LIBRO I.- NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO

TÍTULO IX.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS

CAPÍTULO XII.- NORMA DE CONTROL PARA LA GESTIÓN INTEGRAL Y ADMINISTRACIÓN DE RIESGOS DE LAS ENTIDADES DE SERVICIOS FINANCIEROS TECNOLÓGICOS (Expedido con Resolución Nro. SB-2025-02323 de 25 de septiembre de 2025; Rectificada el número del capítulo con Resolución Nro. SB-2025-02809 de 26 de noviembre de 2025)

SECCIÓN I.- DISPOSICIONES GENERALES

ARTÍCULO 1.- Objeto. La presente norma tiene por objeto establecer los lineamientos para la gestión integral de riesgos aplicables a las entidades de servicios financieros tecnológicos, con el fin de salvaguardar la estabilidad financiera, la continuidad operativa y la protección al usuario.

ARTÍCULO 2.- Ámbito de aplicación. La presente norma será de cumplimiento obligatorio para las entidades de servicios financieros tecnológicos controladas por la Superintendencia de Bancos.

Sin perjuicio de lo anterior, en lo relativo a sistemas y servicios de pago, las entidades observarán la normativa del Banco Central del Ecuador; y, en materia de protección de datos personales, cumplirán la Ley Orgánica de Protección de Datos Personales y las directrices de la autoridad competente.

ARTÍCULO 3.- Principios. La gestión integral de riesgos de las entidades de servicios financieros tecnológicos se regirá por los siguientes principios:

1. **Proporcionalidad.** Las políticas, procesos, procedimientos y metodologías deberán adecuarse al tamaño, complejidad y volumen de operaciones de la entidad partiendo de una línea base que esta normativa establezca;

2. **Integralidad.** La gestión de riesgos abarcará todos los procesos, actividades y operaciones de la entidad, incluidas aquellas tercerizadas;

3. **Transparencia.** La información sobre riesgos y controles deberá estar debidamente documentada y disponible para la Superintendencia de Bancos;

4. **Innovación responsable.** Los servicios financieros tecnológicos deberán gestionarse con enfoque prudencial, mitigando riesgos inherentes a la digitalización; y,

5. **Protección al usuario.** Todas las decisiones en materia de gestión integral y administración de riesgos deberán priorizar la seguridad, confianza y continuidad de los servicios a los usuarios.

ARTÍCULO 4.- Definiciones. Para efectos de esta norma, se entenderá por:

1. **Actividad.** Es el conjunto de tareas que ejecutan las entidades controladas.
2. **Administración de la continuidad del negocio.** Es un proceso permanente que garantiza la continuidad de las operaciones de las entidades de servicios financieros

tecnológicos, a través del mantenimiento efectivo de un sistema de gestión de continuidad del negocio.

3. **Apetito al riesgo.** Es el nivel de exposición al riesgo operativo, definido por la entidad de servicios financieros tecnológicos, que está dispuesta a asumir o aceptar, en el desarrollo de sus operaciones con la finalidad de alcanzar sus objetivos estratégicos.
4. **Canales electrónicos.** Se refiere a todas las vías o formas a través de las cuales los usuarios pueden efectuar transacciones con las entidades de servicios financieros tecnológicos, mediante el uso de elementos o dispositivos electrónicos o tecnológicos, utilizando o no tarjetas, conforme a los tipos de canales (tabla 107) definidos en el manual de tablas de la normativa vigente de la Superintendencia de Bancos.
5. **Causa raíz.** Es la causa principal que genera un incidente o problema; su identificación permite aplicar soluciones adecuadas, prevenir y resolver sistemáticamente la ocurrencia de un incidente o problema, con el objetivo de evitar futuras ocurrencias.
6. **Ciberseguridad.** Conjunto de medidas de protección de la infraestructura tecnológica y de la información, a través del tratamiento de las amenazas que ponen en riesgo la información procesada por los diferentes componentes tecnológicos interconectados.
7. **Cliente/Usuario.** Es la persona natural o jurídica que contrata los servicios prestados por las entidades de servicios financieros tecnológicos.
8. **Confidencialidad.** Es un principio y una práctica que se refiere a la protección y resguardo de la información sensible o privada para evitar su acceso o divulgación no autorizada.
9. **Cumplimiento.** Se refiere a la observancia y aplicación de las leyes, reglamentos y demás normativa, así como los acuerdos contractuales en los procesos, actividades y operaciones a los que las entidades de servicios financieros tecnológicos están sujetas.
10. **Datos.** Es cualquier forma de registro sea este electrónico, óptico, magnético, impreso o en otros medios, susceptible de ser capturado, almacenado, procesado y distribuido.
11. **Datos personales crediticios.** Datos que integran el comportamiento económico de personas naturales, para analizar su capacidad financiera.
12. **Datos personales sensibles.** Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.
13. **Disponibilidad.** Es el atributo de que los usuarios autorizados tienen acceso a la información cada vez que lo requieran a través de los medios que satisfagan sus necesidades.
14. **Evento de riesgo operativo.** Es el hecho que deriva en pérdidas para las entidades de servicios financieros tecnológicos, originado por fallas o insuficiencias en los factores de riesgo operativo.
15. **Factor de riesgo operativo.** Es la causa primaria o el origen de un evento de riesgo operativo. Los factores son: procesos, personas, tecnología de la información y eventos externos.
16. **Indicadores Claves de Riesgo.** Es una métrica que permite monitorear la exposición a un determinado riesgo, y ayudan a tomar acciones oportunas en el caso de desviaciones.
17. **Incidente.** Es una interrupción no planificada de un servicio o la reducción de su calidad, que afecta el normal funcionamiento de sus servicios.
18. **Infraestructura tecnológica.** Conjunto de elementos tecnológicos agrupados y organizados cuya función es soportar las operaciones de una entidad.
19. **Integridad.** Es el atributo de mantener la totalidad y exactitud de la información y de los métodos de procesamiento.
20. **Línea de negocio.** Es una especialización del negocio que agrupa procesos encaminados a generar productos y servicios especializados para atender un

