



BANCO CENTRAL DE BOLIVIA
ESTADO PLURINACIONAL DE BOLIVIA

BCB-DGD-VUC

2018 ENE -3 PM 12: 02

N°
TRAMITE GENERAL
DESPACHADO

CIRCULAR EXTERNA

La Paz, 29 de diciembre de 2017

SGDB N° 046/2017

DE: GERENCIA GENERAL
GERENCIA DE ENTIDADES FINANCIERAS
A: ENTIDADES FINANCIERAS, EMPRESAS DE SERVICIOS DE
PAGO, ACCL S.A., EDV S.A.
ASUNTO: **REQUERIMIENTOS OPERATIVOS MÍNIMOS DE SEGURIDAD
PARA INSTRUMENTOS ELECTRÓNICOS DE PAGO**

Señoras y Señores:

El Banco Central de Bolivia en el marco de sus atribuciones de regulación del sistema de pagos nacional y conforme lo establecido en el Artículo 27 del Reglamento de Servicios de Pago, Instrumentos Electrónicos de Pago, Compensación y Liquidación, aprobado mediante R.D. N°134/2015 de 28.07.15 y sus modificaciones aprobadas mediante R.D. N°071/2017 de 23.05.17 remite para su aplicación y cumplimiento la actualización a los Requerimientos Operativos Mínimos de Seguridad para:

- I. Órdenes electrónicas de transferencia de fondos.
- II. Tarjetas electrónicas.
- III. Billeteras móviles.

Los Requerimientos Operativos Mínimos de Seguridad para los citados instrumentos electrónicos de pago constituyen el marco referencial normativo para la aplicación de estándares y buenas prácticas en los sistemas de pago que operan con estos instrumentos. Se deja sin efecto la Circular Externa SGDB N° 005/2016 de 12.02.16.

Atentamente,

RONALD O. PINTO RIBERA
GERENTE DE ENTIDADES
FINANCIERAS a.i.
BANCO CENTRAL DE BOLIVIA

CCL/RPR/APM/PMS/AGA/RAI
Adj.: Lo citado

CARLOS A. COLODRO LÓPEZ
GERENTE GENERAL a.i.
BANCO CENTRAL DE BOLIVIA



BANCO CENTRAL DE BOLIVIA
ESTADO PLURINACIONAL DE BOLIVIA

I. Requerimientos Operativos Mínimos de Seguridad para Órdenes Electrónicas de Transferencia de Fondos – OETF

Los siguientes requerimientos marcan las condiciones operativas mínimas de OETF para su aplicación en el territorio nacional.

1. Los servicios transaccionales deben funcionar utilizando canales de comunicación cifrados sobre un servidor seguro bajo el protocolo SSL o TLS.
2. El sitio seguro (página *web*) debe indicar el nombre de la entidad que emite el certificado y un vínculo a la entidad certificadora que permita acceder a la siguiente información para verificar su validez: entidad certificante, nombre de la página *web*, nombre de la entidad propietaria del sitio y validez del certificado. El proveedor de los servicios transaccionales no deberá habilitar una cuenta de acceso sin previo consentimiento del cliente o titular.
3. El certificado digital estará vigente hasta la fecha de expiración indicada en el mismo. En ningún caso la vigencia del certificado digital debe ser superior a la definida en el Reglamento de Firma Digital para el Sistema de Pagos emitido por el BCB.
4. Las entidades financieras deben implementar en su operativa, a través de portales de *internet* y banca móvil, mecanismos de autenticación robusta. Es decir, establecer al menos doble factor para la autenticación de usuarios en las siguientes instancias operativas:
 - a) Inicio de sesión en la aplicación móvil o portal de banca por *internet*.
 - b) Autorización para el procesamiento de las OETF.
 - c) Autorización para la introducción y modificación de los datos de beneficiarios u otra información sensible cuya modificación podría facilitar la comisión de delitos o fraudes.
 - d) Otras autorizaciones que involucren el procesamiento de OETF, como por ejemplo habilitación de tarjeta de débito para pagos por *internet*.

