RESOLUCIÓN No. SEPS-IGT-IR-IGJ-2018-0279

CATALINA PAZOS CHIMBO
INTENDENTE GENERAL TÉCNICO

CONSIDERANDO:

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

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

Que, el numeral 7 del artículo 62 del aludido Código, establece como función de la Superintendencia de Economía Popular y Solidaria, velar por la estabilidad, solidez y correcto funcionamiento de las entidades sujetas a su control y, en general, vigilar que cumplan las normas que rigen su funcionamiento, las actividades financieras que presten, mediante la supervisión permanente, preventiva, extra situ y visitas de inspección in situ que permitan determinar la situación económica y financiera de las entidades, el manejo de sus negocios, evaluar la calidad y control de la gestión de riesgo y verificar la veracidad de la información que generan;

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

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

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

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

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

Que, la Junta de Política y Regulación Monetaria y Financiera mediante Resolución 128-2015-F del 23 de septiembre de 2015, reformada por la Resolución 366-2017-F de 8 de mayo de 2017, expidió las "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 expedir las normas de control necesarias para la aplicación de dicha resolución. Dichas resoluciones se encuentran incluidas en la Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros emitida por dicho cuerpo colegiado;

Que, la Junta de Política y Regulación Monetaria y Financiera mediante Resolución 346-2017-F expidió la "Norma para la administración integral de riesgos de la Corporación Nacional de Finanzas Populares y Solidarias", la misma que se encuentra en la Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros emitida por la dicho cuerpo colegiado; cuya Disposición General Segunda determina que la Superintendencia de Economía Popular y Solidaria podrá expedir las normas de control necesarias para la aplicación de dicha resolución;

Que, la Superintendencia de Economía Popular y Solidaria, mediante resolución No. SEPS-IGT-ISF-IGJ-2018-0105, de 6 de abril de 2018, expidió la "Norma de control para la calificación y supervisión de las compañías y organizaciones de servicios auxiliares del sector financiero popular y solidario";

Que, conforme consta en el literal b) del artículo 1 de la Resolución No. SEPS-IGJ-2018-001 de 2 de enero de 2018, el Superintendente de Economía Popular y Solidaria delegó al Intendente General Técnico: "*Dictar las normas de control en el ámbito de su competencia, conforme a lo dispuesto en el literal b) del artículo 151 de la Ley Orgánica de Economía Popular y Solidaria, en concordancia con subnumeral 2), literal b), numeral 10.1 del artículo 10 del Estatuto Orgánico de Gestión Organizacional por Procesos de la Superintendencia de Economía Popular y Solidaria;*";

Que, mediante acción de personal No. 733 de 25 de junio de 2018, el Intendente General de Gestión Encargado, delegado por el Superintendente de Economía Popular y

Solidaria, "*según lo dispuesto en la letra a) del numeral 1.2 del artículo 1 de la Resolución No. SEPS-IGG-2016-090 de 28 de abril de 2016, en concordancia con lo dispuesto en la letra d) del artículo 2 de la Resolución No. SEPS-IGJ-2018-001 de 2 de enero de 2018*", nombró como Intendente General Técnico a Catalina Pazos Chimbo; y,

Que, es necesario que la Superintendencia de Economía Popular y Solidaria expida una norma de control para la administración del riesgo operativo y riesgo legal.

En ejercicio de sus atribuciones, resuelve expedir la siguiente:

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

SECCIÓN I. ÁMBITO Y OBJETO DE APLICACIÓN

Artículo 1.- Ámbito: Las disposiciones de la presente norma se aplicarán a las cooperativas de ahorro y crédito, cajas centrales, asociaciones mutualistas de ahorro y crédito para la vivienda, en adelante "entidades" y a la Corporación Nacional de Finanzas Populares y Solidarias, en lo sucesivo "Corporación", de acuerdo a su naturaleza, complejidad de sus operaciones y segmento al que pertenezcan.

También se aplicará a las compañías y organizaciones de servicios auxiliares del sector financiero popular y solidario, que brindan servicios de red, software financiero y de computación, transaccionales y de pago, red de cajeros automáticos y puntos de pago.

Las entidades y la Corporación observarán también, según corresponda, las "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" y la "Norma para la administración integral de riesgos de la Corporación Nacional de Finanzas Populares y Solidarias", emitidas por la Junta de Política y Regulación Monetaria y Financiera.

Artículo 2.- Objeto: La presente resolución tiene por objeto normar la administración de riesgo operativo y riesgo legal para una adecuada administración integral de riesgos, a fin de minimizar las pérdidas que se puedan derivar de eventos ocasionados por fallas o insuficiencias de procesos, personas, tecnología de la información y eventos externos.

SECCIÓN II.-DEFINICIONES

Artículo 3.- Glosario de términos: *Para la aplicación de esta normativa, se consideran las siguientes definiciones:*

- ***Administración de la información:*** *Es el proceso mediante el cual se captura, procesa, almacena y transmite información por cualquier medio.*

- ***Aplicación informática:*** *Son los procedimientos programados a través de alguna herramienta tecnológica.*

- ***Base de datos:*** *Sistema formado por un conjunto de datos almacenados en discos o cualquier otro medio magnético que permite el acceso directo a ellos, estructurados de manera fiable y homogénea, organizados independientemente, accesibles en tiempo real*

- ***Ciberseguridad:*** *Políticas, procedimientos y medidas de protección de la infraestructura tecnológica y de activos de información, a través del tratamiento de las amenazas que ponen en riesgo la información procesada, almacenada y transportada por los diferentes componentes tecnológicos interconectados.*

- ***Computación en la nube, servicios en la nube o nube:*** *Es la provisión de servicios informáticos accesibles a través de internet. Estos pueden ser de infraestructura, plataforma y/o software.*

- ***Dato personal:*** *Dato que identifica o hace identificable a una persona natural, directa o indirectamente.*

- ***Datos****: Es cualquier forma de registro electrónico, óptico, magnético, impreso o en otros medios, susceptible de ser capturado, almacenado, procesado y distribuido.*

- ***Elasticidad en la nube:*** *Es la capacidad que se tiene en la nube para adaptarse a las demandas variables de infraestructura y los recursos que se dispone, según las necesidades de la entidad.*

- ***Estándar ANSI/TIA-942:*** *Es una norma de calidad creada por el American National Standards Institute (ANSI, por sus siglas en inglés) y el Telecommunications Industry Association (TIA, por sus siglas en inglés) para lograr la adecuada implementación de Data Center a nivel mundial que proporciona una serie de recomendaciones y directrices para la instalación de las infraestructuras de centros de procesamiento de datos en los aspectos de: telecomunicaciones, arquitectura, sistema eléctrico y sistema mecánico.*

- ***Evento de riesgo operativo:*** *Es el incidente o hecho que se ha presentado o puede presentarse que puede derivar en pérdidas financieras o de información, suspensión de operaciones para la entidad, originadas por fallas o insuficiencias en los factores de riesgo operativo.*

- ***Factores de riesgo operativo:*** *Son las fuentes generadoras de riesgos operativos tales como: personas, procesos, tecnología de la información y eventos externos.*

- ***Incidente de tecnología de la información:*** *Es el evento asociado a posibles fallas en la tecnología de la información, fallas en los controles, o situaciones con probabilidad de comprometer las operaciones del negocio.*

- ***Información crítica****: Es la considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones.*

- ***Instalaciones:*** *Es la infraestructura que permite alojar los recursos físicos relacionados con la tecnología de la información.*

- ***Impacto:*** *Es la afectación financiera que podría tener la entidad, en el caso de que ocurra un evento de riesgo.*

- ***Línea de negocio:*** *Procesos encaminados a generar productos y servicios especializados para atender un segmento del mercado objetivo definido en la planificación estratégica de la entidad.*

- ***Mapa de calor:*** *Es una herramienta que permite visualizar de una manera rápida la probabilidad de los riesgos y su intensidad, en caso de que estos se materialicen.*

- ***Mapa de procesos:*** *Diagrama que presenta la visión global de la estructura de la entidad, donde se presentan todos los procesos que forman parte de la organización y sus principales relaciones.*

- ***Medios electrónicos:*** *Son los elementos de la tecnología que tienen características digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares.*

- ***Nivel administrativo:*** *Lo integra los miembros del consejo de administración o directorio según corresponda, consejo de vigilancia, representante legal y los responsables máximos de cada área y/o departamento de acuerdo a la estructura organizacional de cada entidad.*

- ***Nivel de riesgo:*** *Representa el grado de exposición de riesgo al que podría encontrarse expuesta una entidad de ocurrir un evento identificado.*

- ***Pista de auditoría:*** *Es el registro de datos lógicos de las acciones o sucesos ocurridos en los sistemas aplicativos, bases de datos, sistemas operativos y demás elementos tecnológicos, con el propósito de mantener información histórica para fines de control, supervisión y auditoría.*

- ***Plan de contingencia:*** *Es el conjunto de procedimientos alternativos para el funcionamiento normal de los procesos críticos y de aquellos definidos por la entidad que permitan su operatividad, a fin de minimizar el impacto operativo y financiero que pueda ocasionar cualquier evento inesperado específico. El plan de contingencia se ejecuta en el momento que se produce dicho evento.*

- ***Plan de continuidad:*** *Es el conjunto de procesos y procedimientos orientados a mantener la operatividad de la entidad ante eventos inesperados.*

- ***Plan de recuperación de desastres de tecnología de información:*** *Es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que una entidad pueda comenzar de nuevo sus operaciones ante eventos de caso fortuito o fuerza mayor.*

- ***Plataforma tecnológica:*** *Conjunto de equipos, aplicaciones y sistemas interconectados destinados a ofrecer productos y servicios a través del uso de los recursos tecnológicos disponibles, a socios, clientes y/o usuarios.*

- ***Probabilidad:*** *Es la posibilidad de que ocurra un evento de riesgo en un determinado período de tiempo.*