segmento del mercado objetivo, definido en la planificación estratégica de la entidad de servicios financieros tecnológicos.

21. **Perfil de Riesgo Operativo.** Es el nivel del riesgo de la entidad de servicios financieros tecnológicos que refleja la naturaleza y magnitud de los riesgos operativos a los que está expuesto.
22. **Plan de continuidad del negocio.** Es el conjunto de procedimientos que orientan a las entidades a mantener su operatividad en el caso de que ocurran interrupciones que afecten sus servicios.
23. **Problema.** Consecuencia de uno o varios incidentes críticos o un incidente que se repite muchas veces y por ello se debe encontrar su causa raíz.
24. **Proceso crítico.** Es el conjunto de actividades indispensables para la continuidad del negocio y las operaciones de la entidad de servicios financieros tecnológicos, y cuya falta de identificación o aplicación deficiente puede generarle un impacto negativo.
25. **Protección de datos.** Son las medidas técnicas, organizativas, legales y de cualquier otra índole, que sean necesarias, para que el tratamiento de los datos sea utilizado exclusivamente para el propósito con el que fueron solicitados y/o autorizados, de conformidad con la ley vigente para el efecto.
26. **Proveedor crítico.** Tercero cuya falla pueda generar un incidente o impedir el cumplimiento de los tiempos y puntos de recuperación objetivo RTO/RPO aprobados.
27. **Punto de recuperación objetivo (RPO).** Es la cantidad máxima aceptable de pérdida de los datos medidos en el tiempo.
28. **Resiliencia Operativa.** Capacidad de una entidad de servicios financieros tecnológicos para seguir entregando los servicios críticos durante eventos disruptivos; esta capacidad le permite a la entidad identificar y protegerse de amenazas y potenciales fallas, respondiendo y adaptándose a ellas; así como, recuperarse y aprender de los eventos disruptivos con la finalidad de minimizar su impacto hacia el futuro en la entrega de los servicios críticos.
29. **Seguridad de la información.** Son los mecanismos adoptados por la entidad que le permiten preservar la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella, incluye los aspectos relacionados con ciberseguridad.
30. **Servicios en la nube.** Es la provisión de servicios informáticos accesibles a través de la internet, estos pueden ser de infraestructura, plataforma y/o software.
31. **Servicio crítico.** Proceso o funcionalidad cuya indisponibilidad impide la ejecución de transacciones, el acceso a cuentas, la sincronización de datos financieros, la emisión de órdenes o la continuidad del negocio dentro de los tiempos y puntos de recuperación objetivo (RTO/RPO) aprobados.
32. **Tecnología de la información.** Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes y comunicaciones, entre otros.
33. **Tecnología Regulatoria (RegTech).** Es el uso de tecnologías innovadoras, como la automatización, inteligencia artificial y análisis de datos, para mejorar la eficiencia, precisión y trazabilidad del cumplimiento normativo en las entidades.
34. **Tiempo de recuperación objetivo (RTO).** Es el período de tiempo transcurrido después de un incidente, para reanudar una actividad o recuperar los recursos antes de que la entidad controlada genere pérdidas significativas.
35. **Tolerancia al riesgo.** Es el grado de desviación del riesgo operativo respecto del nivel de apetito de riesgo definido por el órgano de gobierno que la entidad de servicios financieros tecnológicos puede soportar.
36. **Transacciones.** Son movimientos que realizan los clientes y/o usuarios a través de los canales que brindan las entidades; y pueden ser monetarias y no monetarias.
37. **Transacciones monetarias.** Son las que implican movimiento de dinero y son realizadas por los clientes a través de canales presenciales o canales electrónicos,

tales como: transferencias, depósitos, retiros, operaciones de crédito, pagos, recargas de telefonía móvil, entre otras.

38. **Transacciones no monetarias.** Son las que no implican movimiento de dinero y son realizadas por los clientes a través de canales presenciales o canales electrónicos, tales como: consultas, cambios de clave, personalización de condiciones.

