

AVISO LEGAL
Términos y Condiciones App BBVA

Las presentes condiciones de uso (en adelante, las "CONDICIONES") regulan los términos y condiciones para el uso de los servicios ofrecidos en la aplicación móvil y/o software de Banca móvil (en adelante, la "APLICACIÓN") del Banco BBVA Perú (en adelante, el "BANCO"), por clientes del BANCO, sean Persona Natural o Persona Natural con Negocio, en su dispositivo celular, tableta, así como cualquier otro dispositivo compatible con la APLICACIÓN (en adelante, "DISPOSITIVO" O "DISPOSITIVOS").

1. DESCARGA Y ACEPTACIÓN DE USO

La descarga de la APLICACIÓN se podrá realizar a través de la tienda o "store" que la empresa fabricante del DISPOSITIVO o la empresa distribuidora de aplicaciones, proveen para tal efecto.

Una vez descargada la APLICACIÓN en el DISPOSITIVO, el cliente del BANCO podrá revisar las CONDICIONES antes del uso de la APLICACIÓN, y en cualquier momento desde la zona pública o desde la zona privada de la misma.

El acceso y uso de la APLICACIÓN, tanto a la zona de Personas como a la zona de Negocio (para Personas Naturales con Negocio), le atribuye inmediatamente al cliente la condición de usuario de la APLICACIÓN (en adelante, "USUARIO") y, por tanto, implica la aceptación sin reservas de todas las disposiciones contenidas en las presentes CONDICIONES, así como en cualquier otro aviso legal, condiciones de uso o términos y condiciones que las sustituyan, complementen y/o modifiquen y que puedan encontrarse en la APLICACIÓN.

Las CONDICIONES se formalizan única y exclusivamente entre el USUARIO y el BANCO. La licencia de uso de la aplicación que se otorga en virtud de estas CONDICIONES se limita a una intransferible, para utilizar la APLICACIÓN en un DISPOSITIVO de titularidad o bajo el control del USUARIO.

El acceso a la APLICACIÓN no otorga al USUARIO derecho ni titularidad alguna sobre los derechos de propiedad intelectual de los contenidos que alberga la APLICACIÓN. El BANCO se reserva la posibilidad de ejercer las acciones legales que correspondan contra el USUARIO que viole o infrinja los derechos de propiedad intelectual.

El acceso y uso del servicio a través de la APLICACIÓN queda condicionado a que la identificación del USUARIO se realice de acuerdo con lo establecido por el BANCO. Se entenderá que dicho acceso y uso es efectuado por el USUARIO registrado en la APLICACIÓN.

Bajo ningún motivo o circunstancia el BANCO asumirá responsabilidad alguna por las operaciones que se realicen haciendo uso de la APLICACIÓN; así como, por cualquier inconveniente imputable al USUARIO o a terceros, incluso ante un caso fortuito o de fuerza mayor que no permita la realización exitosa de la plataforma.

Algunas de las funcionalidades podrían no ser exactamente iguales a las disponibles o podrían no estar totalmente operativas, debido a las características de los DISPOSITIVOS. Estas circunstancias podrían variar, en la medida que la tecnología lo permita, y serán puestas en conocimiento del USUARIO a través de los medios que el BANCO tenga establecidos.

El BANCO se reserva el derecho a modificar, de forma parcial o total, las presentes condiciones, así como a incluir otras nuevas, conforme a la normativa sobre la materia. Las nuevas condiciones se mostrarán al USUARIO a través de la APLICACIÓN y podrán ser consultadas en cada momento en la APLICACIÓN.

2. LIMITACIÓN DE RESPONSABILIDADES

El USUARIO será responsable de comprobar que la APLICACIÓN es compatible con su DISPOSITIVO, por lo que asume los daños que la instalación o utilización del software pudiera ocasionar en el DISPOSITIVO. El BANCO no otorga ningún tipo de garantía sobre la APLICACIÓN.

El BANCO no asumirá ninguna garantía y/o responsabilidad en el supuesto de que los USUARIOS hayan recibido el Software de un tercero distinto al BANCO, tratándose de una infracción grave de los derechos de propiedad intelectual.

