RESOLUCIÓN No. SEPS-IGT-IGS-IGJ-INR-INSESF-INSEPS-INGINT-2026-0085

FREDDY ALFONSO MONGE MUÑOZ
INTENDENTE GENERAL TÉCNICO

CONSIDERANDO:

Que el inciso primero del artículo 283 de la Constitución de la República del Ecuador, determina que: "El sistema económico es social y solidario; reconoce al ser humano como sujeto y fin; propende a una relación dinámica y equilibrada entre sociedad, Estado y mercado, en armonía con la naturaleza; y tiene por objetivo garantizar la producción y reproducción de las condiciones materiales e inmateriales que posibiliten el buen vivir […]";

Que según el artículo 309 de la Carta Fundamental: "El sistema financiero nacional se compone de los sectores público, privado, y del popular y solidario, que intermedian recursos del público. Cada uno de estos sectores contará con normas y entidades de control específicas y diferenciadas, que se encargarán de preservar su seguridad, estabilidad, transparencia y solidez. Estas entidades serán autónomas. Los directivos de las entidades de control serán responsables administrativa, civil y penalmente por sus decisiones.";

Que de conformidad a lo establecido en el artículo 213 de la Constitución de la República del Ecuador "Las superintendencias son organismos técnicos de vigilancia, auditoría, intervención y control de las actividades económicas, sociales y ambientales, y de los servicios que prestan las entidades públicas y privadas, con el propósito de que estas actividades y servicios se sujeten al ordenamiento jurídico y atiendan al interés general […];

Que el artículo 13 del Libro I del Código Orgánico Monetario y Financiero, en su parte pertinente prevé que la Junta de Política y Regulación Financiera y Monetaria como parte de la Función Ejecutiva, como órgano con autonomía funcional, técnica, institucional, y en sus decisiones, será responsable de la formulación de la política y regulación monetaria, crediticia, financiera, de valores, seguros y servicios de atención integral de salud prepagada";

Que el numeral 1 del artículo 62 del Libro I del Código *ibidem*, en concordancia con el quinto inciso del artículo 74, establece como función de la Superintendencia de Economía Popular y Solidaria ejercer la vigilancia, auditoría, control y supervisión del cumplimiento de las disposiciones del Código Orgánico Monetario y Financiero y de las regulaciones dictadas por la Junta de Política y Regulación Financiera y Monetaria, en lo que corresponde a las actividades financieras ejercidas por las entidades que conforman el sector financiero popular y solidario;

Que el último inciso del invocado artículo 62, 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 o innovar las disposiciones legales ni las regulaciones que expida la Junta de Política y Regulación Financiera y Monetaria;

Que el inciso tercero del artículo 74 del Libro I del Código Orgánico Monetario y Financiero determina: 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 […];

Que el artículo 163 del Código *ut supra*, 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;

Que el artículo 444 del mismo Código, establece que las entidades financieras populares y solidarias están sometidas a la regulación de la Junta de Política y Regulación Financiera y Monetaria 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 el literal b del artículo 151 de la Ley Orgánica de Economía Popular y Solidaria determina entre las atribuciones del Superintendente, dictar las normas de control;

Que el literal g) del mencionado artículo 151 establece también como atribución del Superintendente de Economía Popular y Solidaria delegar sus facultades siempre en forma concreta y precisa, a los funcionarios que juzgue del caso;

Que de acuerdo con los artículos 158 y 165 de la citada Ley Orgánica, la Corporación Nacional de Finanzas Populares y Solidarias es una entidad financiera de derecho público, dotada de personalidad jurídica; sometida al control y supervisión de la Superintendencia de Economía Popular y Solidaria;

Que el artículo 387 del Código Orgánico Monetario y Financiero previene que el control de las actividades financieras de la entidad financiera pública a la que se refiere la Ley Orgánica de Economía Popular y Solidaria, esto es la Corporación Nacional de Finanzas Populares y Solidarias, estará a cargo de la Superintendencia de Economía Popular y Solidaria;

Que la Sección III, Capítulo XXXVI "Sector Financiero Popular y Solidario", Título II "Sistema Financiero Nacional", Libro I "Sistema Monetario y Financiero", de la Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros, contiene la: […] NORMAS PARA LA ADMINISTRACIÓN INTEGRAL DE RIESGOS EN LAS COOPERATIVAS DE AHORRO Y CRÉDITO, CAJAS CENTRALES Y ASOCIACIONES MUTUALISTAS DE AHORRO Y CRÉDITO PARA LA VIVIENDA", en cuya Disposición General Cuarta, señala: […] La Superintendencia de Economía Popular y Solidaria emitirá las normas de control necesarias para la aplicación de la presente resolución […];

Que mediante Resolución No. JPRFM-2026-002-F de 30 de enero del 2026, la Junta de Política y Regulación Financiera y Monetaria resolvió agregar el "CAPÍTULO LXVI: NORMA PARA EL ESTABLECIMIENTO DE LAS MEDIDAS MÍNIMAS DE SEGURIDAD, SEAN FÍSICAS O NO, PARA LA OPERACIÓN Y FUNCIONAMIENTO DE LAS OFICINAS, PUNTOS DE ATENCIÓN Y CUALQUIER OTRO DE LAS ENTIDADES DEL SISTEMA FINANCIERO NACIONAL", determinando a través de su Disposición Transitoria Única que la Superintendencia de Economía Popular y Solidaria expedirá o actualizará las normas de control para la aplicación de tal Resolución, de acuerdo con la naturaleza específica y diferenciada por cada sector;

Que mediante Resolución No. SEPS-IGT-IR-IGJ-2018-021 de 13 de julio del 2018, la Superintendencia de Economía Popular y Solidaria expidió la "NORMA DE CONTROL RESPECTO DE LA SEGURIDAD FÍSICA Y ELECTRÓNICA", reformada con la Resolución No. SEPS-IGT-IR-IGJ-2018-0259 de 10 de octubre de 2018;

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 mediante Acción de Personal No. 200, de 10 de febrero del 2025, la Intendente General de Desarrollo Organizacional, delegada de la Señorita Superintendente de Economía Popular y Solidaria, nombró como Intendente General Técnico al señor Freddy Alfonso Monge Muñoz.

