RESOLUCIÓN Nro. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009

JORGE ANDRÉS MONCAYO LARA
SUPERINTENDENTE DE ECONOMÍA POPULAR Y SOLIDARIA
SUBROGANTE

CONSIDERANDO:

Que, los numerales 1 y 7 del artículo 62, en concordancia con el inciso segundo del artículo 74 del Libro 1 del Código Orgánico Monetario y Financiero, determinan como funciones de la Superintendencia de Economía Popular y Solidaria ejercer la vigilancia, auditoría, control y supervisión de las disposiciones de dicho Código y de las regulaciones dictadas por la Junta de Política y Regulación Financiera, en lo que corresponde a las actividades financieras ejercidas por las entidades que conforman el sector financiero popular y solidario; y,

Que, velar por la estabilidad, solidez y correcto funcionamiento de las entidades sujetas a su control y, en general, vigilar que cumplan las normas que rigen su funcionamiento, las actividades financieras que presten, mediante la supervisión permanente preventiva extra situ y visitas de inspección in situ, que permitan determinar la situación económica y financiera de las entidades, el manejo de sus negocios, evaluar la calidad y control de la gestión de riesgo y verificar la veracidad de la información que generan;

Que, el último inciso del artículo 62 del aludido Código determina que, para el cumplimiento de sus funciones, la Superintendencia podrá expedir las normas en las materias propias de su competencia, sin que puedan alterar o innovar las disposiciones legales ni las regulaciones que expida la Junta de Política y Regulación Financiera;

Que, los incisos segundo, tercero y quinto del artículo 74 del mencionado Código, establecen: *"(...) A la Superintendencia le compete el control de las entidades del sector financiero popular y solidario acorde a lo determinado en este Código.*

La Superintendencia de Economía Popular y Solidaria, en su organización, funcionamiento y funciones de control y supervisión del sector financiero popular y solidario, se regirá por las disposiciones de este Código y la Ley Orgánica, de Economía Popular y Solidaria.

La Superintendencia de Economía Popular y Solidaria, además de las atribuciones que le otorga la Ley Orgánica de Economía Popular y Solidaria, tendrá las funciones determinadas en los artículos 71 y 62 excepto los numerales

19 y 28, y el numeral 10 se aplicará reconociendo que las entidades de la economía popular y solidaria tienen capital ilimitado. Los actos expedidos por la Superintendencia de Economía Popular y Solidaria gozarán de la presunción de legalidad y se sujetarán a lo preceptuado en la normativa legal vigente, respecto de su impugnación, reforma o extinción.";

Que, en el artículo 163 del referido Código, determina que las cooperativas de ahorro y crédito, las cajas centrales, las asociaciones mutualistas de ahorro y crédito para la vivienda y las empresas de servicios auxiliares del sistema financiero calificadas por la Superintendencia de Economía Popular y Solidaria en el ámbito de su competencia; entre otras forman parte del sector financiero popular y solidario;

Que, el artículo 444 del Código Orgánico Monetario y Financiero, determina que las entidades financieras populares y solidarias están sometidas a la regulación de la Junta de Política y Regulación Monetaria y Financiera y al control de la Superintendencia de Economía Popular y Solidaria, quienes en las políticas que emitan tendrán presente la naturaleza y características propias del sector financiero popular y solidario;

Que, la Ley Orgánica de la Economía Popular y Solidaria, en el numeral 6 del artículo 132, establece que las organizaciones que conforman la Economía Popular y Solidaria podrán utilizar medios de pago complementarios, sea a través de medios físicos o electrónicos, para facilitar el intercambio y la prestación de bienes y servicios, dentro de las prescripciones establecidas en la Ley, su Reglamento y las regulaciones que para el efecto emita el órgano regulador competente;

Que, los literales b) y g) del artículo 151 ejusdem establecen como atribuciones del Superintendente de Economía Popular y Solidaria dictar las normas de control; y, delegar algunas de sus facultades, siempre en forma concreta y precisa, a los funcionarios que juzgue del caso;

Que, mediante Resolución Nro. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103 de 23 de noviembre de 2017, la Superintendencia de Economía Popular y Solidaria expidió la "*NORMA DE CONTROL DE LAS SEGURIDADES EN EL USO DE TRANSFERENCIAS ELECTRÓNICAS*", misma que fue reformada por la resolución número SEPS-IGT-IR-ISF-ITIC-IGJ-2017-113, de 21 de diciembre de 2017;

Que, en virtud de la Resolución Nro. PLE-CPCCS-T-O-081-13-08-2018, emitida por el Consejo de Participación Ciudadana y Control Social Transitorio el 13 de agosto de 2018, el pleno de la Asamblea Nacional posesionó como

Superintendente de Economía Popular y Solidaria a la doctora Sofía Margarita Hernández Naranjo el 04 de septiembre de 2018;

Que, conforme consta en la Acción de Personal Nro. 1395 de 24 de septiembre de 2021, el Intendente General de Desarrollo Organizacional, delegado por la señora Superintendente de Economía Popular y Solidaria, nombró como Intendente General Técnico, al señor Jorge Andrés Moncayo Lara; y,

Que, mediante Acción de Personal Nro. 598 de 28 de marzo de 2023, la Intendente Nacional Administrativa Financiera, delegada por la Superintendente de Economía Popular y Solidaria, resolvió la subrogación de Jorge Andrés Moncayo Lara en las funciones del puesto de Superintendente de Economía Popular y Solidaria desde el 03 de abril de 2023 al 16 de abril de 2023.