Al menos uno de los factores que se aplique no debe ser reutilizable ni replicable ni ser susceptible de ser robado vía *internet* (por ejemplo, una contraseña de un solo uso específica para un pago y generada por un *software* generador de claves (*tokens*) o una combinación de números a partir de una tarjeta de coordenadas, etc).

Handwritten signature in blue ink, consisting of stylized letters 'P', 'Q', and 'R'.



BANCO CENTRAL DE BOLIVIA
ESTADO PLURINACIONAL DE BOLIVIA

5. Las transferencias de fondos deberán ser abonadas a las cuentas de los clientes 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.
6. Las OETF deben cumplir con las siguientes características:
 - a) Autenticidad. Deben contar con mecanismos que permitan verificar la identidad del titular del instrumento electrónico de pago.
 - b) Integridad. Deben tener la cualidad de estar protegidos contra alteraciones accidentales o fraudulentas durante su procesamiento, transporte y almacenamiento.
 - c) Confidencialidad. Deben contar con mecanismos de cifrado estándar que eviten la difusión o divulgación no autorizada de la información contenida en la operación.
 - d) No repudio. Deben garantizar que ninguna de las partes implicadas en la transacción puedan negar su participación en la misma.
 - e) Disponibilidad. El emisor en el ámbito de su control debe garantizar que el sistema de procesamiento esté disponible para los usuarios según las condiciones publicitadas, informadas o pactadas con los consumidores financieros y lo establecido contractualmente.
7. 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 punto 6.
8. 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.
9. Las entidades financieras deben realizar campañas de información con respecto a la seguridad del uso del instrumento dirigidas a los usuarios de OETF que además incluyan:
 - a) Descripción de las operaciones y/o funcionalidades.
 - b) Uso del servicio.
 - c) Uso de los mecanismos de autenticación robusta: operativa y casos de aplicación.
 - d) Cambios en la operativa y/o mecanismos de autenticación y/o procesamiento de órdenes de pago.
 - e) Sistema de atención de reclamos y consultas de clientes.



BANCO CENTRAL DE BOLIVIA
ESTADO PLURINACIONAL DE BOLIVIA

Abreviaturas

SSL = *Secure Sockets Layer*, capa de conexión segura
TLS = *Transport Layer Security*, seguridad de la capa de transporte

Glosario

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

Autenticación de doble factor o mecanismo de autenticación robusta: Es una forma de verificar la identidad de los usuarios basada en el uso de la combinación de dos de los tres factores de autenticación siguientes:

- ♦ Algo que el usuario sabe
- ♦ Algo que el usuario tiene
- ♦ Algo que el usuario es

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.

2



BANCO CENTRAL DE BOLIVIA
ESTADO PLURINACIONAL DE BOLIVIA

II. Requerimientos Operativos Mínimos de Seguridad para Tarjetas Electrónicas

Los siguientes requerimientos marcan las condiciones operativas mínimas de las tarjetas electrónicas para su aplicación en el territorio nacional.

1. Las tarjetas electrónicas deben ser emitidas de manera física y pueden ser utilizadas de manera virtual a solicitud del titular.
2. Las tarjetas electrónicas 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. La tarjeta de crédito debe incluir fecha de vencimiento.
3. 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.
4. Cuando se trate de tarjetas de débito o prepagadas, 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.
5. La banda magnética de las tarjetas electrónicas debe contener la siguiente información: número de cuenta principal (PAN), fecha de vencimiento, valor de verificación del PIN, valor de verificación de la tarjeta (CVV) y código de servicio. Esta información debe ser validada por el emisor al momento de procesar las transacciones.
6. El código de validación de la tarjeta (CAV2, CID, CVC2, CVV2) o los datos de validación del PIN no deben poder almacenarse en sistemas o bases de datos.
7. 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.
8. Las Empresas Administradoras de Tarjetas Electrónicas que procesen transacciones con tarjetas electrónicas deberán comunicar con una anticipación de 30 días calendario a sus participantes, al BCB y la ASFI las actualizaciones que se realicen al estándar ISO 8583.