En ejercicio de sus atribuciones, resuelve expedir la siguiente:

NORMA DE CONTROL DE SEGURIDAD FÍSICA Y ELECTRÓNICA DEL SECTOR FINANCIERO POPULAR Y SOLIDARIO

TÍTULO I
OBJETO Y ÁMBITO

Artículo 1. Objeto.- La presente resolución tiene por objeto normar las medidas mínimas de seguridad física y electrónica que las entidades del sector financiero popular y solidario deben implementar, de manera que se garantice la seguridad de los empleados, socios, clientes, usuarios, establecimientos y bienes, así como para el resguardo del transporte de efectivo y valores.

Artículo 2. Ámbito.- Las disposiciones de la presente resolución se aplicarán a las cooperativas de ahorro y crédito, asociaciones mutualistas de ahorro y crédito para la vivienda y cajas centrales, en adelante denominadas como: "entidad o entidades"; y, a

la Corporación Nacional de Finanzas Populares y Solidarias, en lo posterior denominada como: "la Corporación".

Artículo 3. Definiciones.- Para la aplicación de la presente resolución, se considerará las siguientes definiciones:

a) **Administración de la información:** Es el proceso mediante el cual se captura, procesa, almacena y transmite información por cualquier medio.
b) **Áreas sensibles:** Son aquellos espacios dentro de las entidades tales como bóvedas, cajas fuertes, cajeros automáticos, centros de procesamiento de datos entre otras, en donde se manejan o almacenan dinero en efectivo, documentos valorados o información crítica, entendiéndose esta última como aquella indispensable para la sostenibilidad y continuidad de las operaciones de la entidad, cuya falta puede generar un impacto negativo. Estas áreas requieren de medidas reforzadas, para minimizar riesgos de sustracción de dinero, pérdida de valores o mal uso de información.
c) **Comité de Administración Integral de Riesgos:** Es el órgano responsable de proponer y recomendar al Consejo de Administración los manuales y políticas de seguridad y protección; así como, las políticas, principios y procedimientos básicos de seguridad y protección para sus empleados, socios, clientes, usuarios, establecimientos, activos y patrimonio; así como, de proponer y presentar al Consejo de Administración el informe de cumplimiento y seguimiento de dicha norma.
d) **Oficinas:** Entiéndase como los lugares en los que las entidades del sector financiero popular y solidario realizan actividades de intermediación financiera; entre los cuales pueden ser: la matriz, sucursales, agencias, oficinas temporales, puntos móviles,
e) **GSM (Sistema Global para las Comunicaciones Móviles)**: Es una tecnología utilizada para la transmisión de señales de alarma o comunicación entre dispositivos de seguridad y centrales de monitoreo, permitiendo la transmisión de alertas en tiempo real.
f) **Manuales y Políticas de Seguridad y Protección:** Son documentos obligatorios que deben contener los principios, las políticas, y procesos básicos para la formulación, implementación y evaluación de las medidas de seguridad y protección en las entidades. Deben ser aprobados por el directorio o consejo de administración y contemplar al menos, los aspectos establecidos en la presente norma.
g) **NIJ II:** Es el estándar internacional de resistencia balística para chalecos antibalas y otros equipos de protección, emitido por el National Institute of Justice (NIJ) de Estados Unidos. El nivel II indica protección contra armas de fuego de bajo y mediano calibre, relevante para el personal de seguridad física.
h) **Oficial de seguridad física y electrónica:** Persona responsable de coordinar, supervisar y controlar la implementación de las medidas de seguridad física, electrónica y dispositivos tecnológicos de seguridad (alarmas, video vigilancia, control de accesos, etc.), así como de la coordinación con el personal de seguridad física para la protección integral de la entidad. Asegurando el cumplimiento de la normativa y la protección de personas, bienes e información.

i) **Protectores de teclado para cajeros automáticos (ATM):** Son cubiertas, comúnmente de plástico rígido o metal, diseñadas para proteger contra manipulación física, visualización de PIN y daños.
j) **Sensor de Doble Tecnología:** Es un dispositivo que combina dos tecnologías de detección (por ejemplo, infrarrojo pasivo y microondas) para reducir falsas alarmas y aumentar la fiabilidad en la detección de intrusos en áreas sensibles.
k) **Sistema de protección pasivo**: Se refiere a las construcciones o instalaciones realizadas para impedir el paso o proteger los bienes.
l) **Seguridad activa**: Son los dispositivos instalados para la detección y disuasión de posibles riesgos.
m) **TCP/IP (Protocolo de Control de Transmisión/Protocolo de Internet):** Es el conjunto de reglas que permite la comunicación y transmisión de datos en redes informáticas, incluyendo la transmisión de señales de sistemas de seguridad, video vigilancia y alarmas entre dispositivos y centros de monitoreo.

TÍTULO II
MEDIDAS MÍNIMAS DE SEGURIDAD FÍSICA Y ELECTRÓNICA

Artículo 4. Medidas mínimas de seguridad.- Sin perjuicio de la instalación de aquellas medidas de seguridad adicionales, las entidades, deberán adoptar al menos las siguientes:

1. Las cooperativas de ahorro y crédito ubicadas en los segmentos 1, 2 y 3; las asociaciones mutualistas de ahorro y crédito para la vivienda y cajas centrales, contarán con:

a) Dispositivos, mecanismos y equipos de seguridad física y electrónica, con el objetivo de brindar seguridad a los socios, clientes, usuarios, empleados y bienes en sus establecimientos, determinando parámetros de acuerdo a la ubicación de los mismos;
b) Sistemas de seguridad y video vigilancia adecuado al tipo de establecimiento;
c) Iluminación adecuada y suficiente en los lugares donde se maneje efectivo o documentos valorados. En las bóvedas, cajas y cajeros automáticos, deberá asegurarse la iluminación permanente, sobre todo ante un eventual corte de suministro eléctrico con equipos auxiliares de iluminación;
d) Para garantizar el funcionamiento permanente del sistema eléctrico, la entidad deberá realizar un mantenimiento con una frecuencia de seis meses junto con el cumplimiento del cronograma correspondiente y el plan de mantenimiento;
e) Puertas de ingreso al establecimiento equipadas con al menos dos cerraduras con llaves codificadas, códigos de seguridad o ambos. Se requerirá la presencia de un empleado de la entidad junto con el personal de seguridad externa al momento de la apertura y cierre del establecimiento. El personal de la entidad encargado de la custodia de llaves o códigos debe ser definida por la entidad y formalizada a través de la firma de responsabilidad;
f) Sistemas efectivos de vigilancia y seguridad en el interior de los establecimientos, además de contar con guardias de empresas de seguridad privada que deberán contar en todo momento con un contrato vigente;

g) El ingreso al área de cajas deberá ser de acceso restringido al público, al personal no autorizado de la entidad y contar con medidas que minimicen los riesgos de sustracciones de dinero u otras actividades ilícitas. Además, esta área deberá contar con sistemas de protección pasivos y activos, vidrios blindados y lámina de protección con el correspondiente certificado extendido por la empresa proveedora del producto y mampostería reforzada de hormigón o materiales similares con su respectivo certificado emitido por la empresa que la construyó de acuerdo con las disposiciones emitidas por el Ministerio del Interior a través de la Unidad Nacional de Policía de Control de Servicios de Seguridad Privada y Control de Armas Letales y no Letales COSP. El vidrio templado debe contar con certificación de normativa internacional o su equivalente, mientras dure la vigencia;

h) Controles de acceso a las cajas, bóvedas, cuarto de cajeros automáticos y cuarto de equipos y similares:

- **i.** Autentificar a la persona responsable de cada área; en el caso de acceso para terceras personas se deberá registrar una bitácora previa autorización del personal de seguridad.
- **ii.** Contar con la función de anti retorno a nivel de todas las áreas sensibles, permitiendo la apertura de una sola puerta a la vez, evitando que un usuario que ingresó a una de estas áreas, pueda ingresar a otra sin haber salido de la anterior;
- **iii.** Contar con alarmas que alerten cuando la puerta no se encuentre totalmente cerrada; y,
- **iv.** Disponer del certificado de la empresa proveedora sobre las características técnicas del sistema de control de accesos.

i) Garantizar el cumplimiento de la prohibición de que los empleados del área de cajas o áreas sensibles porten y utilicen cualquier tipo de equipo de comunicación o de captación de imágenes;

j) Botones de pánico ubicados estratégicamente de acuerdo al estudio de seguridad, conectados al centro de monitoreo de la empresa de seguridad privada y al de la entidad. Cada incidente deberá ser notificado en tiempo real al oficial de seguridad; y,

k) Las entidades deberá contar con el protocolo de seguridad de actuación en el que certifique la gestión con las unidades de policía comunitaria (UPC) y el Sistema Integrado de Seguridad ECU 911.

2. Las cooperativas de ahorro y crédito ubicadas en los segmentos 4 y 5, deberán establecer las medidas mínimas de seguridad, determinadas en los literales a), d), i) y j) del numeral anterior, y las siguientes:

a) Iluminación suficiente en los lugares en donde se maneje efectivo o documentos valorados, en donde existan cajas fuertes y en cajas de atención al público; y,

b) El ingreso al área de cajas deberá ser de acceso restringido al público, al personal no autorizado de la entidad y contar con medidas que minimicen los riesgos de sustracciones de dinero u otras actividades ilícitas. Además, esta área deberá contar con sistemas de protección pasivos y activos, vidrio templado con lámina de protección y mampostería reforzada de hormigón o materiales similares con el

respectivo certificado emitido por la empresa que la construyó o informe técnico del responsable.

Artículo 5. Manual y políticas de seguridad y protección.- Las entidades ubicadas en los segmentos 1, 2 y 3, asociaciones mutualistas de ahorro y crédito para la vivienda y las cajas centrales contarán con un "Manual y Políticas de Seguridad y Protección", que debe ser elaborado por el oficial de seguridad física y electrónica y aprobado por el Consejo de Administración. Estos manuales y políticas contendrán por lo menos los aspectos fundamentales para la seguridad de los empleados, socios, clientes, usuarios, establecimientos y bienes, así como para el resguardo en el transporte de efectivo y valores.

Para las entidades ubicadas en los segmentos 4, 5 y la Corporación, el responsable de la elaboración de los "Manuales y Políticas de Seguridad y Protección" será el delegado del representante legal, quien deberá contar un nivel técnico de conocimiento avalado por una institución controlada por el órgano rector de la educación superior.

Las entidades de acuerdo a su segmento deberán cumplir con lo dispuesto en la siguiente tabla:

Literal	Requerimientos de los manuales y políticas de seguridad y protección	Segmento 1, 2,3 y Mutualistas	Caja Central,	Corporación	Segmento 4 y 5
a)	Las políticas, normas, principios y procesos básicos conforme a los cuales las entidades deben formular sus medidas de seguridad y protección:	X	X	X	X
b)	Las medidas mínimas de seguridad contenidas en la presente normativa, precisando sus características: dimensiones, calidad de los materiales u otros según corresponda;	X	X	X	X
c)	Las medidas de seguridad que las entidades deseen adoptar como adicionales a las contenidas en la presente normativa, que minimicen posibles eventos de riesgo;	X	X	X	X
d)	Los criterios técnicos de seguridad de sus establecimientos, especialmente en centros de procesamiento de datos, de comunicación, equipo técnico de protección para la prestación de los servicios que le corresponda y áreas sensibles;	X	X	X	N/A
e)	Los procesos, sistemas y controles operativos para la prevención y detección de irregularidades en la ejecución de sus operaciones y en el manejo de los recursos, concernientes a efectivo y/o valores que tengan bajo su responsabilidad;	X	X	X	X

Literal	Requerimientos de los manuales y políticas de seguridad y protección	Segmento 1, 2,3 y Mutualistas	Caja Central,	Corporación	Segmento 4 y 5
f)	Las características que deberán reunir los sistemas de monitoreo y alarma, incluyendo los índices de calidad y disponibilidad, así como las demás características técnicas o tecnológicas necesarias para la efectiva emisión y transmisión de las señales e imágenes;	X	X	N/A	N/A
g)	Los criterios para la contratación de servicios profesionales que brinden seguridad y protección a los establecimientos, que incluya al menos capacitación y evaluación, validación periódica de indicadores de confianza y validación de registros en los sistemas biométrico;	X	X	N/A	N/A
h)	Los lineamientos y planes de capacitación e información al personal que labora en sus entidades, específicamente con respecto del entrenamiento en caso de siniestros o durante el cometimiento de un delito, lineamientos que deberán actualizarse por lo menos una vez al año;	X	X	X	X
i)	Los dispositivos, sistemas y procedimientos para controlar la entrada y salida de los empleados de la entidad;	X	X	X	X
j)	Los sistemas y procedimientos para controlar la entrada y salida de socios, clientes, usuarios, supervisores y proveedores;	X	X	X	X
k)	Los planes de seguridad, emergencia, contingencia y continuidad de negocios de la entidad en caso de siniestros o actos delictivos, cuya efectividad deberá revisarse y probarse mediante simulacros por lo menos una (1) vez al año dejando la constancia escrita de su ejecución y evaluación, con informe técnico con firma de responsabilidad y aprobación de la máxima autoridad. Al efecto se coordinará con la Policía Nacional, Cuerpo de Bomberos y la Secretaría Nacional de Gestión de Riesgos. Esta documentación deberá ser revisada y de ser el caso actualizada cada año.	X	X	N/A	N/A
l)	Las características que deberán reunir los sistemas de monitoreo y alarma, incluyendo los índices de calidad y disponibilidad	N/A	N/A	X	X
m)	Los planes de seguridad y emergencia de la entidad, en caso de siniestros o actos delictivos cuya efectividad deberá revisarse y probarse mediante simulacros una vez cada dos años, dejando la constancia escrita de su ejecución y evaluación con informe técnico con firma de	N/A	N/A	X	X

