

## REQUERIMIENTOS OPERATIVOS MÍNIMOS DE SEGURIDAD PARA INSTRUMENTOS Y CANALES ELECTRÓNICOS DE PAGO

La Gerencia de Entidades Financieras del Banco Central de Bolivia (BCB), en el marco del del Artículo 29 del Reglamento de Servicios de Pago, Instrumentos Electrónicos de Pago, Compensación y Liquidación, establece los Requerimientos Operativos Mínimos de Seguridad para los siguientes Instrumentos y Canales Electrónicos de Pago:

### 1. Órdenes Electrónicas de Transferencia de Fondos

- a) Los servicios transaccionales deben funcionar utilizando canales de comunicación cifrados sobre un servidor seguro bajo el protocolo *Transport Layer Security*<sup>1</sup> (TLS) en su versión 1.2 o superior, aplicando las actualizaciones de seguridad que correspondan.

En caso de que se utilice *Virtual Private Network*<sup>2</sup> (VPN) Cliente-Sitio, se deberá utilizar el protocolo TLS versión 1.2 o superior. Cuando se utilice VPN Sitio-Sitio, se deberán aplicar mecanismos y protocolos de cifrado de al menos AES-256 y encriptación IKE/IPSec.

- b) El sitio web debe tener un certificado TLS con validación extendida, emitido por una entidad certificadora autorizada, de acuerdo a la legislación y normativa nacional, que permita validar la siguiente información: la entidad certificante, el nombre del sitio web, la razón social de la entidad financiera propietaria del sitio, número de serie del certificado, así como las fechas de emisión y de vencimiento del certificado.

En ningún caso la vigencia de este certificado debe ser superior a la definida en el Reglamento de Firma Digital para el Sistema de Pagos emitido por el BCB.

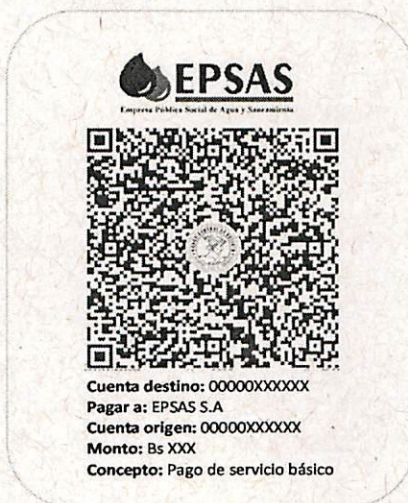
- c) Las transferencias de fondos deberán ser abonadas a las cuentas de los beneficiarios una vez que se completen los procesos de validación exigidos por el sistema de procesamiento y como máximo al finalizar el ciclo en caso de que el procesamiento involucre procesos de compensación y liquidación.
- d) Las Órdenes Electrónicas de Transferencia de Fondos (OETF) deben cumplir con las siguientes características:

<sup>1</sup> Seguridad de la capa de transporte.

<sup>2</sup> Red privada virtual.

- **Autenticidad:** Contar con mecanismos que permitan verificar la identidad del titular del instrumento electrónico de pago y que éste se encuentre debidamente autorizado.
  - **Integridad:** Estar protegidas contra alteraciones originadas por contingencias tecnológicas, acciones intencionales o accidentales durante su procesamiento, transporte y almacenamiento.
  - **Confidencialidad:** Contar con mecanismos de cifrado estándar que eviten la difusión o divulgación no autorizada de la información contenida en la operación que pueda ser utilizada para materializar eventos de fraude.
  - **No repudio:** Garantizar que ninguna de las partes implicadas en la transacción pueda negar su participación en la misma.
  - **Disponibilidad:** El emisor debe garantizar, en el ámbito de su control, que el sistema de procesamiento de OETF esté disponible para los clientes según las condiciones publicitadas, informadas o pactadas contractualmente.
- e) El intercambio de información entre las entidades financieras y las empresas proveedoras de servicios externos de tecnologías deberán cumplir con las características de seguridad descritas en el inciso d).
- f) El intercambio de información para el procesamiento de OETF entre las entidades financieras y sistemas de compensación y liquidación deberá cumplir con lo definido en el Reglamento de Firma Digital para el Sistema de Pagos emitido por el BCB.
- g) Las entidades financieras deben implementar en sus sistemas de monitoreo y seguimiento, mecanismos de detección, alerta y, cuando corresponda, bloqueo automatizado de operaciones inusuales para la detección de actividades sospechosas y prevención de eventos de fraude, basados en la creación de reglas de frecuencia, velocidad, montos límite, uso de dispositivo de confianza, ubicación geográfica no habitual y otros que respondan a un análisis y evaluación de riesgos en seguridad de la información.
- h) Las entidades financieras deben realizar campañas de información respecto a la seguridad del uso de instrumentos electrónicos de pago, dirigidas a los usuarios de OETF, con una periodicidad mínima semestral y en caso de cambios en la operativa, que incluyan al menos:
- Descripción de las operaciones y/o funcionalidades.
  - Uso del servicio.

