SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

RESOLUCIÓN No. SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002

SOFÍA MARGARITA HERNÁNDEZ NARANJO
SUPERINTENDENTE DE ECONOMÍA POPULAR Y SOLIDARIA

CONSIDERANDO:

Que, la Constitución de la República del Ecuador, en su artículo 66, numeral 19, prescribe: *"Se reconoce y garantizará a las personas: (...) 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley"*;

Que, el artículo 82 de la Norma Suprema dispone: *"El derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes"*;

Que, el artículo 226 ibídem señala: *"Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución"*;

Que, el artículo 283, inciso segundo ejusdem establece: *"(...) El sistema económico se integrará por las formas de organización económica pública, privada, mixta, popular y solidaria, y las demás que la Constitución determine. La economía popular y solidaria se regulará de acuerdo con la ley e incluirá a los sectores cooperativistas, asociativos y comunitarios"*;

Que, el Código Orgánico Monetario y Financiero regula los sistemas monetario y financiero, así como los regímenes de valores y seguros del Ecuador;

Que, el artículo 13 del Libro 1 de dicho Código crea la Junta de Política y Regulación Financiera, parte de la Función Ejecutiva, responsable de la formulación de la política y regulación, crediticia, financiera, de valores, seguros y servicios de atención integral de salud prepagada;

Que, el numeral 7 y el último inciso del artículo 62 del aludido Código, en concordancia con el último inciso del artículo 74, establece como una de las funciones de la Superintendencia de Economía Popular y Solidaria,: " *7. 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, sin restricción alguna, de acuerdo a las mejores prácticas, 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; (...)

La superintendencia, para el cumplimiento de estas funciones, podrá expedir todos los actos y contratos que fueren necesarios. Asimismo, 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, el artículo 163 del referido Código determina que las cooperativas de ahorro y crédito, las asociaciones mutualistas de ahorro y crédito para la vivienda, cajas centrales, de servicios auxiliares del sistema financiero, entre otras, forman parte del sector financiero popular y solidario;

Que, el artículo 387 del citado Código previene que es competencia de la Superintendencia de Economía Popular y Solidaria el control de las actividades financieras de las entidades del Sector Financiero Popular y Solidario y de la entidad financiera pública a la que se refiere la Ley Orgánica de Economía Popular y Solidaria;

Que, los artículos 434 y 436 ibídem en su parte pertinente, en su orden, disponen: *"**Naturaleza**. Los servicios auxiliares serán prestados por personas jurídicas no financieras constituidas como sociedades anónimas o compañías limitadas, cuya vida jurídica se regirá por las disposiciones de la Ley de Compañías. El objeto social de estas compañías será claramente determinado. (...)" "**Calificación**. Las compañías, para prestar los servicios auxiliares a las entidades del sistema financiero nacional, deberán calificarse previamente ante el organismo de control correspondiente, la que como parte de la calificación podrá disponer la reforma del estatuto social y el incremento del capital, con el propósito de asegurar su solvencia. (...)"*;

Que, el artículo 444 ejusdem determina que: *"**Regulación y control.** Las entidades financieras populares y solidarias están sometidas a la regulación de la Junta de Política y Regulación 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 solidario"*;

Que, la Disposición Transitoria Quincuagésima Cuarta ibídem determina: "*Régimen transitorio de Resoluciones de la Codificación de la Junta de Política y Regulación Monetaria y Financiera. Las resoluciones que constan en la Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros de la Junta de Política y Regulación Monetaria y Financiera y las normas emitidas por los organismos de control, mantendrán su vigencia hasta que la Junta de Política y Regulación Monetaria y la Junta de Política y Regulación Financiera resuelvan lo que corresponda, en el ámbito de sus competencias*";

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, la de: *"Dictar las normas de control (...)"*;

Que, el artículo 158 de la aludida Ley Orgánica crea la Corporación Nacional de Finanzas Populares y Solidarias, como una entidad financiera de derecho público;

Que, el artículo 165 del citado cuerpo legal establece que la Corporación Nacional de Finanzas Populares y Solidarias CONAFIPS estará sometida al control y supervisión de la Superintendencia de Economía Popular y Solidaria, y tendrá una unidad de auditoría interna encargada de las funciones de su control interno;

Que, en la Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros, en el Libro I "Sistema Monetario y Financiero", Título II "Sistema Financiero Nacional", Capítulo XXXVII "Sector Financiero Popular y Solidario", consta la Sección III, "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", cuya Disposición General Cuarta determina que la Superintendencia de Economía Popular y Solidaria podrá emitir las normas de control necesarias para su aplicación;

Que, en la Codificación ibídem, en el Libro I "Sistema Monetario y Financiero", Título II "Sistema Financiero Nacional", Capítulo XXXVII "Sector Financiero Popular y Solidario", consta la Sección VIII "NORMA PARA LA ADMINISTRACIÓN INTEGRAL DE RIESGOS DE LA CORPORACIÓN NACIONAL DE FINANZAS POPULARES Y SOLIDARIAS"; cuya Disposición General Segunda determina que la Superintendencia de Economía Popular y Solidaria podrá emitir las normas de control necesarias para su aplicación;

Que, mediante Resolución No. SEPS-IGT-IR-IGJ-2018-021, de 13 de julio de 2018, la Superintendencia de Economía Popular y Solidaria emitió la *"Norma de control respecto de la seguridad física y electrónica"*, reformada por la Resolución No. SEPS-IGT-IR-IGJ-2018-0259, de 10 de octubre de 2018;

Que, mediante Resolución No. SEPS-IGT-IR-IGJ-2018-0279, de 26 de noviembre de 2018, la Superintendencia de Economía Popular y Solidaria emitió la *"Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del Sector Financiero Popular y Solidario, bajo el control de la Superintendencia de Economía Popular y Solidaria"*, reformada por las resoluciones Nos. SEPS-IGT-IR-IGJ-2018-0284 de 13 de diciembre de 2018 y SEPS-IGT-IGS-INR-INGINT-2020-0221 de 2 de junio de 2020;

Que, mediante Resolución No. SEPS-IGT-IGS-INFMR-INGINT-IGJ-2020-0153, de 12 de mayo de 2020, la Superintendencia de Economía Popular y Solidaria emitió la *"Norma de control sobre los principios y lineamientos de educación financiera"*;

Que, es necesario que la Superintendencia de Economía Popular y Solidaria expida una norma de control para la seguridad de la información que coadyuve al fortalecimiento de los procesos internos de las entidades del Sector Financiero Popular y Solidario, bajo el control de la Superintendencia de Economía Popular y Solidaria; y,

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.