En ejercicio de sus funciones, resuelve expedir la siguiente:

NORMA DE CONTROL DE SEGURIDADES EN EL USO DE CANALES ELECTRÓNICOS PARA LAS ENTIDADES FINANCIERAS CONTROLADAS POR LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

SECCIÓN I
AMBITO, OBJETO Y DEFINICIONES

Artículo. 1.- Ámbito.- La presente norma es aplicable a las cooperativas de ahorro y crédito, asociaciones mutualistas de ahorro y crédito para la vivienda, cajas centrales, en adelante "entidad o entidades", que operan a través de canales electrónicos.

Artículo. 2.- Objeto.- La presente norma tiene como objeto regular las medidas de seguridad mínimas que deben cumplir las entidades y empresas auxiliares que operen y ofrezcan servicios por medio de canales electrónicos, a través de los cuales se recopila, procesa, transmite y almacena información de los productos y servicios financieros.

Artículo. 3.- Definiciones.- Los términos utilizados en la presente norma tendrán el siguiente significado:

1. **Activos de información críticos**.- Son aquellos que presentan un riesgo ya que se encuentran directamente asociados a las actividades de las entidades.
2. **Administrador del convenio de asociación.-** Es la entidad que proporciona servicios a los intervinientes del convenio de asociación y que se encarga de la representación y correcta implementación del mismo.

3. **Autorización de accesos:** Acto por el cual se permite acceder a los usuarios a zonas restringidas, a distintos equipos y/o servicios, después de haber superado el proceso de autenticación.
4. **Autenticar:** Proceso, dispositivo o sistema utilizado para la comprobación de credenciales de acceso y la verificación de la identidad de un usuario.
5. **Autenticación de múltiples factores:** Es la combinación de al menos dos factores para garantizar que el usuario que se autentica es realmente quien dice ser. Toda autenticación fuerte es, además, una autenticación multifactor, donde el usuario verifica su identidad tantas veces como factores se combinen.
6. **Billeteras digitales (Wallet):** Interfaz o software que permite a los usuarios realizar transferencias o transacciones en dinero y pagos de manera digital.
7. **Banca Móvil:** Canal digital que utiliza un aplicativo móvil para tener acceso a servicios y transacciones financieras.
8. **Banca en línea:** Canal digital asociado a cuentas de depósito, líneas de crédito o cuentas de ahorro con requisitos simplificados, que utiliza un portal transaccional para tener acceso a servicios y transacciones financieras.
9. **Banca Telefónica:** Canal digital para tener acceso a servicios y transacciones financieras a través de llamadas a los centros de atención telefónica.
10. **Canales electrónicos o digitales:** Se refieren a todas las vías o formas a través de las cuales los usuarios pueden efectuar transacciones con las entidades financieras, mediante el uso de elementos o dispositivos electrónicos o tecnológicos utilizando tarjetas, teléfonos móviles, programas de cómputo, aplicaciones en línea, entre otros.
11. **Cajero automático o ATM (Automated Teller Machine):** Es una máquina, expendedora y receptora de dinero que utiliza tarjetas con chip, claves u otros medios electrónicos sin que se requiera la presencia del personal de la institución financiera, con las que también se puede realizar transferencias electrónicas, pagos y recargas de servicios tanto públicos como privados, entre otros.
12. **Centros de atención no presenciales.-** Son aquellos que no tienen presencia del usuario, estos pueden ser teléfono, correo electrónico, fax e internet.
13. **Cifrar:** Es el proceso mediante el cual la información o archivos son codificados en forma lógica y controlada, con el objetivo de evitar que alguien no autorizado pueda interpretarla, verla o copiarla.
14. **Confidencialidad:** Es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados.
15. **Convenio de asociación:** Es un acto jurídico que tiene fines comunes para las partes, es decir beneficios recíprocos en cuanto a la prestación de servicios financieros o complementarios y, que se formalizan en los acuerdos firmados entre dos o más entidades o empresas auxiliares que se encuentran en funcionamiento, para la ampliación o prestación de uno o varios servicios específicos.
16. **Disponibilidad:** Acceso a la información en el tiempo y forma en que ésta sea requerida.