El acceso y uso de la APLICACIÓN está dirigido únicamente a clientes del BANCO, lo cual incluye la reproducción total o parcial del Software exclusivamente mediante su utilización, descarga, ejecución y exhibición en un Dispositivo; por lo que está expresamente restringida al uso anteriormente expuesto; su empleo para cualquier otro fin queda expresamente prohibido y será considerado como acto de piratería de software que infringe las leyes de propiedad intelectual e industrial, de tal forma que el BANCO podrá exigir responsabilidad por el incumplimiento de esta condición, según la normativa vigente. Asimismo, queda expresamente prohibida la manipulación, total o parcial, por parte del USUARIO o de terceros, del Software.

El USUARIO asumirá completamente la responsabilidad que pudiera emanar de la realización de estos usos prohibidos y mantendrá indemne al BANCO en cualquier procedimiento o proceso que derive de éstos malos usos.

El USUARIO se obliga a mantener a buen resguardo y bajo su posesión física el DISPOSITIVO a través del cual tenga acceso a la APLICACIÓN, así como en total reserva sus claves de acceso. Toda operación realizada a través del DISPOSITIVO del USUARIO se presumirá hecha por él, bajo su total responsabilidad, salvo las excepciones expresamente establecidas por la legislación aplicable.

El BANCO deslinda de cualquier responsabilidad en caso de pérdida, daños o perjuicios de cualquier tipo que surjan por acceder y usar la APLICACIÓN, incluyéndose, pero no limitándose, a los producidos como consecuencia del extravío, robo, hurto, sustracción o uso no autorizado de la(s) Tarjeta(s) (física y/o digital) o la(s) adicional(es), códigos secretos y/o claves o información de ésta, DISPOSITIVOS o teléfonos móviles desde donde pueda ingresar a la APLICACIÓN para realizar operaciones con su(s) Tarjeta(s), o cualquier otro DISPOSITIVO desde el cual pueda acceder a sus aplicaciones móviles. En caso se produzcan dichos hechos, Usted es responsable de comunicarlo inmediatamente al BANCO, a través de la Banca por Teléfono, de acuerdo a lo establecido en su(s) Contrato(s) de Tarjeta(s) y/o Cuenta(s).

El BANCO tampoco será responsable de los daños que pudiera sufrir por un uso inadecuado de la APLICACIÓN, el que pueda traer consigo la introducción de virus y/o ciberataques, tales como phishing, vishing, smishing, skimming, pharming, keylogger, entre otras modalidades de fraude electrónico, además de la disposición de fondos no autorizada, producto de las actividades mencionadas, además de otras modalidades de fraude electrónico.

La responsabilidad del BANCO sólo será exigible si el incumplimiento, modificación, deficiencia, suspensión, indisponibilidad o cancelación de la instalación del Software tiene su origen en causas imputables al BANCO y no por información que aparezca en la APLICACIÓN que no sea de su directa autoría y en modo alguno, de las caídas, interrupciones, ausencia o defecto en las telecomunicaciones a excepción de aquellos que se compruebe que provengan de dolo o culpa inexcusable del BANCO, según fuera el caso.

EL USUARIO asume la responsabilidad total frente al BANCO y/o frente a terceros por el uso indebido de los servicios regulados en estas CONDICIONES para operar con la APLICACIÓN. En tal sentido, exonera al BANCO de cualquier responsabilidad.

3. DERECHOS QUE TIENE EL BANCO

El BANCO se reserva el derecho a actualizar, eliminar información contenida en la APLICACIÓN, pudiendo incluso limitar o no permitir el acceso a dicha información, realizar modificaciones y/o mejoras en la APLICACIÓN, en cualquier momento y sin previo aviso, las que pasarán a ser propiedad exclusiva del BANCO. Siendo así, la APLICACIÓN podría contar con actualizaciones, buscando una mejor experiencia para el USUARIO, o correcciones de las funcionalidades que están disponibles.

El BANCO podrá eliminar, limitar o impedir el acceso a la APLICACIÓN cuando surjan dificultades técnicas por hechos o circunstancias ajenas al BANCO que, a su criterio, disminuyan o anulen los niveles de seguridad adoptados para el adecuado funcionamiento de la APLICACIÓN, El BANCO es el único responsable de la prestación de servicios de mantenimiento y soporte en relación con la APLICACIÓN según se establece en las presentes CONDICIONES.