ARTÍCULO 5.- Riesgos sujetos a normativa específica. Los riesgos de crédito, liquidez, mercado y de prevención y administración del riesgo de lavado de activos y financiación de delitos, se regularán en lo que aplique conforme a las normas específicas emitidas por la Superintendencia de Bancos para los sectores financiero público y privado, sin perjuicio de lo dispuesto en relación con estos riesgos en la norma emitida por la Junta de Política y Regulación Financiera y Monetaria para las entidades de servicios financieros tecnológicos.

Por su parte, los riesgos operativos, tecnológicos, de seguridad de la información, ciberseguridad, continuidad del negocio, servicios provistos por terceros, legales y demás riesgos no financieros inherentes a la naturaleza de las entidades de servicios financieros tecnológicos, se regirán conforme lo establecido en la presente norma.

SECCIÓN II.- ADMINISTRACIÓN DE RIESGOS

ARTÍCULO 6.- Modelo de gestión de riesgos. En el marco de la administración integral de riesgos, y alineado al apetito y tolerancia del riesgo definidos por la organización; la entidad controlada debe definir políticas, procesos, procedimientos y metodologías para la administración del riesgo; y, 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 demás características propias.

Las líneas de defensa de las entidades controladas deben cumplir y sin limitarse con las siguientes funciones:

1. Primera línea

a) Identificar y evaluar la materialidad de los riesgos inherentes a su gestión de negocio y operativa mediante el uso de herramientas de gestión de riesgos;
b) Establecer controles apropiados para mitigar los riesgos inherentes y evaluar el diseño y la efectividad de estos controles;
c) Reportar los perfiles de riesgo de la gestión de negocio y operativa; y,
d) Informar sobre los riesgos residuales no mitigados por los controles, incluidos los eventos de pérdida, deficiencias de control, deficiencias de procesos y sus incumplimientos.

2. Segunda línea

a) Desarrollar una visión independiente con respecto a las unidades de negocio, identificar riesgos, proponer controles clave y monitorear permanentemente el apetito y la tolerancia al riesgo;
b) Evaluar periódicamente en la gestión de negocio y operativa la implementación de las metodologías o herramientas de gestión del riesgo, manteniendo evidencias de la evaluación realizada;
c) Desarrollar y mantener políticas, estándares y directrices de gestión y medición de riesgos;
d) Monitorear y reportar los perfiles de riesgo; y,
e) Diseñar y brindar capacitación y concientización sobre los riesgos.

3. Tercera línea

a) Revisar el diseño y la implementación de los sistemas de gestión de riesgos y los procesos asociados de la primera y segunda línea de defensa;
b) Revisar los procesos para garantizar que sean independientes y se implementen de manera coherente con las políticas establecidas; y,
c) Asegurar que los sistemas de cuantificación utilizados para evaluar los riesgos reflejen el perfil de riesgo de la entidad.

ARTÍCULO 7.- Comité de Administración Integral de Riesgos. Las entidades de servicios financieros tecnológicos deberán contar con un Comité de Administración Integral de Riesgos, cuya conformación, atribuciones y funcionamiento observarán el principio de proporcionalidad, en función del tamaño, complejidad y volumen de operaciones de cada entidad.

El Comité estará conformado, como mínimo por: un miembro de la Junta General de Accionistas, Directorio u órgano de gobierno que haga sus veces, quien lo presidirá; el representante legal de la entidad; y, el jefe de la Unidad de Riesgos o el responsable de riesgos.

En los casos en que la entidad no cuente con Junta General de Accionistas ni con Directorio, el Comité será presidido por un representante de los socios o accionistas según corresponda.

El Comité se reunirá ordinariamente al menos una vez al mes y, de manera extraordinaria, cuando así lo requiera la naturaleza de los riesgos identificados. El quórum de las reuniones se cumplirá con la mayoría simple de sus miembros, y las decisiones se adoptarán por mayoría de votos; en caso de empate, el presidente tendrá voto dirimente.

La Superintendencia de Bancos, en función del tamaño, volumen de operaciones y naturaleza jurídica de la entidad, podrá exigir requisitos diferenciados para la conformación y periodicidad de sesiones.

ARTÍCULO 8.- Funciones del Comité de Administración Integral de Riesgos. Las funciones principales que debe cumplir el Comité de Administración Integral de Riesgos, son las siguientes:

1. Aprobar y mantener actualizados los manuales, políticas, procedimientos, metodologías, algoritmos y/o modelos automatizados para la gestión de riesgos; así como, el plan de continuidad del negocio, cuando exista delegación expresa del órgano de gobierno de la entidad;

2. Evaluar periódicamente la efectividad de los controles internos y externos implementados, proponiendo y adoptando acciones correctivas cuando se identifiquen deficiencias;

3. Supervisar la adecuada administración de riesgos, incluidos los riesgos operativos y tecnológicos, aquellos vinculados a la ciberseguridad, seguridad de la información y uso de algoritmos, de ser el caso;

4. Informar oportunamente al Directorio, a la Junta General de Accionistas o, en su defecto, al órgano de gobierno que haga sus veces, sobre la evolución de los niveles de exposición a riesgos y la probabilidad de afectación ante cambios en el entorno económico, tecnológico o regulatorio;