- ***Procedimiento:*** *Es el método específico y estandarizado para llevar a cabo una actividad o un proceso.*

- ***Proceso crítico:*** *Es el conjunto de procedimientos indispensables para la sostenibilidad y continuidad de las operaciones de la entidad, y cuya falta de identificación o aplicación deficiente puede generarle un impacto negativo.*

- ***Procesos:*** *Es el conjunto de actividades estandarizadas que transforman insumos en productos o servicios.*

- ***Propietario de la información.-*** *Es la persona encargada de cuidar la integridad, confidencialidad y disponibilidad de la información; debe tener autoridad para especificar y exigir las medidas de seguridad necesarias para cumplir con sus responsabilidades.*

- ***Protección de datos personales:*** *Es un conjunto de medidas técnicas, organizativas y prácticas de seguridad que se debe aplicar para evitar el uso indebido e ilegal de datos personales y salvaguardarlos contra filtraciones, pérdida o compromiso de los mismos.*

- ***Resiliencia operativa:*** *Es la capacidad de una entidad de seguir prestando servicios a sus usuarios a pesar de una disrupción repentina. Para ello, la entidad debe conocer cuáles son sus servicios críticos y las circunstancias en las que no podrían prestarlos.*

- ***Riesgo inherente:*** *Es el nivel de riesgos propio de la actividad con los controles existentes en el momento de la evaluación del riesgo.*

- ***Riesgo legal:*** *Es la probabilidad de que una entidad incurra en pérdidas debido a la inobservancia e incorrecta aplicación de disposiciones legales, normativas e instrucciones emanadas por organismos de control; aplicación de sentencias o resoluciones judiciales o administrativas adversas; deficiente redacción de textos, formalización o ejecución de actos, contratos o transacciones o porque los derechos de las partes contratantes no han sido debidamente estipuladas.*

- ***Riesgo operativo:*** *Es la posibilidad de que se produzcan pérdidas para la entidad, debido a fallas o insuficiencias originadas en procesos, personas, tecnología de información y eventos externos.*

  El riesgo operativo no incluye los originados por el entorno político, económico y social, los riesgos sistémico, estratégico y de reputación.

- ***Riesgo residual:*** *Nivel de riesgo esperado después de aplicar los controles.*

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

- ***Sistemas internos de control integral:*** *Son el conjunto integrado de políticas, procesos, procedimientos y niveles de control formalmente establecidos y validados periódicamente, tendientes a evitar la ocurrencia de eventos de riesgo o mitigar su impacto.*

- ***Tecnología de la información:*** *Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el*

hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes y comunicaciones, entre otros.

- ***TIER III**: Certificación o clasificación de los centros de datos que permite el mantenimiento concurrente, con una disponibilidad de 99.982% al año, y un tiempo de parada de 1.6 horas, e incluye redundancia en sus componentes de infraestructura, así como fuentes alternativas de electricidad y refrigeración en caso de emergencia.*

- ***Tipo de evento:** Identificación de los eventos de riesgo operativo de acuerdo a su origen.*

(Artículo reemplazado por el Artículo 1 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

SECCIÓN III.- ADMINISTRACIÓN DEL RIESGO OPERATIVO

Artículo 4.- Administración de Riesgo Operativo: En el marco de la administración integral y control de riesgos, las entidades y la Corporación incluirán la metodología y los procedimientos para gestionar el riesgo operativo como un riesgo específico, al que se encuentran expuestas en el desarrollo de sus actividades y operaciones.

Con la finalidad de reducir las consecuencias y efectos de riesgo operativo, también deberán decidir si el riesgo identificado se debe asumir, compartir, mitigar o transferir, de acuerdo a lo establecido en las "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"; y, en la "Norma para la administración integral de riesgos de la Corporación Nacional de Finanzas Populares y Solidarias", emitidas por la Junta de Política y Regulación Monetaria y Financiera.

***4.1.- Sistema de Gestión de Riesgo Operativo:** Para una adecuada administración de riesgo operativo y legal, las entidades y la Corporación deberán implementar un Sistema de Gestión del Riesgo Operativo (SIGRO) que corresponde al conjunto de etapas y elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo, órganos de control, plataforma tecnológica, divulgación de información y capacitación, mediante los cuales las entidades identifican, miden, priorizan, controlan/mitigan, monitorean y comunican dicho riesgo.*

(Numeral reemplazado por el numeral 1 del Artículo 2 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

4.2.- Etapas del Sistema de Gestión de Riesgo Operativo: *Las entidades y la Corporación deben ejecutar las etapas definidas para el Sistema de Gestión de Riesgo Operativo que consisten en:*

4.2.1 Identificar: Debe realizarse con anterioridad a la ejecución de cualquier proceso, con el fin de determinar los riesgos operativos que han ocurrido, así como aquellos riesgos operativos en potencia que van a suponer una serie de obstáculos al logro de los objetivos definidos. En esta etapa de identificación pueden a su vez diferenciarse dos sub-etapas:

- *Inventario de procedimientos*
- *Recolección de información*

4.2.2 Medir: Una vez que los riesgos operativos de los diferentes procesos han sido identificados, el siguiente paso es evaluar la posibilidad de materialización de los mismos (en función de la frecuencia con la que los mismos suceden) así como, definir el impacto que los mismos podrían generar en caso de ocurrencia.

Como resultado de esta segunda etapa, establecemos el llamado riesgo inherente, que no es más que el nivel de riesgos que presenta una actividad concreta, sin aplicarle ningún tipo de control.

4.2.3 Priorizar: Los resultados de la matriz de probabilidad e impacto, permiten identificar aquellos riesgos que representan una mayor amenaza, a los cuales se les puede dar mayor prioridad o gestión de respuesta, con los recursos de los que dispone la entidad.

4.2.4 Controlar/mitigar: En esta etapa se busca definir las medidas de control que permitan reducir la probabilidad de ocurrencia y/o impactos ocasionados por los riesgos inherentes detectados.

Tras esta etapa, la entidad obtiene el conocido riesgo residual, que es el riesgo que resulta tras la aplicación de los oportunos controles que hayan sido considerados por la entidad.

4.2.5 Monitorear: En esta etapa se debe llevar a cabo el seguimiento adecuado a los riesgos con el fin de ir analizando su evolución.

4.2.6 Comunicar: Las entidades deben definir una política sobre los eventos de riesgo operativo que deban informar interna o externamente y que esté sujeta a revisión periódica, en función de las estrategias organizacionales. Además, deben implementar un

proceso para evaluar el impacto de la información a comunicar en función a su gestión de riesgos.

(Numeral incluido por el numeral 2 del Artículo 2 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

4.3.- Líneas de negocio.- Para una adecuada administración del riesgo operativo las entidades y la Corporación, deberán agrupar justificada y documentadamente sus procesos por líneas de negocio de acuerdo a la siguiente clasificación:

a) Línea minorista.- Contempla las actividades de intermediación financiera tales como: recepción de depósitos en cualquier modalidad; asesoramiento de inversiones; otorgamiento de créditos en las modalidades de consumo y vivienda. Este grupo incluye, servicios financieros, negociación de letras de cambio, libranzas, pagarés, facturas y otros documentos que representen obligación de pago creados por ventas a crédito, así como el anticipo de fondos con respaldo de los documentos referidos. No incluye las operaciones y servicios relacionados con tarjetas de crédito, débito, pago y prepago.

b) Línea de microfinanzas.- Incluye operaciones financieras como préstamos en el segmento de microcrédito, ahorro o transferencias a personas naturales cuyo sustento provenga de actividades económicas de menor escala.

c) Línea de tarjetas.- Contempla las actividades y servicios relacionados con tarjetas de crédito, débito, pago y prepago.

d) Línea Comercial.- Incluye las operaciones de crédito comercial de primer piso, operaciones financieras de segundo piso con cooperativas de ahorro y crédito y asociaciones mutualistas de ahorro y crédito para la vivienda.

e) Línea Inmobiliaria.- Corresponde a la planificación, construcción y comercialización de proyectos orientados al desarrollo de la vivienda y construcción sean estos propios o de terceros.

f) Línea de compensación de pagos.- Contempla todas las actividades relacionadas con la gestión de pagos, transferencias y compensación de acuerdo a lo establecido en el artículo 470 del Código Orgánico Monetario y Financiero.

g) Línea de tesorería tradicional.- Representan actividades cotidianas de la gestión de liquidez y administración de flujo de fondos.

Los procesos productivos deberán asignarse a las líneas de negocio de acuerdo con los productos y servicios que generan, de forma que a cada uno de los procesos les corresponda una sola línea de negocio y que ningún proceso permanezca sin asignar.

Las líneas de negocio también deberán agrupar los procesos gobernantes y los procesos habilitantes que intervienen en las mismas. Si algún proceso gobernante o proceso habilitante interviene en más de una línea de negocio, la entidad deberá utilizar un criterio de asignación objetivo, considerando su línea de negocio principal.

(Incisos incluidos por el numeral 4 del Artículo 2 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

(Numeral renumerado por el numeral 2 del Artículo 2 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

4.4.- Las entidades de los segmentos 1, 2, 3, cajas centrales, asociaciones mutualistas de ahorro y crédito para la vivienda y la Corporación, deberán implementar lo determinado en los siguientes numerales:

4.4.1.- Manual de Riesgo Operativo: Elaborar un manual de riesgo operativo de acuerdo a su estructura, tamaño y complejidad de sus operaciones, el que contendrá al menos, lo siguiente:

a) Las políticas, procesos y procedimientos para la administración del riesgo operativo;
b) Los roles y responsabilidades de quienes participan en la administración del riesgo operativo;
c) Las medidas necesarias para asegurar el cumplimiento de las políticas y objetivos de la administración de riesgo operativo;
d) Las metodologías y procedimientos para identificar, medir (cuantificar), priorizar, controlar, mitigar, monitorear y comunicar los riesgos operativos y su nivel de aceptación;
e) Los procedimientos para priorizar y gestionar los eventos de riesgo, a excepción del segmento 3;
f) Las estrategias de capacitación en temas de administración de riesgo operativo;
g) Los mecanismos o sistemas de reporte de la administración de riesgo operativo; y,
h) El proceso de análisis de riesgos para nuevas operaciones, productos o servicios.