El BANCO podrá introducir en el futuro alguna contraprestación por el servicio (comisiones), lo cual será comunicado al USUARIO con 45 días de anticipación como mínimo y conforme a los mecanismos establecidos por las normas de la materia. Además, podrá cancelar la licencia de uso de la APLICACIÓN otorgada, mediante comunicación previa al USUARIO, en el plazo mencionado.

4. OBLIGACIONES DEL USUARIO

El USUARIO acepta y se obliga a:

- Utilizar la APLICACIÓN conforme a las presentes CONDICIONES.
- Respetar, en cada momento, las normas en vigor en materia de telecomunicaciones.
- Custodiar el dispositivo móvil donde se haya descargado la APLICACIÓN y donde estén emuladas las Tarjetas, así como conservarlos en buen estado.
- Tomar las medidas razonables a fin de proteger las credenciales de seguridad personalizadas: documento nacional de identidad (DNI), registro único de contribuyentes (RUC), pasaporte, carnet de extranjería, carnet de identidad militar, carnet diplomático o partida de nacimiento, cualquier contraseña de acceso y gestión de los servicios telemáticos y claves comunicadas por el BANCO para la firma o aceptación de operaciones.
- No utilizar, como contraseñas o claves secretas, datos o fechas que se encuentren en documentos de su uso habitual.
- Notificar al BANCO a la brevedad posible, en cuanto el USUARIO tenga conocimiento del uso indebido por terceros de sus claves secretas o contraseñas, número de Tarjeta o cualquier otro dato para ingresar a su APLICACIÓN.

- Notificar el extravío, pérdida, robo, hurto, sustracción, acceso o uso no autorizado del DISPOSITIVO o la(s) Tarjeta(s) (física y/o digital) o la(s) adicional(es), códigos secretos y/o claves o información de ésta y contraseñas de la APLICACIÓN o acceso indebido a cualquiera de los mismos, así como cualquier otra causa que pueda provocar dicho acceso indebido, a la brevedad posible, en cuanto tenga conocimiento de ello. Podrá comunicarlo en las Oficinas del BANCO o al teléfono: (01) 595-0000.

5. TOKEN DIGITAL

El uso del Token Digital en la Banca Móvil o en la Banca por Internet, le atribuye inmediatamente a Usted la condición de USUARIO; y por lo tanto, genera la aceptación sin reservas de cada uno de las siguientes condiciones de uso del Sistema del Token Digital, así como en cualquier otro aviso legal o condiciones que las sustituyan, complementen y/o modifiquen:

5.1 Afiliación al Token Digital:

Para activar el Token Digital, Usted deberá ingresar a su Banca Móvil, y elegir el método de activación que prefiera: 1. con una tarjeta BBVA activa sin contacto, si cuentas con un dispositivo con sistema operativo Android con NFC (*esta opción no está disponible para celulares con sistema operativo iOS - iPhone*); 2. mediante biometría facial escaneando el DNI y tomándose un selfie más una clave SMS que llegará al celular seguro; o, 3. desde un Cajero Automático (ATM) escaneando un código QR desde el App y validando con una clave SMS enviada al celular seguro (*esta opción solo está disponible dentro del territorio peruano*). Una vez elegido el método, Usted deberá completar los datos requeridos por el Banco y solicitar el código de activación, conformado por seis (06) dígitos y con una vigencia máxima de dos (02) minutos aproximadamente. Dicho código será enviado por SMS al teléfono móvil registrado y deberá ser ingresado en el campo correspondiente de la aplicación. Cumplidos estos pasos, el Token Digital quedará activado y Usted recibirá un mensaje de confirmación.

En algunos casos, si el BANCO lo considera conveniente, se le solicitará realizar una validación adicional para afiliarse al Token Digital. Esta validación puede incluir el reconocimiento facial mediante fotografía y/o selfies así como el ingreso de un código de activación enviado por SMS a su celular seguro.

En caso Usted no haya recibido el código de activación o éste haya vencido por exceder el plazo señalado anteriormente, podrá solicitar uno nuevo en la sección "Pedir nueva Clave SMS" desde la Banca Móvil. Considerar que el SMS sólo llegará a celulares con operador peruano activo y que cuenten con cobertura telefónica

El "celular seguro" es el número de teléfono que el USUARIO ha registrado oficialmente ante el banco. Como parte del proceso de verificación de identidad, el USUARIO recibirá una clave SMS en su celular seguro. Esta clave es necesaria para confirmar la activación del Token Digital.