En ejercicio de sus atribuciones y funciones, resuelve expedir la siguiente:

NORMA DE CONTROL RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN EN LAS ENTIDADES DEL SECTOR FINANCIERO POPULAR Y SOLIDARIO BAJO CONTROL DE LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

CAPÍTULO I
ÁMBITO, OBJETO, REGÍMENES Y DEFINICIONES

Artículo 1.- Ámbito.- Las disposiciones de la presente norma, de acuerdo a su segmento, aplicarán para:

a) Las cooperativas de ahorro y crédito, asociaciones mutualistas de ahorro y crédito para la vivienda y cajas centrales, en adelante denominadas "entidad o entidades"; y, a la Corporación Nacional de Finanzas Populares y Solidarias, en lo sucesivo CONAFIPS; y,
b) Las compañías y organizaciones de servicios auxiliares que prestan servicios a las actividades financieras de las entidades y CONAFIPS, en adelante "empresas".

Artículo 2.- Objeto.- La presente norma tiene por objeto regular los niveles mínimos para la administración de seguridad de la información que las entidades, la CONAFIPS y las empresas, deben definir e implementar con el fin de resguardar y proteger sus activos de información, preservando su confidencialidad, disponibilidad e integridad.

Artículo 3.- Regímenes.- Para efectos de esta norma, se aplicarán los siguientes regímenes:

1. Régimen general: a las cooperativas de ahorro y crédito de los segmentos 1 y 2; a las asociaciones mutualistas de ahorro y crédito para la vivienda y a la CONAFIPS;
2. Régimen especial: a las cooperativas de ahorro y crédito del segmento 3; y,
3. Régimen simplificado: a las cooperativas de ahorro y crédito de los segmentos 4 y 5.

A las empresas se aplicarán los regímenes anteriores según el tipo de servicio que presten, de acuerdo con la siguiente tabla:

Tipos de Servicios Auxiliares	General	Especial	Simplificado
Software financiero y computación	x		
Transaccionales y de pago	x		
Transporte de especies monetarias y de valores		x	
Red de cajeros automáticos	x		
Cobranzas		x	
Generadoras de cartera	x		

Administradoras de tarjetas	x		
Giro inmobiliario			x
Servicios contables			x

Artículo 4.- Definiciones.- Para la aplicación de esta norma, se considerarán las siguientes definiciones:

- **Activo de información:** se consideran a los servicios o herramientas creados o utilizados en medios digital, físico, electromagnético y otros; hardware o software, utilizados para el procesamiento, transferencia o almacenamiento de información; y, cualquier dato que tenga información valorada por la entidad, CONAFIPS o empresa.
- **Autorización de accesos:** acto por el cual se permite el acceso de los usuarios a zonas restringidas, a distintos equipos y/o servicios, después de haber superado el proceso de autenticación.
- **Bitácora de eventos de riesgos:** registro de eventos de riesgo durante un periodo en particular. Se registrará acorde a la "Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del Sector Financiero Popular y Solidario bajo el control de la Superintendencia de Economía Popular y Solidaria".
- **Cifrar:** es el proceso mediante el cual la información o archivos son transformados en forma lógica y controlada, con el objetivo de evitar que alguien no autorizado pueda interpretarlos, verlos o copiarlos.
- **Confidencialidad:** es la propiedad por la que se garantiza que la información es accesible solo al personal autorizado.
- **Disponibilidad:** acceso a la información en el tiempo y forma en que ésta sea requerida.
- **Información:** es cualquier forma de registro físico, electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado y distribuido.
- **Integridad:** es la cualidad de que la información se mantiene inalterada y completa.
- **ISO/IEC 27000:** Se refiere a la Norma Técnica emitida por el Servicio Ecuatoriano de Normalización, INEN, NTE INEN-ISO/IEC 27000 Cuarta edición 2016-11 TECNOLOGÍAS DE LA INFORMACIÓN — TÉCNICAS DE SEGURIDAD — SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN — DESCRIPCIÓN GENERAL Y VOCABULARIO (ISO/IEC 27000:2016, IDT)
- **Partes interesadas:** son todas las personas naturales o jurídicas que, de alguna forma, puedan verse afectadas por la actividad de la entidad, de la CONAFIPS o de la empresa.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Zonas restringidas:** son aquellas que requieren de una autorización de acceso.

CAPÍTULO II
SEGURIDAD DE LA INFORMACIÓN – RÉGIMEN GENERAL

Artículo 5.- Régimen General.- Conforman el régimen general de seguridad de la información:

a) El Consejo de Administración o el Directorio, según corresponda;
b) El Comité de Seguridad de la Información (CSI);
c) El Gerente General o Representante Legal;

d) La Unidad o Departamento de Seguridad de la Información; y,
e) El Oficial de Seguridad de la Información (OSI).

Artículo 6.- Comité de Seguridad de la Información (CSI).- Las entidades, empresas y la CONAFIPS que conforman este régimen, deberán contar con un Comité de Seguridad de la Información (CSI), conformado por los siguientes miembros:
a) El presidente del Comité de Administración Integral de Riesgos, quien presidirá también el Comité de Seguridad de la Información y tendrá voto dirimente;
b) El Gerente General o representante legal;
c) El oficial de seguridad de la información, quien actuará como secretario del Comité;
d) El responsable del área de tecnología o su delegado; y,
e) Un delegado de Auditoría Interna.

El Comité podrá invitar a las sesiones a los responsables de las áreas de negocio que juzgue del caso, quienes tendrán voz pero no voto.

Artículo 7.- Sesiones del Comité de Seguridad de la Información.- Las sesiones del Comité de Seguridad de la Información (CSI), se instalarán con la asistencia de al menos tres de sus miembros, entre los cuales deberá estar presente su presidente.

El Comité sesionará de manera ordinaria al menos dos veces al año. Podrá reunirse extraordinariamente cuando el presidente lo convoque por iniciativa propia, o a petición de uno de sus miembros y/o cuando por eventos de fuerza mayor o caso fortuito lo amerite. En las sesiones extraordinarias se tratarán únicamente los puntos del orden del día.

