

RESOLUCIÓN Nro. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-IGJ-0116**JORGE ANDRÉS MONCAYO LARA**
INTENDENTE GENERAL TÉCNICO**CONSIDERANDO:**

Que, los numerales 1 y 7 del artículo 62, en concordancia con el inciso segundo del artículo 74 del Libro I del Código Orgánico Monetario y Financiero determinan como funciones de la Superintendencia de Economía Popular y Solidaria ejercer la vigilancia, auditoría, control y supervisión de las disposiciones de dicho Código y de las regulaciones dictadas por la Junta de Política y Regulación Financiera; así como, 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;

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

Que, los incisos segundo, tercero y quinto del artículo 74 del mencionado Código establecen: “(...) *A la Superintendencia le compete el control de las entidades del sector financiero popular y solidario acorde a lo determinado en este Código.*”

La Superintendencia de Economía Popular y Solidaria, en su organización, funcionamiento y funciones de control y supervisión del sector financiero popular y solidario, se regirá por las disposiciones de este Código y la Ley Orgánica de Economía Popular y Solidaria. (...)

La Superintendencia de Economía Popular y Solidaria, además de las atribuciones que le otorga la Ley Orgánica de Economía Popular y Solidaria, tendrá las funciones determinadas en los artículos 71 y 62 excepto los numerales 19 y 28, y el numeral 10 se aplicará reconociendo que las entidades de la economía popular y solidaria tienen capital ilimitado. Los actos expedidos por la Superintendencia de Economía Popular y Solidaria gozarán de la presunción de legalidad y se sujetarán a lo preceptuado en la normativa legal vigente, respecto de su impugnación, reforma o extinción.”;

Que, en el artículo 163 del Código *ibídem* determina que forman parte del sector financiero popular y solidario, entre otras, las cooperativas de ahorro y crédito, las cajas centrales, las asociaciones mutualistas de ahorro y crédito para la vivienda, en el ámbito de su competencia;

Que, el artículo 243 del Código Orgánico Monetario y Financiero, prescribe: “*Las infracciones sobre lavado de activos y financiamiento de delitos como el terrorismo, se sancionarán de conformidad con las disposiciones del Código Orgánico Integral Penal y la Ley de Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos*”;

- Que,** el artículo 244 del Código de marras previene que las entidades del sistema financiero nacional tienen la obligación de establecer sistemas de control interno para la prevención de delitos, incluidos el lavado de activos y el financiamiento de delitos como el terrorismo, en todas las operaciones financieras;
- Que,** el artículo 444 del Código *Ut supra*, determina que las entidades financieras populares y solidarias están sometidas a la regulación de la Junta de Política y Regulación Monetaria y Financiera y al control de la Superintendencia de Economía Popular y Solidaria, quienes en las políticas que emitan tendrán presente la naturaleza y características propias del sector financiero popular y solidario;
- Que,** los literales b) y g) del artículo 151 de la Ley Orgánica de Economía Popular y Solidaria, establecen como atribuciones del Superintendente de Economía Popular y Solidaria dictar las normas de control; y, delegar algunas de sus facultades, siempre en forma concreta y precisa, a los funcionarios que juzgue del caso;
- Que,** el artículo 158 de la ley *Ut supra*, determinó, Créase la Corporación Nacional de Finanzas Populares y Solidarias, como una entidad financiera de derecho público, dotada de personalidad jurídica, patrimonio propio y autonomía administrativa, técnica y financiera, con jurisdicción nacional;
- Que,** en la Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros, Libro I: Sistema Monetario y Financiero, Título II: Sistema Financiero Nacional, Capítulo XXXVI: Sector Financiero Popular y Solidario, constan las Secciones III: Normas para la Administración Integral de Riesgos en las Cooperativas de Ahorro y Crédito, Cajas Centrales y Asociaciones Mutualistas de Ahorro y Crédito para la Vivienda y VIII: Norma para la Administración Integral de Riesgos de la Corporación Nacional de Finanzas Populares y Solidarias;
- Que,** conforme consta en el literal j) del numeral 1.2.1.2 “Gestión General Técnica”, del artículo 9 de la Resolución No. SEPS-IGT-IGS-IGD-IGJ-001 de 31 de enero de 2022, que contiene el Estatuto Orgánico de Gestión Organizacional por Procesos de la Superintendencia de Economía Popular y Solidaria, es atribución y responsabilidad del Intendente General Técnico, dictar las normas de control, en el ámbito de su competencia; y,
- Que,** mediante Acción de Personal No. 1395 de 24 de septiembre de 2021, el Intendente General de Desarrollo Organizacional, delegado por la Superintendente de Economía Popular y Solidaria, nombró como Intendente General Técnico, al señor Jorge Andrés Moncayo Lara.

En ejercicio de sus funciones, resuelve expedir la siguiente:

NORMA DE CONTROL PARA LA ADMINISTRACIÓN DEL RIESGO OPERATIVO EN LAS ENTIDADES DEL SECTOR FINANCIERO POPULAR Y SOLIDARIO

SECCIÓN I OBJETO Y ÁMBITO DE APLICACIÓN

Artículo 1.- Objeto.- La presente resolución tiene por objeto normar la administración de riesgo operativo para una adecuada administración integral de riesgos.

Las entidades y la Corporación Nacional de Finanzas Populares y Solidarias 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” respectivamente, emitidas por la Junta de Política y Regulación Monetaria y Financiera.

Artículo 2.- Ámbito.- Las disposiciones de la presente norma se aplicarán a las cooperativas de ahorro y crédito, asociaciones mutualistas de ahorro y crédito para la vivienda y cajas centrales, en adelante “entidad” o “entidades”; y, a la Corporación Nacional de Finanzas Populares y Solidarias, en lo sucesivo “Corporación”, de acuerdo con su naturaleza, complejidad de las operaciones y segmento en el que se encuentren ubicadas.

SECCIÓN II DEFINICIONES

Artículo 3.- Glosario de términos.- Para la aplicación de esta normativa, se considera 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.
- **Datos:** Información almacenada en cualquier forma de registro electrónico, óptico, magnético, impreso o en otros medios, susceptible de ser capturado, almacenado, procesado y distribuido.

