

**RESOLUCIÓN Nro. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-2023-0270**

**MARÍA BELÉN FIGUEROA GRIJALVA**  
**INTENDENTE GENERAL TÉCNICO, SUBROGANTE**

**CONSIDERANDO:**

- 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 último inciso del artículo 62 de la ley ídem 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,** los literales b) y g) del artículo 151 de la Ley Orgánica de Economía Popular y Solidaria, determinan como las 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,** con Resolución Nro. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009 de 14 de abril de 2023, la Superintendencia de Economía Popular y Solidaria expidió la “Norma de Control de Seguridades en el Uso de Canales Electrónicos para las Entidades Financieras Controladas por la Superintendencia de Economía Popular y Solidaria”;
- Que,** a efectos de dar una atención óptima a los usuarios financieros y procurar una supervisión eficaz sobre sus entidades controladas, resulta necesario incorporar directrices respecto del cumplimiento de seguridades electrónicas;
- Que,** conforme consta en el literal j) del numeral 1.2.1.2 “Gestión General Técnica”, del artículo 9 de la Resolución Nro. SEPS-IGT-IGS-IGD-IGJ-001 de 31 de enero de 2022, que contiene el Estatuto Orgánico de Gestión Organizacional por Procesos de la Superintendencia de Economía Popular y Solidaria, es atribución y responsabilidad del Intendente General Técnico, dictar las normas de control, en el ámbito de su competencia; y,
- Que,** acorde a la Acción de Personal Nro. 1519 de 21 de julio de 2023, se dispuso la subrogación de la señora ingeniera María Belén Figueroa Grijalva, en las funciones y responsabilidades del cargo de Intendente General Técnico, desde el 31 de julio de 2023 hasta el 6 de agosto de 2023.

En ejercicio de sus funciones, resuelve expedir la siguiente:

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

**Artículo 1.-** Sustitúyase la Disposición Transitoria Primera de la Resolución Nro. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009 de 14 de abril de 2023, por la siguiente:

**“PRIMERA.-** Las entidades y compañías u organizaciones de servicios auxiliares que a la fecha de expedición de esta resolución presten servicios a través de canales electrónicos, deberán implementar lo dispuesto en la misma hasta el 1 de abril del 2024; sin embargo, de manera obligatoria e inmediata, deben observar y aplicar lo señalado en el Anexo 1: “Medidas mínimas operativas de seguridad en transferencias electrónicas”, adjunto a la presente norma.

**Artículo 2.-** Agréguese al final del texto de la Resolución Nro. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009 de 14 de abril de 2023 el siguiente anexo:

**“ANEXO 1”**

**MEDIDAS MÍNIMAS OPERATIVAS DE SEGURIDAD EN TRANSFERENCIAS  
ELECTRÓNICAS**

Las entidades deberán implementar las siguientes medidas operativas de seguridad:

1. Medidas de autenticación con 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”, con el fin de precautelar la seguridad de la transacción;
2. Informar a sus socios, clientes o usuarios del acceso, inicio de sesión, modificación de datos y la ejecución de transacciones realizadas mediante cualesquiera de los terminales y canales electrónicos disponibles por mensajes en línea enviados simultáneamente a dos canales, tales como: mensajería móvil, correo electrónico u otro mecanismo inmediato;
3. 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;
4. 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;
5. 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;
6. 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;

7. Incorporar en los procedimientos de administración de seguridad de la información la renovación de las claves para el acceso a los sistemas de transacciones electrónicas por lo menos una vez al año. Las claves utilizadas en las transacciones electrónicas deberán ser diferentes por cada canal empleado;
8. 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;
9. Registrar las direcciones IP y números de telefonía móvil desde las que se realizan las transacciones en los canales electrónicos predeterminados. Para permitir transacciones desde direcciones IP o telefonía móvil de otros países, se debe contar con la autorización expresa del socio, cliente o usuario;
10. 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 transacciones;
11. 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;
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, R.U.C. 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 a través del cual 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 transacciones 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, deben 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.

### **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.

**DISPOSICIÓN FINAL.-** La presente resolución 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 3 de agosto del 2023.

**MARÍA BELÉN FIGUEROA GRIJALVA**  
**INTENDENTE GENERAL TÉCNICO, SUBROGANTE**