4.4.2.- Tipos de eventos de riesgo operativo: Identificar por línea de negocio, los riesgos operativos, agrupados por tipo de evento y las fallas o insuficiencias en los factores de riesgo relacionados con personas, procesos, tecnología de la información y eventos externos, conforme al detalle del anexo 1, que forma parte de esta norma.

Los tipos de eventos son los siguientes:

a) **Fraude interno.-** Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o eludir regulaciones, leyes o políticas, infidelidades de empleados o uso de información privilegiada para beneficio propio;

b) **Fraude externo.-** Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes o recursos indebidamente o eludir la legislación, por parte un tercero, incluyendo daños ocasionados por individuos, grupos u organizaciones externas que buscan explorar la dependencia de la institución en recursos tecnológico;

c) **Prácticas laborales y seguridad del ambiente de trabajo.-** Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, pago de reclamaciones por daños personales, casos relacionados con la diversidad o discriminación y por responsabilidades generales en el trabajo;

d) **Prácticas relacionadas con los clientes, los productos y el negocio**.- Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a socios, clientes o usuarios, o de la naturaleza o diseño de un producto;

e) **Daños a los activos físicos.-** Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales o por terrorismo, vandalismo, incendio o inundaciones;

f) **Interrupción del negocio por fallas en la tecnología de la información**.- Pérdidas derivadas por la ocurrencia de problemas de telecomunicaciones, servicios públicos y apagones; y,

g) **Deficiencias en la ejecución de procesos, en el procesamiento de operaciones; y en las relaciones con proveedores y terceros.-** Pérdidas derivadas de errores en el procesamiento de operaciones, en la gestión de procesos y en relaciones con contrapartes comerciales y proveedores.

Los eventos de riesgo operativo y las fallas o insuficiencias serán identificados en relación con los factores de este riesgo a través de una metodología formal, debidamente documentada y aprobada por el consejo de administración o el directorio, según corresponda.

4.4.3 Metodologías: La metodología definida para la gestión del riesgo operativo, cuando sea tomada en su conjunto, deberá considerar los factores de riesgo operativo y cumplir con los siguientes criterios:

a) La metodología debe ser implementada en toda la entidad en forma consistente;
b) Asignación de recursos suficientes para aplicar la metodología en las principales líneas de negocio, en los procesos de control y de apoyo;
c) Aplicación de metodologías integradas a los procesos de gestión de riesgos de la entidad;
d) Establecimiento de mecanismos que permitan una mejora continua de la gestión del riesgo operativo;
e) La aplicación de la metodología de gestión del riesgo operativo debe estar adecuadamente documentada;
f) Instaurar procedimientos que permitan asegurar el cumplimiento de la metodología de gestión del riesgo operativo; y,
g) Determinación de los límites de pérdidas aceptadas o administradas de acuerdo a lo señalado en las políticas de riesgo operativo.

4.4.4 Base de eventos de riesgo: Las entidades de los segmentos 1, 2, cajas centrales, asociaciones mutualistas de ahorro y crédito para la vivienda y la Corporación, deberán registrar los eventos de riesgo identificados, con el fin de construir una base de eventos que sea centralizada, histórica, actualizada y suficiente, que permita ordenar, clasificar y disponer de información sobre fallas o insuficiencias, incluidas las de orden legal, su impacto cuantitativo o cualitativo.

Los eventos de riesgo se caracterizan por generar:

a) Pérdidas que afecten al estado de resultados;
b) Pérdidas que no afecten el estado de resultados; y,
c) Potenciales pérdidas que aún no se hayan materializado.

Contarán con una matriz de riesgo operativo en la que se registren los eventos de riesgo identificados en sus procesos, para lo cual deberán adoptar una metodología de riesgo de acuerdo a lo establecido en las “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” y en la “Norma para la administración integral de riesgos de la Corporación Nacional de Finanzas Populares y Solidarias”, emitidas por la Junta de Política y Regulación Monetaria y Financiera.

Así mismo, deberán usar metodologías complementarias a la matriz de eventos de riesgo para su gestión con el fin de fortalecer la administración de riesgo operativo.

Las entidades del segmento 3 deberán registrar sus eventos de riesgo al menos en un reporte o registro que contemple, fecha de ocurrencia del evento, área, proceso, descripción y valor, que deberá ser presentado al comité de administración integral de riesgos para la definición de medidas correctivas.

4.4.5 Esquema de reportes: Las entidades de los segmentos 1, 2, cajas centrales, asociaciones mutualistas de ahorro y crédito para la vivienda y la Corporación, deben

diseñar y mantener un esquema de reportes que permitan disponer de información suficiente, pertinente y oportuna para la toma de decisiones. Los reportes deberán contener al menos lo siguiente:

a) Detalle de los eventos que representan un mayor nivel de riesgo operativo;
b) Identificación de la evolución de los eventos de riesgo y reporte del grado de cumplimiento de planes de acción (mitigación); y,
c) Mapa de calor en el que se identifique la concentración de eventos de riesgo por nivel de riesgo.
d) Magnitud de pérdida suscitada por riesgo operativo, a partir de la base de eventos de riesgo.

Estos reportes deben ser dirigidos por el responsable de la unidad de riesgos al comité de administración integral de riesgos, con la finalidad de que en el proceso de administración de riesgo operativo se pueda decidir si el riesgo se debe asumir, compartir, mitigar o transferir, reduciendo sus consecuencias y efectos.

El conocimiento de la situación en relación a la administración de riesgo operativo, permitirá que el nivel administrativo tenga una visión clara de la importancia de los diferentes tipos de exposición al riesgo operativo y su prioridad, con el objeto de alertarlos en la toma de decisiones y acciones, que entre otras, pueden ser: revisar estrategias y políticas; actualizar o modificar procesos y procedimientos establecidos; implantar o modificar límites de riesgo; constituir, incrementar o modificar controles; implantar planes de contingencia y de continuidad del negocio; revisar términos de pólizas de seguro contratadas; contratar servicios provistos por terceros; u otros, según corresponda.

Los reportes, matrices de riesgo y todo tipo de información referente a riesgo operativo deben ser presentados por el responsable de la unidad de riesgos al comité de administración integral de riesgos. Dichos reportes deberán estar disponibles cuando la Superintendencia lo requiera.

4.4.6 Capacitación de riesgo operativo: Todas las entidades y la Corporación deben diseñar, programar y coordinar planes de capacitación sobre la administración de riesgo operativo, uso adecuado de tecnología y seguridad de la información, dirigidos a todos los órganos internos y empleados, funcionarios o servidores. Las capacitaciones deben cumplir al menos con las siguientes condiciones:

a) Ser de periodicidad anual;
b) Ser impartidas durante el proceso de inducción de los nuevos funcionarios, empleados o servidores;
c) Contar con mecanismos de evaluación de los resultados obtenidos, con el fin de determinar la eficiencia de dichos programas y el alcance de los objetivos propuestos; y,
d) Mantener un registro del personal capacitado y de las sugerencias realizadas por los participantes.

(Numeral renumerado por el numeral 2 del Artículo 2 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

4.5.- Para mantener una adecuada administración del riesgo operativo las entidades de los segmentos 4 y 5, sin perjuicio de lo dispuesto en el Capítulo III Administración de riesgos en las cooperativas de ahorro y crédito de los segmentos 4 y 5 de las, "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", emitida por la Junta de Política y Regulación Monetaria y Financiera, deberán:

a) Definir adecuadamente los procesos de la entidad, los mismos que incluyan: actividades, responsables, fecha de actualización y fecha de aprobación por parte del consejo de administración;
b) Mantener un registro de sus eventos de riesgo, el mismo que contemple como mínimo, fecha de ocurrencia, descripción, solución e impacto financiero de ser el caso;
c) Garantizar una adecuada separación de funciones que evite la realización o el ocultamiento de fraudes, errores, omisiones u otros eventos de riesgo operativo;
d) Implementar políticas y niveles de aprobación para las distintas líneas de negocio y procesos con el fin de evitar conflictos de interés; y,
e) Elaborar un manual de administración del personal que contemple las políticas, procesos y procedimientos para la incorporación, permanencia y desvinculación del personal.

Así mismo, de acuerdo al segmento al que pertenezcan y al tamaño y complejidad de sus operaciones, desarrollarán sus propias metodologías y procedimientos de administración de riesgo operativo, además de asegurar que se realice en forma continua por lo menos una vez al año evaluaciones integrales de riesgo operativo, en especial para proyectos en curso y nuevos productos y servicios, así como en la prestación de servicios y productos financieros.

(Inciso incluido por el numeral 3 del Artículo 2 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

(Numeral renumerado por el numeral 2 del Artículo 2 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

SECCIÓN IV.- FACTORES DE RIESGO OPERATIVO

Artículo 5.- Para reducir el nivel de riesgo operativo las entidades de los segmentos 1, 2, 3, cajas centrales, asociaciones mutualistas de ahorro y crédito para la vivienda y la Corporación, deberán administrar los factores de riesgo considerando su particularidad y la interrelación entre ellos.

Artículo 6.- Personas: Las entidades y la Corporación deben contar con una estructura orgánico-funcional acorde al tamaño, complejidad de sus operaciones y normativa vigente que le aplica según su segmento. Además, deben identificar las fallas o insuficiencias asociadas al factor "personas", tales como: falta de personal adecuado, negligencia, error humano, conflicto de intereses, falta de segregación de funciones, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros.

6.1.- Manuales de talento humano: Las entidades y la Corporación, deberán documentar en un manual descriptivo de talento humano los procesos de incorporación, permanencia y desvinculación, y en otro manual en el que consten los cargos, las funciones, responsabilidades, así como, la descripción del perfil técnico y de las competencias que debe tener el ocupante de cada cargo.

