SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

RESOLUCIÓN No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017- 103

KLÉVER MEJÍA CAGUASANGO
SUPERINTENDENTE DE ECONOMÍA POPULAR Y SOLIDARIA (E)

CONSIDERANDO:

Que, el Código Orgánico Monetario y Financiero publicado en el Segundo Suplemento del Registro Oficial No. 332 de 12 de septiembre de 2014, regula los sistemas monetarios y financieros, así como los regímenes de valores y seguros del Ecuador;

Que, el numeral 1 del artículo 62, en concordancia con el inciso segundo del artículo 74 del mencionado Código determina como función de la Superintendencia de Economía Popular y Solidaria ejercer la vigilancia, auditoría, control y supervisión de las disposiciones del Código Orgánico Monetario y Financiero;

Que, el numeral 7 del artículo 62 del aludido Código, establece como función de la Superintendencia de Economía Popular y Solidaria, 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 ibídem determina que la Superintendencia de Economía Popular y Solidaria para el cumplimiento de sus funciones, podrá expedir las normas en las materias propias de su competencia sin que pueda alterar las disposiciones legales ni las regulaciones que expida la Junta de Política y Regulación Monetaria y Financiera;

Que, el inciso primero del artículo 74 del citado cuerpo legal, dispone que la Superintendencia de Economía Popular y Solidaria, en su organización, funcionamiento y funciones de control y supervisión del sector financiero popular y solidario, se regirán por las disposiciones de dicho Código y la Ley Orgánica de Economía Popular y Solidaria;

Que, en el artículo 163 del referido Código, determina que las cooperativas de ahorro y crédito, las cajas centrales y las asociaciones mutualistas de ahorro y crédito para la vivienda forman parte del sector financiero popular y solidario;

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

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 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, el literal b del artículo 151 de la Ley Orgánica de Economía Popular y Solidaria, determina entre las atribuciones del Superintendente de Economía Popular y Solidaria dictar las normas de control;

Que, la Disposición General Cuarta, de la Sección III "Normas para la Administración Integral de Riesgo de las Cooperativas de Ahorro y Crédito, Cajas Centrales y Asociaciones Mutualistas de Ahorro y Crédito para la Vivienda", del Capítulo XXXVI "Sector Financiero Popular y Solidario", del Libro I "Sistema Monetario y Financiero", de la Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros aprobada por la Junta de Política y Regulación Monetaria y Financiera, determina que la Superintendencia de Economía Popular y Solidaria podrá expedir las normas de control necesarias para su aplicación;

Que, es necesario que la Superintendencia de Economía Popular y Solidaria expida una norma de control de las seguridades en el uso de transferencias electrónicas; y,

Que, mediante acción de personal No. 855 de 12 de mayo de 2017, se encarga a Kléver Mejía Caguasango, el puesto de Superintendente de Economía Popular y Solidaria, a partir del 15 de mayo de 2017.

En ejercicio de las atribuciones y las funciones que le confiere la Ley,

RESUELVE:

Expedir la siguiente:

NORMA DE CONTROL DE LAS SEGURIDADES EN EL USO DE TRANSFERENCIAS ELECTRÓNICAS

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

SECCIÓN I.- ÁMBITO Y OBJETO.

Artículo 1.- Ámbito. Las disposiciones de esta resolución aplicarán a las cooperativas de ahorro y crédito, cajas centrales y asociaciones mutualistas de ahorro y crédito para la vivienda, en adelante denominadas "entidades".

Artículo 2.- Objeto. La presente resolución tiene por objeto establecer los niveles mínimos de protección en las transferencias electrónicas realizada mediante mensajes o instrucciones telefónicas, electrónicas o celulares desde un ordenador conectado a redes de comunicación propias o de terceros a otro ordenador, mediante el uso de cualquier terminal.

SECCIÓN II.- DEFINICIONES.

Artículo 3.- Para la aplicación de esta norma se considerarán las siguientes definiciones:

- **Administrador del convenio de asociación.-** Es la entidad que proporciona el mayor aporte de servicios a los intervinientes del convenio de asociación y que se encarga de la representación y correcta implementación del mismo.

- **Autorización de accesos:** Controla el acceso de los usuarios a zonas restringidas; a distintos equipos y servicios después de haber superado el proceso de autenticación.

- **Autenticar:** Proceso, dispositivo o sistema utilizado para la comprobación de credenciales de acceso y la verificación de la identidad de un usuario.