- **Evento de riesgo operativo:** Es el incidente o hecho que se ha presentado o puede presentarse que puede derivar en pérdidas financieras, de información o suspensión de operaciones para la entidad, originadas por fallas o insuficiencias en los factores de riesgo operativo.
- **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.
- **Factores de riesgo operativo:** Son las fuentes generadoras de riesgos operativos tales como: personas, procesos, tecnología de la información y eventos externos.
- **Información:** Es cualquier forma de registro físico, electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos que puede ser almacenado y distribuido.
- **Información crítica:** Es la considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones.
- **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.
- **Instalaciones:** Es la infraestructura que permite alojar los recursos físicos y tecnológicos de la entidad o Corporación.
- **Impacto:** Es la afectación financiera que podría tener la entidad, en el caso de que ocurra un evento de riesgo.
- **Incidente:** Es una interrupción temporal no planificada de un servicio o la reducción de su calidad, que afecta su normal funcionamiento.
- **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.
- **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.
- **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 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 del negocio:** Es el documento estratégico que define cómo la entidad o la Corporación se prepara para posibles interrupciones y desastres, garantizando que sus operaciones críticas puedan continuar durante y después de una crisis.
- **Plan de recuperación de desastres de tecnología de información:** Es un proceso de recuperación que cubre los datos, el hardware, el software y el personal críticos, 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.
- **Primera línea de defensa:** Corresponde a la gestión operativa y de negocio que gestionan los riesgos operativos, responsables del control interno efectivo para identificar, evaluar, controlar, mitigar y notificar los riesgos asociados con sus actividades; de que existan controles adecuados; y, de que se sigan las políticas y procedimientos establecidos.
- **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.
- **Procesos:** Es el conjunto de actividades estandarizadas que transforman insumos en productos o servicios.
- **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.
- **Problema:** Causa subyacente de uno o varios incidentes, no necesariamente interrumpe un servicio inmediatamente, pero si no se gestiona, puede llevar a futuros incidentes repetitivos.

- **Resiliencia operativa:** Es la capacidad de una entidad de seguir prestando servicios a sus usuarios a pesar de una interrupción 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 residual:** Nivel de riesgo esperado después de aplicar los controles.
- **Riesgo operativo:** Es la posibilidad de incurrir en pérdidas por eventos derivados de fallas o insuficiencias en los factores de: procesos, personas, tecnología de la información y eventos externos. El riesgo operativo incluye el riesgo legal, pero excluye los riesgos: sistémico, estratégico y de reputación.
- **Riesgo legal:** Es la probabilidad de que una entidad sufra pérdidas debido a que los activos y contingentes se encuentren expuestos a situaciones de mayor vulnerabilidad; que sus pasivos puedan verse incrementados más allá de los niveles esperados, o que el desarrollo de sus operaciones enfrente la eventualidad de ser afectado negativamente, debido a error, negligencia, impericia, imprudencia o dolo, que deriven de la inobservancia, incorrecta o inoportuna aplicación de disposiciones legales o normativas, así como de instrucciones de carácter general o particular emanadas de los organismos de control, dentro de sus respectivas competencias; o, en sentencias o resoluciones jurisdiccionales o administrativas adversas; o, de la deficiente redacción de los textos, formalización o ejecución de actos, contratos o transacciones, inclusive distintos a los de su giro ordinario de negocio, o porque los derechos de las partes contratantes no han sido claramente estipulados.
- **Segunda línea de defensa:** Corresponde a las áreas especializadas, quienes establecen las políticas y estándares de riesgo operativo, monitorean y hacen contraposición de los controles diseñados y evaluados en la primera línea de defensa. También ayudan a definir y mantener el marco de gestión de riesgos de la organización y proporcionan un monitoreo independiente de la evolución de los riesgos.
- **Seguridad de la información:** Son los mecanismos implantados que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella, sean físicos o electrónicos.
- **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 operativo 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, multimedia, servicios asociados, entre otros.

- **Tercera línea de defensa:** Corresponde a la función de auditoría interna quien proporciona una evaluación independiente y objetiva de la eficacia global del marco de gobierno, riesgo y control de una organización. A través de su trabajo de auditoría, verifica si las dos primeras líneas de defensa son efectivas en la identificación, evaluación, control y monitoreo de los riesgos operativos.
- **Tipo de evento:** Identificación de los eventos de riesgo operativo de acuerdo a su origen.
- **TIER III:** Certificación o clasificación de los centros de datos que permite el mantenimiento concurrente, con una disponibilidad del noventa y nueve punto novecientos ochenta y dos por ciento (99.982%) al año, y un tiempo de parada de uno punto seis (1.6) horas, e incluye redundancia en sus componentes de infraestructura, así como fuentes alternativas de electricidad y refrigeración en caso de emergencia.

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, definirán políticas y procesos e incluirán la metodología debidamente documentada 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, evitar, 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, según corresponda.

Adicionalmente, definirán y adoptarán un modelo basado en el esquema de tres líneas de defensa considerando su objeto social, tamaño, naturaleza, complejidad de sus operaciones y otras características. Las líneas de defensa relacionadas con el riesgo operativo deben cumplir y sin limitarse con las siguientes funciones:

Primera línea:

1. Identificar y evaluar la materialidad de los riesgos operativos inherentes a su gestión de negocio y operacional mediante el uso de herramientas de gestión de riesgos operativos;
2. Establecer controles apropiados para mitigar los riesgos operativos inherentes y evaluar el diseño y la efectividad de estos controles, de acuerdo a su nivel de riesgo; e,
3. Informar sobre los riesgos operativos residuales no mitigados por los controles, incluidos los eventos de pérdida, deficiencias de control, deficiencias de procesos y sus incumplimientos.

Segunda línea:

1. Desarrollar el análisis y enfoque de manera independiente con respecto a las unidades de negocio; identificar riesgos operativos, proponer controles y monitorear permanentemente el apetito y la tolerancia al riesgo operativo;
2. Evaluar periódicamente en la gestión de negocio y operativa la implementación de las metodologías o herramientas de gestión del riesgo operativo, manteniendo evidencias de la evaluación realizada;
3. Desarrollar y mantener políticas, directrices de gestión y medición de riesgos operativos;
4. Monitorear y reportar el perfil de riesgo operativo; y,
5. Diseñar y brindar capacitación y concientización sobre los riesgos operativos, en especial a los procesos catalogados como críticos.

