dispositivo móvil, las cuales no pueden ser controladas por el Banco.

26. El cliente debe abstenerse de facilitar o permitir a terceros el acceso a su información de uso personal como: huellas dactilares, registros faciales, número de tarjeta de crédito, contraseñas, números de cuenta, número de tarjeta de débito, pines, claves y cualquier información confidencial que pueda comprometer la seguridad de las cuentas, productos, o servicios financieros.