Literal	Requerimientos de los manuales y políticas de seguridad y protección	Segmento 1, 2,3 y Mutualistas	Caja Central,	Corporación	Segmento 4 y 5
	responsabilidad y aprobación de la máxima autoridad. Esta documentación deberá ser revisada y de ser el caso actualizada a menos cada dos (2) años.				

N/A: No Aplica

Artículo 6. Personal de seguridad.- Las entidades, para la contratación del personal relacionado con la seguridad física y electrónica, considerarán como mínimo los siguientes aspectos:

1. Las entidades de los segmentos 1, 2, 3, cajas centrales, asociaciones mutualistas de ahorro y crédito para la vivienda, deberán:

a) Contar con un oficial de seguridad física y electrónica con título relacionado con el área de seguridad debidamente registrado en el órgano rector de la educación superior, quien será responsable de planificar, elaborar, dirigir, gestionar y coordinar los planes y medidas de seguridad, el manual y políticas de seguridad y protección, el estudio de seguridad (previo a la ocurrencia de eventos) o análisis de riesgos (una vez que existan eventos), acorde con la presente norma y los requerimientos del Ministerio del Interior a través de la Unidad Nacional de Política de Control de Servicios de Seguridad Privada y Control de Armas Letales y no Letales COSP. Este oficial de seguridad será contratado por la entidad bajo relación de dependencia. El oficial de seguridad física y electrónica debe cumplir sus funciones de manera permanente y exclusiva en la entidad;

b) Para las entidades del Segmento 3, el oficial de seguridad física y electrónica podrá mantener una relación laboral a tiempo parcial, pudiendo compartir otras funciones dentro de las entidades sin que generen conflicto interno de responsabilidades.
Los oficiales de seguridad física y electrónica solamente podrán prestar sus servicios en una sola entidad; y,

c) Contratar a las compañías de seguridad privada; suscribiendo los respectivos acuerdos de confidencialidad y observando además los requisitos que establezca la ley y norma correspondiente y el Ministerio del Interior a través de la Unidad Nacional de Policía de Control de Servicios de Seguridad Privada y Control de Armas Letales y no Letales COSP. Las entidades que funcionen dentro de un edificio, centro comercial o empresa que mantenga un contrato de seguridad que incluya el establecimiento de la entidad podrán mantener un acuerdo de alcance del servicio a través de un contrato, convenio o cualquier documento legal.
Los guardias de seguridad privada realizarán las siguientes labores:

i. Custodia de las instalaciones de la entidad desde el momento de la apertura del establecimiento, durante la atención al público, mientras se encuentren empleados o proveedores laborando y hasta el cierre del establecimiento;

ii. Revisión e inspección a los socios, clientes, usuarios, proveedores y otras personas que ingresen al establecimiento, de acuerdo con la política interna de la entidad;
iii. Mantener el orden en el área de atención al cliente; y,
iv. Llevar actualizadas las bitácoras de seguridad.
v. Desarrollar funciones exclusivas de guardia de seguridad.

Los establecimientos que se encuentra ubicados en locales que cuentan con seguridad de terceros de acuerdo a lo estipulado en el literal b) del numeral 1, podrán contar con agentes o guardias de seguridad de manera adicional.

2. Entidades de los segmentos 4 y 5 y la Corporación:

a) El responsable de la **s**eguridad física y electrónica, el delegado del representante legal quien deberá elaborar, dirigir, gestionar y coordinar los planes y medidas de seguridad en las entidades; y,
b) De manera opcional podrán aplicar lo señalado en el literal b, del numeral 1 del presente artículo.

Artículo 7. Bóvedas y cajas fuertes.- Las entidades para lo relacionado con bóvedas y cajas fuertes, considerarán como mínimo los siguientes aspectos:

1. Las entidades de los segmentos 1, 2, 3, cajas centrales y asociaciones mutualistas de ahorro y crédito para la vivienda deberán:

a) Contar con bóvedas, cajas fuertes y sus áreas conexas en que se deposite efectivo y valores, con acceso restringido, por lo que deben tener elementos y sistemas que garanticen la seguridad y protección, tanto en su contenido como durante los procedimientos de depósito o retiro de efectivo y/o valores objeto de transportación y resguardo;
b) Cumplir con estándares mínimos para la construcción de bóvedas, adquisición de cajas fuertes y puertas de bóveda; y, observar las características de alta seguridad según los lineamientos y estándares internacionales o norma nacional que hayan sido homologados, emitidos por el Servicio Ecuatoriano de Normalización o quien haga sus veces o el certificado del personal técnico autorizado de las bóvedas y cajas fuertes, mismas que contarán con un sistema de anclaje;
c) Contratar pólizas de seguro de acuerdo con las políticas establecidas por las entidades relacionadas con los montos máximos de dinero efectivo y valores que deben permanecer dentro de las bóvedas o cajas fuertes;
d) Contar con cerraduras temporizadas en las puertas de las bóvedas y sistemas de ventilación; con sensores de humo, de movimiento, de vibración; y, adicionalmente, con botones de pánico y sistemas de comunicación ubicados estratégicamente;
e) Tener cámaras de seguridad en la parte interior de las bóvedas y áreas sensibles en donde se ubique las cajas fuertes;
f) Establecer procedimientos para la apertura y cierre de las bóvedas y para situaciones de emergencia, tales como asaltos, siniestro o si alguien permanece en su interior luego de su cierre; y,

g) Las bóvedas contarán con sistemas electrónicos o mecánicos, siempre y cuando cumplan con los demás aspectos señalados en los literales anteriores.

La aplicación de los literales d), e) y f) se exceptúan para las cajas centrales.

