

PORTADA				
	CÓDIGO	NOMBRE	EDICIÓN	TIPO
	AN30-CGPC01	Términos y condiciones de uso de Registro de dispositivos móviles en el Banco Nacional	01	Anexo
PARTICIPANTES				
RESPONSABLE			ÁREA ORGANIZACIONAL	
<u>REVISADO POR</u>	<u>VALIDADO</u>	Joaquín Vásquez Soto	Canales de autogestión, Distribución Digital	
		Lilliana Arias Pineda	Distribución Digital, SGBC	
		Laura Jara Morúa	Dirección Planificación y Gestión de Ventas SGBC(Gestora)	
		Carlos Hernandez Hidalgo	Dirección Planificación y Gestión de Ventas SGBC	
<u>APROBADO POR</u>	<u>Diseño del proceso/Sub Proceso</u>			



FD12-PR31MC01, Control de formato para anexo, Edición 6.

Contenido

1. Propósito, Alcance y Responsabilidades	3
2. Definiciones	3
3. Términos Y Condiciones De Uso De Registro De Dispositivos Móviles En El Banco Nacional.....	3
4. Documentos Relacionados.....	10
5. Control de Cambios	10



1. Propósito, Alcance y Responsabilidades

PROPÓSITO	ALCANCE	RESPONSABILIDADES
Regular los términos y condiciones del registro de dispositivos móviles en el Banco Nacional.	Conglomerado Financiero Banco Nacional de Costa Rica (CFBNCR).	Es responsabilidad de la Dirección de Distribución Digital mantener el presente documento actualizado

2. Definiciones

CONCEPTO	DEFINICIÓN
Dispositivo móvil	Cualquier dispositivo electrónico que permita la comunicación a través de las redes de telefonía celular o de redes de conexión WIFI a internet
Código QR:	Patrón que se genera de forma electrónica y que al ser escaneado permite el acceso a un sitio o servidor web para ejecutar una rutina
Registro de dispositivo	El registro de dispositivos es un proceso que permite a los dispositivos digitales, como teléfonos móviles, tabletas y computadoras, ser identificados y autenticados en canales digitales, mediante un proceso previo para la autenticación del cliente en el canal digital. En otras palabras, el registro de dispositivos es un paso importante para garantizar la seguridad de los canales digitales y proteger la información personal del usuario

3. Términos Y Condiciones De Uso De Registro De Dispositivos Móviles En El Banco Nacional

El presente documento regula los términos y condiciones del registro de dispositivos móviles en el Banco Nacional.

PRIMERA. DEFINICIONES: Para los efectos de este documento se entenderá por:

- 1- Dispositivo móvil: Es cualquier dispositivo electrónico que permita la comunicación a través de las redes de telefonía celular o de redes de conexión WIFI a internet, tales como tabletas electrónicas o teléfonos inteligentes, los cuales también proporcionan capacidades de movilidad a sus usuarios.



- 2- Código QR: patrón que se genera de forma electrónica y que al ser escaneado permite el acceso a un sitio o servidor web para ejecutar una rutina, en este caso el registro de características del dispositivo móvil.
- 3- Registro de dispositivo: El registro de dispositivos es un proceso que permite a los dispositivos digitales, como teléfonos móviles, tabletas y computadoras, ser identificados y autenticados en canales digitales, mediante un proceso previo para la autenticación del cliente en el canal digital. En otras palabras, el registro de dispositivos es un paso importante para garantizar la seguridad de los canales digitales y proteger la información personal del usuario.

SEGUNDA. REGISTRO DE DISPOSITIVO MÓVIL: El Banco Nacional pone a disposición del cliente una solución de seguridad, que le permite realizar el registro ante el Banco de su dispositivo electrónico (teléfono celular inteligente o tableta electrónica), para el ingreso a la aplicación BN Móvil y cualquier otra aplicación móvil que el [Banco Nacional](#) ponga a disposición de sus clientes en el futuro. El registro de dispositivo móvil no aplica para el ingreso y la realización de transacciones por medio de [Banca en Línea](#). A partir del registro exitoso del dispositivo, el cliente únicamente podrá ingresar y realizar transacciones desde las aplicaciones móviles del Banco, utilizando el dispositivo que se encuentre debidamente registrado. El cliente no podrá ingresar a dichas aplicaciones ni realizar transacciones utilizando un dispositivo móvil que no sea el que está registrado. Cada cliente podrá registrar un máximo de dos dispositivos móviles. Para cada uno de los dispositivos deberá realizarse el proceso de registro en forma individual.