- **Cajero automático o ATM (Automated Teller Machine):** Es una máquina expendedora de dinero utilizando tarjeta con banda magnética o chip, sin que se requiera la presencia del personal de la institución financiera.

- **Confidencialidad:** Es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados.

- **Disponibilidad:** Acceso a la información en el tiempo y forma en que ésta sea requerida.

- **Encriptar:** Es el proceso mediante el cual la información o archivos son cifrados en forma lógica y controlada, con el objetivo de evitar que alguien no autorizado pueda interpretarla, verla o copiarla.

- **Evento fortuito o de fuerza mayor:** Se refieren a aquellos eventos tales como huelgas o paros, actos de vandalismo, terrorismo, manifestaciones o conmoción civil; y, terremotos, incendios, inundaciones u otros similares.

- **Información:** Es cualquier forma de registro electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado y distribuido.

- **Integridad:** Es la garantía de mantener la calidad y exactitud de la información.

- **No repudio:** Propiedad de las comunicaciones que garantiza la participación de las partes en una comunicación.

- **Punto de venta.-** Dispositivos electrónicos que posibilitan transmitir las instrucciones pagos, realizadas a través de tarjetas de débito y/o tarjetas de crédito.

- **Seguridad de la información:** Son los mecanismos que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella.

- **Servicio financiero por internet:** Son los suministrados a través del sitio web que corresponda a uno o más dominios de la entidad, indistintamente del dispositivo tecnológico a través del cual se acceda.

- **Servicio financiero móvil:** Son los suministrados por las entidades a los socios, clientes o usuarios, a través de terminales electrónicos móviles.

- **Sistemas de audio respuesta o IVR (Interactive voice response):** Es un sistema automatizado de respuesta interactiva, orientado a entregar o capturar información a través del teléfono, permitiendo el acceso a servicios de información.

- **Terminales electrónicos:** Son dispositivos conectados en línea a una plataforma tecnológica de servicios financieros, tales como ATM, POS, PIN Pad, App, entre otros.

- **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.

- **Transacción electrónica**: Es cualquier actividad que involucra la transferencia de información digital para propósitos específicos.

- **Transferencia electrónica**: son las transacciones de fondos e información, 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. Incluye operaciones que atienden mensajes de consultas sobre movimientos o saldos de cuentas.

SECCIÓN III.- MEDIDAS TECNOLÓGICAS DE SEGURIDAD EN EL USO DE TRANSFERENCIAS ELECTRÓNICAS.

Artículo 4.- Sistemas de transferencia electrónica. Los sistemas de transferencia electrónica, sin perjuicio de incorporar en sus procesos las mejores prácticas para la administración del riesgo operacional y estándares internacionales sobre la materia, deberán:

1. Contar con una plataforma tecnológica que permita una encriptación sólida;

2. 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", considerando que uno de ellos debe ser dinámico por cada vez que se efectúa una transacción y otro debe ser una clave de una sola vez (OTP, One Time Password). Las entidades podrán implementar entre otros, controles biométricos para el acceso al ambiente de internet;

3. Precautelar la integridad y privacidad de los registros e información de los socios, clientes o usuarios;

4. Reconocer la validez de las transferencias realizadas;

5. Establecer límites para cada transferencia autorizada;

6. Imposibilitar que el valor de la transferencia supere el saldo disponible o el límite establecido para un período de tiempo;

7. Permitir que el saldo de la cuenta del cliente, socio o usuario se consulte, valide, acredite o debite en tiempo real;

8. Permitir al socio o cliente obtener reportes para la conciliación de sus movimientos realizados a través de cualquier terminal electrónico, informando la temporalidad máxima a la que puede acceder la consulta; y,

9. Generar el comprobante de la transacción con el detalle necesario para la conciliación.

Artículo 5.- Registro y seguimiento de operaciones. Los sistemas utilizados para las transferencias electrónicas, deberán generar archivos que permitan respaldar el detalle de los antecedentes de cada operación, de tal forma que sean usados en procesos de certificación o auditoría.

Artículo 6.- Perfiles de seguridad. Los sistemas para transferencias electrónicas que implementen las entidades deben contar con perfiles de seguridad que garanticen que sea la

persona autorizada la que tenga los privilegios de uso; así como, de no repudio para realizar una transacción.

Artículo 7.- Bloqueo y restauración de operaciones. Los sistemas de transferencias electrónicas deberán permitir en cualquier momento y en tiempo real, el bloqueo al uso del sistema cuando se detecten eventos inusuales o cuando se adviertan situaciones fraudulentas o después de un número máximo de tres intentos fallidos de acceso.
Se deberán establecer procedimientos seguros para levantar el bloqueo, para lo cual se debe proporcionar las notificaciones correspondientes al socio, cliente o usuario.