Las decisiones serán tomadas por mayoría de votos.

Las convocatorias tendrán el orden del día y deberán ser comunicadas por el presidente con, al menos, cuarenta y ocho horas de anticipación, excepto cuando se trate de sesiones extraordinarias que podrán ser convocadas en cualquier momento.

Las sesiones podrán realizarse de manera presencial, o por cualquier medio tecnológico.

Las resoluciones constarán en las respectivas actas, las que deberá elaborar el secretario del Comité, quien además las fechará y numerará en forma secuencial, así como estarán suscritas por los asistentes. Será responsabilidad del secretario la custodia de las actas bajo principios de confidencialidad, integridad y disponibilidad de la información.

Artículo 8.- Unidad o Departamento de Seguridad de la Información.- Las entidades, empresas y la CONAFIPS que conforman este régimen, deberán contar con una Unidad o Departamento de Seguridad de la Información, liderado por el Oficial de Seguridad de la Información (OSI), quien debe tener título universitario de tercer nivel y evidenciar al menos 40 horas de capacitación en seguridad de la información en los dos años inmediatamente anteriores al ejercicio de sus funciones. Dicha Unidad o Departamento, debe estar adscrita a la Gerencia General o representante legal.

Artículo 9.- Requisitos obligatorios para el Régimen General.- Las entidades, empresas y la CONAFIPS pertenecientes a este régimen deberán contar con al menos, lo siguiente:
a) Plan Estratégico de Seguridad de la Información;

b) Plan de Recursos (técnicos, humanos, financieros) para seguridad de la información;
c) Plan de Gestión de Riesgos de Seguridad de la Información. Al efecto podrán tomar como referencia el Anexo 2 de esta resolución;
d) Plan de Concienciación y Formación de Seguridad de la Información;
e) Políticas, procesos, procedimientos, roles y responsabilidades para la gestión de seguridad de la información y del SGSI;
f) Los requerimientos señalados en el Anexo 1 de esta resolución, correspondiente al Régimen General; y,
g) Sistema de Gestión de Seguridad de la Información (SGSI).

Artículo 10.- Sistema de Gestión de Seguridad de la Información (SGSI).- Las entidades, empresas y la CONAFIPS que conforman este régimen, deberán implementar y mantener un SGSI, orientado a garantizar la adecuada gestión de seguridad de la información, con base en la serie de estándares ISO/IEC 27000, y acorde a la normativa legal vigente.

Para establecer el alcance del SGSI, además de lo previsto en el artículo anterior y la serie de estándares ISO/IEC 27000, deberán considerar:

1) Definición de tipos de información con criterios de integridad, confidencialidad y disponibilidad; y,
2) Identificación y clasificación de activos de información, que contendrá:
   a) Personas;
   b) Procesos agregadores de valor y/o catalogados como sensibles o críticos;
   c) Unidades intervinientes en los procesos;
   d) Infraestructura tecnológica;
   e) Ubicaciones físicas y puntos de atención, oficina matriz, sucursales, agencias, puntos móviles, corresponsales solidarios; y,
   f) Relaciones con personas naturales y/o jurídicas que pudieren acceder a información crítica o sensible.

Artículo 11.- Medidas de Seguridad de la Información (controles).- Las entidades, empresas y la CONAFIPS que conforman este régimen, al implementar el SGSI, deberán adoptar las medidas de seguridad de información observando los controles específicos enumerados en la norma técnica ISO/IEC 27002 o las que las sustituyan, de acuerdo al análisis de riesgos establecido. Además deberán implementar los controles obligatorios previstos para este Régimen, en el Anexo 1.

Artículo 12.- Responsabilidades de la gestión de seguridad de la información.- Los órganos internos de dichas entidades, empresas y la CONAFIPS, además de las responsabilidades previstas en la normativa legal vigente, deberán cumplir con lo descrito a continuación, para una gestión adecuada de la seguridad de la información:

1. Consejo de Administración o Directorio:

a) Aprobar el Plan Estratégico de Seguridad de la Información, el mismo que debe estar alineado al Plan Estratégico de la entidades, empresas y la CONAFIPS;
b) Aprobar los recursos humanos, técnicos y financieros que sean necesarios;
c) Aprobar políticas, procesos, procedimientos, roles y responsabilidades;
d) Aprobar el Plan de Concienciación y Formación; y,
e) Aprobar el Plan de Gestión de Riesgos de Seguridad de la Información.

2. **Comité de Seguridad de la Información (CSI).-** Deberá proponer al Consejo de Administración o al Directorio, según corresponda:

a) El Plan Estratégico de Seguridad de la Información;
b) Los recursos humanos, técnicos y financieros necesarios para la gestión de seguridad de la información y verificar que su inversión sea eficiente y eficaz para el logro de los objetivos estratégicos;
c) Las políticas, procedimientos, roles y responsabilidades para la gestión de seguridad de la información y del SGSI;
d) El Plan de Concienciación y Formación de su personal, en temas concernientes a seguridad de la información; y,
e) El Plan de Gestión de Riesgos de Seguridad de la Información y verificar que esté alineado al Plan de Administración de Riesgos.

Además de lo señalado en el numeral anterior, el Comité de Seguridad de la Información, deberá aprobar la implementación de controles de seguridad de la información, propuestos por el Oficial de Seguridad de la Información (OSI); informar los riesgos de seguridad de la información al Comité de Administración Integral de Riesgos, para su consolidación en la matriz de riesgos y su seguimiento; y, evaluar, dirigir, monitorear y supervisar la gestión de seguridad de la información y del SGSI.

3. **Gerente general o representante legal:**

a) Liderar la gestión de seguridad de la información y el SGSI, de acuerdo con las disposiciones del Consejo de Administración o del Directorio y lo dispuesto en esta norma;
b) Designar al Oficial de Seguridad de la Información (OSI); y
c) Coordinar la participación activa de todas las partes interesadas que intervienen en el SGSI y en la gestión de seguridad de la información.