2. Las entidades de los segmentos 4 y 5, deberán:

a) Contar con bóvedas y/o cajas fuertes en que se deposite efectivo y documentos valorados, de acceso restringido, por lo que deben tener medidas que proporcionen una adecuada seguridad y protección, tanto a su contenido como durante los procedimientos de depósito o retiro de efectivo;
b) Ubicar las cajas fuertes en un lugar seguro, libres de material u objetos eléctricos o inflamables o lugares propensos a inundación o humedad;
c) Contratar pólizas de seguro de acuerdo con las políticas establecidas por las entidades relacionadas con los montos máximos de dinero efectivo y valores que deben permanecer dentro de las cajas fuertes; y,
d) Las cajas fuertes deberán contar con un sistema electrónico y un sistema de anclaje.

Artículo 8. Sistemas de alarmas.- En lo relacionado a los sistemas de alarmas antirrobo e incendio.

1. Las entidades de los segmentos 1, 2, 3, cajas centrales y asociaciones mutualistas de ahorro y crédito para la vivienda, deberán:

a) Contar con sistemas de alarma antirrobo e incendio, enlazados por frecuencia de radio o cable con centrales de monitoreo y respuesta, comunicadas con la Policía Nacional, Servicio Integrado de Seguridad ECU 911, Cuerpo de Bomberos y empresas de seguridad privada. Los sistemas de alarma para los riesgos de robo deben cumplir con estándares internacionales o norma nacional que hayan sido homologados y/o emitidos por el Servicio Ecuatoriano de Normalización; y, deberán contar con al menos las siguientes características**:**
    i. Tener comunicación continúa de al menos dos tipos al mismo tiempo, ya sea por cualquier sistema de comunicación electrónica, línea telefónica, GSM o TCP/IP entre otros.
    ii. Los sensores de movimiento deben ser al menos de doble tecnología para evitar falsas alarmas.
b) Verificar permanentemente que los sistemas de alarma se encuentren totalmente operativos, con la finalidad de garantizar el funcionamiento correcto de los equipos, así como, garantizar la presencia permanente del personal encargado. También, deberán confirmar que los sistemas de comunicación se encuentren enlazados con las empresas de seguridad privada, la Policía Nacional, Servicio Integrado de Seguridad ECU 911 y Cuerpo de Bomberos; y, el nivel administrativo y los funcionarios de la entidad; y,
c) Verificar que todos los sistemas electrónicos, alarmas y demás elementos de seguridad estén operativos en todo momento y al menos deberán, captar y grabar, tanto las señales de alarma como las escenas de hechos delictivos o siniestros.

Estas grabaciones serán proporcionadas sin costo a las autoridades competentes que lo requieran.

2. Las entidades de los segmentos 4, 5 y la Corporación, deberán:

Contratar e implementar sistemas de monitoreo y alarma que emitan señales de alerta en el caso de algún siniestro o acto delictivo, las cuales deberán ser monitoreadas por una empresa de seguridad que adoptará las medidas de respuesta correspondientes.

Artículo 9. Sistemas de video vigilancia.- En lo referente a los sistemas de video vigilancia (cámaras), las entidades deberán considerar varios parámetros.

1. Las entidades de los segmentos 1, 2, 3, cajas centrales y asociaciones mutualistas de ahorro y crédito para la vivienda, deberán:

a) Contar con un número adecuado de cámaras fijas y móviles de circuito cerrado de televisión, con imágenes de alta resolución, equipadas con videograbadoras, disco duro o su equivalente las veinticuatro (24) horas, los 7 días de la semana. El sistema de video vigilancia debe ser evaluado permanentemente y mantener un registro actualizado de sus niveles de operación, a fin de garantizar su correcto funcionamiento, la nitidez y fidelidad de las imágenes. Para determinar el número mínimo de cámaras se deberá considerar al menos la densidad de personas, riesgos operativos y dimensión física de cada área de acuerdo al estudio de seguridad;

b) Ubicar adecuadamente cámaras fijas y móviles en los lugares de acceso al público, personal de la entidad, área de cajas, cajeros automáticos, interior de la bóveda y todas las áreas restringidas, evitando dejar puntos sin cobertura (las cajas centrales solo en los lugares que aplique) de acuerdo al estudio de seguridad; y,

c) Asegurar que los sistemas de grabación y almacenamiento de imágenes guarden el archivo de por lo menos tres (3) meses de grabación, a través de cintas, de discos de video digital (DVD/DVR) o cualquier otro dispositivo tecnológico actual.

2. Para las entidades de los segmentos 4, 5 y la Corporación

Deberán cumplir con lo previsto en el literal b) y c).

Artículo 10. Medidas de seguridad en cajeros automáticos.- Las entidades que cuenten con cajeros automáticos propios o proporcionados por un tercero deberán considerar las siguientes medidas:

a) **Ubicación y entorno**.- Deben ser instalados en lugares que minimicen el riesgo tanto del cajero automático, de socios, clientes, usuarios o el público en general, que puedan ser objeto o víctimas de actos delictivos;

b) **Protección al teclado**.- Contar en todo momento con "protectores de teclado", que de una manera efectiva impidan la visibilidad al momento que el usuario digite su clave personal;

c) **Protección contra clonación de tarjetas**.- Contar con dispositivos electrónicos y/o elementos físicos que impidan y detecten de manera efectiva la colocación de

falsas lectoras de tarjetas, con el fin de evitar la clonación de tarjetas de débito, crédito o prepago, además de los correspondientes mecanismos de monitoreo en línea de las alarmas que generen los dispositivos electrónicos en caso de suscitarse eventos inusuales;

d) **Iluminación.-** Los cajeros automáticos deberán estar ubicados en zonas suficientemente iluminadas que permitan la visualización de toda actividad a su alrededor;

e) **Programas de vigilancia en sitio.-** Contar con un programa regular de visitas al sitio donde se encuentra instalado el cajero automático, con la finalidad de garantizar que no existan objetos extraños, dispositivos u otros mecanismos sospechosos instalados en el cajero automático;

f) **Mecanismo de anclaje**.- Los cajeros automáticos deben asegurarse adecuadamente al piso con al menos cuatro puntos de anclaje a fin de impedir su remoción;

g) **Procedimientos para el mantenimiento preventivo y correctivo en los cajeros automáticos**.- Disponer de procedimientos auditables debidamente acordados y coordinados entre la entidad y los proveedores internos o externos para la ejecución de las tareas de mantenimiento preventivo y correctivo del hardware y software, provisión de suministros y recarga de dinero en gavetas. Las claves de acceso tipo "administrador" del sistema del cajero automático deben ser únicas y reemplazadas periódicamente de acuerdo a la política de la entidad;