17. **Exfiltración:** Cuando se incurre en la copia, transferencia o recuperación no autorizadas de datos de un servidor o el ordenador de un individuo.
18. **Fuerza mayor o caso fortuito:** Se refieren al imprevisto que no es posible controlar, tales como: huelgas, paros, guerras, actos de vandalismo, terrorismo, ciberdelincuencia, manifestaciones, conmoción civil, terremotos, incendios, inundaciones actos de autoridad ejercidos por funcionario público, u otros similares.
19. **Información:** Es cualquier forma de registro físico, electrónico, óptico, magnético o de otros medios, previamente procesado a partir de datos, que pueden ser almacenado y distribuido.
20. **Integridad:** Es la garantía de mantener la calidad y exactitud de la información.
21. **Quiosco:** Son dispositivos de autoservicio que brindan el acceso, a los usuarios, a información financiera.
22. **Medio de pagos digitales:** Son los mecanismos electrónicos o digitales, definidos por el organismo regulador, utilizados para la transferencia de recursos y/o pagos.
23. **No repudio:** Propiedad de las comunicaciones que garantiza la participación de las partes en una transacción.
24. **OTP (One time password):** Contraseña de un solo uso.
25. **Seguridad de la información:** Son los mecanismos que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados.
26. **Servicios financieros electrónicos**: Son servicios financieros prestados por medios digitales, que se pueden brindar por canales presenciales o no presenciales.
27. **Sistemas de audio respuesta o IVR (Interactive voice response):** Sistema automatizado de respuesta interactiva, orientado a entregar o capturar información a través del teléfono, permitiendo el acceso a servicios de información.
28. **Terminales de puntos de venta (POS):** Dispositivos electrónicos que posibilitan transmitir las instrucciones de pagos, realizadas a través de tarjetas y otros dispositivos electrónicos.
29. **Terminales electrónicos:** Dispositivos conectados en línea a una plataforma tecnológica de servicios financieros, mismos que pueden ser fijos o móviles, tales como ATM, POS, PIN (personal indentification number) Pad (programa acelerado de datos), App (aplicación), entre otros.
30. **Tiempo real:** Se refiere a las transacciones que se ejecutan de manera inmediata y que sus resultados de ejecución son visualizados en el instante que se realizan.
31. **Transacción electrónica**: Es cualquier actividad que involucra la transferencia de información digital para propósitos específicos.
32. **Transferencia electrónica**: Transacciones de fondos, realizadas por cualquier usuario habilitado para este fin, haciendo uso de los diferentes terminales electrónicos; las transacciones pueden referirse a: órdenes de cobro, órdenes de pago, abonos a cuentas, débitos en puntos de venta, retiros de dinero, entre otros.
33. **Usuarios:** Son los socios, clientes o terceros que utilizan cualquier servicio financiero prestado por las entidades.

SECCIÓN II
MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN EN LOS CANALES ELECTRÓNICOS

Artículo. 4.- Medidas de seguridad de la información.- Las entidades deberán contar con las medidas de seguridad de la información en los canales electrónicos, para poder brindar servicios financieros, con la implementación de al menos las siguientes medidas:

a. Precautelar la integridad, disponibilidad y confidencialidad de los registros e información de los usuarios;
b. Establecer medidas de control y de alerta temprana con el fin de prevenir la materialización de posibles riesgos;
c. Asegurar que exista una adecuada segregación de funciones entre el personal que administra, opera, mantiene y en general accede a los terminales y sistemas usados para transacciones electrónicas;
d. Contar con privilegios de autorización y medidas de autenticación, controles de acceso lógicos que contemplen por lo menos dos de tres factores: "algo que se sabe, algo que se tiene, o algo que es". Las entidades podrán implementar otros mecanismos adicionales de seguridad con el fin de precautelar la transacción;
e. Implementar múltiples factores de autenticación, de tal forma que se agreguen dos o más capas adicionales de seguridad a cada plataforma en línea a la que accede el usuario, en todas sus cuentas;
f. Requerir mecanismos de autenticación de múltiples factores para el registro y modificación de la información de contacto, como número de celular o correo electrónico, cuando los usuarios lo realicen por cualquier canal presencial o no presencial;
g. Para el uso de los factores de autenticación, las entidades deberán cumplir, al menos, con lo siguiente:
    1. Mantener procedimientos que avalen la seguridad de la información de sus usuarios durante la generación, custodia, distribución, asignación y reposición o sustitución de dichos factores;
    2. No divulgar o acceder a la información protegida en relación a los factores de autenticación;
    3. Informar a sus usuarios que la entidad no requerirá bajo ningún medio y bajo ninguna condición la información sobre sus factores de autenticación; y,
    4. Las entidades no podrán solicitar información parcial o completa, de las contraseñas del usuario.
h. Capacitar e informar a los usuarios sobre los riesgos derivados del uso de canales electrónicos; y, sobre las medidas de seguridad que se deben tener en cuenta al momento de efectuar transacciones a través de estos.

Artículo. 5.- Medidas de Seguridad Tecnológicas.- Las entidades deberán contar con las medidas de seguridad tecnológicas en los canales electrónicos, al momento de brindar servicios financieros, con al menos las siguientes medidas:

a. Contar como parte de su infraestructura tecnológica, con protocolos de seguridad que realicen las funciones de autenticación y validación de los usuarios; autorización y uso de los de recursos o servicios, así como el registro de la actividad de los usuarios y su perfilamiento para el respectivo seguimiento;
b. Cifrar la información crítica en reposo o en tránsito, incluso en dispositivos electrónicos y de almacenamiento, extraíbles o móviles; debiendo asegurarse de que los protocolos utilizados sean seguros y se guíen por estándares y buenas prácticas internacionales;
c. Contar con desarrollo de software seguros y adecuados, conforme lo dispuesto en la Norma de Control de Seguridad de la Información emitida por esta Superintendencia;
d. El software que se utilice para las transacciones deberá registrar al menos: accesos, nivel de transaccionalidad, límites individuales de transaccionalidad, perfiles de usuarios financieros, entre otra información disponible para valoración. Deberán generar reportes sobre dicha información;
e. Recolectar datos sobre el comportamiento de usuarios y compararlos con patrones sospechosos;
f. Registrar las direcciones IP y/o números de telefonía móvil desde las que se realizan las transacciones en los canales electrónicos;
g. Mantener sincronizados todos los relojes de sus sistemas informáticos, contables, de información y los dispositivos que integran la plataforma de canales electrónicos;
h. Disponer de canales de comunicación seguros mediante la utilización de técnicas de cifrado acorde con los estándares internacionales vigentes sobre la materia;
i. Utilizar tecnología de propósito específico para la generación y validación de claves para ejecutar transacciones en los diferentes canales electrónicos y dicha información en todo momento debe estar cifrada;
j. Incorporar procesos periódicos de renovación de clave, con una frecuencia de al menos una vez al año, para el acceso a los sistemas de canales electrónicos por parte de los usuarios;
k. Implementar o actualizar las herramientas y mecanismos para monitorear redes y demás infraestructura tecnológica que permita detectar oportunamente eventos que atenten contra la seguridad de la información, actividad o comportamientos inusuales;
l. Contar con procesos ágiles para adquirir, probar e instalar parches para los componentes de la infraestructura tecnológica, de tal forma que los parches se mantengan actualizados; y evitar el uso de aplicaciones, sistemas operativos y manejadores de bases de datos sin el respaldo del fabricante o proveedor de actualizaciones de seguridad;