4. **Oficial de Seguridad de la Información:**

Entre sus responsabilidades, tendrá las siguientes:

a) Desarrollar, gestionar y monitorear el Plan Estratégico de Seguridad de la Información y el SGSI;
b) Diseñar y proponer las políticas, procesos, procedimientos, roles y responsabilidades para la gestión de seguridad de la información y del SGSI, al Consejo de Administración;
c) Solicitar la asignación de los recursos humanos, técnicos y financieros necesarios para la gestión de seguridad de la información, y velar que los mismos sean utilizados de forma eficiente y eficaz, alineados con los objetivos estratégicos institucionales;
d) Elaborar, implementar, mantener y actualizar las políticas, procesos, procedimientos, metodologías, planes y controles concernientes a la gestión de seguridad de la información, del SGSI, su mejora continua; y, una vez aprobados, difundirlos al personal que corresponde;
e) Desarrollar y ejecutar los Planes de Concienciación y Formación a su personal, en temas concernientes a seguridad de la información;
f) Coordinar y supervisar, con los responsables de los procesos del negocio, la implementación efectiva de los controles de seguridad de la información, establecidos en el plan de gestión de riesgos;
g) Desarrollar, coordinar, ejecutar, evaluar, proponer y comunicar el Plan de Gestión de Riesgos de Seguridad de la Información;

23.

h) Coordinar las actividades para la gestión de seguridad de la información y del SGSI, incluyendo su implementación y seguimiento;
i) Definir, ejecutar y mantener procedimientos para la gestión de incidentes de seguridad de la información;
j) Velar que los involucrados internos y/o externos cuenten con los conocimientos y capacitación necesaria para el cumplimiento de sus roles y responsabilidades para la ejecución de procedimientos de respuesta ante incidentes;
k) Ejecutar los procedimientos y lineamientos establecidos, cuando se identifiquen incidentes de seguridad de la información;
l) Informar, de acuerdo con la normativa pertinente, los incidentes de seguridad de la información catalogados como sensibles o críticos, a las instituciones públicas que correspondan;
m) Participar en la evaluación de las amenazas de seguridad de la información y proponer medidas de mitigación;
n) Asesorar en materia de seguridad de la información, a través de su participación en los proyectos que involucren el manejo de información sensible o crítica de la misma, de sus socios, clientes y usuarios;
o) Recomendar medidas correctivas adicionales en temas relacionados de seguridad de la información, alineadas al Anexo 1, Régimen General y/o alineadas a buenas prácticas;
p) Verificar que los servicios prestados por personas naturales o jurídicas cumplan con las políticas de seguridad de la información establecidas; y,
q) Generar la documentación que evidencie la gestión de la seguridad de la información y del SGSI.

5. Auditor interno:
a) Verificar la efectividad de las medidas implementadas por la Unidad de Seguridad de la información;
b) Custodiar los informes de las auditorías y/o pruebas de vulnerabilidades realizadas por la Unidad de Seguridad de la Información y ponerlos a disposición de la Superintendencia de Economía Popular y Solidaria, cuando esta lo requiera; y,
c) Recomendar medidas correctivas a la Unidad de Seguridad de la Información.

Artículo 13.- Evaluación y cumplimiento.- Las entidades, empresas y la CONAFIPS que conforman este régimen, una vez implementado el SGSI, deberán realizar evaluaciones, revisiones, pruebas, exámenes y actualizaciones, anualmente o cuando se requiera, para determinar su efectividad, mediante auditorías internas y/o de terceros. En función de los resultados deberán incorporar las mejoras o adoptar las medidas correctivas, impulsando la mejora continua del SGSI.

CAPÍTULO III
SEGURIDAD DE LA INFORMACIÓN – RÉGIMEN ESPECIAL

Artículo 14.- Régimen Especial.- Conforman el régimen especial de seguridad de la información:

a) El Consejo de Administración o Directorio;
b) El Comité de Seguridad de la Información (CSI);
c) El Gerente General o Representante Legal; y,

d) El Oficial de Seguridad de la Información (OSI).

Artículo 15.- Comité de Seguridad de la Información (CSI).- Las entidades y empresas que conforman este régimen, deberán contar con un Comité de Seguridad de la Información (CSI), conformado por los siguientes miembros:

a) El presidente del Comité de Administración Integral de Riesgos, quien presidirá también el Comité de Seguridad de la Información y tendrá voto dirimente;
b) El Gerente General o representante legal;
c) El oficial de seguridad de la información, quien actuará como secretario del Comité;
d) El responsable del área de tecnología o su delegado; y,
e) Un delegado de Auditoría Interna.

El Comité podrá invitar a las sesiones a los responsables de las áreas de negocio que juzgue del caso, quienes tendrán voz pero no voto.

Artículo 16.- Sesiones del Comité de Seguridad de la Información.- Las sesiones del Comité de Seguridad de la Información (CSI), se instalarán con la asistencia de al menos tres de sus miembros entre los cuales deberá estar presente su presidente.

El Comité sesionará de manera ordinaria al menos dos veces al año. Podrá reunirse extraordinariamente cuando el presidente lo convoque por iniciativa propia, o a petición de uno de sus miembros y/o cuando existieren eventos fortuitos o casos de fuerza mayor. En las sesiones extraordinarias se tratarán únicamente los puntos del orden del día.

Las decisiones serán tomadas por mayoría de votos.

Las convocatorias tendrán el orden del día y deberán ser comunicadas por el presidente con al menos cuarenta y ocho horas de anticipación, excepto cuando se traten de sesiones extraordinarias que podrán ser convocadas en cualquier momento.

Las sesiones se podrán realizar de manera presencial o no presencial, de acuerdo al alcance de las entidades y empresas.

Las resoluciones constarán en las respectivas actas que las deberá elaborar el secretario del Comité, quien las deberá llevar fechadas y numeradas en forma secuencial y suscritas por los asistentes. Será responsabilidad del secretario la custodia de las actas bajo principios de confidencialidad, integridad y disponibilidad de la información.

Artículo 17.- Oficial de Seguridad de la Información.- Las entidades y empresas que conforman este régimen, deberán contar con un Oficial de Seguridad de la Información (OSI), que tenga conocimientos verificables y demuestre entrenamiento continuo en seguridad de la información. Dicho Oficial debe tener título universitario de tercer nivel y evidenciar al menos 40 horas de capacitación en seguridad de la información en los dos años inmediatamente anteriores al ejercicio de sus funciones. El Oficial de Seguridad de la Información deberá estar adscrito a la Gerencia General o representante legal.