5. Mantener registros documentales que respalden el cumplimiento de sus funciones, asegurando que los informes presentados al órgano de gobierno cuenten con la aprobación y legalización correspondiente y estén disponibles para la supervisión de la Superintendencia de Bancos;

6. Revisar los incidentes operativos y tecnológicos reportados por la Unidad o Responsable de Riesgos, verificando la implementación de medidas correctivas;

7. Poner en conocimiento del órgano de gobierno de la entidad y de la Superintendencia de Bancos los incidentes, indicando las causas, impactos y acciones de mitigación adoptadas;

8. Supervisar a los proveedores externos, verificando el cumplimiento de cláusulas de seguridad, continuidad y auditoría, así como el monitoreo periódico de su desempeño;

9. Revisar los resultados del monitoreo a los algoritmos y/o modelos automatizados utilizados por la entidad, asegurando su trazabilidad, explicabilidad y actualización, y verificar la existencia a través del responsable del algoritmo de ser el caso;

10. Aprobar los planes de acción para la mitigación de riesgos, verificando su adecuada implementación y seguimiento hasta su cierre;

11. Promover la cultura de gestión de riesgos en toda la organización, a través de programas de capacitación y sensibilización del personal;

12. Validar los planes de comunicación y atención al usuario en caso de incidentes, asegurando protocolos claros de transparencia y mecanismos efectivos de respuesta a consultas, quejas y reclamos;

13. Supervisar el diseño, implementación y actualización de sistemas de indicadores de alerta temprana, que permitan identificar, medir y reportar oportunamente riesgos emergentes, incidentes potenciales y desviaciones significativas respecto de los parámetros normales de operación; y,

14. Cumplir con las demás funciones que determine el órgano de gobierno de la entidad o que establezca la Superintendencia de Bancos.

La Superintendencia de Bancos, en función del tamaño, volumen de operaciones, naturaleza jurídica y tipo de la entidad de servicios financieros tecnológicos, con base en los correspondientes informes técnicos y/o jurídicos podrá establecer requisitos diferenciados para las competencias del Comité de Administración Integral de Riesgos, a fin de asegurar la proporcionalidad en su aplicación.

ARTÍCULO 9.- Unidad de Riesgos. Las entidades de servicios financieros tecnológicos deberán contar con una Unidad de Riesgos responsable de la implementación y ejecución del sistema de gestión de riesgos, con independencia funcional de las áreas de negocio.

En aplicación del principio de proporcionalidad, cuando la dimensión, volumen de operaciones, naturaleza y tipo de entidad de servicios financieros no justifique la creación de una Unidad de Riesgos independiente, la Superintendencia de Bancos, con base en los correspondientes informes técnicos y/o jurídicos, podrá en su lugar disponer la designación de un responsable de Riesgos con competencias técnicas verificables, quien reportará directamente al representante legal.

El responsable de Riesgos deberá contar con conocimientos, experiencia y un perfil profesional adecuado en materia de administración de riesgos financieros, operativos y tecnológicos, acreditando formación académica o experiencia equivalente que garantice el cumplimiento de sus funciones.

ARTÍCULO 10.- Funciones de la unidad o responsable de riesgos. Las funciones principales que debe cumplir la unidad o responsable de riesgos, son las siguientes:

1. Elaborar y proponer al Comité de Administración Integral de Riesgos los manuales, políticas, procedimientos y metodologías de gestión de riesgos, así como los planes de continuidad del negocio, para su revisión y aprobación;

2. Implementar y monitorear la efectividad de los controles internos y externos, elaborando reportes periódicos al Comité con recomendaciones de acciones correctivas cuando se identifiquen deficiencias;

3. Gestionar y mantener actualizada la matriz de riesgos, identificando y evaluando los riesgos operativos y tecnológicos, incluidos aquellos vinculados a la ciberseguridad, seguridad de la información y uso de algoritmos de ser el caso, y reportando al Comité los hallazgos;

4. Preparar informes técnicos para el Comité y el órgano de gobierno sobre la evolución de los niveles de exposición a riesgos y los posibles impactos derivados de cambios en el entorno económico, tecnológico o regulatorio;

5. Mantener registros actualizados y sistematizados sobre los procesos de gestión de riesgos, asegurando que estén disponibles para el Comité y para la Superintendencia de Bancos en procesos de supervisión;

6. Registrar y analizar los incidentes operativos y tecnológicos, proponiendo planes de acción de mitigación y remitiendo al Comité los resultados de la implementación de medidas correctivas;

7. Elaborar reportes sobre incidentes que incluyan causas, impactos y acciones adoptadas, y ponerlos a conocimiento oportuno del Comité, del órgano de gobierno de la entidad y de la Superintendencia de Bancos;

8. Evaluar periódicamente a los proveedores externos respecto del cumplimiento de cláusulas contractuales de seguridad, continuidad y auditoría, informando al Comité sobre los resultados obtenidos;

9. Verificar la trazabilidad, explicabilidad y actualización de algoritmos y/o modelos automatizados, generando informes técnicos que permitan al Comité adoptar decisiones sobre ajustes o validaciones necesarias;