6.1.1 Incorporación: Comprende la planificación de necesidades, el reclutamiento y la selección, la contratación e inducción de nuevo personal. Las entidades deben evaluar su organización con el objeto de definir el personal mínimo necesario y las competencias idóneas para el desempeño de cada puesto, considerando no sólo experiencia profesional, formación académica, sino también los valores, actitudes y habilidades personales que puedan servir como criterio para garantizar la excelencia institucional.

6.1.2 Permanencia: Comprende la creación de condiciones laborales idóneas mediante la planificación y ejecución de actividades de capacitación y formación que permitan al personal aumentar y perfeccionar sus conocimientos, competencias y destrezas; un sistema de evaluación del desempeño que permita medir y estimular la gestión del personal de la entidad y a su vez aplicar incentivos que motiven la adhesión a los valores institucionales; identificar los puestos críticos y el personal clave de la entidad; y, definir el personal de reemplazo en el caso de ausencia temporal o definitiva, con la finalidad de dar continuidad a las operaciones del negocio.

6.1.3 Desvinculación: Comprende la planificación de la salida del personal por causas regulares o irregulares a través de la preparación de aspectos jurídicos para llegar al finiquito y a la finalización de la relación laboral.

(Numerales incluidos por el numeral 1 del Artículo 3 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

6.2.- Independencia de funciones: Deberá existir una adecuada separación de funciones que evite concentraciones de carácter incompatible, entendidas éstas como aquellas tareas cuya combinación en las competencias y responsabilidades de una sola persona, eventualmente, podría permitir la realización o el ocultamiento de fraudes, errores, omisiones u otros eventos de riesgo operativo.

6.3.- Base de datos: Las entidades y la Corporación, deben mantener una base de datos con información actualizada del recurso humano, que permita una adecuada toma de decisiones por parte del nivel administrativo y la realización de análisis de la cantidad y calidad del recurso humano de acuerdo con sus necesidades.

Dicha información debe contener como mínimo:

a) Datos personales del funcionario;
b) Formación académica, experiencia y referencias;
c) Fechas de selección, reclutamiento y contratación;
d) Cargos que han desempeñado en la entidad;
e) Resultados de evaluaciones realizadas;
f) Fechas, número de horas y temas de capacitaciones;
g) Fechas y días de vacaciones gozadas;
h) Días y horas de vacaciones disponibles;
i) Fechas y causas por las que el personal se ha desvinculado de la entidad; y,
j) Motivos de multas, sanciones y amonestaciones.

*6.4.- Acuerdo de confidencialidad**:** Las entidades y la Corporación deben asegurar que se mantengan actualizados los acuerdos de confidencialidad relacionados con los procesos que ejecuta el empleado y los riesgos asociados a las funciones que desempeña, así mismo, debe determinar responsabilidades y deberes de seguridad de la información que permanezcan vigentes después del cambio de funciones o de la terminación de la relación laboral, conforme lo establecido en dicho acuerdo*.

(Numeral incluido por el numeral 2 del Artículo 3 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

Artículo 7.- Procesos: Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, las entidades de los segmentos 1, 2, 3, cajas centrales, asociaciones mutualistas de ahorro y crédito para la vivienda y la Corporación, deberán contar con procesos definidos, documentados, aprobados, actualizados y socializados que se encuentren alineados con la estrategia institucional y con las políticas adoptadas.

Las entidades y la Corporación, deberán definir formalmente procesos, políticas y procedimientos que aseguren una apropiada planificación, administración y cumplimiento de los objetivos institucionales; en concordancia, principalmente, con los factores de riesgo personas y tecnología de la información.

Los procesos deberán ser agrupados de la siguiente manera:

7.1.- Procesos gobernantes o estratégicos: Se considerarán a aquellos que proporcionan directrices y políticas a los demás procesos cuya responsabilidad compete al consejo de administración o directorio y al representante legal, según corresponda, con el fin de

cumplir con los objetivos y políticas institucionales. Se refieren a la planificación estratégica, los lineamientos de acción básicos, definición de estructura organizacional, la administración integral de riesgos, entre otros.

7.2.- Procesos productivos, fundamentales u operativos: Son los procesos propios del giro del negocio, que permitan ejecutar efectivamente las políticas y estrategias relacionadas con la calidad de los productos o servicios que ofrecen a sus socios, clientes o usuarios.

7.3. Procesos habilitantes, de soporte o apoyo: Son los procesos administrativos, financieros, tecnología de información, contabilidad, control interno y talento humano, que apoyan a los procesos gobernantes y productivos.

7.4.- Manual de administración de procesos: Las entidades y la Corporación, deberán definir formalmente políticas, procesos y metodologías para un adecuado diseño, control, actualización y mejoramiento de los procesos, que les permita adaptar sus procesos oportunamente a los cambios y condiciones de mercado, mejores prácticas o disposiciones normativas. Las políticas deberán actualizarse de acuerdo a la normativa vigente y abarcarán por lo menos, los siguientes aspectos:

a) Diseño claro y actualización de los procesos, los cuales deben ser dinámicos y compatibles con la entidad;
b) Descripción en secuencia lógica y ordenada de las actividades, tareas, y controles;
c) Determinación de los responsables de los procesos, que serán aquellas personas encargadas de su correcto funcionamiento, a través del establecimiento de objetivos y estrategias para gestionarlos y mejorarlos;
d) Definición de mapa de procesos en el que consten los procesos gobernantes o estratégicos, procesos productivos, fundamentales u operativos y procesos habilitantes, de soporte o apoyo;
e) Definición de límites y alcance, manteniendo contacto con los clientes internos y externos del proceso para garantizar que se satisfagan sus necesidades y expectativas;
f) Actualización y mejora continua a través del seguimiento permanente en su aplicación;
g) Garantizar una adecuada separación de funciones que evite la realización o el ocultamiento de fraudes, errores, omisiones u otros eventos de riesgo operativo; y,
h) Difusión y comunicación de los procesos buscando garantizar su total aplicación.

7.5.- Portafolio de procesos: Las entidades y la Corporación, deberán mantener inventarios actualizados de procesos por línea de negocio, que cuenten, como mínimo con la siguiente información: tipo de proceso, nombre del proceso, responsable, identificación de procesos críticos, productos y servicios que genera el proceso, clientes internos y externos, fecha de actualización y fecha de aprobación.

Artículo 8.- Tecnología de información: Las entidades y la Corporación, deben contar y mantener tecnología de información acorde a su segmento, naturaleza y perfil de riesgo de sus operaciones, que garantice la captura, procesamiento, almacenamiento y transmisión de manera oportuna y confiable de la información para la toma de decisiones, incluyendo aquella que está bajo la modalidad de servicios provistos por terceros.

Artículo 9.- Administración de la tecnología de la información.- Las entidades de los segmentos 1, 2, 3, cajas centrales, asociaciones mutualistas de ahorro y crédito para la vivienda y la Corporación deberán administrar la tecnología de información; para lo cual deben contar con:

9.1 Área de tecnología de la información: Un comité, unidad, o responsable de tecnología de información que garantice el normal funcionamiento de la misma, independiente de las áreas operativas y de negocio de la entidad.

El área de tecnología de la información debe ser consistente de acuerdo al segmento, naturaleza, complejidad y perfil de riesgo de las operaciones de la entidad.

9.2.- Estructura de gestión de tecnología: Con la finalidad de implementar de manera eficiente la administración de la tecnología de información, las entidades deberán contemplar una estructura de gestión de tecnología, de acuerdo al siguiente cuadro:

ÓRGANOS INTERNOS	SEGMENTO 1, CAJAS CENTRALES, MUTUALISTAS Y CORPORACIÓN	SEGMENTO 2	SEGMENTO 3
Comité de Tecnología de la Información	X	X	N/A
Unidad de Tecnología de la Información	X	X	N/A
Responsable de Tecnología de la Información	N/A	N/A	X

N/A = No aplica

Las cooperativas de ahorro y crédito del segmento 3, deberán tener al menos un responsable de tecnología de la información, que brinde soporte tecnológico a la entidad y canalice cualquier requerimiento a los proveedores.

9.2.1.- Conformación del Comité de Tecnología de la Información: El comité estará conformado por: un vocal del consejo de administración o directorio, según corresponda, quien lo presidirá y tendrá voto dirimente; el representante legal o su delegado; y, los responsables de las áreas de riesgo y de tecnología que actuará como secretario, quienes

tendrán voz y voto. En las sesiones del comité podrán participar funcionarios vinculados con los temas a tratarse quienes no tendrán derecho a voto. En el caso de no existir dicho comité, estas atribuciones serán llevadas por el comité de administración integral de riesgos o el organismo que haga sus veces.

9.2.2.- Funciones del Comité de Tecnología de la Información: El comité será responsable principalmente de:

a) Planificar, coordinar y supervisar las actividades relacionadas con la tecnología;
b) Recomendar las políticas, procesos, procedimientos y metodologías de tecnología de información para posterior aprobación del consejo de administración o el directorio, según corresponda;
c) Establecer lineamientos para la formulación del plan estratégico de tecnologías de la información, relacionado con el plan estratégico de la entidad y presupuestos aprobados;
d) Recomendar al consejo de administración o al directorio, según sea el caso, el Plan Estratégico de Tecnologías de la Información (PETI);
e) Priorizar la inversión de tecnologías de la información y proyectos con componente tecnológico;
f) Recomendar al consejo de administración o al directorio, según corresponda, la aprobación de modelos de operación para las tecnologías de la información y comunicación; y,
g) Presentar periódicamente al consejo de administración o al directorio, según sea el caso, informes de cumplimiento de la gestión de tecnología de la información.

9.2.3 Funcionamiento del Comité: Sesionará de manera ordinaria por lo menos cuatro veces al año; y, extraordinariamente, por convocatoria del presidente, que deberá ser notificada con un mínimo de 72 horas de anticipación a la fecha de realización de la sesión.