Artículo 18.- Requisitos obligatorios para el Régimen Especial.- Las entidades y empresas pertenecientes a este régimen deberán contar con al menos, lo siguiente:

a) Asignación de recursos humanos, técnicos y financieros para seguridad de la información;
b) Plan de Gestión de Riesgos de Seguridad de la Información. Al efecto, las entidades y empresas podrán tomar como referencia el Anexo 2 de esta resolución;
c) Plan de Concienciación y Formación para Seguridad de la Información;
d) Políticas, procesos, procedimientos, roles y responsabilidades para la gestión de seguridad de la información;
e) Los requerimientos señalados en el Anexo 1 de esta resolución, correspondiente al Régimen Especial;
f) Clasificación e identificación de tipos de información críticos o sensibles con criterios de integridad, confidencialidad y disponibilidad; y,
g) Identificación de activos de información, tomando en cuenta que contendrá:
   1) Personas;
   2) Procesos agregadores de valor y/o catalogados como sensibles o críticos;
   3) Unidades de las entidades y empresas intervinientes en los procesos;
   4) Infraestructura tecnológica;
   5) Ubicaciones físicas y puntos de atención, oficina matriz, sucursales, agencias, puntos móviles, corresponsales solidarios; y,
   6) Relaciones con personas naturales y/o jurídicas que pudieren acceder a información crítica o sensible.

Artículo 19.- Medidas de seguridad de la información (controles).- Las entidades y empresas que conforman este régimen, para la gestión de seguridad de la información, deberán implementar los controles mínimos previstos para este Régimen en el Anexo 1.

Artículo 20.- Responsabilidades en la gestión de seguridad de la información.- Los órganos internos de dichas entidades y empresas, además de las responsabilidades previstas en la normativa legal vigente, deberán cumplir con lo descrito a continuación, para una gestión adecuada de la seguridad de la información:

1. **Consejo de Administración o Directorio:**

a) Aprobar la asignación de los recursos humanos, técnicos y financieros que sean necesarios;
b) Aprobar las políticas, procesos, procedimientos, roles y responsabilidades;
c) Aprobar los planes de concienciación y formación concernientes a seguridad de la información; y,
d) Aprobar el Plan de Gestión de Riesgos de Seguridad de la Información.

2. **Comité de Seguridad de la Información (CSI).-** Deberá proponer al Consejo de Administración:

a) La asignación de los recursos humanos, técnicos y financieros necesarios para la gestión de seguridad de la información y verificar que su inversión sea eficiente y eficaz para el logro de los objetivos estratégicos de las entidades y empresas;
b) Las políticas, procedimientos, roles y responsabilidades para la gestión de seguridad de la información;
c) Los Planes de Concienciación y Formación concernientes a seguridad de la información; y,
d) El Plan de Gestión de Riesgos de seguridad de la información y verificar que esté alineado al Plan de Administración de riesgos de las entidades y empresas.

Además de lo señalado en el inciso anterior, el Comité de Seguridad de la Información, deberá aprobar la implementación de controles de seguridad de la información, propuestos por el Oficial de Seguridad de la Información (OSI) e informar los riesgos de Seguridad de la Información al Comité de Administración Integral de Riesgos, para su consolidación en la matriz de riesgos y su seguimiento.

3. **Gerente general o representante legal:**

a) Liderar la gestión de seguridad de la información de acuerdo con las disposiciones del Consejo de Administración o del Directorio y lo dispuesto en esta norma;
b) Designar un Oficial de Seguridad de la Información (OSI); y,
c) Promover la participación activa de todas las partes interesadas que intervienen en el proceso y la gestión de seguridad de la información.

4. **Oficial de Seguridad de la Información:** entre sus responsabilidades, tendrá las siguientes:

a) Definir, elaborar, supervisar la ejecución; mantener y actualizar las políticas, procesos, procedimientos, metodologías, planes y controles concernientes a la gestión de seguridad de la información, los cuales deben ser difundidos al personal correspondiente de las entidades y empresas;
b) Solicitar la asignación de los recursos humanos, técnicos y financieros necesarios para la gestión de seguridad de la información y velar que los mismos sean utilizados de forma eficiente y eficaz alineados con los objetivos estratégicos institucionales;
c) Diseñar y proponer al Consejo de Administración, las políticas, procesos, procedimientos, roles y responsabilidades, para la gestión de seguridad de la información;
d) Desarrollar y ejecutar los Planes de Concienciación y Formación a su personal, en temas concernientes a seguridad de la información;
e) Coordinar y supervisar, con los responsables de los procesos del negocio, la implementación efectiva de los controles de seguridad de la información, establecidos en el plan de gestión de riesgos; así como, desarrollar, coordinar, ejecutar, evaluar, proponer y comunicar el Plan de Gestión de Riesgos de seguridad de la información;
f) Coordinar las actividades para la gestión de seguridad de la información;
g) Ejecutar los procedimientos y lineamientos establecidos cuando se identifiquen incidentes de seguridad de la información;
h) Informar, de acuerdo con la normativa pertinente, los incidentes de seguridad de la información catalogados como sensibles o críticos, a las instituciones públicas que correspondan;
i) Participar en la evaluación de las amenazas de seguridad de la información y proponer medidas de mitigación;
j) Asesorar en materia de seguridad de la información, a través de su participación en los proyectos que involucren el manejo de información sensible o crítica de la misma, o de sus socios, clientes y usuarios;
k) Recomendar medidas correctivas adicionales en temas relacionados de seguridad de la información, alineadas al Anexo 1 y/o a buenas prácticas;
l) Verificar que los servicios brindados por personas naturales o jurídicas cumplan con las políticas de seguridad de la información establecidas; y,
m) Generar la documentación que evidencie la gestión de la seguridad de la información.

5. **Auditor interno:**

a) Verificar la efectividad de las medidas implementadas por el Oficial de Seguridad de la Información (OSI);
b) Custodiar los informes de las auditorías y/o exámenes especiales realizados por el Oficial de Seguridad de la Información (OSI) y ponerlos a disposición de la Superintendencia de Economía Popular y Solidaria, cuando esta lo requiera; y,
c) Recomendar medidas correctivas al Oficial de Seguridad de la Información (OSI).

Artículo 21.- Revisión y actualización.- Las entidades y empresas deberán revisar anualmente y actualizar cuando corresponda, la documentación referida en la presente norma.