10. Elaborar y ejecutar planes de acción para la mitigación de riesgos, de acuerdo con las decisiones adoptadas por el Comité, y reportar su avance hasta el cierre definitivo;

11. Desarrollar e implementar programas de capacitación y sensibilización interna, que fortalezcan la cultura de riesgos, y presentar al Comité informes sobre su cumplimiento y efectividad;

12. Diseñar protocolos de comunicación y atención al usuario en caso de incidentes, remitiéndolos al Comité para su validación y asegurando su ejecución cuando corresponda;

13. Desarrollar, mantener y reportar sistemas de indicadores de alerta temprana, informando periódicamente al Comité sobre riesgos emergentes, incidentes potenciales y desviaciones respecto de los parámetros normales de operación; y,

14. Ejecutar las demás funciones que disponga el Comité de Administración Integral de Riesgos o la Superintendencia de Bancos, en el marco de la normativa vigente.

La Superintendencia de Bancos, en función del tamaño, volumen de operaciones, naturaleza jurídica y tipo de entidad de servicios financieros tecnológicos, podrá establecer funciones diferenciadas para la unidad o responsable de riesgos, a fin de asegurar la proporcionalidad en su aplicación.

SECCIÓN III.- ADMINISTRACIÓN DEL RIESGO OPERATIVO

ARTÍCULO 11.- Identificación de riesgos operativos. Las entidades de servicios financieros tecnológicos deberán identificar los riesgos operativos considerando sus líneas de negocio, los tipos de eventos, los factores de riesgo operativo y las fallas o insuficiencias detectadas en sus procesos. Para el efecto, deberán contar con una metodología debidamente documentada y aprobada por el Comité de Administración Integral de Riesgos, que incorpore el uso de herramientas acordes a la naturaleza, complejidad y tamaño de la entidad, tales como autoevaluaciones, mapas de riesgos, indicadores clave de riesgo (KRI), tablas de control (scorecards), bases de datos de incidentes u otras técnicas equivalentes.

Los tipos de eventos de riesgo operativo que, como mínimo, deberán considerarse son los siguientes:

1. Fraude interno;
2. Fraude externo;
3. Prácticas laborales y seguridad del ambiente de trabajo;
4. Prácticas relacionadas con los clientes, productos y el negocio;
5. Daños a los activos físicos;
6. Interrupción del negocio por fallas en la tecnología de la información; y,
7. Deficiencias en el diseño y/o la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.

Para mayor detalle, las entidades de servicios financieros tecnológicos deberán observar lo dispuesto en el anexo 1 eventos de riesgo operativo de acuerdo con Basilea, que forma parte integrante de esta norma.

ARTÍCULO 12.- Medición y cuantificación del riesgo operativo. Una vez identificados los riesgos operativos y las fallas o insuficiencias en relación con los eventos de riesgo, las entidades de servicios financieros tecnológicos deberán medirlos determinando su probabilidad de ocurrencia y su impacto potencial, de manera que el Comité de Administración Integral de Riesgos y el órgano de gobierno de la entidad cuenten con una visión clara de la exposición, con el fin de apoyar la toma de decisiones y acciones oportunas.

Con base en los resultados de la medición, el órgano de gobierno estará en capacidad de decidir si mitiga, transfiere, asume o evita los riesgos identificados, aplicando las medidas que resulten más adecuadas para reducir sus efectos en la operación y en la protección de los usuarios.

Las entidades de servicios financieros tecnológicos deberán implementar mecanismos de cuantificación periódica sobre los eventos de pérdida producidos por riesgos operativos, que permitan evaluar su materialidad y actualizar la declaración institucional de apetito y tolerancia al riesgo operativo, en concordancia con lo aprobado por el Comité de Administración Integral de Riesgos.

La medición y cuantificación del riesgo operativo se realizará en función del tamaño, naturaleza, complejidad y volumen de operaciones de cada entidad, conforme a los lineamientos que para el efecto establezca la Superintendencia de Bancos.

ARTÍCULO 13.- Control y mitigación del riesgo operativo. La administración del riesgo operativo en las entidades de servicios financieros tecnológicos deberá sustentarse en la existencia de planes de mitigación formalmente establecidos, aprobados por el Comité de Administración Integral de Riesgos y revisados de manera periódica. Dichos planes deberán contemplar, al menos:

1. Revisión y actualización de las estrategias, políticas, procesos y procedimientos de gestión de riesgos;
2. Implementación o modificación de límites de exposición al riesgo operativo;
3. Adopción, implementación y actualización de controles internos y tecnológicos;
4. Formulación, prueba y actualización del plan de continuidad del negocio;
5. Revisión periódica de los términos y coberturas de pólizas de seguros contratadas, de existir;
6. Evaluación y gestión de riesgos derivados de servicios provistos por terceros;
7. Evaluación de coberturas de seguros relacionadas con riesgo operativo y tecnológico (incluidos ciber riesgos y fraude), definiendo, de ser pertinente, límites mínimos acordes al tamaño y materialidad de los riesgos de la entidad; y,
8. Otros mecanismos de control y mitigación que resulten pertinentes en función del tamaño, naturaleza y complejidad de las operaciones de la entidad.

