BANCO CENTRAL DE BOLIVIA | ESTADO PLURINACIONAL DE BOLIVIA

CIRCULAR EXTERNA

La Paz, 22 de junio de 2022
CIEX N° 26/2022

DE: GERENCIA GENERAL
GERENCIA DE ENTIDADES FINANCIERAS

A: ENTIDADES FINANCIERAS, EMPRESAS DE SERVICIOS DE PAGO, ACCL S.A., UNILINK S.A., EDV S.A.

ASUNTO: REQUERIMIENTOS OPERATIVOS MÍNIMOS DE SEGURIDAD PARA INSTRUMENTOS ELECTRÓNICOS DE PAGO

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 (RSPIEPCL), aprobado mediante Resolución de Directorio del BCB N° 069/2021 de 27.04.2021 y sus modificaciones, remite para su aplicación y cumplimiento la actualización a los Requerimientos Operativos Mínimos de Seguridad para:

I. Órdenes electrónicas de transferencia de fondos.
II. Canales electrónicos de pago.
III. Tarjetas electrónicas.
IV. Billeteras móviles.

Los Requerimientos Operativos Mínimos de Seguridad para los citados instrumentos y canales 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 CIEX N° 08/2021 de 24.02.2021.

Atentamente.

DOCUMENTO FIRMADO DIGITALMENTE

Rolando Sergio Colque Soldado
GERENTE DE ENTIDADES FINANCIERAS

Rubén Gonzalo Ticona Chique
GERENTE GENERAL

Validar firmas digitales en: validar.firmadigital.bo
RGTCH/RSCS/ampm/pmms

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

1. Los servicios transaccionales deben funcionar utilizando canales de comunicación cifrados sobre un servidor seguro bajo el protocolo TLS en su versión 1.2 o superior, aplicando las actualizaciones de seguridad que correspondan.
2. El sitio *web* debe tener un certificado digital de conexión segura, emitido por una entidad certificadora que permita validar la siguiente información: la entidad certificante, el nombre de la página *web*, la razón social de la entidad financiera propietaria del sitio y el tiempo de validez del certificado.

   En ningún caso la vigencia de este certificado digital debe ser superior a la definida en el Reglamento de Firma Digital para el Sistema de Pagos emitido por el BCB.
3. La entidad financiera no deberá habilitar una cuenta de acceso a una aplicación *web* o móvil, que permita el procesamiento de OETF, sin previo consentimiento del cliente o titular de la cuenta asociada.
4. 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:

   a) Procesamiento de OETF.

   b) 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.

   c) Habilitación de tarjetas electrónicas para pagos por *internet*, así como para su uso en el extranjero.

   d) Definición y modificación de límites transaccionales.

   e) Otros inherentes al procesamiento de OETF.

   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.
5. 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.

6. Las OETF deben cumplir con las siguientes características:
   a) Autenticidad. Contar con mecanismos que permitan verificar la identidad del titular del instrumento electrónico de pago y que éste se encuentre debidamente autorizado.
   b) Integridad. Estar protegidas contra alteraciones originadas por contingencias tecnológicas, acciones intencionales o accidentales 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 que pueda ser utilizada para materializar eventos de fraude.
   d) No repudio. Garantizar que ninguna de las partes implicadas en la transacción pueda negar su participación en la misma.
   e) 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.
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 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.
10. Las entidades financieras deben realizar campañas de información con 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:

a) Descripción de las operaciones y/o funcionalidades.
b) Uso del servicio.
c) Utilización de los mecanismos de autenticación robusta, describiendo su operativa y los casos de aplicación.
d) Sistema de atención de reclamos y consultas de clientes.

Abreviaturas

OETF = Órdenes Electrónicas de Transferencia de Fondos
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.

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

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 y 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.

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.