Si el USUARIO se encuentra en el extranjero y tiene registrado un celular seguro, deberá tener el servicio de roaming activado en su celular para poder recibir la clave SMS de verificación necesaria para confirmar la activación del Token Digital.

5.2 Finalidad:

Token Digital es un mecanismo de seguridad que genera automáticamente una clave aleatoria válida por un tiempo determinado. Este código le permite confirmar las operaciones que realice por Banca Móvil o por Banca por Internet.

Como parte de la transición hacia un modelo de mayor seguridad y experiencia al cliente, la activación de Token Digital es obligatoria para operar en la Banca Móvil y en la Banca por Internet. Si el Usuario

decide no activar Token Digital solo podrá acceder a consultas y movimientos y transferencias y pagos entre y hacia sus propios productos, ya sea desde la app instalada en su celular o desde un navegador web en computadora o celular.

5.3 Beneficios:

Dentro de los principales beneficios que contiene el Token Digital, podemos resaltar:

- Funciona en cualquier parte del mundo.
- Crea claves de manera automática para confirmar sus operaciones.
- Sólo entregará dichas claves cuando Usted lo necesite.
- Es más seguro ya que son claves asociadas a una operación y con un único uso.

5.4 Uso del Token Digital:

Para realizar una operación desde la Banca Móvil, Usted deberá seleccionar la operación deseada y luego presionar el botón de confirmación. Según el tipo de operación, el Token Digital se generará automáticamente o se mostrará en pantalla para su validación. Finalmente, la operación será confirmada. En el caso de Banca por Internet, deberá elegir la operación que desea realizar. Luego, deberá ingresar a su Banca Móvil, acceder a la opción Token Digital y escanear el código QR que aparecerá en la Banca por Internet. Esto generará un Token Digital que deberá ingresar en la Banca por Internet para confirmar la operación.

Es importante resaltar que la clave que se genere se renovará cada 120 segundos. La clave es válida para Banca por Internet. Asimismo, sólo se podrá utilizar una (01) clave por operación.

5.5 Datos biométricos:

EL BANCO podrá utilizar los datos biométricos que haya registrado en su Dispositivo Móvil (huella dactilar, retina, iris ocular, voz, rasgos faciales, así como cualquier otro tipo de biometría que habilite el Dispositivo en cada momento). Para ello deberá dar de alta en su Banca Móvil esta Funcionalidad siguiendo las instrucciones que EL BANCO le indique en cada momento. EL BANCO en ningún caso almacenará o generará una copia de los datos biométricos que el Usuario registre en su Dispositivo. Tampoco compartirá dicha información con algún tercero ajeno al BANCO.

Esta Funcionalidad no es controlada por EL BANCO y depende exclusivamente del Fabricante del Dispositivo. Por ello, antes de utilizar su Banca Móvil le recomendamos asegurarse del funcionamiento del Dispositivo, sus condiciones de seguridad y garantías bajo las condiciones que Usted haya contratado con el Fabricante o Distribuidor del Dispositivo.

EL BANCO determinará los datos biométricos con los cuales podrá utilizar esta Funcionalidad, así como, las distintas operaciones que se le permitirá realizar con los datos biométricos correspondientes.

El BANCO le informa, que, en caso active la presente Funcionalidad, el Token Digital se guardará de manera cifrada e ininteligible en un almacén seguro de claves de su Dispositivo, de conformidad con los estándares de seguridad del fabricante del Dispositivo.

5.6 Responsabilidad:

La Clave que genera el Token Digital es estrictamente personal. Usted no deberá compartirla con nadie. Asimismo, deberá tomar la diligencia debida. EL BANCO no asume responsabilidad por el mal uso del Token Digital.

Sobre ello, en caso de robo, pérdida y/o sustracción del teléfono celular, Usted deberá llamar a Banca por Teléfono o acercarse a cualquiera de nuestras oficinas, indicando que ha sido víctima de este siniestro. De esta manera, se procederá a dar de baja a su Token Digital, así como a activar todos los

mecanismos de seguridad que tenga a su disposición; buscando evitar la ejecución de operaciones por este canal.