El comité de tecnología de información sesionará con, al menos, tres de sus integrantes y las decisiones serán tomadas por mayoría de votos. El presidente del comité tendrá voto dirimente.

Las reuniones del comité de tecnología se las podrá realizar de manera presencial o virtual; las reuniones virtuales deberán cumplir como mínimo con los siguientes requerimientos de seguridad:

1. Disponer de herramientas tecnológicas de videoconferencia que al menos cumplan con las siguientes características:

a. Contar con mecanismos de seguridad para acceder a la videoconferencia (salas de espera, contraseñas, doble factor de autenticación, etc.);
b. Cifrado de datos extremo a extremo; y,
c. Cumplimiento de estándares y certificaciones de privacidad y seguridad;

2. Para iniciar las reuniones virtuales del comité de tecnología se deberá validar que las personas asistentes son las previamente invitadas, valiéndose de los controles de seguridad que dispone la herramienta de videoconferencia mediante las características detalladas en el numeral 1 precedente.

3. Una vez iniciada la reunión virtual, la sala de videoconferencia deberá ser bloqueada para nuevos accesos.

4. Durante las reuniones virtuales del comité de tecnología, los intervinientes deberán mantener activas las cámaras de video para la constatación de su presencia.

5. Las reuniones virtuales del comité de tecnología deberán ser grabadas, respaldadas y custodiadas por la unidad encargada, considerando estándares de seguridad, de tal forma que las últimas cuatro sesiones estén disponibles en la herramienta de videoconferencia, cuando se lo requiera.

(Inciso incluido por el Artículo 4 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

Las resoluciones constarán en las respectivas actas. El secretario de comité, elaborará y llevará actas fechadas y numeradas en forma secuencial de todas las sesiones, debidamente suscritas por todos sus asistentes. Así mismo, será de su responsabilidad, la custodia de las mismas, bajo los principios de confidencialidad, integridad y disponibilidad de la información.

El comité, a través de su presidente, informará por escrito al consejo de administración o al directorio, las evaluaciones y resoluciones adoptadas.

Artículo 9.3.- Políticas, procesos, procedimientos y metodologías para la administración de la tecnología de información: Las entidades de los segmentos 1, 2, 3, cajas centrales, asociaciones mutualistas de ahorro y crédito para la vivienda y la Corporación, deberán definir políticas, procesos, procedimientos y metodologías que:

a) Se encuentren diseñadas bajo estándares de general aceptación que permitan minimizar los riesgos en la tecnología de información y ejecución de los criterios de control interno; y,

b) Contemplen al menos que el consejo de administración de las entidades de los segmentos 1, 2, cajas centrales y asociaciones mutualistas de ahorro y crédito para la vivienda o el directorio, según corresponda, aprueben un plan estratégico de tecnología de la información (PETI) alineado con el plan estratégico institucional; y, un plan operativo anual que establezca las actividades a ejecutar en el corto plazo, traducido en tareas, cronogramas, personal responsable y presupuesto, de manera que se asegure el logro de los objetivos tecnológicos propuestos.

9.3.1.- Con el objeto de garantizar que las operaciones de tecnología de la información satisfagan los requerimientos de las operaciones, las referidas entidades deberán contar al menos con lo siguiente:

a) Planificación Estratégica de Tecnología de la Información (PETI) y Presupuesto de Tecnología de la Información;
b) Procedimientos de operación, acceso y uso de las instalaciones de procesamiento de información;
c) Procedimientos de gestión de incidentes y problemas de tecnología de la información, que considere al menos su registro, priorización, análisis, escalamiento y solución;
d) Respaldos de información periódicos, acorde a los requerimientos de continuidad del negocio que incluya la frecuencia de verificación, las condiciones de preservación, eliminación y el transporte seguro hacia un sitio alterno, que no debe estar expuesta a los mismos riesgos del sitio principal y mantenga las condiciones físicas y ambientales necesarias para su preservación y posterior recuperación; y,
e) Transporte de respaldos entre los centros de resguardo que deban efectuarse con adecuados controles de seguridad (sellos, bitácoras de salida y entrada, personal autorizado, entre otros aspectos) que minimicen ubicación remota, que no debe estar expuesto a los riesgos del sitio principal. La información debe estar resguardada por el lapso no menor a lo que indica la normativa vigente, en condiciones y en formatos que se establezcan para el caso por parte de los entes de control.

9.3.2.- Las entidades señaladas deberán garantizar que el proceso de adquisición, desarrollo, implementación y mantenimiento de las aplicaciones satisfagan los objetivos del negocio, considerando al menos lo siguiente:

a) Una metodología que permita la adecuada administración y control del proceso de compra de software y del ciclo de vida de desarrollo y mantenimiento de aplicaciones, con los usuarios involucrados;
b) Requerimientos funcionales aprobados por el área solicitante;
c) Requerimientos técnicos y el análisis de la relación y afectación a la capacidad de la infraestructura tecnológica actual, aprobados por el área técnica;
d) Ambientes de prueba, desarrollo y producción, con la debida segregación de accesos. Para el caso de entidades que hayan tercerizado el servicio de desarrollo de sistemas, deberán contar al menos con ambientes de prueba y producción;
e) Mitigación de las vulnerabilidades del código fuente de las aplicaciones;
f) Pruebas técnicas y funcionales que reflejen la aceptación de los usuarios autorizados;
g) Procedimientos de control de cambios que considere su registro, manejo de versiones, segregación de funciones y autorizaciones e incluya los cambios emergentes; y,
h) Procedimientos de migración de la información, que incluyan controles para garantizar las características de integridad, disponibilidad y confidencialidad.

En caso de que la entidad contrate el servicio de desarrollo de software o adquiera un sistema informático, debe verificar que el proveedor cumpla con las disposiciones descritas en los numerales precedentes.

9.3.3.- Con el objeto de garantizar que la infraestructura tecnológica que soporta las operaciones sea administrada, monitoreada y documentada, las entidades y la Corporación, deben contar con un manual de gestión de la infraestructura que contengan al menos:

a) Procedimientos que permitan la administración, monitoreo y registros de configuración de las bases de datos, redes de datos, hardware y software base, que incluya límites y alertas;
b) Una metodología documentada de análisis de la capacidad y desempeño de la infraestructura tecnológica que soporte las operaciones del negocio, cuyo resultado debe ser conocido y analizado por el comité de tecnología o el órgano que haga sus veces, con una frecuencia mínima semestral. La metodología debe incluir límites y alertas de al menos: almacenamiento, memoria, procesador, consumo de ancho de banda; y, para bases de datos: áreas temporales de trabajo, log de transacciones y almacenamiento de datos;
c) Procedimientos de migración de la plataforma tecnológica, que incluyan controles para garantizar la continuidad del servicio;
d) Instalaciones de procesamiento de información crítica en áreas protegidas con los suficientes controles que eviten el acceso de personal no autorizado, daños a los equipos de computación y a la información en ellos procesada, almacenada o distribuida; y, condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento del entorno de la infraestructura de tecnología de la información; y,
e) Un procedimiento para mantener un inventario de infraestructura tecnológica actualizado que considere por lo menos, su registro, responsables de uso, fecha y control de ingresos y salidas de los activos.

9.3.4.- En el caso de contratar servicios de infraestructura, plataforma y/o software conocido como computación en la nube, las entidades y la Corporación deben asegurar que el proveedor disponga al menos de:

a) *Centros de procesamiento de datos principal y/o alterno, contratados en la nube, implementados siguiendo el estándar ANSI/TIA-942 o superior y contar como mínimo con la certificación TIER III o su equivalente para diseño, implementación y operación;*
b) *Certificación ISO 27001 en seguridad de la información para los servicios ofertados, así como, la implementación de los controles establecidos en los estándares ISO 27017 (controles de seguridad para servicios en la nube), ISO 27018 (protección de información personal en la nube) y/o aquella que aplique conforme el servicio ofertado;*

(Literales reemplazados por el numeral 1 del Artículo 5 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

c) Si es un proveedor internacional, que tenga una representación comercial en el país, con capacidad para brindar soporte integral con personal y representar legalmente al proveedor internacional en el país; y,

d) Capacidad para transferir sólidamente los conocimientos.

e) *e) Contar con informes de auditorías de seguridad relacionadas con el servicio contratado, con base en el perfil de riesgo del proveedor de servicios en la nube, por lo menos una (1) vez al año, con el fin de identificar amenazas y vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que brindan. Los procedimientos de auditoría deben ser ejecutados por personas o empresas especializadas en seguridad de la información en la nube e independientes al proveedor, aplicando estándares vigentes y reconocidos a nivel internacional. El proveedor de servicios en la nube debe definir y ejecutar planes de acción para gestionar las vulnerabilidades detectadas; y,*

f) *Los acuerdos o contratos que suscriba la entidad controlada con el proveedor de servicios en la nube, adicional a los establecidos en la presente sección de esta norma, deben contemplar entre otros aspectos los siguientes:*

f.1) *La información proporcionada por la entidad no puede ser utilizada para ningún propósito diferente al establecido en los contratos, inclusive bajo el modelo de subcontrataciones; y,*

f.2) *La entrega a la entidad de informes y certificaciones que demuestren la calidad, desempeño y efectividad en la gestión de los servicios contratados, así como la vigencia de las certificaciones enunciadas en el presente artículo.*

(Literales incluidos por el numeral 2 del Artículo 5 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

La información almacenada por el proveedor deberá estar a disposición permanente de la entidad y a través de ésta, del organismo de control, por medio de los canales o mecanismos que disponga para el efecto. La información es de estricta confidencialidad y no podrá ser comercializada o utilizada para otros fines distintos a los manejados por la entidad dueña de la información.

La notificación de término del contrato deberá ser informada por el proveedor con la debida anticipación, con el propósito de garantizar la continuidad de las operaciones de la entidad.