II. Requerimientos Operativos Mínimos de Seguridad para canales electrónicos de pago (banca electrónica y banca móvil)

1. Las entidades 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.
2. Las entidades 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.
3. Las entidades deben garantizar que sus aplicaciones *web* y móviles no almacenen información sensible y/o confidencial en 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.
4. Las aplicaciónes *web* y móviles no deben exponer los datos del usuario en el inicio de sesión.
5. 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.
6. Se debe implementar controles de seguridad, seguimiento y notificación de acceso de dispositivos electrónicos a aplicaciones *web* y móviles.
7. Se debe implementar mecanismos de registro/vinculación de dispositivos para acceso a servicios electrónicos, detección de redes no seguras y monitoreo de transacciones sospechosas.
8. 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 firma digital sin costo adicional para el cliente.
9. Los mensajes de comunicación que remitan los emisores a través de correo electrónico y/o 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.

Abreviaturas

HTML = *HyperText Markup Language*, lenguaje de marcado para la elaboración de páginas *web*
SMS = *Short Message Service*, servicio de mensajes cortos

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.

Banca electrónica: Es la 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 o aplicativos que permiten procesar las órdenes de pago originadas con instrumentos electrónicos de pago.

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 y que se utiliza para autorizar el procesamiento de una determinada acción, cuya validez expira en un tiempo determinado.

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

III. Requerimientos Operativos Mínimos de Seguridad para Tarjetas Electrónicas

1. Las tarjetas electrónicas emitidas de manera física 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 y 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 a sus participantes, al BCB y a ASFI cada actualización que se realice al estándar ISO 8583 en un plazo de cinco (5) días hábiles posteriores a la actualización.
9. Las entidades financieras deben implementar en sus aplicaciones *web* y móviles las siguientes funcionalidades sin costo para el cliente:
    a) Habilitación y deshabilitación de tarjetas electrónicas para compras por *internet* y para uso en el exterior.
    b) 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.

10. 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.

11. 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 un monto máximo de Bs150 (Ciento cincuenta bolivianos) para tarjetas de débito y Bs250 (Doscientos cincuenta bolivianos) para 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.

12. 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:

    a) 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.

    b) 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.

    c) 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.

13. 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.

14. 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 Bs150 (Ciento cincuenta bolivianos).

15. 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.

16. 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.

17. Los adquirentes deben instruir a los establecimientos comerciales o de servicios procesar las transacciones siempre utilizando la lectura del chip, salvo en el caso de pagos con tecnología sin contacto (*contactless)*.

18. 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.

19. Las disputas o reclamos por el procesamiento de transacciones recaerán sobre las entidades emisoras o adquirentes que no operen con tarjetas con 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.

    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.

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

21. 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.
22. 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.
23. 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.
24. 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 limite y otros que permitan controlar la cantidad de transacciones que se aprueban bajo la tecnología sin contacto 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.
25. 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.
26. 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.
27. Los emisores deberán reemplazar la totalidad de su parque de tarjetas en circulación que solamente cuenten con chip por tarjetas que incluyan tecnología sin contacto (*contactless*) hasta el 30 de junio de 2023.

Abreviaturas

CAM = *Card Authentication Method,* método de autenticación de la tarjeta
CAV2 = *Card Security Code*, código de validación de la tarjeta para JCB

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

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.

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 y que se utiliza para autorizar el procesamiento de una determinada acción, cuya validez expira en un tiempo determinado.

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

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*).

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 y el número de su línea de telefonía 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 ser procesadas 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 originadas por contingencias tecnológicas o acciones intencionales o accidentales 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, que pueda ser utilizada para materializar eventos de fraude.

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

   e) 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.

3. 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.

4. Los emisores deben implementar mecanismos de autenticación robusta para sus usuarios en los siguientes procesos de autorización:

   a) Procesamiento de las órdenes de pago.

b) 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.

c) Definición y modificación de límites transaccionales.

d) 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 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 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 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.

6. Las entidades financieras y las ESP deben realizar campañas de información semestrales con respecto a la seguridad del uso de billetera móvil, dirigidas a los clientes y beneficiarios de este instrumento que incluyan como mínimo:

   a) Descripción de las operaciones y/o funcionalidades.

   b) Uso del servicio.

   c) Uso de los mecanismos de autenticación robusta, describiendo la operativa y los 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. 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.

8. 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.

Abreviaturas

ESP = Empresa de Servicios de Pago

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.

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 y que se utiliza para autorizar el procesamiento de una determinada acción, cuya validez expira en un tiempo determinado.

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.

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:

iv. Algo que el usuario sabe
v. Algo que el usuario tiene
vi. 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.