Artículo 8.- Continuidad de operaciones. La continuidad de operaciones de los sistemas utilizados para las transferencias electrónicas, deben cubrir los eventos fortuitos o fuerza mayor considerando el uso de equipo de respaldo a través de procedimientos de contingencia, de tal forma que no interrumpa el normal funcionamiento de los sistemas.

SECCIÓN IV.- MEDIDAS OPERATIVAS DE SEGURIDAD EN EL USO DE TRANSFERENCIAS ELECTRÓNICAS.

Artículo 9.- Medidas operativas de seguridad. Las entidades que utilicen transferencias electrónicas por cuenta propia o a través de terceros, deberán garantizar la calidad y seguridad de la información de los socios, clientes o usuarios, a través de la implementación de al menos las siguientes medidas operativas de seguridad:

1. Informar a sus socios, clientes o usuarios por mensajes en línea a través de mensajería móvil, correo electrónico u otro mecanismo inmediato, del acceso y la ejecución de transacciones realizadas mediante cualquiera de los terminales electrónicos disponibles;

2. Mantener permanentemente informados a los socios, clientes o usuarios acerca de las medidas de seguridad que se deben considerar al momento de efectuar transferencias electrónicas;

3. Informar y capacitar permanentemente a los socios, clientes o usuarios sobre los procedimientos para la utilización, ubicación, bloqueo, inactivación, reactivación y cancelación de las transferencias electrónicas;

4. Establecer y ejecutar procedimientos de auditoría por lo menos una vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad y calidad de los servicios e información de los sistemas para las transferencias electrónicas;

5. Disponer de políticas de desarrollo seguro de software y procedimientos de control de cambios en los sistemas de transferencia electrónica; con el objetivo de precautelar la seguridad de la información a lo largo del ciclo de vida de desarrollo de software;

6. Incorporar en los procedimientos de administración de seguridad de la información la renovación de las claves para el acceso a los sistemas de transferencias electrónicas por lo menos una vez al año. Las claves utilizadas en las transferencias electrónicas que inician la transacción con tarjeta, deben ser diferentes a las que no inician con tarjeta;

7. Permitir a los socios o clientes que el registro y la modificación de la información usada para fines de notificación, como número de teléfono, correo electrónico, entre otros, se realicen con las debidas medidas de verificación y seguridad;

8. Registrar las direcciones IP y números de telefonía móvil desde las que se realizan las transacciones. Para permitir transacciones desde direcciones IP o telefonía móvil de otros países se debe tener la autorización expresa del socio, cliente o usuario;

9. Establecer un tiempo máximo de inactividad, después del cual deberá ser cancelada la sesión y exigir un nuevo proceso de autenticación al socio, cliente o usuario para realizar otras transacciones;

10. 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 transferencias electrónicas;

11. Mantener sincronizados todos los relojes de sus sistemas contables y de información relacionados con el uso de transferencias electrónicas;

12. Conservar para disponibilidad del socio, usuario o cliente, como mínimo durante doce meses el registro electrónico 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 dispositivo. Para operaciones por cajero automático, el código del cajero automático; para transacciones por internet la dirección IP; 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;

13. Mantener los archivos contables físicos y sus respaldos 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;

14. Para transferencias realizadas con tarjeta de débito o crédito, poner a disposición de los socios, clientes o usuarios un acceso directo o un centro de atención telefónica y una línea para emergencias, con atención las veinticuatro horas, siete días a la semana;

15. Los centros de atención telefónica para validar o confirmar la identidad del socio que está siendo atendido, deberán implementar mecanismos que verifiquen la autenticación de la llamada telefónica, mediante preguntas de desafío o información de sus últimas transacciones; y,

16. Conservar al menos durante seis meses la grabación de las llamadas telefónicas realizadas por los socios, clientes o usuarios a los centros de atención telefónica, principalmente en los siguientes casos: consultas de saldos, reclamos, emergencias. En caso de presentarse reclamos, la información deberá conservarse hasta que se agoten las instancias legales.

Artículo 10.- Medidas operativas específicas por terminal electrónico. Además de las medidas operativas de seguridad establecidas anteriormente, las entidades deberán implementar seguridades específicas para los terminales electrónicos que se detallan a continuación:

1. Cajeros Automáticos: Las entidades que ofrezcan servicios a través de cajeros automáticos por cuenta propia o a través de terceros, deberán:

a) Instalar o verificar que los cajeros automáticos se hayan instalado de acuerdo con las especificaciones del fabricante y según lo dispuesto en la normativa vigente, incluyendo el cambio de contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores; y,

b) Asegurar que también procesen la información de tarjetas inteligentes.