Tercera línea:

1. Revisar el diseño y la implementación de los sistemas de gestión de riesgo operativo y los procesos asociados de la primera y segunda línea de defensa;
2. Revisar los procesos para garantizar que sean independientes y se implementen de manera coherente con las políticas establecidas; y,
3. Asegurar que los sistemas de cuantificación utilizados para evaluar el riesgo operativo reflejen el perfil de riesgo operativo de las entidades y la Corporación;

Artículo 5.- Etapas de la administración: Las entidades y la Corporación deben ejecutar las etapas definidas para la administración del riesgo operativo que consisten en:

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:
 - a. Inventario de procedimientos
 - b. Recolección de información
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 o puedan presentarse) 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 riesgo que presenta una actividad concreta, sin aplicarle ningún tipo de control.

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 debe dar mayor prioridad o gestión de respuesta, con los recursos de los que dispone la entidad.

4. **Controlar:** En esta etapa se busca definir las medidas de control que permitan reducir la probabilidad de ocurrencia así como los impactos ocasionados por los riesgos inherentes detectados. el cual requerirá que las entidades y la Corporación cuenten con planes de mitigación formalmente establecidos y validados periódicamente, mediante la revisión de estrategias y políticas; actualización o modificación de procesos y procedimientos establecidos; implementación o modificación de límites de riesgo; implementación o modificación de controles; plan de continuidad del negocio; revisión de términos de pólizas de seguro contratadas; contratación de servicios provistos por terceros; u otros, según corresponda. Los controles deben formar parte integral de las actividades regulares de la entidad para generar respuestas oportunas ante diversos eventos de riesgo operativo y las fallas o insuficiencias que los ocasionaron.

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.

5. **Monitorear:** En esta etapa se debe llevar a cabo el seguimiento adecuado y permanente a los riesgos asociados a sus procesos, su nivel de exposición y deben contar con un esquema organizado de reportes e informes, con el fin de ir analizando su evolución, que permita tener información suficiente, pertinente y oportuna para la toma de decisiones así como conocer el riesgo residual de las medidas tomadas.
6. **Comunicar:** Deben definir una política de comunicación formal 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.

Así mismo, de acuerdo con el segmento al que pertenezcan y al tamaño y complejidad de sus operaciones, desarrollarán sus propias metodologías y procedimientos efectivos de administración y mitigación relacionados a los factores de riesgo operativo.

Una vez identificados los riesgos operativos y las fallas o insuficiencias en relación con los factores de este riesgo, se debe medir el riesgo determinando su probabilidad de ocurrencia e impacto para la entidad, permitiendo a sus representantes contar con una visión clara de la exposición al riesgo operativo, con el objetivo de alertarlos en la toma de decisiones y acciones, de manera que estén en la capacidad de decidir si mitiga, transfiere, asume o evita el riesgo reduciendo sus efectos.

Las entidades y la Corporación deben implementar mecanismos de cuantificación periódica sobre los eventos de pérdidas producidos por este tipo de riesgos, que permitan reevaluar la declaración de tolerancia institucional ante el riesgo operativo.

Artículo 6.- 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 con la siguiente clasificación:

1. **Línea minorista.-** Contempla las actividades de intermediación financiera tales como: recepción de depósitos en cualquier modalidad; 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.
2. **Línea de microfinanzas.-** Incluye operaciones financieras como préstamos en el segmento de microcrédito, ahorro o transferencias a personas naturales cuyo origen de recursos provenga de actividades económicas de menor escala.
3. **Línea de tarjetas.-** Contempla las actividades y servicios relacionados con tarjetas de crédito, débito, pago y prepago.
4. **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.
5. **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.
6. **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.
7. **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 procesos 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.

Artículo 7.- Las entidades ubicadas en los segmentos 1, 2 y 3, asociaciones mutualistas de ahorro y crédito para la vivienda, cajas centrales y la Corporación, deberán cumplir con lo siguiente:

1. Elaborar un manual de riesgo operativo de acuerdo con 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 de las entidades ubicadas en el 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.
2. Identificar los eventos de riesgo operativo por línea de negocio, 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, a través de una metodología formal, debidamente documentada y aprobada por el Consejo de Administración o el Directorio, según corresponda.

La metodología debe contener la forma en la cual se identificarán los eventos de riesgo (materializados o se prevean que ocurran), la forma de identificarlos, la base cualitativa y/o cuantitativa para medirlos y así obtener su riesgo inherente, la manera para tomar las acciones o decisiones frente a ellos, el seguimiento de la efectividad de las mismas y el cálculo de su riesgo residual, aspectos de comunicación a la administración y al personal sobre la gestión de riesgo operativo y las decisiones tomadas.

Los tipos de eventos deben considerarse al menos 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 seguridad y salud en el trabajo, pago de reclamaciones por daños personales, casos relacionados con la diversidad, discriminación, acoso laboral 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,
 - 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.
3. 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. 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 operativo 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.
5. Contar 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 Secciones III: Normas para la Administración Integral de Riesgos en las Cooperativas de Ahorro y Crédito, Cajas Centrales y Asociaciones Mutualistas de Ahorro y Crédito para la Vivienda y VIII: Norma para la Administración Integral de Riesgos de la Corporación Nacional de Finanzas Populares y Solidarias, del Capítulo XXXVI: Sector Financiero Popular y Solidario, del Título II: Sistema Financiero Nacional, del Libro I: "Sistema Monetario y Financiero de la Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros", emitida por la Junta de Política y Regulación Financiera, según corresponda.

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.

6. 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. Reporte de indicadores claves de riesgo operativo que permitan evaluar la eficiencia y eficacia de las políticas, procesos, procedimientos y metodologías aplicadas;
 - c. Identificación de la evolución de los eventos de riesgo y reporte del grado de cumplimiento de planes de acción (mitigación);
 - d. Mapa de calor en el que se identifique la concentración de eventos de riesgo por nivel de riesgo; y,
 - e. 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, evitar, mitigar o transferir, reduciendo sus consecuencias y efectos.

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.

Artículo 8.- Las entidades y la Corporación deben diseñar, programar y coordinar planes de capacitación permanente sobre la administración de riesgo operativo, uso adecuado de tecnología y seguridad de la información, dirigidos a todos sus órganos internos, empleados, funcionarios o servidores.

Las capacitaciones deben cumplir al menos con las siguientes condiciones:

7. Ser impartidas durante el proceso de inducción de los nuevos funcionarios, empleados o servidores;
8. Ser impartidas de forma regular a los funcionarios, empleados o servidores;

9. 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,
10. Mantener un registro del personal capacitado y de las sugerencias realizadas por los participantes.