CAPÍTULO IV
SEGURIDAD DE LA INFORMACIÓN
RÉGIMEN SIMPLIFICADO

Artículo 22.- Régimen Simplificado.- Conforman el régimen simplificado de seguridad de la información:

a) El Consejo de Administración;
b) El Gerente General o representante legal; y,
c) El Responsable de Seguridad de la Información.

Articulo 23.- Responsable de Seguridad de la Información.- Las entidades y empresas que conforman este régimen, deberán contar con un Responsable de Seguridad de la Información, quien debe tener conocimientos generales en seguridad de la información, tecnología o gestión de riesgos y reportará directamente a la Gerencia General o representante legal.

Artículo 24.- Requisitos obligatorios para el Régimen Simplificado.- Las entidades y empresas pertenecientes a este régimen deberán contar con al menos, lo siguiente:

a) Políticas, procesos, procedimientos, roles y responsabilidades para la gestión de seguridad de la información;
b) Asignación de recursos humanos, técnicos y financieros para seguridad de la información;
c) Actividades de concienciación y formación en temas concernientes en seguridad de la información;
d) Los requerimientos señalados en el Anexo 1 de esta resolución, correspondiente al Régimen Simplificado; y,
e) Registro de los eventos relacionados con seguridad de la información en la "Bitácora de Eventos de Riesgos", para lo cual podrán basarse en la metodología de riesgos que se adjunta en el Anexo 2.

Artículo 25.- Medidas de Seguridad de la Información (controles).- Las entidades y empresas que conforman este régimen, para la gestión de seguridad de la información, deberán implementar los controles mínimos previstos para este Régimen, en el Anexo 1.

Artículo 26.- Responsabilidades para la gestión de Seguridad de la Información.- Los órganos internos de dichas entidades y empresas, además de las responsabilidades previstas

en la normativa legal vigente, deberán cumplir con lo descrito a continuación, para una gestión adecuada de la seguridad de la información:

1. **Consejo de Administración:**

a) Aprobar la asignación de los recursos humanos, técnicos y financieros necesarios; y,
b) Aprobar las políticas, procesos, procedimientos, roles y responsabilidades.

2. **Gerencia General o Representante legal:**

a) Liderar la gestión de la seguridad de la información de acuerdo con las disposiciones del Consejo de Administración y lo dispuesto en esta norma;
b) Designar a un funcionario en la entidad o empresa como Responsable de Seguridad de la Información;
c) Identificar y promover la participación activa de todas las partes interesadas que intervienen en la gestión de seguridad de la información y la gestión de riesgos, asociados a la seguridad de la información; y,
d) Aprobar las actividades de concientización y formación para la seguridad de información.

3. **Responsable de Seguridad de la Información.-** Entre sus responsabilidades, tendrá las siguientes:

a) Proponer actividades de concienciación y formación para seguridad de la información;
b) Identificar y gestionar los eventos relacionados a seguridad de la información y registrarlos en la "Bitácora de Eventos de Riesgo";
c) Elaborar los informes de pruebas y controles establecidos en temas relacionados a seguridad de la información;
d) Recomendar medidas correctivas adicionales en temas relacionados a seguridad de la información, alineadas al Anexo 1 atinente al Régimen Simplificado y/o a buenas prácticas;
e) Verificar que los servicios prestados por personas naturales o jurídicas cumplan con las políticas de seguridad de la información establecidas; y,
f) Generar la documentación que evidencie la gestión de la seguridad de la información.

4. **Consejo de Vigilancia:**

a) Verificar el registro y efectividad de las medidas implementadas en temas relacionados a seguridad de la información;
b) Integrar actividades relacionadas a seguridad de la información en Plan de Trabajo Anual;
c) Custodiar los informes de las pruebas y controles establecidos y ponerlos a disposición de la Superintendencia de Economía Popular y Solidaria, cuando esta lo requiera; y,
d) Recomendar medidas correctivas para la gestión de seguridad de la información.

Artículo 27.- Revisión y actualización: Las entidades y empresas que conforman este régimen, deberán revisar anualmente y actualizar cuando corresponda, la documentación referida en la presente norma.

DISPOSICIONES GENERALES

PRIMERA.- Las entidades, empresas y CONAFIPS, sin perjuicio de la información que solicite en cualquier momento este Organismo de Control, deberán reportar a la Superintendencia de Economía Popular y Solidaria, de forma inmediata, los eventos que

afecten directamente a la continuidad del negocio y a la prestación de servicios financieros, incluyendo al menos la fecha del incidente, el impacto, el/los sistemas o servicios, y/o actividades afectadas, en la forma y medios que esta Superintendencia establezca para el efecto.

SEGUNDA.- Las entidades, empresas y CONAFIPS deberán solicitar al menos una vez al año a los prestadores de servicios, sean estos personas naturales o jurídicas, la documentación que demuestre que el servicio prestado cuenta con las revisiones (auditorías, exámenes especiales, certificaciones, entre otros) y controles necesarios para una adecuada administración de la seguridad de la información.

TERCERA.- Las entidades, empresas y CONAFIPS, en los contratos de prestación de servicios que celebren con personas naturales y/o jurídicas, deberán incluir cláusulas específicas por las cuales el contratista se obliga a mantener controles para la seguridad de la información y protección de datos personales, alineados a los estándares y buenas prácticas de aceptación internacional.

CUARTA.- 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, las empresas y la CONAFIPS implementarán esta norma dentro de los plazos previstos en el siguiente cuadro, contados a partir de la presente fecha:

Entidad, empresa y/o CONAFIPS	Segmento	Plazo para la implementación de las medidas de seguridad de la información
Cooperativas de ahorro y crédito	1	12 meses
	2	24 meses
	3	36 meses
	4 y 5	24 meses
Cajas Centrales		12 meses
Asociaciones Mutualistas de ahorro y crédito para la vivienda		12 meses
CONAFIPS		12 meses
Compañías y Organizaciones de servicios auxiliares		24 meses

SEGUNDA.- El primer oficial de seguridad de la información y el primer responsable de seguridad de la información, según corresponda, podrán acreditar el cumplimiento de los requisitos de capacitación previstos en esta norma, dentro del plazo de 6 meses contados a partir de su designación o contratación. La Superintendencia, en casos debidamente justificados y aceptados por este Organismo de Control, podrá ampliar dicho plazo por una sola vez.

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

Publíquese en el portal web de la Superintendencia de Economía Popular y Solidaria.