Los controles deberán integrarse a las actividades regulares de la entidad, de forma que permitan generar respuestas oportunas y efectivas frente a los eventos de riesgo operativo y las fallas o insuficiencias que los ocasionen.

Las entidades de servicios financieros tecnológicos deberán implementar mecanismos efectivos adicionales de mitigación para los riesgos vinculados a los factores de riesgo operativo, sin perjuicio de los establecidos en la presente norma.

ARTÍCULO 14.- Monitoreo y reporte de riesgo operativo. Las entidades de servicios financieros tecnológicos deberán realizar un monitoreo permanente de los riesgos asociados a sus procesos, su nivel de exposición y la efectividad de los controles implementados. Para ello, deberán contar con un esquema organizado de reportes e informes que proporcione información suficiente, pertinente y oportuna para la toma de decisiones del Comité de Administración Integral de Riesgos, del órgano de gobierno y de la Superintendencia de Bancos, cuyo alcance y nivel de detalle se ajustará al tamaño, naturaleza, complejidad y volumen de operaciones de la entidad.

Los reportes e informes deberán incluir, como mínimo:

1. Indicadores clave de riesgo operativo (KRI) que permitan evaluar la eficiencia y eficacia de las políticas, procesos, procedimientos y metodologías aplicadas;
2. Grado de cumplimiento de los planes de mitigación, con detalle de avances, desviaciones y acciones correctivas; y,

3. Matriz y mapas de riesgos operativos, que incorporen al menos: línea de negocio, proceso, tipo de riesgo, evento de riesgo operativo, factor de riesgo, fallas o insuficiencias, impacto y probabilidad inicial, controles existentes, planes de mitigación, impacto y probabilidad final, y riesgo residual.

Las entidades de servicios financieros tecnológicos deberán presentar al Comité de Administración Integral de Riesgos informes periódicos con una periodicidad mínima trimestral, que incluyan:

1. Los niveles de exposición al riesgo operativo y su evolución;
2. Los resultados de los indicadores clave de riesgo;
3. La eficacia de las políticas, procesos, procedimientos y metodologías aplicadas;
4. El grado de cumplimiento de los planes de mitigación; y,
5. Conclusiones y recomendaciones para fortalecer la administración del riesgo operativo.

La forma, alcance y nivel de detalle de los informes se ajustará al tamaño, naturaleza, complejidad y volumen de operaciones de cada entidad que serán establecidos en base a los lineamientos dictados por este organismo de control.

ARTÍCULO 15.- Registro y base de datos de incidentes de riesgo operativo. Las entidades de servicios financieros tecnológicos deberán conformar y mantener una base de datos centralizada que permita registrar, ordenar, clasificar y disponer de información sobre los riesgos y eventos de riesgo operativo, incluidos los de orden legal, de seguridad de la información, ciberseguridad, servicios provistos por terceros, uso de algoritmos y/o modelos automatizados y continuidad del negocio.

La base de datos deberá contener, como mínimo:

1. Descripción del evento de riesgo operativo;
2. Línea de negocio, proceso o servicio afectado;
3. Factor de riesgo operativo que lo originó;
4. Efecto cuantitativo de la pérdida producida o estimada;
5. Frecuencia y probabilidad de ocurrencia; y,
6. Acciones de mitigación adoptadas.

La administración y actualización de la base de datos será responsabilidad de la Unidad o Responsable de Riesgos.

Las entidades considerando su tamaño, volumen o complejidad podrán implementar mecanismos simplificados de registro, siempre que aseguren la trazabilidad de la información, la identificación de eventos y la comunicación oportuna al Comité de Administración Integral de Riesgos, al órgano de gobierno y a la Superintendencia de Bancos**.**

ARTÍCULO 16.- Auditoria del sistema de gestión del riesgo operativo. La función de auditoría interna será responsable de evaluar objetiva e independientemente el cumplimiento de los lineamientos establecidos en esta norma, verificando que las actividades de la primera y segunda línea de defensa se ejecuten de acuerdo con las políticas aprobadas y los estándares de gestión de riesgos.

En el marco de esta evaluación, la auditoría interna deberá, como mínimo:

1. Verificar la efectividad de los controles implementados para mitigar los riesgos operativos en cada uno de sus factores;

2. Revisar periódicamente el funcionamiento del sistema de gestión de continuidad del negocio; y,

3. Revisar la efectividad de las medidas de seguridad de la información y ciberseguridad aplicadas en los servicios y canales electrónicos.