- Utilización de los mecanismos de autenticación robusta, describiendo su operativa y los casos de aplicación.
  - Sistema de atención de reclamos y consultas de clientes.
- i) El código QR de cobro debe incluir en su plantilla mínimamente la siguiente información:
- Nombre de la entidad destinataria de la transferencia.
  - Nombre y apellido del beneficiario si es persona natural o Razón social si es persona jurídica.
  - Número de cuenta del beneficiario de la transacción.
  - Monto (podría estar vacío).
  - Fecha de vencimiento del QR (hasta dos años).
  - Concepto de pago.
- j) Las entidades que procesen pagos de servicios básicos con QR, a través de sus sistemas de banca electrónica y banca móvil deberán implementar una plantilla personalizada que incluya en el encabezado el nombre y/o logo de la entidad y/o empresa pública, así como los datos de la transacción (número de cuenta destino, razón social/nombre del beneficiario, cuenta de origen, monto, concepto) de acuerdo al siguiente modelo:



- k) Las OETF que se canalicen a través de carteras digitales (*E-wallet*) deberán cumplir con las características de seguridad descritas en esta sección.



## 2. Canales electrónicos de pago: Aplicaciones *web* y móviles

- a) Las entidades financieras, deben implementar medidas de seguridad para sus aplicaciones *web* y móviles, en función de su análisis y evaluación de riesgos en seguridad de la información, así como asumir medidas de mitigación de riesgos.
- b) Las entidades financieras, no deben habilitar una cuenta de acceso a una aplicación *web* o móvil, que permita el procesamiento de órdenes de pago, sin previo consentimiento del cliente o titular de la cuenta asociada.
- c) Las entidades financieras, deben implementar en su operativa, a través de aplicaciones *web* y móviles, mecanismos de autenticación robusta para sus usuarios en los siguientes procesos de autorización:
  - Procesamiento de órdenes de pago.
  - Registro y modificación de los datos de beneficiarios, así como otra información sensible o confidencial cuya modificación podría facilitar la comisión de delitos o fraudes.
  - Habilitación de tarjetas electrónicas para pagos por *internet*, así como para su uso en el extranjero.
  - Definición y modificación de límites transaccionales.
  - Otros inherentes al procesamiento de órdenes de pago.

Al menos uno de los factores que se aplique no debe ser reutilizable ni replicable ni ser susceptible de ser robado vía *internet*. En caso de que se utilice una contraseña de un solo uso, su vigencia no deberá ser superior a dos (2) minutos.

Únicamente para el inicio de sesión se podrá utilizar la autenticación de un solo factor, en función del análisis y evaluación de riesgos en seguridad de la información que efectúe la entidad financiera.

Cuando se opte por el uso de mecanismos de autenticación biométrica, éstos deben estar bajo el control y responsabilidad exclusivos de las entidades financieras, incluyendo además métodos de prueba y/o reconocimiento de vida del usuario.

- d) Las entidades financieras deben proporcionar al cliente una contraseña para autenticarse al servicio, siendo su cambio obligatorio después del primer inicio de sesión y contar con mecanismos para recordarle su cambio al menos cada noventa (90) días.
- e) Las entidades financieras deben garantizar que sus aplicaciones *web* y móviles no almacenen información sensible y/o confidencial en *HyperText*

*Markup Language*<sup>3</sup> (HTML) campos ocultos, cookies o cualquier otra forma de almacenamiento del lado del cliente que pueda comprometer su confidencialidad o la integridad de los datos.

