BANCO CENTRAL DE BOLIVIA
ESTADO PLURINACIONAL DE BOLIVIA

CIRCULAR EXTERNA

La Paz, 2 de enero de 2020
CIEX N° 3/2020

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 del Artículo 27 del Reglamento de Servicios de Pago, Instrumentos Electrónicos de Pago, Compensación y Liquidación (RSPIEPCL), aprobado mediante Resolución de Directorio del BCB N° 137/19 de 08.10.2019, remite para su aplicación y cumplimiento la actualización de los Requerimientos Operativos Mínimos de Seguridad para:

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

Estos requerimientos constituyen el marco referencial normativo para la aplicación de estándares y buenas prácticas en los sistemas de pago que operan con instrumentos electrónicos de pago. Se deja sin efecto la Circular Externa SGDB N° 046/2017 de 29.12.17 y SGDB N° 011/2018 de 16.02.2018 de Requerimientos Operativos Mínimos de Seguridad para Instrumentos Electrónicos de Pago.

Atentamente,

JULIO HUMEREZ QUIROZ
GERENTE DE ENTIDADES FINANCIERAS a.i.
BANCO CENTRAL DE BOLIVIA

DAVID ESPINOZA TORRICO
GERENTE GENERAL a.i.
BANCO CENTRAL DE BOLIVIA

DIET/JHQ/ropr/pmms/jmkt.
Adj.: Lo citado

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

1. Los servicios transaccionales deben operar utilizando canales de comunicación cifrados sobre un servidor seguro bajo el protocolo SSL o TLS.
2. La página *web* segura debe indicar el nombre de la entidad que emite el certificado digital de sitio seguro y un vínculo a la entidad certificadora que permita validar: 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) Autorización para el procesamiento de las OETF.
    b) Autorización para la introducción y modificación de los datos de beneficiarios u otra información sensible, cuya modificación podría dar lugar a la comisión de delitos o fraudes.
    c) Otras autorizaciones que involucren el procesamiento de OETF, como la 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.* En este sentido es factible utilizar una contraseña de un solo uso, generada por un *software* generador de claves (*tokens),* o una combinación de números a partir de una tarjeta de coordenadas.

El uso de doble factor de autenticación en el inicio de sesión es opcional.

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:

Calle Ayacucho esquina Mercado - Teléfono: (591-2) 2409090 - Fax: (591-2) 2661590
www.bcb.gob.bo - bancocentraldebolivia@bcb.gob.bo - La Paz – Bolivia

a) Autenticidad. Contar con mecanismos que permitan la verificación de la identidad del titular del instrumento electrónico de pago.

b) Integridad. Estar protegidas contra alteraciones accidentales o fraudulentas durante su procesamiento, transporte y almacenamiento.

c) Confidencialidad. Contar con mecanismos de cifrado estándar que eviten la difusión o divulgación no autorizada de la información contenida en la operación.

d) No repudio. Garantizar que ninguna de las partes implicadas en la transacción pueda 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 contractualmente con los consumidores financieros.

7. El intercambio de información entre las entidades financieras y las empresas proveedoras de servicios externos de tecnologías debe 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 debe 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 para informar 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.

Calle Ayacucho esquina Mercado - Teléfono: (591-2) 2409090 - Fax: (591-2) 2661590
www.bcb.gob.bo - bancocentraldebolivia@bcb.gob.bo - La Paz – 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.

Calle Ayacucho esquina Mercado - Teléfono: (591-2) 2409090 - Fax: (591-2) 2661590
www.bcb.gob.bo - bancocentraldebolivia@bcb.gob.bo - La Paz – Bolivia

II. Requerimientos Operativos Mínimos de Seguridad para Tarjetas Electrónicas

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 figuren en el recibo generado por la terminal, cuando se imprima 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 deben 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.
9. Las habilitaciones de tarjetas electrónicas para compras en *internet* y el procesamiento de pagos en *internet* en páginas *web* de establecimientos

Calle Ayacucho esquina Mercado - Teléfono: (591-2) 2409090 - Fax: (591-2) 2661590
www.bcb.gob.bo - bancocentraldebolivia@bcb.gob.bo - La Paz – Bolivia

comerciales o de servicios 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 pagos presenciales en establecimientos comerciales o de servicios con tarjetas electrónicas, debe introducir el PIN una vez que el encargado del establecimiento introduzca el monto de la transacción, 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.

    Las transacciones presenciales con tarjetas de tecnología sin contacto (*contactless*) estarán exentas de la aplicación del PIN hasta un monto máximo de Bs150 (Ciento cincuenta Bolivianos).

12. Cuando se utilice tarjetas con *chip* para procesar pagos presenciales en establecimientos comerciales o de servicios, no será necesaria la firma manuscrita ni se emitirá un recibo (*voucher)* impreso para el cliente, a no ser que éste lo solicite.

13. 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 debe presentar su documento de identificación y firmar los comprobantes de la transacción.

14. Los adquirentes deben instruir a los establecimientos comerciales o de servicios procesar las transacciones siempre utilizando la lectura del chip.