h) **Accesos físicos al interior de los cajeros automáticos**.- Disponer de cerraduras de alta tecnología y seguridades, que garanticen el acceso controlado a la caja fuerte que se encuentra junto o anexo al cajero automático por parte del personal encargado de la provisión y cuadre del efectivo. Estas cerraduras deben operar con llaves únicas y no con llaves genéricas o maestras. El acceso a las cajas fuertes de los cajeros automáticos deberá lograrse únicamente con la intervención simultánea de dos o más personas encargadas de la custodia de las llaves y/o códigos de acceso diferentes entre sí;

i) **Establecer los mecanismos, políticas y procedimientos adecuados para:**
   1. Revisar al menos semestralmente los anclajes, iluminación y entorno del cajero automático;
   2. Abastecer de dinero a los cajeros automáticos;
   3. Atender oportunamente las alarmas generadas por los dispositivos electrónicos de control, instalados en los cajeros automáticos; y,
   4. Contar con personal capacitado para la operación y mantenimiento del cajero.

j) **Cámaras de vigilancia**.- Para la operación, cada cajero automático debe contar al menos con dos cámaras de vigilancia en las siguientes ubicaciones:
   1. Una periférica con vista panorámica de arriba hacia abajo, que permita captar el entorno del equipo; y,
   2. Una cámara frontal que permita identificar las características personales del socio cliente o usuario.

En el caso de que la entidad cuente con el servicio de cajeros automáticos proporcionado por terceros, deberá asegurar que el proveedor garantice el cumplimiento de todas las medidas de seguridad que se han descrito en este artículo.

Artículo 11. Transporte de fondos y valores.- Las entidades considerarán como mínimo los siguientes aspectos, para el transporte de fondos y valores:

1. Las entidades de los segmentos 1, 2, 3 y asociaciones mutualistas de ahorro y crédito para la vivienda, deberán:

a) Promover el uso de canales electrónicos, digitales u otros medios o mecanismos en lugar del manejo de cantidades significativas de dinero en efectivo por parte de los socios y clientes;
b) Brindar seguridad, en coordinación con la Policía Nacional, a los socios, clientes o usuarios que solicitaren dicho servicio para el retiro o depósito de dinero en efectivo;
c) Efectuar la recepción y envío de especies monetarias y valores en las bóvedas, pre bóvedas y cajas fuertes, a través del personal autorizado por la entidad, que eviten su exposición al riesgo;
d) Realizar el traslado de especies y valores a través de empresas debidamente autorizadas, utilizando vehículos blindados que cumplan con las disposiciones del Ministerio del Interior a través de la Unidad Nacional de Policía de Control de Servicios de Seguridad Privada y Control de Armas Letales y no Letales COSP. Mantener actualizadas las fichas con los nombres, firmas y fotografías del personal de la empresa transportadora de fondos y valores. Definir en el manual de seguridad y protección, los montos mínimos y máximos que serán transportados a través de vehículos blindados;
e) Verificar que la empresa contratada por la entidad para el transporte de fondos y valores cuente con los seguros necesarios que resguarden dichos rubros en caso de robo u otras contingencias. En caso de que la entidad financiera no contrate directamente con el servicio de transporte de especies monetarias y valores, deberá mantener un convenio vigente con otra entidad financiera que le garantice la prestación del servicio al momento de requerirlo; y,
f) El contrato de servicio de transporte de fondos y valores deberá considerar al menos los siguientes aspectos: ubicación en tiempo real (GPS) de los vehículos utilizados, movilización en vehículos que cuenten con blindaje incorporado y mantener protocolo de rutas actualizado permanentemente.

2. Las entidades de los segmentos 4 y 5 deberán:

Establecer las medidas de seguridad determinadas en los literales a), b) y c) del numeral anterior, en los casos que aplique; y, adicionalmente:

a) Transportar si fuere necesario por propios medios, fondos y valores, con apoyo de al menos un guardia de seguridad o personal de la Policía Nacional y dos funcionarios de la entidad; y,
b) Las entidades de los segmentos 4 y 5 podrán mantener un convenio con otra entidad que si lo haya contratado para lo cual deberá presentar dicho convenio y cumplir todos los requisitos establecidos en la presente norma.

TÍTULO III
RESPONSABILIDADES DE LAS ENTIDADES

Artículo 12. Responsabilidades de las entidades de los segmentos 1, 2 y 3, asociaciones mutualistas de ahorro y crédito para la vivienda y cajas centrales:

a) El oficial de seguridades física y electrónica elaborará y propondrá a la Unidad de Riesgos o Administrador de Riesgos, según corresponda, los Manuales y Políticas de Seguridad y Protección, así como, las políticas, principios y procedimientos de seguridad y protección para sus empleados, socios, clientes, usuarios, establecimientos, activos y patrimonio, para que dicha Unidad o Administrador de Riesgos, en el contexto de sus atribuciones, revise la propuesta observando que se encuentre alineada a las políticas, procesos o procedimientos vigentes para la administración integral de riesgos u otros riesgos específicos aplicables. Dicha propuesta, una vez revisada, será presentada al Comité de Administración Integral de Riesgos;

b) El Comité de Administración Integral de Riesgos propondrá y recomendará al Consejo de Administración para su aprobación, los Manuales y Políticas de Seguridad y Protección, así como, las políticas, principios y procedimientos de seguridad y protección para sus empleados, socios, clientes, usuarios, establecimientos, activos y patrimonio;

c) El Consejo de Administración según corresponda, aprobará los Manuales y Políticas de Seguridad y Protección, así como, las políticas, principios y procedimientos de seguridad y protección para sus empleados, socios, clientes, usuarios, establecimientos, activos y patrimonio;

d) El oficial de seguridades físicas y electrónicas elaborará los informes mensuales sobre el cumplimiento de las políticas, normas, principios y procedimientos de seguridad y protección para sus empleados, socios, clientes, usuarios, establecimientos, activos y patrimonio, incluyendo las recomendaciones y acciones correctivas que correspondan; adicionalmente, elaborará el estudio de seguridad (previo a la ocurrencia de eventos) o análisis de riesgos (una vez que existan eventos), acorde con los requerimientos del Ministerio del Interior a través de la Unidad Nacional de Política de Control de Servicios de Seguridad Privada y Control de Armas Letales y no Letales COSP;