Artículo 9.- Las entidades y la Corporación deben definir una política de comunicación formal 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 y la efectividad de la información a comunicar en función a su gestión de riesgos y las medidas adoptadas en su gestión.

Artículo 10.- Las entidades ubicadas en los segmentos 4 y 5, para mantener una adecuada administración del riesgo operativo, deberán:

1. 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;
2. Mantener un registro de sus eventos de riesgo operativo que contemple como mínimo la fecha de ocurrencia, descripción, solución e impacto financiero, de ser el caso;
3. Garantizar una adecuada separación de funciones que evite la realización o el ocultamiento de fraudes, errores, omisiones u otros eventos de riesgo operativo;
4. Implementar políticas y niveles de aprobación para las distintas líneas de negocio y procesos con el fin de evitar conflictos de interés;
5. Elaborar un manual de administración del personal que contemple las políticas, procesos y procedimientos para la incorporación, permanencia y desvinculación del personal; y,
6. Elaborar un procedimiento de análisis de riesgos para nuevas operaciones, productos o servicios.

SECCIÓN IV

FACTORES DE RIESGO OPERATIVO

Artículo 11.- Las entidades y la Corporación para reducir el nivel de riesgo operativo deberán administrar los factores de riesgo considerando su particularidad y la interrelación entre ellos.

Artículo 12.- Factor 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, asociaciones mutualistas de ahorro y crédito para la vivienda, cajas centrales 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, tomando como referencia la Norma ISO 9001.

Las entidades y la Corporación deberán definir formalmente procesos, políticas y procedimientos que aseguren una apropiada planificación, administración y cumplimiento de los objetivos institucionales.

1. **Agrupación de Procesos.-** Los procesos deberán ser agrupados de la siguiente manera:
 - a. **Procesos gobernantes o estratégicos:** Se considerarán a aquellos que proporcionan directrices y políticas a los demás procesos cuya responsabilidad compete a la asamblea general o junta general de socios, 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.
 - b. **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.
 - c. **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.
2. **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 realidad de 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.

3. Metodología de procesos.- La metodología debe contener al menos pero sin limitarse a lo siguiente:

- a. Descripción y diagramación en secuencia lógica y ordenada de las actividades, tareas, y controles.
- b. Determinación de los responsables de los procesos; y, del establecimiento de controles y planes de acción para una correcta administración del riesgo operativo.
- c. Identificación de los clientes internos y externos.
- d. Productos y servicios que genera.
- e. Definir indicadores para cada uno de los procesos que le permitan a la entidad medir la eficacia y eficiencia de éstos.
- f. Difusión y comunicación de los procesos buscando garantizar su correcta aplicación; y,
- g. Actualización y mejora continua a través del seguimiento periódico en su aplicación, al menos, una vez al año para los procesos productivos; y, para el resto, al menos, una vez cada dos años.

4. 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.

5. Separación de funciones.- Mantener separación de funciones que evite concentraciones de carácter incompatible, entendidas estas, como aquellas tareas cuya ejecución por una sola persona, eventualmente, podría permitir la realización o el ocultamiento de fraudes, errores, omisiones u otros eventos de riesgo operativo.

Artículo 13.- Factor Personas.- Las entidades y la Corporación deben contar con una estructura orgánico funcional acorde al tamaño, complejidad de sus operaciones y normativa vigente aplicable 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, debilidades en las capacidades técnicas o conocimientos para desarrollar la función que han sido asignados, entre otros.

1. Definición de políticas, proceso y procedimientos.- Definir políticas, procesos y procedimientos para la incorporación, permanencia y desvinculación del personal, soportados técnicamente y ajustados a las disposiciones legales que aseguren la planificación y administración del capital humano, mismos que corresponden a:

- a. Incorporación: Se refiere a la planificación de necesidades, el reclutamiento y la selección, la contratación e inducción de nuevo personal. Las entidades y la Corporación deben evaluar su organización con el objeto de definir el personal

mínimo necesario, la modalidad de trabajo y las competencias idóneas para el desempeño de cada puesto.

- b. **Permanencia:** Se refiere a 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; identificación de los puestos críticos y el personal clave de la entidad; y, definición del personal de reemplazo en el caso de ausencia temporal o definitiva, con la finalidad de dar continuidad a las operaciones del negocio.
 - c. **Desvinculación:** Se refiere a la planificación respecto a 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.
2. **Acuerdos 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. Adicionalmente deben 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, mismos que deben ser incluidos en el acuerdo de confidencialidad.
3. **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.
4. **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.

Artículo 14.- Factor Tecnologías de la información y comunicación.- Las entidades y la Corporación, deben contar y mantener tecnologías de la información y comunicación

acordes 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.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo tecnológico, las entidades ubicadas en los segmentos 1, 2, 3, asociaciones mutualistas de ahorro y crédito para la vivienda, cajas centrales y la Corporación, deberán contar como mínimo lo siguiente:

1. Área de tecnologías de la información y comunicación: Un comité, unidad, o responsable de tecnologías de la información que garantice el normal funcionamiento de ésta, independiente de las áreas operativas y de negocio de la entidad. El área de tecnología de la información debe ser consistente de acuerdo con el segmento, naturaleza, complejidad y perfil de riesgo de las operaciones de la entidad.

2. Comité de Tecnologías de la Información y Comunicación:

a. Conformación del Comité de Tecnologías de la Información y Comunicación.- El comité estará conformado por: un vocal del Consejo de Administración, o quien haga sus veces, quien lo presidirá y tendrá voto dirimente; el representante legal o su delegado; y, el responsable del área de riesgo, quienes tendrán voz y voto; y, de tecnología que actuará como secretario, solamente tendrá voz. En las sesiones del comité podrán participar funcionarios vinculados con los temas a tratarse, quienes tendrán voz pero no derecho a voto.

El Comité expedirá un reglamento en donde se establezcan, como mínimo, el objetivo, sus funciones y responsabilidades, que será aprobado conforme corresponda dentro de la estructura organizacional.