2. 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) Definir procedimientos que exijan que los técnicos que efectúan la instalación, mantenimiento o desinstalación de los puntos de venta en los establecimientos comerciales, confirmen su identidad;

b) Exigir que los establecimientos procesen en presencia del socio, cliente o usuario el pago de las transacciones efectuadas; y,

c) Asegurar que también procesen la información de tarjetas inteligentes.

3. Servicios financieros a través de internet: Las entidades que ofrezcan estos servicios 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, verificar constantemente que no sean modificados sus enlaces (links), suplantados sus certificados digitales, ni modificada indebidamente la resolución de sistema de nombres de dominio;

b) Implementar mecanismos de autenticación para el acceso a dicho servicio por parte de los socios, clientes o usuarios, en donde el nombre de usuario debe ser distinto al número de cédula de identidad. El nombre de usuario y clave de acceso deben combinar caracteres alfanuméricos con una longitud mínima de seis caracteres; y,

c) Validar o verificar la autenticidad del socio, cliente o usuario a través de un canal diferente al de internet para establecer las condiciones personales bajo las cuales realizarán sus transacciones por internet.

SECCIÓN V.- DE LAS RESPONSABILIDADES.

Artículo 11.- Responsabilidades de las entidades de los segmentos 1, 2, 3, cajas centrales y asociaciones mutualistas de ahorro y crédito para la vivienda:

1. 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;

2. El comité de administración integral de riesgos, conocerá las políticas, procesos y procedimientos referentes a la seguridad en las transferencias electrónicas y recomendará al consejo de administración su aprobación;

3. El representante legal implementará las políticas, procesos y procedimientos referentes a la seguridad en las transferencias electrónicas;

4. La unidad de tecnología de la información o el responsable de tecnología de la información, según corresponda, elaborará y propondrá al comité de administración integral de riesgos las políticas, procesos y procedimientos referentes a la seguridad en las transferencias electrónicas; y, sus respectivas actualizaciones, tomando en cuenta estándares y buenas prácticas internacionales; y,

5. El auditor interno, 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 12.- Responsabilidades de las entidades de los segmentos 4 y 5:

1. 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;

2. El representante legal deberá proponer al consejo de administración las políticas, procesos y procedimientos referentes a la seguridad en las transferencias electrónicas y recomendar su aprobación; y,

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

DISPOSICIONES GENERALES

PRIMERA.- Las operaciones y servicios financieros realizados por las entidades a través de transferencias electrónicas, deberán ser previamente autorizados por la Superintendencia de Economía Popular y Solidaria.

SEGUNDA.- Las entidades que presten servicios financieros por medio de transferencias electrónicas, deberán contabilizar diariamente las transacciones efectuadas con este mecanismo.

TERCERA.- Las entidades, previa autorización de la Superintendencia de Economía Popular y Solidaria, podrán celebrar convenios de asociación entre ellas para ofrecer sus servicios a través de transferencias electrónicas, garantizando que las entidades participantes, cumplan con los niveles de seguridad tecnológica dispuestos en esta norma.

Las entidades intervinientes en el convenio de asociación podrán implementar las políticas, procesos y procedimientos de seguridad de las transferencias electrónicas del administrador del convenio.

CUARTA.- Para prestar servicios de transferencias electrónicas con compañías u organizaciones de servicios auxiliares, las entidades deberán celebrar contratos solo con aquellas que hayan sido calificadas para el efecto por la Superintendencia de Economía Popular y Solidaria.

En los contratos se deberá incluir de manera específica las responsabilidades de la entidad financiera y de la compañía u organización de servicios auxiliares.

DISPOSICIÓN TRANSITORIA.- Las entidades que al momento de la expedición de esta norma presten servicios de transferencias electrónicas, deberán implementar lo dispuesto en esta resolución dentro del plazo de 360 días, contados a partir de la fecha de su expedición.

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

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

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

COMUNÍQUESE Y PUBLÍQUESE.- Dado y firmado en la ciudad de San Francisco de Quito, Distrito Metropolitano, a los 23 NOV 2017

KLÉVER MEJÍA CAGUASANGO
SUPERINTENDENTE DE ECONOMÍA POPULAR Y SOLIDARIA (E)