BANCO CENTRAL DE BOLIVIA
ESTADO PLURINACIONAL DE BOLIVIA

9. Las habilitaciones de tarjetas electrónicas para compras en *internet* y el procesamiento de pagos en *internet* en páginas *web* de comercios nacionales se deben realizar en entornos seguros y de confianza.
10. 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 de los factores que se aplique no debe ser reutilizable ni replicable ni ser susceptible de ser robado vía *internet* (por ejemplo, una contraseña de un solo uso específica para un pago y generada por un *software* generador de claves (*tokens*), una combinación de números a partir de una tarjeta de coordenadas, etc).
11. Como mecanismo de autenticación robusta para tarjetas con chip el titular o usuario del instrumento, para realizar compras presenciales en comercios con tarjetas electrónicas, deberá introducir el PIN una vez que el encargado del comercio introduzca el monto de la compra, el cual deberá estar visible para seguridad y certeza del titular o usuario. En este sentido, los emisores deben prever en el diseño del instrumento que el código de servicio requiera la introducción del PIN para realizar transacciones.
12. Cuando se utilice tarjetas con chip para procesar compras presenciales en comercios, no se emitirá un voucher impreso para el cliente, a no ser que éste lo solicite, en cuyo caso no requerirá firma manuscrita.
13. Para el caso de tarjetas electrónicas de emisores del exterior que cuenten exclusivamente con banda magnética para su procesamiento en comercios de Bolivia el titular o usuario del instrumento al momento de realizar una compra presencial deberá introducir su PIN o presentar su documento de identificación y firmar los comprobantes de la transacción.
14. Los adquirentes deben instruir a los comercios procesar las transacciones siempre utilizando la lectura del chip.
15. Las comisiones que pagan los comercios a las Empresas Administradoras de Tarjetas Electrónicas no podrán ser transferidas al titular o usuario de la tarjeta electrónica.
16. Las disputas o reclamos por el procesamiento de transacciones recaerán sobre las entidades emisoras o adquirentes que no operen con tarjeta chip bajo el estándar EMV de la siguiente manera:
 - a) La responsabilidad por transacciones procesadas con banda magnética en terminales que no tengan la capacidad de procesar tarjetas con chip, será del adquirente.



BANCO CENTRAL DE BOLIVIA

ESTADO PLURINACIONAL DE BOLIVIA

- b) La responsabilidad por transacciones procesadas con tarjetas solamente de banda magnética en una terminal que tenga habilitada la lectura de chip, será del emisor que no opere bajo el estándar EMV.
- 17. Se deben aplicar algoritmos de cifrado estándar para autenticar la tarjeta con chip y los datos de la operación.
- 18. Para verificar la identidad del tarjetahabiente también se pueden utilizar sistemas biométricos de autenticación.
- 19. En caso de que el emisor autorice la realización de operaciones fuera de línea, las tarjetas de pago deberán utilizar un mecanismo de autenticación de la tarjeta (CAM) dinámico de tipo DDA o CDA que permita recalcular el valor de la firma digital en cada transacción para lo que deben estar equipadas con un criptoprocador.
- 20. 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.

Abreviaturas

CAM = *Card Authentication Method*, método de autenticación de la tarjeta
CVV = *Card Verification Value*, valor de verificación de la tarjeta
CDA = *Combined Data Authentication*, autenticación combinada
DDA = *Dynamic Data Authentication*, autenticación dinámica
EMV = Europay, MasterCard y Visa
PAN = *Primary Account Number*, número de cuenta primaria
CAV2 = *Card Security Code*, código de validación de la tarjeta para JCB
CID = *Card Security Code*, código de validación de la tarjeta para *American Express*
CVC2 = *Card Security Code*, código de validación de la tarjeta para MasterCard
CVV2 = *Card Security Code*, código de validación de la tarjeta para VISA
PIN = *Personal Identification Number*, número de identificación personal

Glosario

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

Autenticación de doble factor o mecanismo de autenticación robusta: Es una forma de verificar la identidad de los usuarios basada en el uso de la combinación de dos de los tres factores de autenticación siguientes:

- ★ Algo que el usuario sabe



BANCO CENTRAL DE BOLIVIA
ESTADO PLURINACIONAL DE BOLIVIA

- ♦ Algo que el usuario tiene
- ♦ Algo que el usuario es

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.