- f) Las aplicaciones *web* y móviles no deben exponer los datos del usuario en el inicio de sesión.
- g) El restablecimiento de las sesiones en las aplicaciones *web* o móviles, después de interrupciones o de un periodo de inactividad, debe requerir una nueva autenticación del usuario.

Toda sesión debe ser finalizada automáticamente después de cinco (5) minutos de inactividad como máximo.

- h) Se debe implementar controles de seguridad, seguimiento y notificación de acceso de dispositivos electrónicos a aplicaciones *web* y móviles.
- i) Se deben implementar mecanismos de registro/vinculación de dispositivos para acceso a servicios electrónicos, así como la detección de redes no seguras, ubicaciones geográficas no habituales, parámetros anormales y monitoreo de transacciones sospechosas.
- j) Implementar mecanismos no presenciales para la actualización de información personal, la modificación de funcionalidades habilitadas, confirmación de cambios y actualizaciones en canales electrónicos con el uso de mecanismos de autenticación robustos que estén bajo el control y responsabilidad de la entidad. En caso de implementar factores biométricos de autenticación, éstos deben incluir métodos de prueba y/o reconocimiento de vida del usuario.
- k) Los mensajes de comunicación que remitan los emisores a través de correo electrónico y/o *Short Message Service*<sup>4</sup> (SMS) no deben ser genéricos y deben especificar la operación a ser autorizada, considerando, según corresponda, el código de confirmación, monto, entidad financiera destino, cuenta del beneficiario, fecha y hora de la operación.
- l) Las aplicaciones *web* y móviles deben desplegar la opción de cobros y pagos inmediatos con código *Quick Response Code*<sup>5</sup> (QR) de manera genérica, sin hacer alusión a marcas, logos, productos de forma específica.
- m) Las aplicaciones *web* y móviles deben permitir al usuario definir el periodo de validez de los códigos QR de cobro, que podrá ser de hasta 2 años.

<sup>3</sup> Lenguaje de marcado para la elaboración de páginas web.

<sup>4</sup> Servicio de mensajes cortos.

<sup>5</sup> Código de respuesta rápida.

- n) Las entidades financieras habilitarán de manera obligatoria y automática el procesamiento de transferencias electrónicas síncronas (pagos inmediatos con QR) y asíncronas (normales) por un monto mínimo de Bs69.600 (Sesenta y nueve mil seiscientos 00/100 bolivianos) o el equivalente a USD10.000 (Diez mil 00/100 dólares estadounidenses) a través de todos sus canales de pago presenciales y electrónicos, informando a sus clientes este aspecto y poniendo a su disposición los mecanismos correspondientes para la ampliación o disminución de este límite en cualquier momento.
- o) Las aplicaciones *web* y móviles deben permitir al usuario definir y/o modificar de manera automática el monto máximo OETF de pago inmediato con QR (generación y pago), no pudiendo aplicar restricciones unilaterales.

A objeto de cumplir con las disposiciones de la Unidad de Investigaciones Financieras, las entidades deberán obtener a través de sus aplicaciones *web* y móviles, información de origen y destino de fondos.

- p) Las aplicaciones *web* y móviles, antes y después de la confirmación para la ejecución de una transacción, deben desplegar la siguiente información que sea exacta y completa:
- Nombre de la entidad financiera destinataria sin prefijos, ni códigos o siglas de los sistemas de procesamiento (no debe incluirse otra información que pueda causar confusión en el usuario).
  - Nombre y apellido del beneficiario (persona natural) o razón social (persona jurídica).
  - Carnet de identidad o número de NIT del beneficiario.
  - Número de cuenta del beneficiario de la transacción.
  - Importe de la transacción.
  - Moneda de la transacción.

El procesamiento de las transacciones es de manejo interno de cada entidad.