En caso de terminación del contrato de servicios de infraestructura, plataforma y/o software, la información será devuelta por el proveedor a la entidad de forma inmediata, conservando un respaldo de seguridad por un período de al menos tres meses debiendo observar estricta confidencialidad y el impedimento para utilizarla y comercializarla.

Como parte del proceso de contratación de servicios en la nube y de aquellos en el exterior, las entidades referidas en este artículo y la Corporación, deberán informar al consejo de administración sobre el detalle de los servicios a ser contratados que incluya informes de los riesgos operativos, legales, tecnológicos, de seguridad de la información y continuidad a los que se exponen al adoptar este servicio; así como los controles para mitigarlo;

Las entidades deben exigir al proveedor del servicio en el exterior, que los servicios objeto de la contratación, sean sometidos anualmente a un examen de auditoría independiente, por una empresa auditora de prestigio.

Como parte del proceso de contratación de servicios en la nube y de aquellos en el exterior, la entidad controlada deberá disponer de un informe técnico, uno de seguridad de la información y uno legal, emitidos por el personal de la entidad controlada conforme a sus competencias, en los cuales se haya identificado los riesgos operativos asociados al servicio y su gestión respectiva.

(Incisos reemplazados por el numeral 3 del Artículo 5 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

Artículo 10.- Las entidades de los segmentos 4 y 5 deberán inclu**i**r dentro de su gestión, la administración de la tecnología de información; para lo cual deben contar al menos con:

a) Un presupuesto aprobado para el funcionamiento de la operación de tecnología de información;
b) Respaldos de los movimientos de operaciones activas, pasivas, contingentes y de servicios, ubicados fuera del área de procesamiento; y,
c) Normas básicas de operación y un inventario de los principales elementos tecnológicos con los que cuenta.

Artículo 11.- Eventos Externos: *En la administración del riesgo operativo, las entidades y la Corporación deben considerar la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos a su control, tales como: incidentes con proveedores, fallas en los servicios públicos, ocurrencia de desastres naturales, ataques cibernéticos, atentados, fraudes externos y otros actos delictivos, los cuales pudieran alterar el desarrollo normal de sus actividades. La gestión de los riesgos relacionados con eventos externos debe formar parte de la administración de la continuidad del negocio, manteniendo procedimientos actualizados, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción del negocio*.

(Artículo reemplazado por el Artículo 6 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

SECCIÓN V.- GESTIÓN DE CONTINUIDAD DEL NEGOCIO

(Denominación reemplazada por el Artículo 7 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

Artículo 12.- Planes de Contingencia y Continuidad: *Las entidades de los segmentos 1,2, cajas centrales, asociaciones mutualistas de ahorro y crédito para la vivienda y la Corporación, deben contar con una persona responsable de liderar el establecimiento, implementación, mantenimiento y mejora continua de los planes de contingencia y de continuidad del negocio que cubran a personas, procesos, tecnología y eventos externos, con el fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción del negocio, de ser el caso, al menos apegados a la Norma ISO 22301 o a la buena práctica que se ajuste para el efecto.*

(Inciso reemplazado por el numeral 1 del Artículo 8 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

12.1.- Procesos críticos: Las referidas entidades deberán adoptar una metodología que les permita identificar y evaluar los procesos críticos, aún en los provistos por terceros, previo a la elaboración del plan de continuidad del negocio; así como realizar un análisis de riesgos y equilibrar el costo de la implementación o no del plan de continuidad, dependiendo de la criticidad de cada proceso.

Los procesos priorizados por la entidad se deberán incluir en el plan de continuidad.

12.2.- Actividades: Las aludidas entidades deberán considerar las siguientes actividades para la definición e implementación de los planes de continuidad y de contingencia, según corresponda:

a) *Definir políticas, estrategias, objetivos, procesos, procedimientos, metodologías, planes operativos y presupuesto para la administración de la continuidad del negocio, que deben ser revisados por el comité de administración integral de riesgos. Dicho comité deberá presentar para aprobación del Consejo de Administración. Esta documentación debe ser difundida y comunicada a todo el personal involucrado, de tal forma que se asegure su cumplimiento;*

b) *Definir funciones y responsables de las actividades de continuidad de las operaciones, que permitan cumplir con el criterio de resiliencia para la disponibilidad de las operaciones, acorde al tamaño y complejidad de los procesos administrados por el negocio;*

(Literales a) y b) reemplazados por el numeral 2 del Artículo 8 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

c) Identificar y analizar los principales escenarios de contingencia tomando en cuenta el impacto y la probabilidad de que sucedan (Análisis de impacto en el negocio);
d) Identificar los riesgos por fallas en la tecnología de información y gestionar un plan de acción para mitigar los riesgos identificados;
e) Definir una estrategia de continuidad de los procesos críticos, en línea con los objetivos institucionales;
f) Desarrollar los planes de contingencia necesarios para implementar la estrategia de continuidad definida.
g) *Definir una estrategia de continuidad que asegure la disponibilidad de los productos y servicios críticos de la entidad y disminuir los efectos de eventos disruptivos, en línea con los objetivos institucionales;*
h) Determinar acciones a realizar para continuar con las actividades de la entidad en instalaciones propias o alternas (reanudación y recuperación);
i) Realizar pruebas periódicas de los planes de continuidad y contingencia que permitan comprobar la aplicabilidad y efectuar los ajustes necesarios;
j) Mantener información actualizada de contacto de las personas responsables de ejecutar cada actividad;
k) Contar con cronogramas y procedimientos de prueba y mantenimiento de los planes de continuidad y contingencia;
l) Definir procedimientos de difusión, comunicación, concientización y cumplimiento de los planes de continuidad y contingencia; y,
m) Designar de su estructura un responsable de la continuidad del negocio. *Contar con cronogramas y procedimientos de prueba y mantenimiento de los planes de continuidad y contingencia que permitan comprobar su efectividad y realizar los ajustes necesarios, cuando existan cambios que afecten la aplicabilidad del plan o, al menos, una vez al año. Las pruebas deben incluir el alcance y el detalle de los aspectos a probar, así como las conclusiones y recomendaciones obtenidas como resultado de su ejecución;*

(Literales g) y m) reemplazados por el numeral 2 del Artículo 8 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

n) *La entidad debe mantener una base de conocimiento de las lecciones aprendidas en función del resultado de las pruebas realizadas al plan de continuidad del negocio, eventos de continuidad materializados, debilidades encontradas en las revisiones efectuadas por la administración de la continuidad del negocio, entre otros; y,*
o) *Monitorear, evaluar y verificar que se mantengan actualizados los planes de contingencia y/o continuidad de las compañías contratadas que soportan los servicios críticos de la entidad, y que estos sean debidamente probados con la*

intención de precautelar los servicios brindados e incluirlos dentro de las pruebas anuales de continuidad de la entidad. El resultado de las pruebas debe ser comunicado a las instancias correspondientes.

(Literales n) y o) incluidos por el numeral 2 del Artículo 8 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

Las entidades del segmento 3 deberán implementar un plan de recuperación de desastres de tecnología de información.

SECCIÓN VI.- SERVICIOS PROVISTOS POR TERCEROS

Artículo 13. Calificación y selección de proveedores: Las entidades de los segmentos 1,2, 3, cajas centrales, asociaciones mutualistas de ahorro y crédito para la vivienda y la Corporación, deberán contar con un proceso integral para la calificación y selección de proveedores, que incluya las actividades previas a la contratación, cumplimiento y renovación del contrato, y el cual deberá contener al menos procedimientos para:

a) Evaluar la experiencia de la empresa y su personal;
b) Evaluar la capacidad financiera para asegurar la viabilidad del proveedor durante todo el período de contratación previsto;
c) Efectuar análisis de costo beneficio;
d) Evaluar la capacidad y oportunidad de respuesta del proveedor a consultas, solicitudes de presupuesto y presentación de ofertas;
e) Evaluar la capacidad y calidad del servicio, instalación y apoyo;
f) Evaluar la capacidad logística del proveedor incluyendo las instalaciones y recursos técnicos y económicos;
g) Exigir que las entidades y organizaciones de servicios auxiliares cuenten con la calificación respectiva de la Superintendencia y cumplan la normativa correspondiente, y;
h) Comprobar que el proveedor cuente con representación técnica, legal, operativa y de contingencia suficientes, en especial si son proveedores internacionales.

13.1.- Para el caso de adquisición, implantación o arriendo de los bienes, servicios o sistemas tecnológicos, todas las entidades y la Corporación deberán verificar:

a) El objeto y especificaciones del servicio contratado;
b) Los requisitos funcionales y técnicos de los bienes o servicios a ser adquiridos;
c) Los costos totales;
d) El nivel de soporte, capacitación y transferencias de conocimiento a ser proporcionados por el proveedor;
e) La existencia de respaldos, seguridad y sigilo de la información;
f) El mantenimiento y continuidad de los bienes y servicios;
g) Adaptación eficiente y oportuna a los requerimientos normativos; y,

h) El documento en que el conste el plan de contingencia y continuidad del servicio que presta el proveedor, según corresponda.

i) *Cumplimiento por parte del proveedor de las políticas que establezca la entidad, las cuales deben incluir, al menos, la normativa vigente expedida por la Superintendencia de Economía Popular y Solidaria, aplicable en función del servicio a ser contratado;*

j) *Facilidades para la revisión y seguimiento del servicio prestado a las entidades, por parte de la unidad de auditoría interna u otra área que estas designen, así como de los auditores externos y la Superintendencia de Economía Popular y Solidaria, principalmente en aquellos procesos definidos como críticos;*

k) *El documento que asegure la existencia de mecanismos de gestión de riesgos que garanticen la continuidad del servicio que presta el proveedor, según corresponda;*

l) *Certificaciones o informes de revisión externa sobre el cumplimiento de los aspectos relacionados con la continuidad del negocio referido en la presente norma, practicado por personal o empresas independientes con experiencia en el ramo. Dichos informes deben ser anualmente entregados a la entidad con su plan de mitigación;*

m) *Las entidades deben exigir al proveedor del servicio en el exterior, que los servicios objeto de la contratación sean sometidos anualmente a un examen de auditoría independiente, por una empresa auditora de prestigio; y,*

n) *Como parte del proceso de contratación de servicios en la nube y de aquellos en el exterior, la entidad controlada deberá disponer de un informe técnico, uno de seguridad de la información y uno legal, emitido por el personal de la entidad controlada conforme a sus competencias, en los cuales, se haya identificado los riesgos operativos asociados al servicio y su gestión respectiva.*"

(Literales incluidos por el Artículo 9 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

En el caso que compañías u organizaciones de servicios auxiliares participen como proveedores, deberán presentar copia de la resolución de calificación de la Superintendencia de Economía Popular y Solidaria.