Las reuniones de este comité se realizarán trimestralmente o cuando la situación lo amerite, dejando evidencia de las decisiones adoptadas, mismas que deben ser comunicadas al Consejo de Administración, u organismo que haga sus veces.

b. Funciones del Comité de Tecnologías de la Información y Comunicación.- El Comité será responsable principalmente de:

- i. Planificar, coordinar y supervisar las actividades relacionadas con las tecnologías de la información y comunicación;
- ii. Recomendar las políticas, procesos, procedimientos y metodologías de las tecnologías de la información y comunicación para posterior aprobación del Consejo de Administración o el Directorio, según corresponda;
- iii. Establecer lineamientos para la formulación del plan estratégico de tecnologías de la información y comunicación, relacionado con el plan estratégico de la entidad y presupuestos aprobados;
- iv. Recomendar al Consejo de Administración o al Directorio, según sea

- el caso, el Plan Estratégico de las Tecnologías de la Información y Comunicación (P.E.T.I.C.);
- v. Priorizar la inversión de tecnologías de la información y proyectos con componente tecnológico;
 - vi. 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,
 - vii. Presentar periódicamente al Consejo de Administración o al Directorio, según sea el caso, informes de cumplimiento de la gestión de las tecnología de la información.
- c. **Sesiones del Comité.-** Sesionará de manera ordinaria de manera trimestral; y, extraordinariamente, por convocatoria del presidente, que deberá ser notificada con un mínimo de setenta y dos (72) horas de anticipación a la fecha de realización de la sesión.

El Comité de Tecnologías de la Información y Comunicación sesionará con al menos tres de sus integrantes y las decisiones serán tomadas por mayoría de votos.

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 estas, 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, según corresponda, las evaluaciones y resoluciones adoptadas.

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

- a. El apoyo y compromiso formal del Consejo de Administración o del Directorio, a través de la aprobación de un plan estratégico de las tecnologías de la información y comunicación 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; y,
- b. Deberán definir políticas, procesos, procedimientos y metodologías de tecnología de la información alineado a los objetivos y actividades de la entidad, que:
 - i. 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;

- ii. Contemplan al menos que el Consejo de Administración de las entidades de los segmentos 1, 2, 3, asociaciones mutualistas de ahorro y crédito para la vivienda, cajas centrales o el Directorio, según corresponda, aprueben un Plan estratégico de las tecnologías de la información y comunicación (P.E.T.I.C.) 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; y,
 - iii. Las consecuencias de su incumplimiento, de existir.
4. **Estructura de gestión de tecnología:** Con la finalidad de implementar de manera eficiente la administración de las tecnología de la información y comunicación, las entidades deberán contemplar una estructura de gestión de tecnología, de acuerdo al siguiente cuadro:

ÓRGANOS INTERNOS	SEGMENTO 1, MUTUALISTAS, CAJAS CENTRALES Y CORPORACIÓN	SEGMENTO 2	SEGMENTO 3
Comité de las Tecnologías de la Información y Comunicación	X	X	N/A
Unidad de las Tecnologías de la Información y Comunicación	X	X	N/A
Responsable de las Tecnologías de la Información y Comunicación.	N/A	N/A	X

N/A = No aplica

Las cooperativas de ahorro y crédito ubicadas en el 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.

5. **Operaciones de las tecnologías de la información y comunicación:** Con el objeto de garantizar que las operaciones de las tecnologías de la información y comunicación satisfagan los requerimientos de las operaciones, las referidas entidades deberán contar al menos con lo siguiente:
- a. Procedimientos que establezcan las actividades y responsables de la operación y el uso de los centros de datos, que incluyan controles que eviten accesos no autorizados;
 - b. Procedimientos de gestión de incidentes y problemas de tecnología de la información, que considere al menos:
 - i. El análisis de la causa raíz del problema con personal técnico independiente del personal que administra y opera las plataformas

- afectadas por los incidentes;
- ii. Mantener una base de conocimiento y errores conocidos; definición e implementación de planes de acción efectivos que les permita mitigar la recurrencia, así como la correlación de eventos e incidentes catalogados como problemas;
 - iii. Implementación de técnicas de gestión de incidentes de las tecnologías de la información y comunicación de acuerdo con la naturaleza, tamaño y complejidad de la entidad controlada;
 - iv. Definición e implementación de indicadores clave de rendimiento para la gestión de problemas de las tecnologías de la información y comunicación; y
 - v. Procedimientos de respaldo de información periódicos, acorde a los requerimientos legales y de continuidad del negocio, que incluyan: la frecuencia de verificación, eliminación y el transporte seguro hacia una ubicación remota, 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, este respaldo podría ser en la nube.
6. 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 tengan 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 solo 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.

7. 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 políticas y procedimientos 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. Un informe de análisis de la capacidad y desempeño de la infraestructura tecnológica;
 - d. Procedimientos de migración de la plataforma tecnológica, que incluyan controles para garantizar la continuidad del servicio;
 - e. 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;
 - f. 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; y,
 - g. Ambientes aislados con la debida segregación de accesos para desarrollo, pruebas y producción, los cuales deben contar con la capacidad requerida para cumplir sus objetivos. Al menos, se debe contar con dos ambientes: desarrollo y producción.
8. En el caso de contratar servicios de infraestructura, plataforma así como servicio 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 y contar como mínimo con la certificación TIER III para diseño o su equivalente, implementación y operación y así garantizar la disponibilidad de los servicios brindados;
 - b. Certificación 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;
 - c. Un informe de análisis de la capacidad y desempeño de la infraestructura tecnológica;
 - d. 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;
 - e. Capacidad para transferir sólidamente los conocimientos; y,
 - f. 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,

- g. 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:
- h. 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,
- i. 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.”

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 así como *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 o presentar la certificación actualizada del cumplimiento de la ISO 27000, TIER III y ANSI-TIA-942.

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.”;