TERCERA: PROCESO DE REGISTRO. Para realizar el registro de su dispositivo móvil es importante que tome en cuenta los siguientes requerimientos técnicos: a) El teléfono o tableta que se va a registrar debe contar con sistema operativo iOS, Android o HarmonyOS debidamente actualizado y sin ningún tipo de alteración o manipulación no autorizada por el fabricante, b) El teléfono o tableta debe tener espacio de memoria (mínima de 32 MB) para realizar los procesos que exige la aplicación y c) Debe contar con un adecuado servicio de conexión a internet. d) Tener instalado, configurado y actualizado un antivirus, e) No utilizar redes WIFI públicas para trámites bancarios. Para realizar el registro el cliente debe seguir los siguientes pasos:

- 1- El cliente debe mantener contratado el servicio de [Banca en Línea](#), así como tener instalada la aplicación BN Móvil o cualquier otra que el [Banco Nacional](#) habilite en el futuro, en el teléfono o tableta que desea registrar.
- 2- El cliente debe ingresar primeramente a [Banca en Línea](#) a la sección de Preferencias donde encontrará un vínculo llamado Dispositivos Móviles. Al acceder a esta opción deberá evidenciar mediante la activación del botón para tal fin, que leyó y que acepta los términos y condiciones del servicio regulados en este documento, para generar un código QR.



- 3- En el dispositivo móvil que desea registrar, deberá ingresar a la aplicación BN Móvil en el menú principal ubicado en la esquina superior derecha y acceder a la opción Mis Dispositivos.
- 4- Presionar el botón Agregar.
- 5- Leer y aceptar los términos y condiciones del servicio regulados en este documento.
- 6- Generar un **código de verificación** y seleccionar el medio por el que será enviado **y este** será enviado al correo electrónico o número de teléfono autorizado.
- 7- Registrar el código de verificación y presionar el botón Continuar, con lo que se generará el código QR.
- 8- Dirigir el dispositivo móvil hacia la pantalla de la computadora donde se generó el código QR y capturar la imagen por medio del escáner del dispositivo móvil.
- 9- Si el proceso tiene éxito, recibirá un mensaje de que la transacción fue realizada satisfactoriamente.
- 10- Una vez registrado el dispositivo móvil, este queda habilitado para el ingreso a cualquier aplicación móvil del **Banco Nacional** que requiera de esta funcionalidad de seguridad.
- 11- Si el usuario registra al menos un dispositivo móvil, no podrá ingresar a las aplicaciones que el **Banco Nacional** habilite con esta funcionalidad desde un dispositivo no registrado, ya que en cada uno de sus ingresos se validará que esté ingresando por un dispositivo registrado.

El dispositivo móvil que se registre debe ser de uso personal, es decir, debe estar en custodia absoluta de su propietario, quien únicamente podrá realizar el ingreso a las aplicaciones móviles del **Banco Nacional** y podrá ejecutar las transacciones autorizadas si cuenta con el dispositivo móvil en su poder y en correcto funcionamiento. El **Banco Nacional** no asume ninguna responsabilidad por daños al dispositivo móvil que se pudieran dar durante el proceso de Registro de dispositivo. **El cliente es responsable único y exclusivo por el mal uso que se le dé al dispositivo.** En caso de extravío o robo de su teléfono celular, si el mismo no cuenta con clave de bloqueo, se podrían realizar transacciones en su nombre hasta el monto autorizado por el cliente sin responsabilidad por parte de la institución. Por lo anterior el Banco recomienda mantener el dispositivo móvil bloqueado con la clave de acceso y en caso de extravío o robo hacer la gestión inmediata de suspensión de la línea con el operador telefónico y reportar lo anterior al



Banco. En caso de cambio de número o dispositivo telefónico móvil, es responsabilidad del cliente inactivar el servicio antes para realizar el cambio con su operador.

CUARTA: PASOS PARA DESAFILIAR O DAR DE BAJA UN DISPOSITIVO MÓVIL:

Para desafiliar o dar de baja un dispositivo móvil el cliente deberá ingresar a [Banca en Línea](#), la aplicación BN Móvil o cualquiera de las aplicaciones que el [Banco Nacional](#) habilite en el futuro para utilizar esta funcionalidad, utilizando para ellos los elementos de seguridad y autenticación requeridos, una vez completado el proceso de autenticación deberá seguir los siguientes pasos:

1. En [Banca en Línea](#) el usuario debe ingresar al menú de Preferencias en la opción Dispositivos Móviles. En esta se le mostrarán los dispositivos que tiene registrados, con un ícono que simula un [basurero](#).
2. El usuario deberá accionar el ícono del [basurero](#) del dispositivo móvil que desea dar de baja, aceptar haber leído este documento de términos y condiciones a través de la activación del botón para tal fin y completar la acción de eliminar mediante el botón Aceptar.
3. Cuando se completa la acción, se le presentará un mensaje al usuario que indica cuando el dispositivo ha sido eliminado con éxito.
4. Si la gestión se realiza en la app BN Móvil, en el menú de tres barras horizontales en la esquina superior derecha, en la opción Mis Dispositivos, le aparecerán los dispositivos que tiene registrados con el ícono del [basurero](#) a la derecha.
5. Deberá accionar el ícono del [basurero](#) y aceptar haber leído este documento de términos y condiciones con la activación del botón para tal fin, al presionar el botón aceptar se procederá a eliminar el dispositivo seleccionado.
6. Cada vez que el cliente desee cambiar uno o más dispositivos móviles que ha registrado previamente, debe dar de baja el o los que ya no utilice, ya que la cantidad de dispositivos que se pueden registrar por usuario se limita a dos dispositivos.
7. El cliente declara conocer y aceptar que mientras mantenga al menos un dispositivo registrado, únicamente podrá ingresar y realizar transacciones desde las aplicaciones móviles del Banco, utilizando el dispositivo que se encuentre debidamente registrado. Si el cliente mantiene registrados dos dispositivos e inhabilita uno de estos dispositivos, a partir de ese momento solo podrá ingresar y realizar transacciones desde las aplicaciones móviles del Banco, utilizando el dispositivo que se encuentre debidamente registrado, ya que en cada uno de sus ingresos se validará que esté ingresando a través de un dispositivo registrado. En caso de que el cliente inhabilite o elimine todos los dispositivos registrados, se



entenderá para todos los efectos que no desea utilizar la solución de seguridad de registro de dispositivo móvil, y a partir de ese momento podrá ingresar y realizar transacciones desde las aplicaciones móviles del Banco, utilizando los medios de autenticación y seguridad que el Banco mantenga implementados al efecto, pero sin que para el ingreso se le requiera el registro del dispositivo. Si el cliente desea volver a utilizar el servicio de registro de dispositivo móvil, deberá realizar nuevamente el proceso de registro establecido en este documento.

Es responsabilidad del cliente realizar la desafiliación inmediata del dispositivo en caso de que pierda la custodia del mismo por cualquier causa, liberando al [Banco Nacional](#) de cualquier responsabilidad por transacciones que deriven del incumplimiento de esta obligación. [El Banco Nacional recomienda altamente la afiliación y uso del servicio de registro de dispositivos, como un mecanismo complementario y que aumenta la seguridad de las transacciones digitales, sugiriendo a todos sus clientes el uso del mismo, lamentando aquellos que por condiciones personales decidan no utilizarlo.](#)

QUINTA: OBLIGACIONES DE SEGURIDAD. El servicio de registro de dispositivo móvil en el [Banco Nacional](#) es un mecanismo de seguridad adicional a las medidas de seguridad existentes. La incorporación de esta tecnología de seguridad no implica de ninguna manera que el sistema de información que en la actualidad mantiene el [Banco Nacional](#) sea inseguro. El Cliente en su condición de titular de una clave de acceso y tecnologías de protección que el [Banco Nacional](#) brinda para el servicio, se compromete a no suministrar, divulgar o de ninguna forma facilitar el acceso a terceras personas, información asociada a los métodos de autenticación o esquemas de seguridad, tales como: contraseñas, PIN, Token, códigos de seguridad, códigos de verificación, entre otros; y a observar las más estrictas normas de confidencialidad y resguardo de su información personal y de seguridad. Durante el tiempo de uso del servicio el Cliente debe verificar que la computadora y los dispositivos móviles cuenten con la más reciente versión y actualizaciones del APP, navegador o "browser", sistema operativo y antivirus. El Cliente se compromete a mantener sus equipos y dispositivos móviles en óptimas condiciones, libres de virus informáticos, con programas "anti-spyware" (que evitan el ingreso de programas espías) y resguardados de manera tal que no perjudiquen los equipos o sistemas del Banco o la intercepción de los códigos de ingreso. En forma adicional el cliente se compromete a acceder el servicio únicamente en el sitio oficial del Banco [HTTPS://www.bnrcr.fi.cr](https://www.bnrcr.fi.cr) o a través del software dispuesto por el Banco en las Tiendas oficiales en Apple Store, Google Play o AppGallery. El incumplimiento de estas obligaciones por parte del Cliente, libera al [Banco Nacional](#) de todo tipo de responsabilidad con ocasión de eventos que hayan perjudicado al Cliente por violaciones al sistema de seguridad del propio Cliente. El Cliente entiende y acepta que las condiciones del servicio establecidas en el presente contrato corresponden a mejores prácticas de la industria y que por su naturaleza corresponden ser ejecutadas por el propio Cliente en su beneficio; por consiguiente, el Cliente se compromete a acatar las



recomendaciones que en materia de seguridad emita el [Banco Nacional](#), entre estas, pero no limitadas a las siguientes:

- a) Evitar acceder hipervínculos o ejecutar archivos adjuntos en mensajes de correo electrónico o SMS.
- b) No proporcione información personal o referente a sus claves de acceso o Tokens cuando es solicitada por medio de correo electrónico, teléfono (llamada telefónica o SMS) o cualquier otro medio.
- c) 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.
- d) Realizar 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.
- e) Utilizar siempre las opciones tecnológicas para la generación de claves aleatorias (OTP), seguros, firma digital y cualquier otro mecanismo que el Banco Nacional brinde e implemente a futuro.
- f) Mantener 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.
- g) Reportar a cualquiera de nuestras oficinas, o al teléfono 2212-2000 del Centro de Contacto del [Banco Nacional](#) o a la cuenta de correo bnseg@bnqr.fi.cr todo correo sospechoso.
- h) Eliminar correos sospechosos o que no conoce su procedencia. Sospeche de direcciones numéricas o vínculos desconocidos que se presenten visualmente parecidos a los presentados por el Banco Nacional.
- i) Sospechar 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, [claves aleatorias \(OTP\)](#), [Token](#), [códigos de seguridad](#), [códigos de verificación](#), entre otros.
- j) Nunca brinde sus claves o accesos de servicios electrónicos a otras personas.
- k) Ninguna entidad bancaria le solicitará a sus clientes información confidencial como claves, pines o tokens de acceso ni números de tarjetas de débito o crédito. Tampoco lo hará mediante mensajes de texto o de correo electrónico. Reporte inmediatamente al [Banco Nacional](#) si detecta una situación sospechosa.
- l) Se aconseja no utilizar las mismas claves para ingresar a sitios de banca electrónica, en otros servicios como redes sociales o cuentas de correo.



- m) No se recomienda utilizar los servicios de Wi-Fi públicos para realizar transacciones bancarias, porque otros podrían estar mirando su información. Las transacciones bancarias solo deben realizarse en conexiones de internet privadas.
- n) Active el servicio gratuito de alertas en su celular y reciba notificaciones cada vez que realice transacciones.

El incumplimiento de estas obligaciones facultará al [Banco Nacional](#) a suspender el servicio.

SEXTO: AUTORIZACIÓN PARA EL TRATAMIENTO DE LA INFORMACIÓN.

Mediante la suscripción del servicio el cliente autoriza al Banco para tratar, recopilar, almacenar, ceder y transferir la información de sus datos personales, incluidos los de uso restringido. Esta autorización incluye: 1) la posibilidad de compartir la información indicada con el BANCO NACIONAL y las demás subsidiarias del Conglomerado BANCO NACIONAL existentes o futuras, a terceros por convenio de afinidad para este servicio, o a terceros subcontratados 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, incluye pero no limita a los contratos de tarjetas, 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 cualquier otras que ayude a llevar a cabo estas 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. 2) 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. Por otra parte, de "El cliente" autoriza expresamente y en forma irrevocable al BANCO NACIONAL, para que como entidad supervisada acceda y consulte su información en el Centro de Información Crediticia (CIC) de la Superintendencia General de Entidades Financieras. Así mismo, 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 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.

SÉTIMA: MODIFICACIÓN DE LOS TÉRMINOS Y CONDICIONES. El Banco se reserva la facultad de realizar modificaciones a los términos y condiciones de uso de este servicio.



FD12-PR31MC01, Control de formato para anexo, Edición 6.

Las modificaciones serán comunicadas mediante publicación en la página electrónica del Banco www.bnccr.fi.cr. Las modificaciones entrarán en vigencia en un plazo de dos meses contados a partir de la comunicación. Si el cliente, una vez transcurrido dicho plazo, continúa utilizando la plataforma, se entenderá que ha aceptado las modificaciones introducidas. En igual sentido el Banco podrá suspender en forma temporal o definitiva la prestación del servicio, cuando lo considere pertinente.

OCTAVA: ACEPTACIÓN DE LOS TÉRMINOS Y CONDICIONES: El cliente declara que ha leído y comprendido los términos y condiciones de uso del servicio de Registro de dispositivo móvil. En caso de estar de acuerdo con lo establecido, deberá pulsar el botón "acepto", en señal expresa de su consentimiento, y a partir de ese momento podrá acceder al registro del dispositivo y el servicio. Si el cliente no está de acuerdo con los términos y condiciones del servicio, deberá abandonar el sitio y abstenerse de pulsar el botón acepto.

4. Documentos Relacionados

CÓDIGO	NOMBRE

5. Control de Cambios

TEMA	EDICIÓN	ORIGEN DEL CAMBIO
Creación de documento	N/A	En atención a solicitud de creación de Canales de Autogestión y Sistemas de Gestión
Actualización de documento de términos y condiciones con base en el contexto a diciembre 2023	2	Actualización a diciembre 2023