- q) Las entidades deben implementar mecanismos de notificación de depósitos, transacciones con tarjetas, y transferencias electrónicas en los aplicativos móviles.
- r) Las entidades financieras deben implementar mecanismos que permitan a los usuarios registrar reclamos de manera no presencial a través de sus aplicaciones *web* y móviles, así como, hacer seguimiento al estado de los mismos y emitir respuesta en el plazo indicado en el Reglamento de Protección del Consumidor de Servicios Financieros, incluido en el Libro 4°, Título I, Capítulo I, Sección 4, Artículo 3 de la Recopilación de Normas del Sistema Financiero de la Autoridad de Supervisión del Sistema Financiero.

### 3. Tarjetas Electrónicas

- a) Las tarjetas electrónicas pueden ser emitidas y utilizadas de manera física o virtual, implementando controles que eviten posibles hechos delictivos en su utilización, como por ejemplo, la tokenización.

Las entidades financieras tienen la obligación de ofrecer a sus clientes el uso virtual de las tarjetas electrónicas que emitan.

- b) Las tarjetas electrónicas emitidas físicamente deben contener en forma impresa, grabada o embozada, según corresponda, los siguientes datos: nombre del emisor, número de tarjeta, valor de verificación de la tarjeta y cuando corresponda, nombre, logo y holograma de la marca internacional y fecha de vencimiento.
- c) Los últimos cuatro dígitos embozados, grabados o impresos en la tarjeta deben concordar con los dígitos que figuran en el recibo generado por la terminal al momento de realizar retiros o compras presenciales.
- d) Cuando se trate de tarjetas de débito o prepagadas emitidas físicamente, el emisor debe ofrecer al titular la opción de impresión del nombre del tarjetahabiente en el plástico explicando las ventajas y desventajas de la selección. En caso de que el cliente no desee incluir este dato el emisor debe registrar y guardar la selección realizada con la firma del titular.
- e) La banda magnética de las tarjetas electrónicas debe contener la siguiente información: número de cuenta principal (PAN<sup>6</sup>), fecha de vencimiento, valor de verificación del PIN<sup>7</sup>, valor de verificación de la tarjeta (CVV<sup>8</sup>) y código de servicio. Esta información debe ser validada por el emisor al momento de procesar las transacciones.
- f) El código de validación de la tarjeta (CAV2<sup>9</sup>, CID<sup>10</sup>, CVC2<sup>11</sup>, CVV2<sup>12</sup>) o los datos de validación del PIN no deben poder almacenarse en sistemas o bases de datos.
- g) Los mensajes que se intercambien entre las terminales deben generarse bajo el estándar ISO 8583, que podrá ser adaptado a las necesidades particulares para facilitar la interoperabilidad de las plataformas involucradas.

<sup>6</sup> PAN = *Primary Account Number*, número de cuenta primaria

<sup>7</sup> PIN = *Personal Identification Number*, número de identificación personal.

<sup>8</sup> CVV = *Card Verification Value*, valor de verificación de la tarjeta.

<sup>9</sup> CAV2 = *Card Security Code*, código de validación de la tarjeta para JCB.

<sup>10</sup> CID = *Card Security Code*, código de validación de la tarjeta para American Express.

<sup>11</sup> CVC2 = *Card Security Code*, código de validación de la tarjeta para MasterCard.

<sup>12</sup> CVV2 = *Card Security Code*, código de validación de la tarjeta para Visa.



- h) Las Empresas Administradoras de Tarjetas Electrónicas (EATE) que procesen transacciones con tarjetas electrónicas deberán comunicar a sus participantes, al BCB y a la Autoridad de Supervisión del Sistema financiero (ASFI) cada actualización que se realice al estándar ISO 8583 en un plazo de cinco (5) días hábiles posteriores a la actualización.
- i) Las entidades financieras deben implementar en sus aplicaciones *web* y móviles las siguientes funcionalidades sin costo para el cliente:
- Habilitación y deshabilitación de tarjetas electrónicas para compras por *internet* y para uso en el exterior.
  - Generación de extractos históricos y/o periódicos de las operaciones realizadas.

Solamente se aplicarán tarifas a la emisión de extractos impresos a solicitud del titular del instrumento electrónico de pago.

- j) Las habilitaciones de tarjetas electrónicas para compras por *internet* y el procesamiento de pagos por internet en páginas *web* de establecimientos comerciales o de servicios nacionales se deben realizar en entornos seguros y de confianza.
- k) Las entidades financieras tienen la obligación de informar al titular o usuario del instrumento que las tarjetas electrónicas están exentas automáticamente del proceso de habilitación para compras por internet hasta determinados montos diferenciados para tarjetas de débito y tarjetas de crédito.