5.7 Finalización del servicio:

Es importante resaltar que en el momento que Usted lo desee, podrá desafiliarse de los canales digitales a través de la Banca por teléfono o enviando un correo a soporte.digital.peru@bbva.com con los siguientes datos:

- Tipo y número de documento de identidad
- Motivo de la cancelación de tu cuenta

El tiempo de atención de la solicitud es de 2 días útiles.

5.8 Sobre el reconocimiento facial y huella dactilar (aplica solo si usted cuenta con un dispositivo con funciones biométricas y tiene dichas funciones activadas):

Al aceptar estos Términos y Condiciones, e ingresar las funciones biométricas para validación, como son: la imagen de su rostro y/o huella dactilar, autoriza al BBVA a que verifique dicha información con aquella que esté almacenada en su Dispositivo Móvil. De esta manera, las funciones biométricas, como son: las el reconocimiento de su rostro y el ingreso de su huella dactilar, solo se realizan con la finalidad de que Usted pueda acceder a la Banca Móvil BBVA y pueda firmar sus operaciones de manera más rápida y segura, en reemplazo de su Token Digital.

BBVA no almacenará sus datos personales (imagen de su rostro y huella) en algún Banco de Datos Personales de nuestra titularidad, con lo cual no compartirá tampoco su información con algún tercero. Asimismo, BBVA no tratará sus datos personales para una finalidad distinta a la antes señalada.

BBVA no se hace responsable si otra persona que ha registrado su huella dactilar y/o imagen en su dispositivo móvil accede a esta funcionalidad desde su Banca Móvil.

6. VIGENCIA DE LAS ESTIPULACIONES

En caso de que cualquier disposición contenida en las CONDICIONES sea declarada nula, anulable o inaplicable, las demás disposiciones de las presentes CONDICIONES permanecerán en vigor y continuarán vinculando a las partes.

Todas las notificaciones por parte del BANCO al USUARIO se considerarán eficaces si se efectúan de las siguientes maneras:

- Correo electrónico a la dirección que el USUARIO haya proporcionado a BANCO.
- Mediante mensajes emergentes, notificaciones push o mensajes de texto.

7. DESINSTALAR LA APLICACIÓN

El USUARIO podrá desinstalar la APLICACIÓN de su DISPOSITIVO, si lo cree conveniente y en cualquier momento, sin que eso conlleve a realizar algún pago al BANCO ni tendrá que comunicar esta circunstancia al BANCO. Esto se entenderá como la desafiliación del USUARIO de la APLICACIÓN. Si al desinstalar la APLICACIÓN se originara algún problema en el equipo, el BANCO no se hará responsable.

8. TRATAMIENTO DE DATOS PERSONALES

8.1 Responsable del tratamiento de la información y finalidades. Banco BBVA Perú (BBVA), con RUC Nro. 20100130204, con domicilio en Av. República de Panamá Nro.3055, Distrito de San Isidro, Provincia y Departamento de Lima, es el Responsable del Tratamiento y seguridad de los datos personales que el USUARIO proporcione al afiliarse a la APLICACIÓN, los que están almacenados en un banco de datos de su titularidad denominado: "Usuarios" con registro N O RNPDP – PJP – 171 y gestionados con todas las medidas de seguridad y confidencialidad, específicamente para garantizar el cumplimiento de las funcionalidades de la APLICACIÓN, según lo detallado en el presente documento; y para dar cumplimiento a obligaciones y/o requerimientos legales o regulatorios.

Así, le informamos que el BANCO tendrá acceso a la ubicación precisa y/o aproximada de su dispositivo móvil para que la APLICACIÓN pueda acceder a un sistema de localización de cajeros corresponsales, cajeros ATM; así como a la red de oficinas del BANCO disponibles. También, para el efectivo desarrollo de determinadas funcionalidades de la APLICACIÓN, como: envío de dinero a través del servicio Efectivo Móvil u otros servicios similares, o ponerse en contacto con un asesor de servicio del BANCO, entre otros; se podrá acceder a la lectura de contactos, al estado del teléfono, incluyendo el número de teléfono del dispositivo, información de la red celular, el estado de las llamadas en curso, el registro de llamadas recibidas y realizar llamadas sin pasar por la interface de marcación; este último sólo cuando usted requiera comunicarse con un asesor directamente desde la APLICACIÓN.