e) La Unidad de Riesgos o el Administrador de Riesgos, según corresponda ,analizará y evaluará los informes del oficial de seguridades físicas y electrónicas y el estudio de seguridad (previo a la ocurrencia de eventos) o análisis de riesgos (una vez que existan eventos) y los presentará al Comité de Administración Integral de Riesgos, incluyendo de ser el caso, las recomendaciones y acciones correctivas que correspondan;

f) El Comité de Administración Integral de Riesgos propondrá y presentará al Consejo de Administración para su aprobación los informes analizados y evaluados por la Unidad de Riesgos con relación al cumplimiento de las políticas, normas, principios y procedimientos de seguridad y protección para sus empleados, socios, clientes, establecimientos, activos y patrimonio, recomendando, de ser el caso acciones correctivas o preventivas; además, propondrá y presentará al Consejo de Administración para su aprobación el

estudio de seguridad (previo a la ocurrencia de eventos) o análisis de riesgos (una vez que existan eventos) analizados y evaluados por la Unidad de Riesgos;

g) El Consejo de Administración aprobará los informes relacionados al cumplimiento de las políticas, normas, principios y procedimientos de seguridad y protección para sus empleados, socios, clientes, usuarios, establecimientos, activos y patrimonio, propuesto por el Comité de Administración Integral de Riesgos y sus recomendaciones, analizará y aprobará las medidas preventivas y correctivas, de ser el caso, en función de la pertinencia y efectividad de su implementación; además, aprobará el estudio de seguridad (previo a la ocurrencia de eventos) o análisis de riesgos (una vez que existan eventos);

h) El representante legal implementará las políticas, principios y procesos de seguridad y protección aprobados por el Consejo de Administración en aplicación a la presente norma; y,

i) El auditor interno verificará la efectividad de la implementación y cumplimiento de las políticas, principios y procesos básicos de seguridad y protección contemplados en la presente norma y en documentos internos previamente aprobados, de manera permanente junto con las recomendaciones correspondientes. Presentará al menos de manera anual los informes al Consejo de Vigilancia sobre las medidas correctivas, incluyendo los casos de reclamos de los usuarios financieros que involucren debilidades o vulneraciones de los niveles de seguridad.

Artículo 13. Responsabilidades de las entidades de los segmentos 4 y 5 y la Corporación:

a) El delegado del representante legal elaborará y propondrá al Consejo de Administración o Directorio, según corresponda, para su aprobación los Manuales y Políticas de Seguridad y Protección, así como, las políticas, principios y procedimientos básicos de seguridad y protección para sus empleados, socios, clientes, usuarios, establecimientos, activos y patrimonio;

b) El Consejo de Administración o Directorio, aprobará los manuales, políticas, principios y procedimientos básicos de seguridad y protección enfocados en los empleados, socios, clientes, usuarios, establecimientos, activos y patrimonio;

c) El delegado del representante legal elaborará los informes trimestrales sobre el cumplimiento de las políticas, normas, principios y procedimientos de seguridad y protección para sus empleados, socios, clientes, usuarios, establecimientos, activos y patrimonio, incluyendo las recomendaciones y acciones correctivas que correspondan;

d) El Consejo de Administración o Directorio aprobará los informes relacionados al cumplimiento de las políticas, normas, principios y procedimientos de seguridad y protección para sus empleados, socios, clientes, usuarios, establecimientos, activos y patrimonio, propuesto por el delegado del representante legal y sus recomendaciones, y analizará las medidas correctivas, de ser el caso, en función de la pertinencia y efectividad de su implementación; y,

e) El Consejo de Vigilancia o Auditor Interno verificará la efectividad de la implementación y cumplimiento de las políticas, principios y procesos básicos de seguridad y protección contemplados en la presente norma y en documentos internos previamente aprobados, de manera permanente, junto con las

recomendaciones correspondientes. La revisión deberá ser al menos de manera anual.

DISPOSICIONES GENERALES

PRIMERA.- Las entidades, en todas sus áreas restringidas deben contar con:

1. Sistemas y dispositivos de control de acceso, tales como: exclusas, biométrico, tarjetas de proximidad, entre otras determinadas y autorizadas por el ente rector de seguridad ciudadana y orden público. Adaptadas al tamaño y tipo de punto de atención; y,
2. En el caso de las entidades que cuentan con puertas blindadas el nivel de blindaje requerido es NIJ II o sus equivalentes.

SEGUNDA.- Las entidades, en los casos que sea aplicable, deberán mantener actualizadas y en custodia las certificaciones con las respectivas especificaciones e informes técnicos sobre lo siguiente:

a) Blindaje transparente para vidrio y opaco para puertas y mampostería en las áreas sensibles y restringidas de la entidad;
b) Sistema de alarma;
c) Sistema de video vigilancia;
d) Bóvedas y las puertas;
e) Cajas fuertes;
f) Sensores de movimiento;
g) Controles de acceso; y,
h) Sistema eléctrico y de iluminación.

Las certificaciones serán emitidas por el fabricante, por un profesional calificado que evalué la instalación o informe técnico del responsable que avale los dispositivos y/o estructuras.

Esta información deberá presentarse a la Superintendencia de Economía Popular y Solidaria, el Ministerio del Interior a través de la Unidad Nacional de Policía de Control de Servicios de Seguridad Privada y Control de Armas Letales y no Letales COSP, cuando así lo requieran.

TERCERA.- Las entidades que operen mediante ventanillas de extensión de servicios o puntos de atención móviles, deberán contar con una póliza de seguro de vida (se puede considerar la póliza que mantenga vigente la entidad para sus empleados) y robo que ampare al personal involucrado, así como los insumos utilizados para el servicio otorgado y el efectivo administrado. Asimismo, deberán emitir y mantener actualizadas políticas y procedimientos orientados a la prevención, gestión y respuesta frente a incidentes, contingencias o cualquier eventualidad que pudiera presentarse durante la prestación del servicio, priorizando la seguridad física del personal, socios, clientes y usuarios. Dichas políticas deberán contemplar responsabilidades, protocolos de actuación, mecanismos de notificación y medidas de mitigación, a fin de asegurar una

gestión oportuna y efectiva de riesgos operativos asociados al funcionamiento en estos establecimientos.