m. Contar con programas o software actualizados para detectar, proteger y eliminar software malicioso, así como revisar los ajustes de configuración y la vigencia de las licencias para garantizar el nivel de protección esperado;
n. Contar con herramientas para prevenir la suplantación de identidad ante amenazas basadas en phishing, spam, spear-phishing, entre otros; y considerar la idoneidad de estas herramientas, de tal manera que sean consistentes con el tamaño de la entidad. Las entidades deberán contar con programas de capacitación constante para sus empleados sobre este tipo de amenazas. Las entidades deberán contar con herramientas de prevención de pérdida de datos para tener una visibilidad de los efectos ante dicho evento, de tal forma que se fortalezca la detección y prevención de la fuga de datos;
o. Adecuar los sistemas y demás componentes de la infraestructura tecnológica, para generar la capacidad de contar con un registro de información que permita detectar de forma activa e investigar incidencias, asegurándose de que los registros de actividades estén disponibles para su análisis cuando sea necesario;
p. Mantener un proceso continuo de técnicas que se enfoquen en la configuración segura de hardware y software (hardening), para la matriculación o enrolamiento de los dispositivos electrónicos de los usuarios que se utilicen en la prestación de servicios financieros a través de canales electrónicos; y,
q. Establecer procedimientos para monitorear, controlar y emitir alertas en línea, que informen oportunamente sobre el estado de los canales electrónicos.

Artículo. 6.- Transacciones en canales electrónicos.- Las entidades que ofrezcan sus servicios en canales electrónicos, deberán aplicar buenas prácticas para la administración del riesgo operacional y estándares internacionales, poniendo énfasis en:

a. Reconocer la validez de las operaciones y transacciones realizadas;
b. Establecer límites, los cuales pueden ser personalizados por el usuario para cada operaciones y transacción autorizada;
c. Imposibilitar que el valor de la transferencia supere el saldo disponible o el límite establecido, ya sea por la entidad o el usuario;
d. Permitir que el saldo de la cuenta del usuario se consulte, verifique, acredite o debite en tiempo real;
e. Permitir al usuario realizar consultas de los movimientos realizados a través de cualquier dispositivo electrónico, informando la temporalidad máxima a la que puede acceder la consulta;
f. Ofrecer a los usuarios los mecanismos necesarios para que, a través de métodos de autenticación fuerte, personalicen las condiciones bajo las cuales desean realizar sus transacciones monetarias mediante los diferentes canales electrónicos;
g. Establecer procedimientos de control y mecanismos que permitan determinar el perfil de riesgo de las transacciones, realizadas por los usuarios, que impliquen movimiento de dinero en el uso de canales electrónicos; lo cual deberá ser inmediatamente

notificado al usuario mediante mensajería móvil, correo electrónico, u otro mecanismo;

h. Incorporar procedimientos de bloqueo de los canales electrónicos cuando se presenten eventos inusuales que adviertan situaciones fraudulentas, o después de un número máximo de tres intentos de acceso fallido; lo cual se debe notificar inmediatamente al usuario a través de mensajería móvil, correo electrónico u otro mecanismo, así como su reactivación de manera segura;
i. Establecer procesos y mecanismos automáticos para bloquear preventivamente el acceso a cualquiera de los canales electrónicos, en los siguientes casos:
    1. Cuando se detecten tres intentos de ingreso al canal digital, utilizando información de autenticación incorrecta;
    2. Cuando los sistemas de monitoreo detecten comportamiento transaccional inusual o irregular de acuerdo al perfil del usuario;
    3. Cuando los sistemas de seguridad detecten un ataque informático que comprometa los datos o información de los usuarios; y,
    4. Cuando existan situaciones que comprometan la seguridad de los sistemas de información y del usuario.
j. Poner a disposición de los usuarios una línea telefónica para emergencias con atención las veinticuatro (24) horas, siete (7) días a la semana; adicionalmente podrán contar con accesos directos de atención al usuario de otra naturaleza;
k. Los centros de atención no presenciales al usuario, para validar la identidad de la persona que está siendo atendida, deberán implementar mecanismos que verifiquen que el usuario es quien dice ser;
l. Conservar para disponibilidad del usuario, como mínimo durante doce (12) meses el registro de las transacciones electrónicas, el cual deberá contener al menos lo siguiente: fecha, hora, monto, números de cuenta (origen y destino en caso de aplicarse), identificación del usuario, RUC de la entidad de origen y de destino, número de transacción, código del terminal electrónico y el canal utilizado. Para transacciones por internet la dirección IP, ubicación geográfica aproximada y el proveedor de internet; para transacciones a través de sistemas de audio respuesta y para transacciones del servicio financiero móvil, el número de teléfono con el que se hizo la conexión; y,
m. Determinar la disponibilidad histórica de los registro de las transacciones electrónicas que superen los doce (12) meses el registro.