Las cooperativas de los segmentos 4 y 5 deberán contratar los servicios de proveedores tecnológicos siempre y cuando cumplan con lo dispuesto en este numeral. En el caso de que a la fecha de expedición de esta norma, dichas cooperativas hubieran contratado un proveedor que no cumpla con tales requisitos, las entidades le solicitarán que dentro de un plazo de dos años, cumplan con este requerimiento normativo.

Artículo 14.- Proveedores alternos para los servicios críticos: Las entidades de los segmentos 1, 2, 3, cajas centrales, asociaciones mutualistas de ahorro y crédito para la

vivienda y la Corporación, deberán contar con proveedores alternos que tengan la capacidad técnica y operativa para proveer los bienes y prestar los servicios que se requiera, para lo cual se deberá observar lo previsto en el artículo 13 de la presente norma.

Artículo 15.- Proveedores del exterior: Los proveedores de servicios críticos domiciliados en el exterior y que presten servicios a las entidades y a la Corporación, deberán tener una subsidiaria o una contraparte en el país que responda ante posibles fallas o requerimientos de mejora del servicio o sistema adquirido. Esta contraparte deberá ser calificada por los organismos de control pertinentes del país y deberá garantizar los mismos estándares de calidad y responsabilidad que un proveedor local.

Artículo 16.- Para la calificación y selección de proveedores las entidades y la Corporación, deberán analizar ofertas, de acuerdo a su política de contratación establecida, de tal manera que se evite posibles conflictos de interés.

SECCIÓN VII.- RIESGO LEGAL

Artículo 17.- Administración de riesgo legal: Las entidades y la Corporación deben determinar de manera oportuna las fallas o insuficiencias de orden legal, de tal manera que les proporcione una visión clara sobre su exposición a este tipo de riesgo.

Artículo 18.- Aspectos de enfoque de riesgo legal: Las fallas o insuficiencias de orden legal deben ser establecidas por las entidades y la Corporación de acuerdo con su propia percepción y perfil de riesgos y enfocarlas, principalmente, en los siguientes aspectos: actos societarios; gestión de crédito; operaciones del giro financiero; actividades complementarias no financieras; empresas proveedoras extranjeras, estipulaciones contractuales y, cumplimiento legal y normativo, entendiéndolos dentro de las siguientes conceptualizaciones:

18.1.- Actos societarios: Son todos aquellos procesos jurídicos que se deben realizar en orden de ejecutar y perfeccionar las decisiones de los órganos de gobierno, necesarios para el desenvolvimiento societario de las entidades y la Corporación, de acuerdo a su naturaleza jurídica.

18.2.- Gestión de crédito: Es el conjunto de actividades que deben ejecutar en relación al otorgamiento de operaciones crediticias, su instrumentación y su recuperación.

18.3.- Operaciones del giro financiero: Es el conjunto de actividades o procesos que realiza la entidad para la ejecución de operaciones propias de su giro financiero, distintas a la gestión de crédito.

18.4.- Actividades complementarias de las operaciones del giro financiero: Es el conjunto de actividades o procesos que debe ejecutar la entidad, que sin ser propias del giro financiero, son necesarias para el cumplimiento y desarrollo de su objeto social.

18.5.- Proveedores extranjeros: Son las personas jurídicas constituidas en el exterior y que proveen bienes o servicios críticos. Deberán estar domiciliadas en el país o contar con un representante legal en el Ecuador, con capacidad para responder solidariamente por las obligaciones contraídas por el proveedor con la entidad.

18.6 Estipulaciones contractuales: Los contratos deben ser debidamente suscritos, legalizados y contener estipulaciones al menos sobre: los niveles mínimos de servicio acordado; garantías técnicas y financieras, tales como: buen uso del anticipo, fiel cumplimiento del contrato, buen funcionamiento y disponibilidad del servicio, entre otros; penalizaciones por incumplimientos; y, facilidades para la revisión y seguimiento del servicio prestado, ya sea, por la unidad de auditoría interna u otra área que la entidad designe, así como, por parte de los auditores externos o de la Superintendencia.

Los contratos con proveedores que presten servicios tecnológicos críticos, a más de las estipulaciones señaladas en el inciso anterior, deberán contener cláusulas respecto de: garantías de acceso a los programas fuentes, bases de datos, respaldos de datos, plataformas de prestación de servicio o infraestructura tecnológica, en caso de quiebra del proveedor o situaciones contingentes que así lo requieran. Se deberá establecer la protección, privacidad y confidencialidad de los activos de información de la entidad que serán accedidos y manejados por el proveedor de servicios, siempre sujetos a verificación; y, la facultad de realizar auditorías informáticas al proveedor en el caso de ser requerido, tanto por la entidad como por el ente de control.

18.7 Cumplimiento legal y normativo: Es el proceso mediante el cual la entidad controla que sus actividades y sus operaciones se ajusten a las disposiciones legales y normativas vigentes, así como la capacidad de adecuarse rápida y efectivamente a nuevas disposiciones legales y normativas.

Artículo 19.- Clasificación del riesgo legal: El riesgo legal se puede clasificar en:

19.1 Riesgo de Documentación: Es el riesgo de que no existan documentos que respalden las operaciones de crédito, garantías, entre otros, o que de existir, tengan deficiencias en su redacción, no estén completos, o no contengan los requisitos necesarios para su validez, de acuerdo a la normativa vigente.

19.2 Riesgo de Legislación: Riesgo de que una operación no pueda ser ejecutada por prohibición, limitación o incertidumbre acerca de la legislación del país o por errores en la interpretación de la misma.

19.3 Riesgo de Capacidad: Está compuesto por el riesgo de que la contraparte no tenga capacidad legal para operar en un sector, producto o moneda determinada y por el riesgo de que las personas que actúan en nombre de la contraparte no cuenten con poder legal suficiente para comprometerla.

SECCIÓN VIII.- RESPONSABILIDADES EN LA ADMINISTRACIÓN DE RIESGO OPERATIVO

Artículo 20.- Responsabilidades de las entidades de los segmentos 1, 2, 3, cajas centrales, asociaciones mutualistas de ahorro y crédito para la vivienda y la Corporación: Los órganos internos de dichas entidades, además de las responsabilidades previstas en las "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" y en las "Norma para la administración integral de riesgos de la Corporación Nacional de Finanzas Populares y Solidarias", expedidas por la Junta de Política y Regulación Monetaria y Financiera, tendrán las siguientes:

20.1.- Consejo de Administración o Directorio:

a) Crear una cultura organizacional con principios y valores de comportamiento ético que priorice la gestión eficaz del riesgo operativo;
b) Aprobar las políticas y metodologías propuestas por el comité de administración integral de riesgos;
c) Aprobar el manual de gestión de riesgo operativo;
d) Conocer los principales riesgos operativos afrontados por la entidad, estableciendo cuando ello sea posible, adecuados niveles de tolerancia; y,
e) Las demás determinadas por la Superintendencia.

20.2.- Comité de Administración Integral de Riesgos:

a) Evaluar y proponer al consejo de administración o el directorio, según corresponda, las políticas, los manuales y metodologías de administración del riesgo operativo para su aprobación;
b) Aprobar los procesos y procedimientos de administración de riesgo operativo;
c) Evaluar la aplicación de manuales y metodologías de gestión de riesgo previo a la aprobación del consejo de administración o el directorio, según corresponda;
d) Definir los mecanismos para monitorear y evaluar la exposición a riesgos;
e) Recomendar al consejo de administración o el directorio, según corresponda, la aprobación de una metodología consistente para administrar la matriz de riesgos y límites de riesgo;
f) Someter a aprobación del consejo de administración o el directorio, según corresponda, los planes de contingencia y de continuidad del negocio, asegurar la aplicabilidad y cumplimiento de los mismos, para el caso de las entidades de los segmentos 1, 2, cajas centrales, asociaciones mutualistas de ahorro y crédito para la vivienda y Corporación. Las entidades del segmento 3 deberán someter a aprobación del consejo de administración, el plan de recuperación de desastres de tecnología de información; y,
g) Las demás que determine el consejo de administración o el directorio, según corresponda o la Superintendencia.