9. Con la finalidad de asegurar que los cambios a los aplicativos e infraestructura que soportan las operaciones estén debidamente autorizados, documentados, probados, y aprobados por el propietario de la información previo a su paso a producción, las entidades controladas deben implementar procedimientos de control de cambios, acorde a las metodologías y mejores prácticas nacionales e internacionales de la industria, que considere aspectos como los siguientes, pero sin limitarse a:
- a. Mecanismos mediante los cuales se iniciarán las solicitudes de cambio;
 - b. Una metodología para analizar, dar prioridad y aprobar las solicitudes de cambio;
 - c. Evaluación del impacto de los cambios sobre los aplicativos e infraestructura de producción, considerando como una arista del análisis que no contravenga con la normativa vigente;
 - d. Mecanismos de marcha atrás, de modo que el impacto por cualquier falla pueda ser minimizado;
 - e. Librerías de desarrollo separadas de las librerías de producción, para evitar que una versión de prueba pueda contener código no autorizado;
 - f. Mecanismos que aseguren que los cambios a los aplicativos y a su documentación, se realizan sobre las versiones fuente de los elementos en producción, y que los cambios realizados al código de las aplicaciones informáticas corresponden a aquellos solicitados por el propietario de la información;
 - g. El responsable de aseguramiento de la calidad supervisa el mantenimiento de versiones de programa, código fuente o registros de configuración de la infraestructura, para garantizar su integridad;
 - h. El responsable del aseguramiento de la calidad debe realizar, en ambientes no productivos, junto con el propietario de información, las pruebas y certificación sobre los cambios para garantizar que: ejecuten las funciones requeridas, que la funcionalidad y desempeño existente no se vean afectadas por el cambio, que no se hayan generado riesgos de seguridad debido al cambio y que se cuente con toda la documentación actualizada; una vez concluidas exitosamente las pruebas, se debe registrar la aprobación del cambio;
 - i. Mecanismos para garantizar que el paso de programas desde el ambiente de desarrollo a pruebas y de producción, sea realizado por un grupo independiente a los programadores; y,
 - j. Procedimientos de cambios de emergencia para casos excepcionales en donde no sea posible seguir el proceso completo de control de cambios que incluya su posterior regularización y que permitan asegurar que no se compromete la integridad del sistema e infraestructura.
10. Las entidades ubicadas en los segmentos 4 y 5 deberán incluir 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 15.- 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.

SECCIÓN IV

GESTIÓN DE INCIDENTES Y PROBLEMAS

Artículo 16.- Las entidades y la Corporación deben desarrollar e implementar planes de respuesta y recuperación para gestionar los incidentes y problemas que puedan afectar el normal funcionamiento de sus servicios, especialmente, de sus servicios críticos en línea con el apetito y la tolerancia al riesgo definidos, de manera que contribuya a la resiliencia operativa de la entidad; para lo cual, deben garantizar la disponibilidad de los servicios críticos que se ofrecen a los usuarios financieros en un noventa y nueve punto noventa y nueve por ciento (99.99%) anual, dicha disponibilidad no considerará el mantenimiento de la plataforma tecnológica o aplicativos; y, mantener lo siguiente pero sin limitarse a:

1. Asignar un gestor de incidentes y problemas, quien deberá encargarse de la trazabilidad hasta finalizar la atención de los incidentes y problemas; y, su respectivo registro en la base de datos.
2. Establecer políticas, procesos, procedimientos y metodologías para la gestión de incidentes y de problemas, que puedan afectar a los factores de riesgo operativo.
3. La gestión de incidentes debe abarcar el ciclo de vida del incidente, que incluya entre otros: registro, priorización en función de la gravedad, análisis, escalamiento, solución, monitoreo, lecciones aprendidas y reporte a las partes interesadas tanto internas como externas.
4. La gestión de problemas debe considerar al menos: el análisis de la causa raíz del problema con personal técnico independiente del personal que administra y opera las plataformas afectadas por los incidentes; y, mantener una base de conocimiento y errores conocidos; definición e implementación de planes de acción efectivos que les permita mitigar la recurrencia, así como la correlación de eventos e incidentes catalogados como problemas.
5. Ejecutar pruebas controladas de gestión de incidentes y problemas.
6. Mantener una base de conocimiento de respuesta a incidentes y recuperación que incluya recursos internos y de terceros, según aplique, para respaldar las capacidades de respuesta y reanudación de los servicios. Los procedimientos asociados deben revisarse, probarse y actualizarse periódicamente por las áreas involucradas.

7. Las entidades controladas deben aplicar los planes de contingencia y continuidad del negocio cuando los incidentes afecten a sus servicios críticos conforme a la evaluación del impacto del incidente, mismos que deberán ser comunicados inmediatamente al organismo de control.
8. Los mantenimientos programados, deben ser informados a sus usuarios, con al menos veinticuatro (24) horas de anticipación. Estos mantenimientos se computarán en la disponibilidad del servicio.

SECCIÓN V

GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Artículo 17.- Sistema de Gestión de Continuidad del Negocio.- Las entidades y la Corporación deben establecer, implementar, mantener y mejorar un sistema de gestión de la continuidad del negocio, de acuerdo al tamaño y complejidad, para garantizar su capacidad de operar de forma continua y limitar las pérdidas en caso de una interrupción grave del negocio, tomando como referencia los estándares de la serie ISO 22301, de manera que contribuya a la resiliencia operativa de la entidad; por lo cual, debe contar con, al menos lo siguiente:

1. **Definición de Procesos críticos:** Las referidas entidades deberán adoptar una metodología que les permita identificar y evaluar los procesos críticos, que serán definidos por el Comité de Administración Integral de Riesgos, 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.
2. **Un Comité de Continuidad del Negocio:** El Comité de Continuidad del Negocio, conformado al menos por: los responsables de riesgos, de tecnología, negocios, crédito, administrativo y el representante legal, expedirá un reglamento en donde se establezcan, como mínimo, el objetivo, sus funciones y responsabilidades. Las reuniones de este comité se realizarán, al menos, trimestralmente, o cuando se las requiera. El comité de continuidad del negocio debe dejar evidencia de las decisiones adoptadas, las cuales deben ser conocidas y aprobadas por el comité de administración integral de riesgos. El comité de continuidad del negocio debe tener, al menos, las siguientes responsabilidades:
 - a. Evaluar y supervisar el sistema de gestión de continuidad del negocio;
 - b. Monitorear la implementación del plan de continuidad del negocio y asegurar el alineamiento de este con la metodología de administración de la continuidad del negocio;
 - c. Proponer para la revisión y aceptación del comité de administración integral de riesgos, el plan de continuidad del negocio y sus actualizaciones;
 - d. Revisar el presupuesto del plan de continuidad del negocio y ponerlo en conocimiento del comité de administración integral de riesgos;
 - e. Dar seguimiento a las potenciales amenazas que pudieran derivar en una interrupción de la continuidad de las operaciones y coordinar las acciones preventivas; y,
 - f. Realizar un seguimiento a las medidas adoptadas en caso de presentarse una interrupción de la continuidad del negocio.