SUBSECCIÓN I.- FACTORES DEL RIESGO OPERATIVO

ARTÍCULO 17.- Administración del riesgo operativo por factores. Con el propósito de minimizar la probabilidad de incurrir en pérdidas atribuibles al riesgo operativo, las entidades de servicios financieros tecnológicos deberán administrar este riesgo considerando, al menos, los siguientes factores:

1. Procesos;
2. Personas;
3. Tecnología de la información; y,
4. Eventos externos.

El alcance y nivel de detalle en la administración de cada factor se ajustará al tamaño, naturaleza, complejidad y volumen de operaciones de la entidad**.**

ARTÍCULO 18.- Factor procesos. Las entidades de servicios financieros tecnológicos deberán gestionar sus procesos bajo un enfoque eficiente y eficaz de gestión por procesos, tomando como referencia estándares internacionales como ISO 9001 e ISO 31000, de conformidad con su estrategia institucional y las políticas aprobadas por el Comité de Administración Integral de Riesgos.

Para el efecto, deberán observar, al menos, lo siguiente:

1. Definición del mapa de procesos, agrupados en:

a) **Procesos estratégicos o gobernantes**: proporcionan directrices y políticas institucionales (planificación estratégica, estructura organizacional, administración integral de riesgos, continuidad del negocio, seguridad de la información, entre otros).

b) **Procesos productivos u operativos:** permiten ejecutar efectivamente los productos o servicios ofrecidos a los usuarios.

c) **Procesos habilitantes o de apoyo:** respaldan la ejecución de los procesos estratégicos y productivos.

2. Asignación de procesos a líneas de negocio, garantizando que cada proceso productivo corresponda a una línea de negocio definida. En caso de que un proceso intervenga en más de una línea, deberá aplicarse una metodología formal que asegure consistencia y trazabilidad.

3. Metodología formal para el diseño, control, actualización, seguimiento y medición de los procesos, que deberá contemplar al menos:

a) Descripción y diagramación en secuencia lógica y ordenada de las actividades, tareas y controles;
b) Determinación de responsables del proceso y de la implementación de controles y planes de acción;
c) Identificación de clientes internos y externos;
d) Productos y servicios generados;
e) Difusión y comunicación de los procesos, garantizando su correcta aplicación; y,
f) Actualización y mejora continua mediante revisiones periódicas: al menos una vez al año para procesos críticos o productivos, y al menos una vez cada dos años para los demás.

4. Inventarios actualizados de procesos, que incluyan como mínimo: categoría (estratégico, productivo, de apoyo), línea de negocio, nombre del proceso, criticidad, procedimientos asociados, responsables, productos o servicios entregados, fecha de aprobación y última actualización.

5. Separación de funciones, evitando concentraciones de carácter incompatible que permitan la ocurrencia u ocultamiento de fraudes, errores u otros eventos de riesgo operativo.

6. Definición de indicadores clave de desempeño y de riesgo (KPI/KRI) para los procesos, que permitan medir su eficacia, eficiencia y niveles de exposición al riesgo operativo.

ARTÍCULO 19.- Factor personas. Las entidades de servicios financieros tecnológicos deberán administrar el capital humano de manera que les permita gestionar adecuadamente los riesgos asociados a este factor, garantizando la idoneidad, continuidad y seguridad en la prestación de los servicios.

Para el efecto, deberán observar, como mínimo, lo siguiente:

1. **Políticas y procedimientos de gestión de personal.** Definir formalmente políticas, procesos y procedimientos para la incorporación, permanencia y desvinculación del personal, en cumplimiento de la normativa laboral aplicable y en concordancia con la estrategia de la entidad. Dichas políticas deberán asegurar la adecuada planificación y administración del capital humano.

a) **Incorporación.** Incluir procesos de reclutamiento, selección, contratación e inducción que garanticen la idoneidad del personal en función de las competencias requeridas, tanto técnicas como éticas.

b) **Permanencia.** Establecer programas de capacitación continua, sistemas de evaluación del desempeño y mecanismos de identificación de puestos críticos y personal clave, asegurando planes de reemplazo en caso de ausencias temporales o definitivas.

c) **Desvinculación.** Implementar procedimientos formales para la terminación de la relación laboral, que incluyan aspectos jurídicos y la adecuada transferencia de responsabilidades, protegiendo la continuidad del negocio.

2. **Confidencialidad y seguridad de la información.** Mantener actualizados los acuerdos de confidencialidad relacionados con las funciones que desempeñe el personal y los riesgos asociados, incluyendo la obligación de resguardar información sensible aún después del cambio de funciones o de la desvinculación.

3. **Archivo digital centralizado.** Contar con un registro digital actualizado del capital humano, que incluya, al menos, información sobre formación académica, experiencia, procesos de selección, historial de capacitación, evaluaciones de desempeño y desvinculación.

El alcance y nivel de detalle de estas obligaciones se ajustará al tamaño, naturaleza, complejidad y volumen de operaciones de la entidad.

ARTÍCULO 20.- Factor tecnología de la información. Las entidades de servicios financieros tecnológicos deberán administrar los riesgos asociados a la tecnología de la información, de manera que se garantice la captura, procesamiento, almacenamiento y transmisión de la información de forma oportuna, confiable y segura; la continuidad de las operaciones; y la disponibilidad de la información para la toma de decisiones, incluso cuando los servicios sean provistos por terceros.