Artículo. 7.- Continuidad de operaciones.- El proceso de continuidad de operaciones de los sistemas utilizados por las entidades para las transferencias electrónicas, debe cubrir eventos fortuitos o de fuerza mayor; considerando el uso de equipos, sistemas y plataformas de respaldo a través de procedimientos de contingencia establecidos por las áreas del negocio.

Artículo. 8.- Planes de mitigación.- Las entidades deberán contar con planes de respuesta para mitigar el impacto ante un incidente de seguridad información. Estos planes deben ser probados para verificar la capacidad de respuesta e identificar brechas y oportunidades de mejora continuamente.

SECCIÓN III
MEDIDAS DE SEGURIDAD ESPECÍFICAS POR CADA SERVICIO

Artículo. 9.- Cajeros automáticos, quioscos y similares.- Las entidades que ofrezcan servicios a través de cajeros automáticos, quioscos y similares por cuenta propia o a través de terceros deberán:

a. Verificar que la información de las claves no se almacenen en ningún momento;
b. Verificar que los dispositivos utilizados para la autenticación del usuario cifren la información ingresada a través de ellos;
c. Implementar mecanismos internos de autenticación que permitan asegurar que es un dispositivo autorizado por la entidad;
d. Enviar a sus usuarios notificaciones, por al menos dos vías, tales como: mensajería de texto, correo electrónico u otros mecanismos reconocidos por el usuario; notificando las transacciones realizadas; y,
e. Verificar el cumplimiento respecto a la normativa vigente relacionada a las seguridades físicas y electrónicas.

Artículo. 10.- Terminales de puntos de venta.- Las entidades que ofrezcan servicios a través de los terminales de puntos de venta por cuenta propia o a través de terceros, deberán:

a. Exigir que los establecimientos procesen en presencia del usuario el pago de las transacciones efectuadas;
b. Asegurar que también procesen la información de otros medios de pago digitales, enviar a sus usuarios notificaciones, por al menos dos vías, tales como: mensajería de texto, correo electrónico u otros mecanismos reconocidos por el usuario; notificando las transacciones realizadas y sus modificaciones; y,
c. Establecer los mecanismos para confirmar que los técnicos que efectúan la instalación, mantenimiento o desinstalación de los puntos de venta en los establecimientos comerciales, sean parte de la entidad o de terceros contratados por la misma

Artículo. 11.- Banca electrónica o banca móvil.- Las entidades que ofrezcan servicios de banca electrónica o banca móvil por cuenta propia o a través de terceros, deberán:

a. Implementar mecanismos que permitan detectar la copia de los diferentes componentes de su sitio web;

b. Verificar constantemente que no sean modificados sus enlaces, suplantados sus certificados digitales, ni modificada indebidamente la resolución de sistema de nombres de dominio;
c. Implementar mecanismos de autenticación para el acceso a dicho servicio por parte de los usuarios, en donde el nombre de usuario y clave de acceso cumplan con las mejores prácticas de seguridad;
d. Validar o verificar la autenticidad del usuario a través de un canal diferente al internet, o por medios biométricos, para establecer las condiciones personales bajo las cuales realizará y recibirá sus servicios y transacciones por internet, o modificará sus datos de contacto; y,
e. Para los casos de inicio de sesión por medio de banca móvil la entidad deberá remitir un mensaje al usuario, a través de al menos dos medios electrónicos de los que disponga, tales como correo electrónico y/o mensajes de texto.

Artículo. 12.- Banca telefónica a través de IVR.- Además de lo especificado en las medidas de seguridad operativa, para el uso del servicio de banca telefónica los usuarios deberán autenticar su identidad a través del IVR con un factor de autenticación adicional como una contraseña que sólo el usuario conozca.

SECCIÓN IV
DE LOS SERVICIOS OFRECIDOS A LOS USUARIOS

Artículo. 13.- Medidas de seguridad en la afiliación de los usuarios a los productos o servicios financieros.- Para la afiliación de los usuarios a los productos o servicios financieros por medio de canales electrónicos, las entidades deberán al menos:

a. Implementar la aceptación de contratos por medios digitales, utilizando múltiples factores de autenticación, los cuales deberán ser certificados por el organismo encargado de regular y controlar las actividades relacionadas con el comercio electrónico y firma electrónica, de conformidad con el ordenamiento jurídico vigente;
b. Implementar algoritmos y protocolos seguros, así como certificados digitales, mismos que deberán incluir el uso de técnicas de cifrado para las transacciones realizadas;
c. Implementar mecanismos de control y monitoreo que reduzcan la posibilidad de que los usuarios accedan a páginas web falsas y/o fraudulentas. En caso de materialización de eventos adversos, se deberán implementar mecanismos de mitigación;
d. Enviar a sus usuarios notificaciones, por al menos dos vías, tales como: mensajería de texto, correo electrónico u otros mecanismos reconocidos por el usuario; notificando al menos el acceso a la banca en línea, banca móvil, transacciones realizadas, productos financieros adquiridos y sus modificaciones;
e. Informar al usuario al inicio de cada sesión la fecha, hora, dirección IP y dispositivo del último ingreso al canal de banca electrónica; y,

f. Implementar mecanismos de autenticación al inicio de sesión de los usuarios, en donde el nombre de usuario debe ser distinto al número de cédula, número de pasaporte, u otro documento de identidad.