Las entidades financieras deberán poner a disposición del titular los mecanismos necesarios para deshabilitar su tarjeta electrónica para compras por internet por los montos establecidos automáticamente en cualquier momento.

Los emisores deberán diferenciar en sus sistemas los canales (local/exterior) de las transacciones con tarjetas electrónicas y no podrán aplicar restricciones a los usuarios en cuanto a monto para las compras locales por *internet*. Los límites se establecerán en función de la habilitación que haga el usuario y del saldo de la cuenta o de la línea de crédito a la que la tarjeta esté vinculada.

- l) La responsabilidad ante reclamos y disputas por el procesamiento de transacciones o compras virtuales recaerá sobre las entidades emisoras o adquirentes que no operen bajo protocolos de seguridad que contengan mecanismos de autenticación robusta de acuerdo a lo siguiente:

- La responsabilidad por transacciones procesadas con tarjetas que no se encuentren bajo protocolos de seguridad que contengan mecanismos de autenticación robusta en plataformas de comercio electrónico que no operen bajo protocolos de seguridad que contengan mecanismos de autenticación robusta, será del adquirente.
- La responsabilidad por transacciones procesadas con tarjetas que no se encuentran bajo protocolos de seguridad que contengan mecanismos de autenticación robusta en plataformas de comercio electrónico que sí operen bajo protocolos de seguridad que contengan mecanismos de autenticación robusta, será del emisor.
- La responsabilidad por transacciones procesadas con tarjetas que se encuentran bajo protocolos de seguridad que contengan mecanismos de autenticación robusta que hayan sido autenticadas en plataformas de comercio electrónico que no se encuentren bajo protocolos de seguridad que contengan mecanismos de autenticación robusta, será del adquirente.

m) Los emisores deben implementar mecanismos de autenticación robusta para las autorizaciones de las tarjetas electrónicas que se usen de manera virtual, considerando que al menos uno (1) de los factores que se aplique no debe ser reutilizable, ni replicable, ni ser susceptible de ser robado vía internet.

Cuando se utilice una contraseña de un solo uso, la vigencia de ésta no deberá ser superior a dos (2) minutos.

n) Como mecanismo de autenticación robusta para tarjetas con chip el titular o usuario del instrumento al realizar pagos presenciales en establecimientos comerciales o de servicios con tarjetas electrónicas, deberá introducir el PIN correspondiente una vez que el encargado del establecimiento introduzca el monto de la transacción, el cual deberá estar visible para la validación previa por parte del titular o usuario.

Las transacciones presenciales con tarjetas de tecnología sin contacto (*contactless*) estarán exentas de la aplicación del PIN hasta un monto máximo de Bs200 (Doscientos 00/100 bolivianos).

Los adquirentes pueden configurar los POS<sup>13</sup> para que las transacciones *contactless* por montos inferiores a Bs200 requieran la aplicación de PIN con base en el análisis de riesgo acorde al rubro del establecimiento o actividad.

<sup>13</sup> POS = Point of Sale, Terminal Punto de Venta.



- o) Cuando se utilice tarjetas con chip para procesar pagos presenciales en establecimientos comerciales o de servicios, no será necesaria la firma manuscrita del cliente, ni se emitirá el *voucher* impreso, a menos que éste lo solicite.
- p) Para el caso de tarjetas electrónicas de emisores del exterior que cuenten exclusivamente con banda magnética para su procesamiento en establecimientos comerciales o de servicios de Bolivia, el titular o usuario del instrumento al momento de realizar una compra presencial deberá presentar su documento de identificación y firmar los comprobantes de la transacción.
- q) Los adquirientes deben instruir a los establecimientos comerciales o de servicios procesar las transacciones utilizando la lectura del chip, salvo en el caso de pagos con tecnología sin contacto (*contactless*).
- r) Las comisiones que pagan los establecimientos comerciales o de servicios a las EATE no se pueden transferir al titular o usuario de la tarjeta electrónica.
- s) Las disputas o reclamos por el procesamiento de transacciones recaerán sobre las entidades emisoras o adquirientes que no operen con tarjetas con chip bajo el estándar EMV<sup>14</sup> de la siguiente manera:
- La responsabilidad por transacciones procesadas con banda magnética en terminales que no tengan la capacidad de procesar tarjetas con chip, será del adquiriente.
  - La responsabilidad por transacciones procesadas con tarjetas únicamente de banda magnética en una terminal que tenga habilitada la lectura de chip, será del emisor que no opere bajo el estándar EMV.
- t) Se debe aplicar algoritmos de cifrado estándar para autenticar la tarjeta con chip y los datos de la operación.
- u) Adicionalmente a los factores de autenticación robusta con el uso de PIN, se puede utilizar sistemas biométricos de autenticación para verificar la identidad del tarjetahabiente. Estos sistemas deben estar bajo el control y responsabilidad del emisor.