- 3. Políticas y procedimientos:** Políticas, estrategias, objetivos, procesos, procedimientos, metodologías, planes y presupuesto para la administración de la continuidad del negocio, que deben ser revisados y actualizados al menos una vez al año o cuando existan cambios significativos; y, aceptados por el comité de continuidad del negocio; y, propuestos por el comité de administración integral de riesgos, para la posterior aprobación del directorio o consejo de administración. Esta documentación debe ser difundida y comunicada a todo el personal involucrado, de tal forma que se asegure su cumplimiento.
- 4. Planes de contingencia y continuidad del negocio:** Las entidades ubicadas en los segmentos 1, 2, 3 asociaciones mutualistas de ahorro y crédito para la vivienda, cajas centrales y la Corporación, deben implementar planes de contingencia y de continuidad y de procesos críticos que cubran a personas, procesos y tecnología, 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.

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 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;
- b. Incorporar el proceso de administración del plan de continuidad del negocio al proceso de administración integral de riesgos;
- c. Definir técnicamente períodos de recuperación y tiempos máximos de interrupción que puedan soportar los procesos identificados como críticos, sin que afecte a la sostenibilidad de la institución;
- d. 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);
- e. Tiempo de recuperación objetivo (R.T.O.) y punto de recuperación objetivo (R.P.O.) de cada proceso crítico, conforme lo identificado en el análisis de impacto en el negocio;
- f. Plan de recuperación de desastres que detalle los procedimientos tecnológicos de restauración en una ubicación remota de los servicios de tecnología de la información;
- g. Identificar los riesgos por fallas en la tecnología de información y gestionar un plan de acción para mitigar los riesgos identificados;
- h. Definir una estrategia de continuidad de los procesos críticos, en línea con los objetivos institucionales;
- i. Desarrollar los planes de contingencia necesarios para implementar la estrategia de continuidad definida.
- j. Definir acciones a ejecutar antes, durante y una vez ocurrido el incidente que ponga en peligro la operatividad de la entidad;
- k. Determinar acciones a realizar para continuar con las actividades de la entidad en instalaciones propias o alternas (reanudación y recuperación);
- l. Realizar pruebas periódicas de los planes de continuidad y contingencia que permitan comprobar la aplicabilidad y efectuar los ajustes necesarios;

- m. Mantener información actualizada de contacto de las personas responsables de ejecutar cada actividad;
- n. Contar con cronogramas y procedimientos de prueba y mantenimiento de los planes de continuidad y contingencia;
- o. Criterios de invocación y activación del plan de continuidad del negocio;
- p. Definir procedimientos de difusión, comunicación, concientización y cumplimiento de los planes de continuidad y contingencia;
- q. Designar de su estructura un responsable de la continuidad del negocio.
- r. 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;
- s. 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,
- t. 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.

SECCIÓN VI

SERVICIOS PROVISTOS POR TERCEROS

Artículo 18.- Calificación y selección de proveedores.- Las entidades de los segmentos 1, 2, 3, asociaciones mutualistas de ahorro y crédito para la vivienda, cajas centrales 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:

1. Evaluar la experiencia de la empresa y su personal;
2. Evaluar la capacidad financiera para asegurar la viabilidad del proveedor durante todo el período de contratación previsto;
3. Efectuar análisis de costo beneficio;
4. Evaluar la capacidad y oportunidad de respuesta del proveedor a consultas, solicitudes de presupuesto y presentación de ofertas;
5. Evaluar la capacidad y calidad del servicio, instalación y apoyo;
6. Evaluar la capacidad logística del proveedor incluyendo las instalaciones y recursos técnicos y económicos;
7. Exigir que las entidades y organizaciones de servicios auxiliares cuenten con la calificación respectiva de la Superintendencia y cumplan la normativa correspondiente;
8. Comprobar que el proveedor cuente con representación técnica, legal, operativa y de contingencia suficientes, en especial si son proveedores internacionales;
9. Niveles mínimos de calidad del servicio acordado;
10. Garantías financieras y técnicas, tales como: buen uso del anticipo, fiel cumplimiento del contrato, buen funcionamiento y disponibilidad del servicio, entre otros;
11. Multas y penalizaciones por incumplimiento;

12. Seguridad de la información incluyendo ciberseguridad y protección de datos personales sobre la gestión de información usada de la entidad controlada en la provisión del servicio proporcionado por el proveedor;
13. Análisis del riesgo reputacional de la empresa;
14. Gestión de riesgos asociados a los servicios críticos provistos por terceros, que garanticen la gestión de seguridad de la información incluyendo ciberseguridad y la gestión de la continuidad del negocio, en función a la naturaleza del servicio contratado;
15. 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, en aquellos procesos definidos como críticos;

Artículo 19.- Para el caso de adquisición, implantación o arriendo de los bienes, servicios o sistemas tecnológicos, todas las entidades y la Corporación deberán verificar:

1. El objeto y especificaciones del bien o servicio contratado;
2. Los requisitos funcionales y técnicos de los bienes o servicios a ser adquiridos;
3. Los costos totales;
4. El nivel de soporte, capacitación y transferencias de conocimiento a ser proporcionados por el proveedor;
5. La existencia de respaldos, seguridad y sigilo de la información;
6. El mantenimiento y continuidad de los bienes y servicios;
7. Adaptación eficiente y oportuna a los requerimientos normativos;
8. El documento en que conste el plan de contingencia y continuidad del servicio que presta el proveedor, según corresponda;
9. 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;
10. 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;
11. El documento que asegure la existencia de mecanismos de gestión de riesgos que garanticen la continuidad del servicio que presta el proveedor, según corresponda;
12. 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; y,
13. 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.

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

Las entidades ubicadas de los segmentos 4 y 5 deberán contratar los servicios de

proveedores tecnológicos siempre y cuando cumplan con lo dispuesto en este numeral.

Artículo 20.- Para el caso de contratación de servicios de infraestructura, plataforma y/o *software* en la nube, tanto con proveedores nacionales o extranjeros, las entidades controladas deberán disponer, conforme el servicio contratado, de un informe técnico, uno de seguridad de la información y uno legal emitido por el personal de la entidad controlada, en función de sus competencias, en los cuales se hayan identificado los riesgos operativos asociados al servicio y la gestión respectiva.

Además de identificar y gestionar los riesgos asociados a estos servicios, la entidad y la Corporación deben:

1. Contar con un informe sobre el detalle de los servicios asociados a los procesos críticos a ser contratados que incluya entre otros: el tipo de servicio contratado, el detalle del servicio alojado, la arquitectura tecnológica contratada, según aplique; el análisis de los riesgos operativos, legales, tecnológicos, de seguridad de la información incluida la ciberseguridad y continuidad de operaciones a los que se exponen al adoptar este servicio; así como los controles para mitigarlos;
2. Cerciorarse de que los centros de procesamiento de datos principal o alternativo, contratados en la nube tanto con proveedores nacionales o extranjeros, hayan sido 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 y así garantizar la disponibilidad de los servicios brindados; y,
3. Verificar que el proveedor de servicios en la nube tanto con proveedores nacionales o extranjeros cuente, para los servicios ofertados, como mínimo, con certificación en los estándares ISO 27017 (controles de seguridad para servicios en la nube), ISO 27018 (protección de información personal en la nube) u otras similares que aplique conforme el servicio ofertado.