COMUNÍQUESE.- Dado y firmado en la ciudad de San Francisco de Quito, Distrito Metropolitano, a 3 de mayo de 2022.

SOFÍA MARGARITA HERNÁNDEZ NARANJO
SUPERINTENDENTE DE ECONOMÍA POPULAR Y SOLIDARIA

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

ANEXO 1
CONTROLES OBLIGATORIOS DE SEGURIDAD DE LA INFORMACIÓN

Las entidades, empresas y/o CONAFIPS controladas, además de los requisitos exigidos en la presente norma para cada régimen, deberán desarrollar e implementar al menos los siguientes controles, los mismos que deberán ser revisados con una periodicidad mínima anual.

Controles Seguridad de la Información

Nombre / Control	Descripción	General	Especial	Simplificado
Políticas, procesos y procedimientos, roles y responsabilidades (Normativa interna de Seguridad de la Información)				
Políticas				
Seguridad de la información	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán al menos contar con el marco de políticas correctamente detallado. El contenido de las políticas deberá estar alineado a los objetivos estratégicos.	x	x	x
Clasificación de información		x	x	x
Gestión de riesgos de seguridad de la información. (Alineada a la Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del Sector Financiero Popular y Solidario bajo el control de la Superintendencia de Economía Popular y Solidaria)		x	x	x
Control de accesos físicos y tecnológicos		x	x	
Gestión de incidentes		x	x	
Gestión de software		x	x	
Gestión de infraestructura tecnológica		x	x	
Seguridad de la información para recursos humanos		x		
Seguridad física (Alineada a la Norma de control respecto de la seguridad física y electrónica emitida por la Superintendencia de		x	x	

Nombre / Control	Descripción	General	Especial	Simplificado
Economía Popular y Solidaria)				
Gestión con terceros		x	x	x
Ciberseguridad		x	x	
Procesos				
Identificación de los procesos agregadores de valor				
Documento de identificación de procesos agregadores de valor. (Alineada a la Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del Sector Financiero Popular y Solidario bajo el control de la Superintendencia de Economía Popular y Solidaria)	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda deberán disponer de un documento evidenciable en el cual se identifique y defina los procesos agregadores de valor.	x	x	x
Gestión de vulnerabilidades				
Auditorias informáticas	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán realizar auditorías, revisiones generales y/o focalizadas internas y externas.	x	x	
Pruebas de penetración	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán al menos una vez al año: a) Revisar la seguridad de sus activos mediante ejercicios prácticos y controlados, tales como ethical hacking, pentesting, entre otros, que simulen varios tipos de amenazas; y, b) Evaluar la infraestructura y aplicativos que soportan todos los servicios, en diferentes escenarios.	x		

Nombre / Control	Descripción	General	Especial	Simplificado
	Las pruebas y/o ejercicios deberán ser ejecutadas por personas naturales o jurídicas externas que acrediten experiencia en este tipo de evaluaciones.			
Plan de mitigación de los hallazgos	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán contar con un plan de mitigación de los hallazgos identificados de las auditorias o exámenes realizados. Este plan deberá incluir un análisis comparativo con los hallazgos previamente encontrados en exámenes y/o auditorias anteriores.	x	x	
Adquisición y desarrollo de software; hardware y servicios.				
Procedimiento de adquisición, desarrollo de software y mantenimiento de sistemas informáticos, hardware y servicios.	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán disponer de procedimientos para la adquisición y desarrollo de software, hardware y servicios, en los cuales se incluyan temas relacionados con controles de seguridad de la información.	x	x	
Planes de Contingencia tecnológica y continuidad del negocio				
Planes, procesos y procedimientos de Contingencia tecnológica y continuidad del negocio	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán elaborar los planes de contingencia tecnológica y continuidad del negocio. Dichos planes deberán ser evaluados periódicamente a fin de tomar acciones que correspondan.	x	x	
Cifrado				
Procedimientos de cifrado de la información sensible o Crítica	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán:	x		

Nombre / Control	Descripción	General	Especial	Simplificado
	a) Disponer de procedimientos de cifrado de sus datos sensibles o críticos, conforme al análisis de riesgos de seguridad de la información; y, b) Verificar periódicamente la vigencia de los elementos de cifrado.			
Procedimientos				
Inventario y Clasificación de información (Alineada a la Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del Sector Financiero Popular y Solidario bajo el control de la Superintendencia de Economía Popular y Solidaria)				
Identificación de tipos de información	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán disponer de un documento evidenciable en el cual se identifique y cuantifique los tipos y activos de información considerando los criterios de disponibilidad, confidencialidad e integridad así como su custodio, responsable y ubicación.	x	x	x
Inventario de activos de información.		x	x	x
Clasificación de activos de información.		x	x	x
Gestión de riesgos				
Análisis y evaluación de riesgos de las aplicaciones, servicios y activos de seguridad de la información. (Alineada a la Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del Sector Financiero Popular y Solidario bajo el control de la Superintendencia de Economía Popular y Solidaria)	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda deberán disponer de un documento evidenciable en el cual se evalúen vulnerabilidades y amenazas con el fin de determinar el nivel de riesgo. Para lo cual pueden usar cualquier método de gestión de riesgos de seguridad de la información, estructuradas y generalmente aceptadas. Podrán tomar como referencia el Anexo 2 de la presente norma.	x	x	x
Respaldos y resguardo de información sensible o crítica.				

Nombre / Control	Descripción	General	Especial	Simplificado
Procedimientos y mecanismos de resguardo de información física y digital, sensible o crítica (Alineada a la Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del Sector Financiero Popular y Solidario bajo el control de la Superintendencia de Economía Popular y Solidaria)	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán: a) Respaldar la información sensible o crítica (física y digital) en lugares y ubicaciones adecuadas, considerando la triada de seguridad de la información; y, b) Disponer al menos de un documento evidenciable que compruebe el correcto funcionamiento de los respaldos.	x	x	x
Cultura de seguridad de la información.				
Plan de capacitación de seguridad de la Información. (Alineada a la Norma de control sobre los principios y lineamientos de educación financiera)	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán: a) Evaluar periódicamente el plan de Capacitación de Seguridad de la Información; b) Definir dentro del plan de capacitación indicadores de madurez que permitan medir el nivel de aprendizaje; c) Proporcionar capacitaciones al personal, así como a proveedores, clientes, socios y usuarios.	x	x	
Gestión de accesos tecnológicos.				
Procedimiento de control de accesos	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán: Definir los perfiles y roles asignados al personal y establecer el procedimiento para su administración.	x	x	x
	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán: Implementar el registro de los accesos a los datos	x	x	