En caso de implementar factores biométricos de autenticación, éstos deben incluir métodos de prueba y/o reconocimiento de vida del usuario.

- v) En caso de que el emisor autorice la realización de operaciones fuera de línea, las tarjetas deben utilizar un mecanismo de autenticación dinámico

<sup>14</sup> EMV = Europay, MasterCard y Visa.

(CAM<sup>15</sup>) de tipo DDA<sup>16</sup> o CDA<sup>17</sup>, que permita recalcular el valor de la firma digital en cada transacción para lo que deben estar equipadas con un criptoprocesador.

- w) El sistema operativo de las tarjetas podrá ser de plataforma nativa o abierta, ambos deberán tener la capacidad de manejar DDA o CDA en caso que el emisor acepte el procesamiento de transacciones fuera de línea.
- x) Para los pagos con tecnología sin contacto (*contactless*) los emisores deben implementar en sus sistemas de monitoreo y seguimiento, mecanismos de control interno, parámetros estrictos de seguridad y alertas para la prevención de fraude basados en la creación de reglas de frecuencia, velocidad, montos límite y otros que permitan controlar la cantidad de transacciones que se aprueban bajo la tecnología sin contacto (*contactless*) que respondan a un análisis de riesgos por tipo de producto y volumen de transacciones de la citada tecnología. Entre dichas medidas deben ofrecer a sus clientes la posibilidad de establecer un monto límite diario por producto.
- y) Para los pagos realizados con tarjetas electrónicas en entornos virtuales, los emisores deben implementar en sus sistemas de monitoreo y seguimiento, mecanismos de detección, alerta y cuando corresponda, bloqueo automatizado de operaciones inusuales basados en la creación de reglas de frecuencia, velocidad, montos límite y otros que respondan a un análisis de riesgo.
- z) Los emisores, a efectos de incentivar el uso seguro de tarjetas de tecnología sin contacto (*contactless*), deben brindar a sus clientes capacitación sobre el uso de este tipo de tarjetas y en cuanto al monto límite para transacciones presenciales exentas de la aplicación de PIN.
- aa) Todas las tarjetas en circulación deben tener incorporada la tecnología sin contacto (*contactless*).
- bb) Los emisores deben procesar en línea las operaciones de devolución de fondos por operaciones rechazadas para pagos generados con tarjetas electrónicas de manera presencial o en entornos virtuales.
- cc) Las solicitudes de autorización para pagos a nivel nacional o internacional tendrán un límite de tiempo máximo de 10 segundos para su respuesta por parte del emisor, periodo después del cual se debe desplegar el mensaje "timeout".

<sup>15</sup> CAM = Card Authentication Method, método de autenticación de la tarjeta.

<sup>16</sup> DDA = Dynamic Data Authentication, autenticación dinámica.

<sup>17</sup> CDA = Combined Data Authentication, autenticación combinada.



- dd) Todas las transacciones efectuadas con tarjetas electrónicas de marca blanca deben ser procesadas a través de la interconectante desarrollada por las EATE.
- ee) Los emisores deberán prever el bloqueo de transacciones con tarjetas electrónicas por rubro de actividad en el marco de disposiciones emanadas por autoridades competentes.
- ff) Las transacciones con tarjetas electrónicas que se canalicen a través de carteras digitales (*E-wallet*) deberán cumplir con las características de seguridad descritas en esta sección.