De esta manera, se debe tener en cuenta lo siguiente:

a) Ubicación del dispositivo móvil – Geolocalización

Si el DISPOSITIVO o la versión de la APLICACIÓN lo permiten, el USUARIO podrá acceder a un sistema de localización de cajeros ATM de las redes de BANCO, así como de oficinas del BANCO disponibles, con indicación de su ubicación, así como acceder a la dirección y teléfono de contacto, en su caso, de cada uno de los mismos, según lo que a continuación se establece.

Si se tiene disponible esta funcionalidad, el propio DISPOSITIVO define su posición geográfica, automática (a través del GPS incorporado en el mismo) o manualmente (a través de la celda GSM en la que se localiza), y en base a dicha ubicación, el BANCO le mostrará la relación de cajeros ATM, así como las oficinas BBVA disponibles a su alrededor en un determinado radio, ordenados por distancia de menor a mayor. El USUARIO, al seleccionar cualquier oficina o cajero, podrá conocer la dirección exacta del cajero y/o oficina y teléfono de contacto de la oficina, así como la ruta a seguir para alcanzar tal ubicación.

b) Almacenamiento Externo

Si el DISPOSITIVO o la versión de la APLICACIÓN lo permite, podrá almacenar y acceder a los datos que el USUARIO haya decidido guardar como parte del uso de esta. Por ejemplo, si el USUARIO decide guardar la información de una tarjeta como frecuente, el aplicativo podrá acceder a dicha información almacenada y, de esta forma, mostrarla como frecuente en una siguiente sesión. Cabe resaltar que la información se almacenará de forma encriptada con la finalidad de preservar la confidencialidad y seguridad de la misma.

El BANCO únicamente gestionará los permisos para la finalidad descrita en la presente Funcionalidad.

c) Contactar con el Servicio de Atención al cliente del BANCO "Línea BBVA"

Si el DISPOSITIVO o la versión de la APLICACIÓN permiten contactar con el Servicio de Atención al Cliente del BANCO "Línea BBVA", la APLICACIÓN, una vez descargada por el USUARIO, le permitirá contactar con dicho servicio. Si el USUARIO acepta contactar, la APLICACIÓN le facilitará la posibilidad de llamar de forma automática, a través del operador de telefonía móvil que el USUARIO tenga contratado.

El USUARIO deberá asumir los costes de conexión y llamadas que realice según la tarifa que tenga contratada con Su operador.

d) Uso de la Agenda de Contactos del usuario por el BANCO

Si el DISPOSITIVO o la versión de la APLICACIÓN lo permite, el USUARIO podrá acceder y seleccionar de su agenda de contactos del DISPOSITIVO el número al que quiere enviar o transferir dinero. Para poder realizar la citada operación solicitada por el USUARIO, será necesario que el BANCO acceda a la agenda de contactos del DISPOSITIVO. Al utilizar esta Funcionalidad se solicitará al USUARIO el permiso de acceso a la agenda de contactos, en caso de que el USUARIO acepte, estará consintiendo que el BANCO acceda a la agenda de contactos siempre que el USUARIO lo solicite con ocasión de esta Funcionalidad.

El BANCO únicamente utilizará el contenido de su agenda de contactos para la finalidad prevista en la presente Funcionalidad.

e) Condiciones de acceso a conexión Wi-Fi - Acceso a la red

Si el DISPOSITIVO o la versión de la APLICACIÓN lo permite, el USUARIO podrá ser informado del estado de la conexión a redes Wi-Fi e Internet, así como usarla para el intercambio de datos con el BANCO o para el uso de otros servicios que requieran de dicha conexión.

El BANCO únicamente utilizará los datos de conexión a red para la finalidad prevista en la presente Funcionalidad.

f) Uso de cámara

Si el DISPOSITIVO o la versión de la APLICACIÓN lo permite, será necesario que el USUARIO facilite permisos de acceso de cámara, así como permisos para evitar que el DISPOSITIVO entre en modo suspensión.

Finalmente, con relación a la captura de imagen que realiza el USUARIO de su documento de identificación (anverso y reverso) y selfie (normal + alive) que realiza de su persona, ello se realiza exclusivamente para fines de descargar su Token Digital, y a fin que EL BANCO valide su identidad como un factor de autenticación para proteger la seguridad de sus transacciones monetarias y no monetarias.

Asimismo, a través del reconocimiento facial se realizará el desbloqueo de productos ante supuestos escenarios de fraude.