Artículo. 14.- Información al usuario.- Las entidades deberán informar a sus usuarios de forma escrita o a través de cualquier otro medio de comunicación previamente registrado y aceptado, al momento de activar por primera vez el uso de los canales electrónicos al menos lo siguiente:

a. Servicios ofrecidos y las responsabilidades de su uso;
b. Procedimientos para la afiliación, cancelación, suspensión y reactivación del servicio;
c. Límites de montos y transacciones a realizar;
d. Comisiones y tarifas por el uso, con su respectiva descripción;
e. Riesgos inherentes por su utilización;
f. Procedimiento para informar cualquier irregularidad o actividad potencialmente no reconocida o no autorizada y que ha sido detectada, ya sea por el usuario o por la entidad;
g. Procedimiento para la atención de consultas y reclamos de los usuarios;
h. Aceptación de responsabilidades por parte del usuario y la entidad;
i. Consejos para el adecuado uso de canales electrónicos por parte del usuario; y,
j. En todos los canales electrónicos, cuando corresponda, las entidades deberán proveer información al usuario, de acuerdo con lo siguiente:
    1. Elementos que identifiquen que se encuentran utilizando plataformas tecnológicas y/o dispositivos electrónicos que pertenezcan a la entidad antes de ingresar los elementos de autenticación; y,
    2. Una vez que el usuario verifique que se trata de una plataforma tecnológica, dispositivo electrónico, o canal digital oficial de la entidad e inicie una sesión segura, se deberá proporcionar de forma notoria y visible, al menos la información siguiente:

        2.1.- Fecha, hora, dirección IP y dispositivo de su último inicio de sesión;

        2.2.- Nombre, apellido u otro identificador único del usuario.

Artículo. 15.- Identificación del usuario al inicio de sesión.- Para permitir el inicio de sesión a los usuarios a través de los canales electrónicos, las entidades deberán solicitar y validar al menos, lo siguiente:

a. Un identificador de usuario único y su contraseña o clave de acceso de acuerdo a las mejores prácticas internacionales; y,
b. El uso de uno de los factores de autenticación adicional.

Artículo. 16.- Verificación de la identidad de los usuarios .- Las entidades deberán utilizar múltiples factores de autenticación para verificar la identidad de sus usuarios al momento de realizar transacciones por medio de canales digitales, tales como: preguntas de desafío, contraseñas que solo el usuario conoce, claves dinámicas de un solo uso (OTP), información del usuario de acuerdo a características biométricas, entre otros.

Artículo. 17.- Métodos adicionales de autenticación.- Las entidades podrán establecer métodos adicionales de autenticación con el fin de reforzar las transacciones realizadas en canales electrónicos.

Las entidades podrán poner a disposición del usuario al menos un mecanismo que permita lo siguiente:

a. Obtener el historial de transacciones realizadas en los últimos 90 días, que como mínimo incluirá el número de referencia, monto, fecha, hora, tipo de transacción, tipo de producto y canal;
b. Un procedimiento para el desbloqueo de usuario y contraseña; y,
c. Un procedimiento para definir una nueva clave o contraseña.

Artículo. 18.- Uso de factores de autenticación.- Los sistemas de canales electrónicos de las entidades deberán requerir a sus usuarios un factor para inicio de sesión; y, para la autenticación de acceso a los siguientes servicios, deberá exigir al menos un segundo factor para los siguientes servicios:

a. Afiliación, desafiliación y registro de productos, servicios y transacciones programadas;
b. Utilización de productos y servicios;
c. Pagos de servicios, canje de beneficios, retiros o adelantos de efectivo, desactivación de productos, generación y cambios de contraseñas, transferencias electrónicas a terceros;
d. Actualización de datos de la ficha del usuario y límites para las transacciones a efectuar;
e. Consultas; y,
f. Transacciones ofrecidas a través de dispositivos de autoservicio.

Artículo. 19.- Inhabilitación del acceso.- Las entidades deberán inhabilitar inmediatamente el acceso a los servicios ofrecidos por canales electrónicos cuando el usuario o la propia entidad presuman que se puede ver afectada o se ha visto afectada la seguridad de los servicios financieros ofertados, debiendo las entidades contar con diferentes medios, tanto presenciales como digitales para tal efecto.

Artículo. 20.- Confirmación de transacción.- Las entidades deberán generar una confirmación inmediata al usuario, contando con mecanismos de no repudio, sobre las transacciones que se realicen por medio de canales electrónicos, mediante mensajes de texto a su dispositivo móvil u otro medio de comunicación registrado, que le servirá para determinar que la misma se ha completado; salvo aquellos casos en que el usuario haya manifestado expresamente no querer recibirlas, lo cual deberá estar debidamente documentado por la entidad.

Asimismo, las entidades enviarán vía electrónica la notificación que deberá incluir, como mínimo el texto: "*transacción exitosa*", detallando fecha, hora, tipo de producto, tipo de transacción, número de referencia y monto de la operación, entre otra información. En caso de que la transacción no sea exitosa enviarán un mensaje al usuario notificando que la transacción solicitada no fue completada.

Artículo. 21.- Notificación de transacciones y operaciones inusuales, irregulares o sospechosas.- La entidad deberá contar con información del número y monto de las transacciones realizadas por medio de canales electrónicos por usuario y tipo de producto, monitoreando además, el cumplimiento de los límites y otras medidas prudenciales que se hayan establecido, dependiendo del producto o servicio, e identificando en tiempo real, posibles operaciones, inusuales, irregulares o sospechosas de acuerdo al perfil del usuario y los hábitos de uso de sus productos y servicios financieros, generando las alertas correspondientes sobre tales operaciones.