#### 4. Billetera Móvil

- a) El emisor debe vincular al número de cuenta de billetera móvil, el nombre completo del titular, documento de identidad y el número de su línea de telefonía móvil, previa verificación positiva de la identidad del titular de la billetera móvil. Asimismo, debe mantener el registro de las operaciones procesadas por un periodo de al menos diez (10) años.
- b) Las órdenes de pago deben ser procesadas a través de medios que garanticen el cumplimiento de las siguientes características de seguridad:
- **Autenticidad:** Contar con mecanismos que permitan verificar la identidad del titular del instrumento electrónico de pago en cada transacción.
  - **Integridad:** Estar protegidos contra alteraciones originadas por contingencias tecnológicas o acciones intencionales o accidentales durante su procesamiento, transporte y almacenamiento.
  - **Confidencialidad:** Contar con mecanismos de cifrado estándar que eviten la difusión o divulgación no autorizada de la información contenida en la operación durante toda la transacción, que pueda ser utilizada para materializar eventos de fraude.
  - **No repudio:** Garantizar que ninguna de las partes implicadas en la transacción puedan negar su participación en la misma.
  - **Disponibilidad:** El sistema de procesamiento de transacciones de billetera móvil debe estar disponible para los clientes según las condiciones publicitadas, informadas o pactadas contractualmente con los consumidores financieros.

- c) El emisor debe proporcionar al usuario una contraseña para autenticarse al servicio, la cual debe ser cambiada después del primer inicio de sesión y contar con mecanismos para recordarle su cambio al menos cada noventa (90) días. En ningún momento esta clave deberá almacenarse en la billetera móvil.
- d) Los emisores deben implementar mecanismos de autenticación robusta para sus usuarios en los siguientes procesos de autorización:
- Procesamiento de las órdenes de pago.
  - Registro y modificación de los datos de beneficiarios, así como otra información sensible y confidencial cuya modificación podría facilitar la comisión de delitos o fraudes.
  - Definición y modificación de límites transaccionales.
  - Otras inherentes al procesamiento de órdenes de pago.

Al menos uno de los factores que se aplique no debe ser reutilizable, ni replicable, ni ser susceptible de ser robado vía *internet*. Cuando se utilice una contraseña de un solo uso, la vigencia de ésta no deberá ser mayor a dos (2) minutos.

Únicamente para el inicio de sesión se podrá utilizar la autenticación de un solo factor, en función del análisis y evaluación de riesgos en seguridad de la información que efectúe la entidad financiera o Empresa de Servicios de Pago (ESP).

Las operaciones de compra de saldo de telefonía móvil, estarán exentas de la aplicación del mecanismo de doble o múltiple factor de autenticación hasta un monto máximo de Bs50 (Cincuenta 00/100 Bolivianos).

Cuando se opte por el uso de mecanismos de autenticación biométrica, estos deben estar bajo el control y responsabilidad del emisor, incluyendo además métodos de prueba y/o reconocimiento de vida del usuario.

- e) Para los pagos de compra de saldo de telefonía móvil exentos de aplicación del mecanismo de autenticación robusta, los emisores deberán implementar en sus sistemas de monitoreo y seguimiento, mecanismos de control interno, parámetros estrictos de seguridad y alertas, para la prevención de fraude. Adicionalmente, deberán establecer límites transaccionales máximos diarios, semanales y mensuales predeterminados, modificables a solicitud del cliente para el procesamiento de este tipo de transacciones y que cuando estos límites sean superados, las transacciones se rechacen.