15. Las comisiones que pagan los establecimientos comerciales o de servicios a las Empresas Administradoras de Tarjetas Electrónicas no se pueden transferir 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:

Calle Ayacucho esquina Mercado - Teléfono: (591-2) 2409090 - Fax: (591-2) 2661590
www.bcb.gob.bo - bancocentraldebolivia@bcb.gob.bo - La Paz – Bolivia

a) La responsabilidad por transacciones procesadas con banda magnética en terminales que no tengan la capacidad de procesar tarjetas con chip, será del adquirente.

b) 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.

17. Se deben aplicar algoritmos de cifrado estándar para autenticar la tarjeta con *chip* y los datos de la operación.

18. Adicionalmente a los factores de autenticación robusta con el uso de PIN, se pueden utilizar sistemas biométricos de autenticación para verificar la identidad del tarjetahabiente.

19. En caso de que el emisor autorice la realización de operaciones fuera de línea, las tarjetas deben utilizar un mecanismo de autenticación dinámico (CAM) 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 criptoprocesador.

20. El sistema operativo de las tarjetas podrá ser de plataforma nativa o abierta, ambos deben tener la capacidad de manejar DDA o CDA, en caso que el emisor acepte el procesamiento de transacciones fuera de línea.

21. 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. Entre dichas medidas, deben establecer para sus clientes un monto límite diario para este tipo de transacciones, modificable a solicitud del titular, para que cuando éste sea superado las transacciones sean rechazadas.

22. Los emisores deben proporcionar a sus clientes mecanismos seguros que les permitan habilitar y deshabilitar el uso de PIN en transacciones presenciales con tarjetas de tecnología sin contacto *(contactless)*.

Calle Ayacucho esquina Mercado - Teléfono: (591-2) 2409090 - Fax: (591-2) 2661590
www.bcb.gob.bo - bancocentraldebolivia@bcb.gob.bo - La Paz – Bolivia

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
- 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.

III.

Calle Ayacucho esquina Mercado - Teléfono: (591-2) 2409090 - Fax: (591-2) 2661590
www.bcb.gob.bo - bancocentraldebolivia@bcb.gob.bo - La Paz – Bolivia

IV. Requerimientos Operativos Mínimos de Seguridad para Billetera Móvil

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, debe mantener el registro de las operaciones procesadas por un periodo de al menos diez (10) años.

2. Las órdenes de pago deben procesarse a través de medios que garanticen el cumplimiento de las siguientes características de seguridad:

    a) Autenticidad. Contar con mecanismos que permitan verificar la identidad del titular del instrumento electrónico de pago en cada transacción.

    b) Integridad. Estar protegidos contra alteraciones accidentales o fraudulentas durante su procesamiento, transporte y almacenamiento.

    c) 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.

    d) No repudio. Garantizar que ninguna de las partes implicadas en la transacción pueda negar su participación en la misma.

    e) Disponibilidad. El sistema de procesamiento debe estar disponible para los usuarios según las condiciones publicitadas, informadas o pactadas contractualmente con los consumidores financieros.

3. El emisor debe proporcionar al usuario una contraseña para autenticarse al servicio y generar mecanismos para recordarle su cambio al menos cada noventa (90) días. En ningún momento esta contraseña deberá almacenarse en la billetera móvil.

4. Los emisores 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) Autorización para el procesamiento de las órdenes de pago.

    b) Autorización para la introducción y modificación de los datos de beneficiarios u otra información sensible, cuya modificación podría dar lugar a la comisión de delitos o fraudes.

Calle Ayacucho esquina Mercado - Teléfono: (591-2) 2409090 - Fax: (591-2) 2661590
www.bcb.gob.bo - bancocentraldebolivia@bcb.gob.bo - La Paz – Bolivia

c) Otras autorizaciones que involucren el procesamiento de órdenes de pago como o compras por internet o establecimientos comerciales y de servicios.

Al menos uno de los factores que se aplique no debe ser reutilizable ni replicable ni ser susceptible de ser robado vía internet. En este sentido es factible utilizar una contraseña de un solo uso, generada por un software generador de claves (tokens), o una combinación de números a partir de una tarjeta de coordenadas.

El uso de doble factor de autenticación en el inicio de sesión es opcional.

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 Bs20 (Veinte Bolivianos).

5. 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 internos, parámetros estrictos de seguridad y alertas, para la prevención de fraude. Adicionalmente, deberán establecer límites para las transacciones, modificables a solicitud del cliente, para que cuando éstos sean superados las transacciones sean rechazadas.

6. Los emisores deben realizar campañas de información sobre 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.

7. El tiempo máximo de inactividad en una sesión no debe superar los 60 segundos.

Calle Ayacucho esquina Mercado - Teléfono: (591-2) 2409090 - Fax: (591-2) 2661590
www.bcb.gob.bo - bancocentraldebolivia@bcb.gob.bo - La Paz – Bolivia

Abreviaturas

ESP = Empresa de Servicios de Pago

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.

Calle Ayacucho esquina Mercado - Teléfono: (591-2) 2409090 - Fax: (591-2) 2661590
www.bcb.gob.bo - bancocentraldebolivia@bcb.gob.bo - La Paz – Bolivia