Las entidades deben notificar en forma inmediata a los usuarios, las alertas asociadas a las operaciones realizadas a través de los canales electrónicos, que se desvíen de su perfil transaccional, de manera oportuna y de forma automática, a través de los medios que la entidad estime conveniente.

La notificación o el mensaje enviado deberá describir como mínimo fecha y hora de la transacción, monto de la operación, número de referencia de la transacción, nombre y número de teléfono de la entidad, canal utilizado, tipo de producto y de operación.

El monitoreo de las transacciones al que hace referencia el presente artículo deberá ser efectuado por la entidad mediante herramientas informáticas robustas, especializadas en prevención de fraude.

Artículo. 22.- Reclamos del usuario.- Las entidades deberán contar con un procedimiento establecido y actualizados que les permita atender, los reclamos verbales y/o escritos por el uso de canales electrónicos.

Artículo. 23.- Medios de notificación de reclamos, bloqueos suspensiones y posibles fraudes.- La entidad establecerá mecanismos y procedimientos adecuados que operen las

veinticuatro horas del día, todos los días del año, para atender bloqueos, suspensiones, posibles fraudes y reclamos de los clientes sobre sus transacciones, especificando el medio oficial de recepción de los mismos, debiendo la entidad atender y responder el reclamo en los tiempos determinados en el Libro 1 del Código Orgánico Monetario y Financiero.

Artículo. 24.- Campañas de educación.- Las entidades deberán informar a sus usuarios, mediante campañas educacionales, sobre el funcionamiento de los canales electrónicos que pongan al alcance de éstos, a fin de prevenir actos que pudieran derivar en operaciones irregulares o ilegales que afecten a los usuarios o a las propias entidades.

Artículo. 25.- Comunicación por medios oficiales.- Las entidades deberán informar a sus usuarios los medios oficiales a través de los cuales comunicarán el correcto uso de los productos o servicios que ofrecen.

Artículo. 26.- Canal de notificación de transacciones no reconocidas.- Las entidades deberán incorporar en los mensajes de notificación de transacciones de productos y servicios el canal de comunicación disponible para que el usuario gestione ante la entidad transacciones no reconocidas.

Artículo. 27.- Reporte de operaciones y transacciones fraudulentas o no reconocidas.- Las entidades deberán asegurar que los IVR, o cualquier otro medio de comunicación facilitado por la entidad, permita al usuario acceder a opciones para reportar, de forma expedita, las presuntas transacciones u operaciones fraudulentas o no reconocidas y obtener asistencia inmediata a su reclamo, para lo cual deberán establecer procesos específicos con personal debidamente capacitado que brinden atención oportuna a sus usuarios.

Artículo. 28.- Devolución de valores.- Cuando la plataforma tecnológica que soporta los canales digitales no detecte operaciones fraudulentas o inusuales, así como transacciones no autorizadas, ni reconocidas por el usuario, y que de acuerdo al análisis realizado por la entidad, dichos casos no serán atribuibles al usuario; las entidades serán las responsables de reintegrar, compensar o revertir los montos comprometidos, sin que esto incluya el cobro de comisiones o recargos adicionales para el usuario. Adicionalmente, deberán mantener a disposición de la Superintendencia de Economía Popular y Solidaria los reportes o estadísticas que resulten por estos eventos.

Artículo. 29.- Cobertura de pérdidas.- Las entidades, con la finalidad de gestionar riesgos originados en incidentes relacionados a vulneraciones a la seguridad de la información asociada a sus canales electrónicos, deberán contratar pólizas de seguros que les permitan cubrir las pérdidas económicas que se deriven de la materialización de estos

eventos, o contar con otros mecanismos que en el contexto de la administración de estos riesgos mitiguen su impacto.

Artículo. 30.- Seguridad en la sesión del usuario.- Con respecto a la sesión del usuario, las entidades deberán garantizar lo siguiente:

a. Finalizar la sesión en forma automática en los siguientes casos:
    1. Cuando existan más de dos (2) minutos de inactividad en canales electrónicos y cinco (5) minutos para banca de empresas;
    2. Cuando el período de inactividad alcance como máximo los treinta segundos en las operaciones realizadas mediante cajeros automáticos, quioscos o puntos de ventas; y,
    3. Cuando se detecten sesiones simultáneas; debiendo comunicar del hecho al usuario titular del servicio.
b. Comunicar a sus usuarios que ingresaren desde su sitio web a enlaces de páginas web de terceros, que la seguridad no depende ni es responsabilidad de la entidad.

SECCIÓN V
DE LOS RESPALDOS Y AUDITORÍA

Artículo. 31.- Inventario de activos de información críticos.- Las entidades deberán mantener actualizado el inventario de activos de información críticos e identificar los datos.

Artículo. 32.- Auditoría de seguridad.- Las entidades deberán establecer y ejecutar procedimientos de auditoría de seguridad en sus canales electrónicos, por lo menos, una vez al año.

Artículo. 33.- Plan anual de trabajo.- La unidad de auditoría interna de la entidad debe considerar en su plan anual de trabajo, la evaluación del cumplimiento de las disposiciones de la presente norma.

Artículo. 34.- Registro y seguimiento de operaciones.- Los sistemas utilizados en los canales electrónicos de las entidades, deberán generar archivos que permitan respaldar el detalle de los antecedentes de cada operación, de tal forma que estén disponibles para procesos de certificación o auditoría.

Deberán mantener los archivos contables y sus respaldos en físico por el plazo de diez años contados a partir de la fecha de conclusión de la operación y por quince años en formato digital. En caso de presentarse reclamos, la información deberá conservarse hasta que se agoten las instancias legales.