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.

P
Z
/



BANCO CENTRAL DE BOLIVIA
ESTADO PLURINACIONAL DE BOLIVIA

III. Requerimientos Operativos Mínimos de Seguridad para Billeteras Móviles

Los siguientes requerimientos marcan las condiciones operativas mínimas de las billeteras móviles para su aplicación en el territorio nacional.

1. El emisor debe vincular al número de cuenta de billetera móvil, el nombre completo del titular, documento de identidad, número de dispositivo móvil, siempre y cuando previamente se efectúe la verificación positiva de la identidad del titular de la billetera móvil. Asimismo, el emisor debe mantener el registro de las operaciones procesadas por un periodo de al menos diez (10) años.
2. Las órdenes de pago deben ser procesadas a través de medios que garanticen el cumplimiento de las siguientes características de seguridad:
 - a) Autenticidad. Deben contar con mecanismos que permitan verificar la identidad del titular del instrumento electrónico de pago en cada transacción.
 - b) Integridad. Deben tener la cualidad de estar protegidos contra alteraciones accidentales o fraudulentas durante su procesamiento, transporte y almacenamiento.
 - c) Confidencialidad. Deben 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.
 - d) No repudio. Deben garantizar que ninguna de las partes implicadas en la transacción puedan negar su participación en la misma.
 - e) Disponibilidad. El emisor debe garantizar que el sistema de procesamiento esté disponible para los usuarios según las condiciones publicitadas, informadas o pactadas con los consumidores financieros y lo establecido contractualmente.
3. El usuario debe tener una contraseña para autenticarse al servicio. El emisor debe generar mecanismos para recordarle al usuario cambiar su contraseña con periodicidad, al menos cada noventa (90) días. En ningún momento esta clave deberá almacenarse en la billetera móvil.



BANCO CENTRAL DE BOLIVIA
ESTADO PLURINACIONAL DE BOLIVIA

4. Las entidades financieras y las ESP deben implementar mecanismos de autenticación robusta. Es decir, establecer al menos un doble factor para la autenticación de usuarios en las siguientes instancias operativas:
- a) Inicio de sesión.
 - b) Autorización para el procesamiento de las órdenes de pago.
 - c) Autorización para la introducción y modificación de los datos de beneficiarios u otra información sensible cuya modificación podría facilitar la comisión de delitos o fraudes.
 - d) Otras autorizaciones que involucren el procesamiento de órdenes de pago como por ejemplo pagos en comercios o compras por *internet*.

Al menos uno de los factores que se aplique no debe ser reutilizable ni replicable ni ser susceptible de ser robado vía *internet* (por ejemplo, una contraseña de un solo uso específica para un pago y generada por un software generador de, claves (*tokens*), una combinación de números a partir de una tarjeta de coordenadas, etc).

5. El emisor debe prever que el tiempo máximo de inactividad en una sesión no supere los sesenta (60) segundos.
6. Las entidades financieras y las ESP deben realizar campañas de información con respecto a la seguridad del uso del instrumento dirigidas a los usuarios de billeteras móviles que además incluyan:
- a) Descripción de las operaciones y/o funcionalidades
 - b) Uso del servicio
 - c) Uso de los mecanismos de autenticación robusta: operativa y casos de aplicación.
 - d) Cambios en la operativa y/o en los mecanismos de autenticación y/o procesamiento de órdenes de pago.
 - e) Sistema de atención de reclamos y consultas de clientes.

Abreviaturas

ESP = Empresa de Servicios de Pago



BANCO CENTRAL DE BOLIVIA
ESTADO PLURINACIONAL DE BOLIVIA

Glosario

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

Autenticación de doble factor o mecanismo de autenticación robusta: Es una forma de verificar la identidad de los usuarios basada en el uso de la combinación de dos de los tres factores de autenticación siguientes:

- ♦ Algo que el usuario sabe
- ♦ Algo que el usuario tiene
- ♦ Algo que el usuario es

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.