Recuerda:

- La funcionalidad de Afiliación al Token Digital con Biometría Facial y el Desbloqueo de Producto con Biometría Facial, no se conservará ninguna de las capturas.
- El BANCO no compartirá la información proporcionada por el USUARIO en el uso de la APLICACIÓN con algún tercero.
- Realizamos flujo transfronterizo a España garantizado con un nivel suficiente de protección para los datos personales.

- Puedes realizar el desbloqueo de tus productos que fueron bloqueados preventivamente ante escenarios de supuestos fraudes.

8.2. Encargados. El BANCO no compartirá la información proporcionada por el USUARIO en el uso de la APLICACIÓN con algún tercero.

8.3. Duración del tratamiento de los datos. Los datos personales del USUARIO proporcionados para afiliarse a LA APLICACIÓN se mantendrán almacenados mientras su tratamiento sea necesario para cumplir con la finalidad descrita en dicho documento, o hasta por diez (10) años luego de concluida la relación contractual de conformidad con lo establecido en la legislación pertinente. Se precisa, no obstante, que EL BANCO no conservará las imágenes del documento de identificación ni del selfie (normal + alive).

8.4. Derechos ARCO., El USUARIO tiene derecho a acceder a sus datos personales, rectificarlos, cancelarlos u oponerse a su tratamiento. Para ello, podrá presentar una solicitud con los requisitos exigidos por las normas aplicables, en cualquiera de las oficinas del BANCO a nivel nacional o a través de los canales digitales disponibles para dicha finalidad. Finalmente, se informa al USUARIO que puede presentar un reclamo ante la Autoridad Nacional de Protección de Datos Personales en la Mesa de Partes del Ministerio de Justicia y Derechos Humanos: Calle Scipión Llona N° 350, Miraflores, Lima, Perú, de considerar que no ha sido atendido adecuadamente en el ejercicio de sus derechos.

8.5. Principio de Seguridad. Hemos adoptado las medidas legales, técnicas y organizativas de seguridad y confidencialidad apropiadas a cada categoría de los datos personales, las cuales son necesarias para mantener el nivel de seguridad requerido. Todo ello, con el objetivo de evitar la alteración, pérdida o el tratamiento o acceso no autorizado que puedan afectar a la integridad, confidencialidad y disponibilidad de la información.

Cualquier consulta estamos a tu disposición a través del siguiente buzón:
proteccion.datos.peru@bbva.com

9. USO DE COOKIES

¿Qué son las cookies?

- Una cookie es un archivo de información que un servidor web crea cuando visitas un sitio web.
- Los datos brindan información sobre cómo y cuándo usted visita un sitio.
- Se almacena en su dispositivo o equipo (computadora, teléfono inteligente, o tableta) en la forma de un archivo de texto pequeño.

¿Para qué se utilizan las cookies en este Sitio Web?

- Las cookies son importantes para ti, influyen en tu experiencia de navegación.
- Nos ayudan a proteger tu privacidad o darte acceso seguro con tu usuario al Sitio Web.
- Usamos cookies técnicas, analíticas, de personalización y publicitarias (propias y de terceros) para hacer perfiles basados en hábitos de navegación y mostrarte contenido útil.
- Asimismo, podemos identificar problemas para mejorar tu experiencia cuando estés usando este Sitio Web, hacer mediciones y estadísticas de uso.

¿Qué cookies emplea LA APLICACIÓN?

Se informa al USUARIO que LA APLICACIÓN emplea cookies para su mejor funcionamiento.

De igual manera, las cookies nos permiten ver la manera en que LA APLICACIÓN es usada para fines estadísticos. En LA APLICACIÓN utilizamos "Cookies Analíticas" las mismas que, se detallan a continuación:

Denominación	Titular	Tipología	Duración	Finalidad
AMCV_***	Adobe Analytics	Analítica	Sesión	ID de visitante único que se usan en las soluciones de Marketing Cloud
AMCVS_***	Adobe Analytics	Analítica	2 años	ID de visitante único que se usan en las soluciones de Marketing Cloud
demdex (safari)	Adobe Analytics	Analítica	180 días	Crear y almacenar identificadores únicos y persistentes
sessionId	Adobe Analytics	Analítica	Sesión	Cookie interna de Launch usada para realizar serializaciones
gpv_URL	Adobe Analytics	Analítica	Sesión	plugin Adobe Analytics: getPreviousValue Capturar el valor de una determinada variable en la siguiente vista de página, en este caso la prop13"
gpv level1	Adobe Analytics	Analítica	Sesión	Cookie utilizada para almacenar el level1 del DataLayer de la página anterior.
gpv_pageIntent	Adobe Analytics	Analítica	Sesión	Cookie utilizada para almacenar el pageIntent de la página anterior.
gpv_pageName	Adobe Analytics	Analítica	Sesión	Cookie utilizada para almacenar el pagename de la página anterior.
aocs	Adobe Analytics	Analítica	Sesión	Cookie que almacena los primeros valores recogidos al inicio de un proceso.
TTC	Adobe Analytics	Analítica	Sesión	Cookie usada para almacenar el tiempo transcurrido entre el evento App Page Visit y App Completed.
TTCL	Adobe Analytics	Analítica	Sesión	Cookie usada para almacenar el tiempo transcurrido entre el evento

				LogIn y App Completed.
s_cc	Adobe Analytics	Analítica	Sesión	Determinar si las cookies están activas
s_hc	Adobe Analytics	Analítica	Sesión	Cookie usada por Adobe con propósitos de analítica.
s_ht	Adobe Analytics	Analítica	Sesión	Cookie usada por Adobe con propósitos de analítica.
s_nr	Adobe Analytics	Analítica	2 años	Determinar el número de visitas de usuario
s_ppv	Adobe Analytics	Analítica	Persisten	plugin Adobe Analytics: getPercentPageViewed Determinar el porcentaje de página que visualiza un usuario"
s_sq	Adobe Analytics	Analítica	Sesión	Funcionalidades ClickMap/ActivityMap
s_tp	Adobe Analytics	Analítica	Sesión	Cookie usada por Adobe con propósitos de analítica.
s_visit	Adobe Analytics	Analítica	Sesión	Cookie usada por Adobe para saber cuando una sesión se ha iniciado.
s_vi	Adobe Analytics	Analítica	2 años	Esta cookie se usa para identificar a un visitante único
m_box	Adobe Target	Personalización	90 días	Cookie usada por Adobe Target para hacer test de personalización de experiencia del usuario.

¿Cómo puedes desactivar las Cookies?

- Te brindamos la opción de oponerte a la instalación de las cookies.
- Puedes bloquearlas o eliminarlas a las cookies instaladas en tu equipo mediante la modificación de los parámetros de configuración del navegador instalado en tu computadora: Chrome, Explorer, Firefox, Safari u otro.

Internet Explorer:

1. En Internet Explorer, selecciona el botón Herramientas, dirígete a Seguridad y luego elige
2. Eliminar el historial de exploración.
3. Active la casilla Cookies y datos del sitio web y, a continuación, seleccione Eliminar. Mozilla

Firefox:

1. En la parte superior de la ventana de Firefox hacer click en el menú herramientas.

2. Seleccionar opciones .
3. Seleccionar el panel de privacidad.
4. En la opción Firefox podrá elegir usar una configuración personalizada para el historial para configurar las opciones.

Google Chrome

1. En tu ordenador, abre Chrome.
2. Arriba a la derecha, haz clic en Más Configuración.
3. Haz clic en Seguridad y privacidad, Cookies y otros datos de sitios.
4. Haz clic en Ver todos los datos y permisos de sitios Borrar todos los datos.
5. Para confirmar la acción, haz clic en Borrar.

Safari:

1. En el menú de configuración, seleccione la opción de preferencias
2. Abre la pestaña de privacidad
3. Seleccione la opción que quiera de la sección de bloquear cookies
4. Recuerde que ciertas funciones y la plena funcionalidad del sitio pueden no estar disponibles después de deshabilitar las cookies.

Recuerda:

La desactivación de las cookies no impide la navegación por este Sitio Web, aunque el uso de algunos de sus servicios podrá ser limitado, y por tanto, tu experiencia de navegación podrá ser menos satisfactoria.

10. JURISDICCIÓN Y LEY APLICABLE

En caso surgiera alguna controversia o proceso judicial entre BANCO y el USUARIO, éstos se someterán exclusivamente a los Juzgados y Tribunales del Distrito Judicial de Lima, Perú, renunciando a la posibilidad de someterse a otro fuero jurisdicción.