CUARTA.- Las entidades deberán considerar como marco de referencia para la implementación de sus controles técnicos y operativos, los mencionados en los artículos precedentes y los emitidos por el Ministerio del Interior a través de la Unidad Nacional de Policía de Control de Servicios de Seguridad Privada y Control de Armas Letales y no Letales COSP para los fines pertinentes. Además, las entidades deberán implementar controles de seguridad lógica que soporten y refuercen las medidas de seguridad física, aplicando los siguientes requisitos:

1. **Segmentación de Red:** Los sistemas de seguridad física basados en IP (CCTV, Control de Acceso, Alarmas) deberán operar en una red lógica separada y segmentada del resto de la red corporativa;
2. **Protección de Endpoints y Servidores:** Los servidores, dispositivos de grabación (DVR/NVR) y estaciones de trabajo utilizados para el monitoreo y gestión de la seguridad física deberán contar con **protección *endpoint*** (antivirus, antimalware) actualizada y configurada para prevenir ciberataques que comprometan la infraestructura física; y,
3. **Gestión de Vulnerabilidades:** Se deberán aplicar procesos de *hardening* a todos los dispositivos tecnológicos de seguridad (cámaras IP, paneles de acceso, dispositivos de grabación), y se deberá realizar una gestión proactiva de parches y vulnerabilidades para evitar compromisos lógicos que impacten la seguridad física.

QUINTA.- Todos los sistemas, equipos y componentes de seguridad física -incluyendo sistemas de alarma, control de acceso, video vigilancia, sensores, iluminación de emergencia, cajas fuertes con sistema electrónico, bóvedas y demás elementos críticos- deberán someterse a mantenimientos preventivos y revisiones técnicas de acuerdo al cronograma de cada entidad, con una frecuencia mínima de seis meses. Estas actividades deberán ser ejecutadas por proveedores certificados o personal técnico autorizado, con la correspondiente evidencia documental, informe de resultados, registros de pruebas de funcionamiento y cronograma de acciones correctivas. Los reportes de mantenimiento deberán conservarse para garantizar la continuidad operativa y la eficacia de las medidas de protección física. Los resultados de las revisiones técnicas o pruebas de funcionamiento deberán ser documentados y evaluados por el responsable de seguridad física y electrónica, a fin de garantizar la mejora continua de los controles físicos y electrónicos.

Las entidades deberán evaluar anualmente el desempeño, cumplimiento contractual y medidas de seguridad implementadas por los proveedores de servicios de seguridad física, transporte de valores y mantenimiento técnico.

SEXTA.- En referencia a la implementación de señalética institucional de seguridad las entidades, deberán tomar como marco de referencia a la Norma técnica ecuatoriana NTE INEN – ISO 3864-1:2013 “Símbolos gráficos. Colores de Seguridad y Señales de Seguridad”.

SÉPTIMA.- Las entidades deberán garantizar la implementación de medidas específicas de accesibilidad y protección orientadas a personas de atención prioritaria, tales como adultos mayores, personas con discapacidad, mujeres embarazadas y otros grupos vulnerables, de conformidad con la normativa vigente. Estas medidas deberán incluir adecuaciones físicas, señalización, rutas seguras, dispositivos de asistencia y protocolos de atención que faciliten el acceso y la evacuación en condiciones de seguridad.

Adicionalmente, las entidades podrán adoptar medidas complementarias de seguridad física a las establecidas en la presente normativa, con el propósito de reforzar la protección de las personas, bienes e información y minimizar posibles eventos de riesgo derivados de amenazas internas o externas. Dichas medidas adicionales deberán estar debidamente documentadas, justificadas en un análisis de riesgo y aprobadas por la instancia competente de seguridad institucional.

OCTAVA.- Las entidades deberán considerar que las políticas y procedimientos de seguridad física y electrónica constituyen un componente integral del riesgo operativo y la seguridad de la información, debiendo identificar, medir, controlar, monitorear y comunicar los riesgos asociados a la confidencialidad, integridad y disponibilidad de la información, en concordancia con la normativa vigente emitida por la Superintendencia de Economía Popular y Solidaria.

NOVENA.- La entidades deberán gestionar por medio del Ministerio del Interior a través de la Unidad Nacional de Policía de Control de Servicios de Seguridad Privada y Control de Armas Letales y no Letales COSP, las acciones correspondientes para obtener el certificado de seguridad; así como, la renovación de permisos y certificaciones que se requieran en el marco de esta norma.

DÉCIMA.- El control y verificación de la vigencia del certificado de seguridad otorgado por el Ministerio del Interior estará a cargo de la Unidad Nacional de Policía de Control de Servicios de Seguridad Privada y Control de Armas Letales y no Letales COSP, quien emitirá al ente rector el incumplimiento de la obtención del certificado de seguridad.

DISPOSICIONES TRANSITORIAS

PRIMERA.- Las entidades y la Corporación implementarán esta norma hasta dentro de los plazos previstos en la siguiente tabla:

Entidades	Plazo
Segmentos 1, 2, 3, asociaciones mutualistas de ahorro y crédito para la vivienda, la Corporación y Cajas Centrales.	18 meses
Segmentos 4 y 5.	24 meses

SEGUNDA.- En los procesos de supervisión que ejecute esta Superintendencia con respecto a las seguridades físicas y electrónicas, hasta el cumplimiento de los plazos establecidos en la disposición transitoria primera, se considerara lo dispuesto en la Resolución No. SEPS-IGT-IR-IGJ-2018-021 de 13 de julio de 2018 reformada con la Resolución No. SEPS-IGT-IR-IGJ-2018-0259 de 10 de octubre de 2018.

TERCERA.- Las organizaciones y empresas de servicios auxiliares hasta la expedición de la nueva norma general sobre los servicios auxiliares observarán y cumplirán con lo dispuesto en la Resolución SEPS-IGT-IR-IGJ-2018-021 de 13 de julio de 2018 reformada por la Resolución No. SEPS-IGT-IR-IGJ-2018-0259 de 10 de octubre de 2018.

DISPOSICIÓN DEROGATORIA.- La Resolución No. SEPS-IGT-IR-IGJ-2018-021 de 13 de julio de 2018 reformada con la Resolución No. SEPS-IGT-IR-IGJ-2018-0259 de 10 de octubre de 2018, quedará sin efecto para las distintas entidades y la Corporación, en los plazos establecidos en la Disposición Transitoria Primera de la presente norma.

DISPOSICIÓN FINAL.- La presente resolución entrará en vigencia a partir de la fecha de expedición, sin perjuicio de su publicación en el Registro Oficial. Publíquese en la página web de esta Superintendencia.

COMUNÍQUESE Y PUBLÍQUESE.- Dada y firmado en la ciudad de San Francisco de Quito, Distrito Metropolitano, a los 5 días del mes de junio de 2026.

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
FREDDY ALFONSO MONGE MUÑOZ

FREDDY ALFONSO MONGE MUÑOZ
INTENDENTE GENERAL TÉCNICO