Nombre / Control	Descripción	General	Especial	Simplificado
	críticos o sensibles y las actividades que se realicen sobre estos. (Pistas de auditoría).			
Gestión de la configuración.				
Procedimiento para gestión de la configuración	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, implementarán procedimientos para la gestión de configuraciones del activo de tecnologías de información.	x	x	
Gestión de cambios, control de versiones y mantenimiento en hardware, software y servicios tecnologías de la información.				
Procedimiento para gestión de cambios y control de versiones en los servicios de tecnologías de la información.	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, implementarán procedimientos de gestión de cambios y control de versiones en el que se registren las autorizaciones, ajustes y variaciones que se realicen en los servicios de tecnología, de una manera ordenada y controlada.	x	x	

Controles tecnológicos

Nombre / Control	Descripción	General	Especial	Simplificado
Arquitectura segura	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán diseñar, implementar y gestionar, la arquitectura segura para proteger los activos digitales en función de la particularidad tecnológica. La arquitectura deberá contener al menos: a) Una estrategia de defensa en profundidad; b) Controles de flujo de información;	x	x	

Nombre / Control	Descripción	General	Especial	Simplificado
	c) Aislamiento y segmentación; d) Monitoreo y detección; y, e) Técnicas de cifrado.			
Monitoreo y detección	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda y de acuerdo a la clasificación de activos, deberán implementar sistemas que mantengan registros de logs correlacionados de la infraestructura crítica, que permitan su detección, análisis y depuración. Los registros de logs deberán incluir por lo menos: a) Hora del evento; b) Cambios en los permisos de un archivo; c) Periodo de operación; d) Acceso o salida de un usuario; e) Cambios en los datos; f) Errores y violaciones; y, g) Tareas fallidas.	x	x	

ANEXO 2
CONSIDERACIONES PARA LA METODOLOGÍA DE RIESGOS

Clasificación de Activos.

La clasificación de activos deberá:

a) Considerar al menos: aspectos del negocio, tipo de información y datos almacenados, importancia a la continuidad del servicio, consecuencias legales e impacto económico.

b) Categorizar a los activos por su privacidad en: público, uso interno y restringido; y, así valorar su proceso de custodia y control, tomando en cuenta una evaluación por activo dentro de los cuatro aspectos principales: confidencialidad, integridad, disponibilidad y privacidad, bajo el esquema de criticidad propuesto.

Gestión de riesgo.

Todas las entidades, empresas y la CONAFIPS en el análisis de riesgo institucional deberán incluir un acápite de seguridad de la información que contenga al menos los criterios básicos señalados por la norma técnica ISO/IEC 27000.

Todas las entidades, empresas y la CONAFIPS, deberán considerar al menos los siguientes aspectos dentro de su metodología:

Descripción del riesgo.

Causa, evento y consecuencia, en el siguiente orden:

a) Evento y/o amenaza: es el riesgo identificado en las tareas o actividades del proceso y/o sistema evaluado;
b) Causa y/o vulnerabilidad: es el motivo o razón que podría generar la materialización del riesgo y dar como resultado pérdidas; y,
c) Consecuencia: es la posibilidad de pérdida o materialización del evento, que puede generar un impacto financiero, por pérdidas o daños en activos, sanciones y multas por incumplimiento regulatorio y otros.

Determinación del riesgo inherente.

Riesgo intrínseco de cada actividad, tomando en cuenta el mapa de calor para determinar la criticidad así como su calificación de acuerdo con la siguiente ecuación:

CRITICO	5
ALTO	4
MEDIO	3
BAJO	2
MUY BAJO	1

$$\text{Nivel de Riesgo de Seguridad} = \text{Probabilidad} \times \text{Impacto}$$

$$\text{Probabilidad} = \text{Amenaza} \times \text{Vulnerabilidad}$$

Implementación de controles.

Incluir controles para la mitigación del riesgo identificado, tomando en cuenta el presupuesto y la criticidad-probabilidad del riesgo.

Evaluar la efectividad de los controles

Clasificar a los controles implementados de acuerdo con la siguiente tabla:

Efectivo	**Efectivo no formalizado**	**Inefectivo prueba**	**Inefectivo diseño**	**Control no existente**
a) Control existente bien diseñado, ejecutado adecuadamente. b) Periodicidad establecida, minimizando exposición al riesgo. c) Formalizado en norma.	a) Control existente bien diseñado, ejecutado adecuadamente. b) Periodicidad establecida, minimizando exposición al riesgo. c) No formalizado.	a) Control existente bien diseñado. b) Formalizado en norma. c) No es ejecutado adecuadamente: Falla en un número limitado de oportunidades y/o sin la periodicidad establecida.	a) Diseño del control existente, no permite mitigar adecuadamente el riesgo. b) Control débil, requiriendo acciones correctivas.	a) No se ha diseñado algún control. b) El control diseñado falla continuamente, por tanto no mitiga el riesgo relacionado.

Medición del riesgo residual.

Aquel que permanece después de que las entidades, empresas y la CONAFIPS desarrollen sus respuestas a los riesgos. El riesgo residual refleja el riesgo remanente, una vez que se ha implantado de manera eficaz las acciones planificadas. Para determinarlo se aplicará la misma ecuación del riesgo inherente.

Tratamiento del riesgo.

Las estrategias de tratamiento para los riesgos de seguridad de la información, se aplicaran a los riesgos determinados como críticos y altos; es decir, de criticidad relevante, a los cuales se los identificará y se propondrán planes de acción o controles. El responsable de proponer y darle seguimiento a la ejecución de los planes de acción, será el Oficial de Seguridad de la Información o quien hiciere sus veces. Para el tratamiento del riesgo se aplicara el siguiente esquema:

RIESGO	**Asumir** Aceptar, convivir con el riesgo y minimizar su impacto.
	Compartir Acuerdos contractuales que permiten traspasar parcialmente parte del riesgo a un tercero.
	Mitigar Tomar medidas encaminadas a impedir la materialización de los eventos de riesgo.
	Transferir Es el traspaso total del riesgo identificado a terceros.