Artículo 21.- Proveedores alternos para los servicios críticos.- Las entidades de los segmentos 1, 2, 3, asociaciones mutualistas de ahorro y crédito para la vivienda, cajas centrales y la Corporación deberán contar con proveedores alternos que acrediten capacidad técnica y operativa para proveer los bienes y prestar los servicios que se requiera, observando lo previsto en la presente norma.

Artículo 22.- 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 23.- Para la calificación y selección de proveedores, las entidades y la Corporación deberán analizar las ofertas de acuerdo a su política de contratación establecida, de tal manera que se evite posibles conflictos de interés.

SECCIÓN VII

RIESGO LEGAL

Artículo 24.- Administración de riesgo legal.- Con el propósito de gestionar adecuadamente el 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 25.- Aspectos de enfoque de riesgo legal.- Las fallas o insuficiencias de orden legal, así como los eventos que podrían ocasionar la materialización del riesgo legal deben ser identificadas, medidas, controladas, mitigadas y monitoreadas 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 nacionales y extranjeras; estipulaciones contractuales; y, cumplimiento legal y normativo, entendiéndolos dentro de las siguientes conceptualizaciones:

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 social de las entidades y la Corporación, de acuerdo a su naturaleza jurídica.
2. **Gestión de crédito:** Es el conjunto de actividades que deben ejecutar en relación al otorgamiento de operaciones crediticias, su instrumentación y su recuperación.
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.
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.
5. **Proveedores nacionales o extranjeros:** Son las personas jurídicas constituidas en el país o en el exterior y que proveen bienes o servicios críticos. Para el caso de proveedores extranjeros, éstos deberán estar domiciliados 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.
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.

7. **Cumplimiento legal y normativo:** Es el proceso mediante el cual la entidad controla que sus actividades y 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 26.- Clasificación del riesgo legal.- El riesgo legal se puede clasificar en:

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.
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.
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 27.- 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, según corresponda, tendrán las siguientes:

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;
- e. Tomar las medidas para la gestión de eventos de riesgo; y,
- f. Las demás determinadas por la Superintendencia.

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, asociaciones mutualistas de ahorro y crédito para la vivienda, cajas centrales 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;
- g. Conocer la matriz de riesgo operativo, priorizar los eventos de conformidad con su criticidad y proponer al Consejo de Administración o el Directorio, según corresponda, medidas de acción a tomar; y,
- h. Las demás que determine el Consejo de Administración o el Directorio, según corresponda o la Superintendencia.

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 ubicadas en los segmentos 1, 2, 3, asociaciones mutualistas de ahorro y crédito para la vivienda, cajas centrales y la Corporación;
- j. Elaborar la metodología para definir y administrar la matriz de riesgos para las entidades ubicadas en los segmentos 1, 2, 3, asociaciones mutualistas de ahorro y crédito para la vivienda, cajas centrales y la Corporación;
- k. Medir el riesgo inherente de los eventos de riesgo, determinar sus factores y proponer medidas de acción al CAIR, presentar valoración del riesgo residual y del seguimiento de las decisiones tomadas por la administración de cada evento gestionado;
- 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 28.- Responsabilidad 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 Directorio, según corresponda. Velar por el cumplimiento de las decisiones para la gestión de cada evento de riesgo discutido y aprobado por el Consejo de Administración o Directorio.

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 así como con la implementación de las medidas aprobadas por los órganos directivos.

Artículo 29.- Responsabilidades de las entidades ubicadas en 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 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 del 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 28, implementará y dará continuidad a los lineamientos definidos en la presente norma y de lo establecido en su artículo 10; 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 correctivas para el cumplimiento de la presente norma.

SEGUNDA.- Los auditores internos deberán evaluar objetiva e independientemente la gestión del riesgo operativo en los siguientes aspectos:

1. Que cumpla 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; y,
2. Revisen si la entidad ha realizado pruebas a los planes de contingencia, continuidad y recuperación y si se han implementado es los referidos planes las correcciones necesarias derivadas de esas pruebas.

Los auditores internos deberán aplicar procesos y procedimientos de auditoria a través de un equipo competente, debidamente capacitado y operativamente independiente de los procesos operativos, que coadyuven al mejoramiento de la efectividad de la administración 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 y la Corporación para el cumplimiento de esta norma, en lo relacionado a la seguridad de la información y canales electrónicos observarán lo dispuesto en las normas expedidas para el efecto.

QUINTA.- Las organizaciones y compañías de servicios auxiliares, en el ámbito del servicio prestado, deberán aplicar la gestión de riesgo operativo establecido en la presente norma.

SEXTA.- Las entidades deben generar planes y programas que les permitan dar cumplimiento con lo dispuesto en la Ley Orgánica de Protección de Datos Personales.

DISPOSICIONES TRANSITORIAS

PRIMERA.- Las disposiciones contenidas en la sección de “Gestión de Incidentes y Problemas” deben ser implementadas por las entidades ubicadas en los segmentos 1 y 2, como máximo hasta el 31 de diciembre del 2024.

SEGUNDA.- Las entidades ubicadas en el Segmento 3, hasta el 30 de junio del 2025, deberán cumplir con lo dispuesto en las secciones IV y V de la presente norma.

DISPOSICIÓN DEROGATORIA.- Deróguese la Resolución No. SEPS-IGT-IR-IGJ-2018-0279, de 26 de noviembre de 2018, reformada con las resoluciones Nos. SEPS-IGT-IR-IGJ-2018-0284, de 13 de diciembre de 2018, SEPS-IGT-IGS-INR-INGINT-2020-0221, de 2 de junio de 2020 y SEPS-IGT-IGS-INR-INGINT-2022-0211 de 7 de julio de 2022.

DISPOSICIÓN FINAL.- Esta Resolución entrará en vigencia a partir 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 los dos días del mes de julio del 2024.

Jorge Andrés Moncayo Lara
INTENDENTE GENERAL TÉCNICO