- f) Las entidades financieras y las ESP deben realizar campañas de información semestrales respecto a la seguridad del uso de billetera móvil, dirigidas a los clientes y beneficiarios de este instrumento que incluyan como mínimo:
- Descripción de las operaciones y/o funcionalidades.
  - Uso del servicio.
  - Uso de los mecanismos de autenticación robusta, describiendo la operativa y los casos de aplicación.
  - Cambios en la operativa y/o en los mecanismos de autenticación y/o procesamiento de órdenes de pago.
  - Sistema de atención de reclamos y consultas de clientes.
- g) Los emisores deben definir el tiempo máximo de inactividad en una sesión con base en una evaluación de riesgo que contemple el tipo de operación, el monto, el perfil del usuario, la frecuencia y otros factores relevantes.
- h) Los emisores deben implementar en sus sistemas de monitoreo y seguimiento, mecanismos de detección, alerta y cuando corresponda, bloqueo automatizado de operaciones inusuales para la detección de actividades sospechosas y prevención de fraude, basados en la creación de reglas de frecuencia, velocidad, montos límite, uso de dispositivo móvil de confianza y otros que respondan a un análisis y evaluación de riesgos en seguridad de la información.
- i) Las transacciones con billetera móvil que se canalicen a través de carteras digitales (*E-wallet*) deberán cumplir con las características de seguridad descritas en esta sección.



PATRICIA MARÍA MÉNDEZ SOLÍS  
SUBGERENTE DE SISTEMA DE PAGOS  
Y SERVICIOS FINANCIEROS  
BANCO CENTRAL DE BOLIVIA



ROLANDO JORGE OJMOS ALCALÁ  
GERENTE DE ENTIDADES FINANCIERAS  
BANCO CENTRAL DE BOLIVIA



## Glosario

**Autenticación:** Procedimiento que permite comprobar la identidad del titular del Instrumento Electrónico de Pago.

**Autorización:** Procedimiento para comprobar si el titular del Instrumento Electrónico de Pago tiene el derecho a realizar una determinada acción, por ejemplo, el derecho a transferir fondos o tener acceso a datos sensibles.

**Aplicación web y móvil:** Prestación de servicios financieros a través de internet u otros medios electrónicos y digitales sin necesidad de presencia física del cliente en las oficinas de la entidad financiera.

**Canales electrónicos de pago:** Son de manera enunciativa y no limitativa, los dispositivos (cajeros automáticos-ATM, terminales de punto de venta-POS), redes de comunicación (internet, telefonía fija o móvil), pasarelas de pago, carteras digitales (*E-Wallet*) o aplicativos que permiten procesar las órdenes de pago originadas con instrumentos electrónicos de pago.

**Código QR:** Matriz de puntos o código de barras bidimensional con estructura cuadrada que permite almacenar datos codificados para el procesamiento de transferencias electrónicas de fondos.

**Contraseña de un solo uso:** Número aleatorio generado por un software generador de claves (*tokens*), una combinación de números a partir de una tarjeta de coordenadas o algún otro mecanismo que se utiliza para autorizar el procesamiento de una determinada acción, cuya validez expira en un tiempo determinado.

**Dispositivo de confianza:** Computadora, tableta electrónica, teléfono inteligente u otro artefacto electrónico que permita verificar, la identidad del ordenante de la transacción y que éste se encuentre debidamente habilitado.

**Dispositivo móvil de confianza:** Tableta electrónica o teléfono inteligente que permita verificar la identidad del ordenante de la transacción y que éste se encuentre debidamente habilitado.

**Entorno seguro:** Los entornos bajo la responsabilidad del emisor en los que se garantiza una autenticación adecuada del cliente así como la protección de información confidencial y sensible.



**Mecanismo de autenticación robusta o autenticación de doble factor:** Es una forma de verificar la identidad de los usuarios basada en el uso de la combinación de al menos dos (2) de los tres (3) factores de autenticación siguientes:

- i. Algo que el usuario sabe
- ii. Algo que el usuario tiene
- iii. Algo que el usuario es

**Ordenante:** Persona natural o jurídica que inicia u origina una orden de pago desde su cuenta a favor de un beneficiario.

**Terminal Punto de Venta:** Dispositivo que permite el uso de instrumentos electrónicos de pago, físicos o virtuales en puntos de venta de bienes y/o servicios para procesar órdenes de pago por contacto o sin contacto, la información es capturada en comprobantes de papel (*vouchers*) o por terminales electrónicas diseñadas para transmitir la información. La Terminal Punto de Venta es también conocida por su sigla en inglés: POS (*Point of Sale*).

**Tokenización:** Proceso de sustitución de datos sensibles/confidenciales por un identificador o *token* único que no tiene valor intrínseco y conserva toda la información esencial sin comprometer su seguridad.