Conservar al menos durante seis meses los registros de las comunicaciones realizadas por los usuarios a los centros de atención no presenciales. En caso de presentarse reclamos, la información deberá conservarse hasta que se agoten las instancias legales.

SECCIÓN VI
DE LAS RESPONSABILIDADES

Artículo. 35.- Responsabilidades de las cooperativas de ahorro y crédito de los segmentos 1, 2, 3, cajas centrales y asociaciones mutualistas de ahorro y crédito para la vivienda.-Las entidades señaladas en el presente artículo tendrán las siguientes responsabilidades:

a. El consejo de administración aprobará las políticas, procesos y procedimientos referentes a la seguridad en las transferencias electrónicas, que incluirá al menos las responsabilidades internas y del proveedor;
b. El comité de administración integral de riesgos, propondrá las políticas, procesos y procedimientos referentes los riesgos en materia de seguridad en las transferencias electrónicas y recomendará al consejo de administración su aprobación;
c. El representante legal implementará las políticas, procesos y procedimientos referentes a la seguridad en las transferencias electrónicas;
d. La unidad de tecnología de la información o el responsable de tecnología de la información, y el responsable de seguridad de la información, según corresponda, elaborará y presentará al comité de administración integral de riesgos las políticas, procesos y procedimientos referentes a la gestión de los riesgos en materia de seguridad en las transferencias electrónicas; y, sus respectivas actualizaciones, tomando en cuenta estándares y buenas prácticas internacionales; y el análisis de riesgo elaborado por la unidad o responsable correspondiente; y,
e. La auditoría interna, verificará la efectividad de las medidas de seguridad en las transferencias electrónicas y recomendará medidas correctivas. Además, deberá custodiar los informes de las pruebas de vulnerabilidad y ponerlos a disposición de la Superintendencia de Economía Popular y Solidaria, cuando esta lo requiera.

Artículo. 36.- Responsabilidades de las cooperativas de ahorro y crédito de los segmentos 4 y 5.- Las entidades descritas en el presente artículo, tendrán las siguientes responsabilidades:

a. El consejo de administración aprobará las políticas, procesos y procedimientos referentes a la seguridad en las transferencias electrónicas, definiendo específicamente las responsabilidades internas y del proveedor;
b. El representante legal deberá proponer al consejo de administración las políticas, procesos y procedimientos referentes a la seguridad en las transacciones electrónicas y su gestión de riesgos, recomendando su aprobación; y,

c. El consejo de vigilancia verificará la efectividad de las medidas de seguridad en las transacciones electrónicas y recomendará medidas correctivas.

DISPOSICIONES GENERALES

PRIMERA.- Los servicios financieros ofrecidos por las entidades a través de canales electrónicas, deberán ser previamente autorizados por la Superintendencia de Economía Popular y Solidaria.

SEGUNDA.- Cuando se usen terminales electrónicos ajenos a la red de la entidad financiera, esta deberá asegurarse que dichos terminales electrónicos cuenten con todas las seguridades requeridas en la presente norma.

TERCERA.- Las entidades para prestar servicios por medio de canales electrónicos a través de otras entidades del sistema financiero y/o con compañías u organizaciones de servicios auxiliares del sistema financiero, deberán celebrar contratos observando lo dispuesto en la presente norma.

En los contratos se deberá incluir de manera específica las responsabilidades de la entidad contratante así como de la compañía u organización de servicios auxiliares o de la entidad financiera contratadas.

CUARTA.- Las entidades, previa autorización de la Superintendencia de Economía Popular y Solidaria, podrán celebrar convenios de asociación para ofrecer sus servicios a través de transferencias electrónicas, garantizando que las entidades participantes, cumplan con lo dispuesto en esta norma.

QUINTA.- Los casos de duda en la aplicación de la presente Norma, serán resueltos por la Superintendencia de Economía Popular y Solidaria.

DISPOSICIONES TRANSITORIAS

PRIMERA.- Las entidades y las compañías u organizaciones de servicios auxiliares que al momento de la expedición de esta norma presten servicios a través de canales electrónicos, deberán implementar lo dispuesto en esta resolución hasta el 01 de abril de 2024.

SEGUNDA.- Las compañías y organizaciones de la Economía Popular y Solidaria que antes de la vigencia de la presente resolución hubieren iniciado el proceso de calificación, cumplirán los requisitos y procedimientos que estaban vigentes a ese momento.

DISPOSICIÓN DEROGATORIA.- Se derogan las resoluciones números SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103 de 23 de noviembre de 2017 y SEPS-IGT-IR-ISF-ITIC-IGJ-2017-113, del 21 de diciembre de 2017.

DISPOSICIÓN FINAL.- La presente Norma entrará en vigencia a partir de su suscripción, sin perjuicio de su publicación en el Registro Oficial.

Publíquese en la página web de la Superintendencia de Economía Popular y Solidaria.

COMUNÍQUESE Y PUBLÍQUESE.- Dado y firmado en la ciudad de San Francisco de Quito, Distrito Metropolitano, a 14 de abril de 2023.

Firmado electrónicamente por:
JORGE ANDRES MONCAYO LARA
SUPERINTENDENTE DE ECONOMÍA POPULAR Y SOLIDARIA (S)
14/04/2023 17:10:46

JORGE ANDRÉS MONCAYO LARA
SUPERINTENDENTE DE ECONOMÍA POPULAR Y SOLIDARIA
SUBROGANTE