20.3.- La Unidad o el administrador de riesgos: La unidad o el administrador de riesgos de la entidad deberá cumplir al menos con las siguientes funciones

a) Proponer políticas para la gestión del riesgo operativo;
b) Participar en el diseño y permanente actualización del manual de gestión del riesgo operativo;
c) Desarrollar la(s) metodología(s) para la gestión del riesgo operativo;
d) Apoyar y asistir a las demás unidades de la entidad para la aplicación de la(s) metodología(s) de gestión del riesgo operativo;
e) Evaluar el riesgo operativo, de forma previa al lanzamiento de nuevos productos, implementación de nuevos procesos y ante cambios importantes en el ambiente operativo o informático en base a los informes de las áreas que corresponda;
f) Realizar el seguimiento al cumplimiento de los planes de acción;

g) Consolidar y desarrollar reportes e informes sobre la gestión del riesgo operativo por unidades, factores y líneas de negocios;

h) Identificar las necesidades de capacitación y difusión para una adecuada gestión del riesgo operativo;
i) Liderar el desarrollo, la aplicabilidad y cumplimiento de los planes de contingencia y de continuidad del negocio; así como proponer los líderes de las áreas que deban cubrir el plan de contingencia y de continuidad del negocio para el caso de las entidades de los segmentos 1, 2, cajas centrales, asociaciones mutualistas de ahorro y crédito para la vivienda y la Corporación;
j) En las entidades del segmento 3, el administrador de riesgos deberá elaborar y liderar la ejecución del plan de recuperación de desastres de tecnología de información;
k) Elaborar la metodología para definir y administrar la matriz de riesgos para las entidades de los segmentos 1, 2, cajas centrales, asociaciones mutualistas de ahorro y crédito para la vivienda y la Corporación;
l) En coordinación con el área legal de la entidad, analizar, monitorear y evaluar los procedimientos de orden legal y emitir informes que determinen su real exposición al riesgo legal, los cuales deben ser puestos en conocimiento del comité de administración integral de riesgos; y,
m) Otras necesarias para el desarrollo de la función.

Artículo 21.- Responsabilidades del representante legal: El representante legal tiene la responsabilidad de implementar la gestión del riesgo operativo conforme a las disposiciones del consejo de administración o el directorio, según corresponda.

Los gerentes de las unidades organizativas de negocios o de apoyo tienen la responsabilidad de gestionar el riesgo operativo en su ámbito de acción, dentro de las políticas, límites y procedimientos establecidos, en especial, con el reporte de los eventos de riesgo identificados.

Artículo 22.- Responsabilidades de las entidades de los segmentos 4 y 5: Los órganos internos de dichas entidades, a más de las responsabilidades previstas en las "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" expedida por la Junta de Política y Regulación Monetaria y Financiera, tendrán las siguientes:

a) El consejo de administración será responsable de aprobar el documento en el que se definan los procesos de la entidad, el manual de administración del personal, así como cualquier política definida en relación a la administración de riesgo operativo, los mismos que deben estar previamente revisados y conocidos por el consejo de vigilancia;
b) El consejo de vigilancia deberá revisar el cumplimiento permanente de la aplicación de los procesos aprobados por el consejo de administración;
c) El representante legal además de las responsabilidades previstas en el artículo 21, implementará y dará continuidad a los lineamientos definidos en el numeral 4.4 del artículo 4 y de lo establecido en el artículo 10 de la presente norma; y,
d) Crear una cultura organizacional con principios y valores de comportamiento ético que priorice la gestión eficaz del riesgo operativo.

Las entidades y la Corporación deberán asignar recursos suficientes para la gestión del riesgo operativo, que les permita un adecuado cumplimiento de las funciones señaladas en la presente norma y asegurar una adecuada independencia entre el área que asuma las funciones de gestión del riesgo operativo y aquellas otras unidades de negocio o de apoyo.

DISPOSICIONES GENERALES

PRIMERA.- La Superintendencia de Economía Popular y Solidaria, sin perjuicio de requerir la información que considere necesaria para cumplir con sus actividades de supervisión y control, podrá disponer la adopción de medidas adicionales a las previstas en esta norma, con el propósito de velar por la aplicación de políticas, normas y procedimientos de riesgo operativo que enfrenten las entidades y la Corporación y las compañías y organizaciones de servicios auxiliares del sector financiero popular y solidario.

SEGUNDA.- *Los auditores internos deberán evaluar objetiva e independientemente, que las unidades y las actividades de las entidades y la Corporación relacionadas con la gestión del riesgo operativo:*

a) Cumplan con los lineamientos establecidos en la presente norma; sin perjuicio de verificar la eficacia de los controles implementados para mitigar el riesgo operativo en cada uno de sus factores;
b) Revisen periódicamente la efectividad de la gestión de continuidad del negocio; y,

Generen los informes respectivos que evidencien el cumplimiento de los literales precedentes. Dichos informes deberán estar a disposición de la Superintendencia de Economía Popular y Solidaria, cuando ésta así lo requiera.

(Inciso reemplazado por el Artículo 10 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

Los auditores internos deberán aplicar procesos y procedimientos de auditoria a través de un equipo competente, debidamente capacitado y operativamente independiente, que coadyuven al mejoramiento de la efectividad de la administración de riesgos. El auditor interno no es el directamente responsable de la gestión del riesgo operativo.

TERCERA.- Las metodologías adoptadas para la administración del riesgo operativo, deben estar disponibles cuando lo requiera la Superintendencia de Economía Popular y Solidaria para su validación.

CUARTA.- Las entidades sujetas a esta norma y la Corporación, deben enviar a la Superintendencia de Economía Popular y Solidaria, la información de eventos de riesgo operativo con el contenido, formato y frecuencia que dicho organismo de control determine.

QUINTA.- *Las entidades deben generar planes y programas que les permitan dar cumplimiento a la Ley Orgánica de Protección de Datos Personales.*

(Disposición General Quinta agregada por el Artículo 11 de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.)

DISPOSICIONES TRANSITORIAS

PRIMERA.- *Las cooperativas de ahorro y crédito, cajas centrales, asociaciones mutualistas de ahorro y crédito para la vivienda y la Corporación, deberán proceder con la implementación de esta norma dentro de las fechas previstas en el siguiente cronograma:*

FECHAS DE CUMPLIMIENTO

N°	*TEMA*	*SEGMENTO 1, CAJA CENTRAL, MUTUALISTAS Y CORPORACIÓN*	*SEGMENTO 2*	*SEGMNTO 3*
1	*Elaborar el manual de administración de procesos*	*31 de agosto de 2020*	*31 de agosto de 2021*	*28 de febrero de 2022*
2	*Levantar los procesos de la entidad*	*28 de febrero de 2021*	*28 de febrero de 2022*	*28 de febrero de 2023*
3	*Elaborar el manual de administración del personal*			*31 de agosto de 2020*
4	*Implementar políticas, procesos, procedimientos y metodologías para las administración de la tecnología de información (manual)*		*31 de agosto de 2020*	*28 de febrero de 2021*
5	*Definir o actualizar los planes de contingencia y continuidad del negocio y cronograma de implementación*		*28 de febrero de 2022*	
6	*Aplicar el cronograma de implementación de plan de contingencia y continuidad del negocio*	*28 de febrero de 2021*	*28 de febrero de 2023*	
7	*Definir un plan de recuperación de desastres de tecnología de información*			*28 de febrero de 2021*
8	*Elaborar e implementar la matriz de riesgo operativo*		*31 de agosto de 2020*	
9	*Actualizar la matriz de riesgo operativo con los eventos de riesgo históricos identificados (base de eventos de riesgo operativo)*	*28 de febrero de 2021*	*28 de febrero de 2022*	
10	*Registro de eventos de riesgo*			*28 de febrero de 2023*
11	*Elaborar el plan estratégico de tecnologías de información (PETI)*	*31 de diciembre de 2020*	*31 de diciembre de 2021*	

12	*Elaborar manual de riesgo operativo que contenga las políticas, procesos y metodologías para la administración del riesgo operativo incluido el riesgo legal*	*28 de febrero de 2022*	*28 de febrero de 2023*	*31 de enero de 2024*

Las cooperativas de ahorro y crédito de los segmentos 4 y 5 deberán proceder con la implementación dentro de las fechas previstas en el siguiente cronograma:

		FECHA DE CUMPLIMIENTO	
N°	***TEMA***	***SEGMENTO 4***	***SEGMENTO 5***
1	*Definir documento de administración de procesos*	*28 de febrero de 2021*	*28 de febrero de 2022*
2	*Levantar procesos productivos (captación, colocación, atención y servicio al socio)*	*28 de febrero de 2022*	*28 de febrero de 2023*
3	*Elaborar manual descriptivo de cargos*	*28 de febrero de 2021*	*28 de febrero de 2022*
4	*Elaborar e implementar la bitácora de eventos de riesgo*	*28 de febrero de 2023*	*31 de enero de 2024*
5	*Elaborar y aprobar el presupuesto de operación de tecnología de información*	*28 de febrero de 2021*	*28 de febrero de 2021*
6	*Respaldar fuera del área de procesamiento, los movimientos de operaciones activas, pasivas, contingentes y de servicios*	*28 de febrero de 2021*	*28 de febrero de 2021*
7	*Realizar el inventario de principales elementos tecnológicos*	*28 de febrero de 2021*	*28 de febrero de 2021*
8	*Definir normar básicas de operación de tecnología de información*	*28 de febrero de 2022*	*28 de febrero de 2022*

(Disposición Transitoria Primera reemplazada por el Artículo Único de la Resolución No. SEPS-IGT-IGS-INR-INGINT-2020-0221 de 2 de junio de 2020.)

SEGUNDA.- Las cooperativas del segmento 1 que al 31 de diciembre de 2012, no estuvieron bajo el control de la Superintendencia de Bancos, observarán los plazos para el segmento 2 establecidos en la Disposición Transitoria Primera.

Las cooperativas de los segmentos 2 y 3 que al 31 de diciembre de 2012, estuvieron bajo el control de la Superintendencia de Bancos, observarán los plazos para el segmento 1, establecidos en la Disposición Transitoria Primera.

TERCERA.- Las compañías de servicios auxiliares deberán cumplir con lo previsto en esta norma dentro del plazo de 1080 días.

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

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

COMUNÍQUESE Y PUBLÍQUESE.- Dado y firmado en la ciudad de San Francisco de Quito, Distrito Metropolitano a 26 NOV 2018

Catalina Pazos Chimbo

INTENDENTE GENERAL TÉCNICO

FUENTE:

- Resolución No. SEPS-IGT-IR-IGJ-2018-0279 de 26 de noviembre de 2018.
- Resolución No. SEPS-IGT-IR-IGJ-2018-0284 de 13 de diciembre de 2018.
- Resolución No. SEPS-IGT-IGS-INR-INGINT-2020-0221 de 2 de junio de 2020.
- Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.