Para el efecto, deberán observar, como mínimo, lo siguiente:

1. **Gobernanza de la tecnología.** Contar con políticas, procesos y procedimientos de gestión tecnológica aprobados por el Comité de Administración Integral de Riesgos, alineados a los objetivos institucionales. Las entidades según su estructura, volumen o complejidad podrán establecer un comité de tecnología o designar un responsable de tecnología y seguridad de la información; que lidere la gestión estratégica de los sistemas tecnológicos y de la seguridad de la información.

   El comité, de existir, de tecnología estará integrado como mínimo por: un miembro de la Junta General de Accionistas, Directorio u órgano de gobierno que haga sus veces, quien lo presidirá, el representante legal de la entidad, el jefe de la unidad de riesgos o el responsable de riesgos, el responsable del área de tecnología y seguridad de la información. El presidente del Comité tendrá voto dirimente.

   En los casos en que la entidad no cuente con Junta General de Accionistas ni con Directorio, el Comité será presidido por un representante de los socios o accionistas según corresponda.

   El Comité se reunirá ordinariamente al menos una vez al mes y, de manera extraordinaria, cuando así lo requiera la naturaleza de los riesgos identificados. El quórum se conformará con la mayoría simple de sus miembros, y las decisiones se adoptarán por mayoría de votos.

   Cuando la entidad no cuente con un Comité de Tecnología independiente, el responsable de tecnología y seguridad de la información deberá integrarse al Comité de Administración Integral de Riesgos, con voz y voto, a fin de garantizar el tratamiento formal de los temas relacionados con tecnología, seguridad de la información y ciberseguridad.

   La Superintendencia de Bancos, en función del tamaño, volumen de operaciones y naturaleza jurídica de la entidad, podrá establecer requisitos diferenciados para la conformación y periodicidad de sesiones.

2. Planificación y gestión tecnológica: Disponer de un plan estratégico y un plan operativo anual de tecnología de la información, alineados con la estrategia institucional, que incluya actividades, responsables, cronogramas y presupuesto, para asegurar el cumplimiento de los objetivos tecnológicos.

3. Seguridad de la información y ciberseguridad: Implementar políticas y controles alineados con estándares internacionales que aseguren la confidencialidad, integridad y disponibilidad de la información, incluyendo:

a) Mecanismos de prevención, detección y respuesta ante incidentes cibernéticos;
b) Procedimientos de gestión de accesos y privilegios;
c) Protocolos de respaldo, recuperación y continuidad de servicios críticos; y,
d) Notificación a la Superintendencia de Bancos de incidentes que afecten la seguridad o continuidad de los servicios.

4. Gestión de incidentes tecnológicos: Contar con procedimientos documentados para la identificación, análisis de causa raíz, mitigación y seguimiento de incidentes y problemas tecnológicos, con registros disponibles para revisión del Comité de Administración Integral de Riesgos y la Superintendencia de Bancos.

5. Proveedores y servicios tecnológicos externos: Cuando se contraten servicios tecnológicos críticos, las entidades de servicios financieros tecnológicos deberán establecer mecanismos de supervisión, asegurando que los contratos incluyan cláusulas de seguridad, continuidad, confidencialidad y derecho de auditoría, en concordancia con la presente norma.

6. Control de cambios y desarrollo de software: Adoptar metodologías que aseguren que los cambios a aplicaciones e infraestructura estén debidamente autorizados, probados, documentados y registrados, considerando medidas de seguridad de la información y pruebas de calidad antes de su paso a producción.

7. Infraestructura tecnológica crítica: Asegurar que la infraestructura que soporta las operaciones críticas cuente con los mecanismos de redundancia, monitoreo y seguridad necesarios para evitar interrupciones del negocio, conforme al tamaño y complejidad de la entidad.

8. Monitoreo en tiempo real: Utilizar soluciones de monitoreo continuo y herramientas de tecnología regulatoria (RegTech) para detectar vulnerabilidades, anomalías y posibles brechas de seguridad y para automatizar la verificación del cumplimiento normativo (gestión de requisitos, control documental y alertas regulatorias), garantizando respuestas oportunas y manteniendo evidencia trazable.

ARTÍCULO 21.- Factor eventos externos. En la administración del riesgo operativo, las entidades de servicios financieros tecnológicos deberán considerar la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos a su control, tales como fallas en los servicios públicos, desastres naturales, ataques cibernéticos, interrupciones en proveedores críticos de servicios tecnológicos, eventos de conmoción social, atentados u otros actos delictivos que pudieran alterar el desarrollo normal de sus actividades, cuyo análisis y nivel de detalle se ajustará al tamaño, naturaleza, complejidad y volumen de operaciones de la entidad**.**

La gestión de los riesgos relacionados con eventos externos deberá formar parte integral de la administración de la continuidad del negocio, manteniendo procedimientos actualizados y probados que permitan garantizar la capacidad de la entidad para operar de manera continua y minimizar las pérdidas en caso de una interrupción, de acuerdo con metodologías que podrán ser simplificadas en el caso de entidades de servicios financieros tecnológicos de menor tamaño o complejidad, siempre que aseguren la identificación, tratamiento y reporte oportuno de dichos riesgos**.**

SUBSECCIÓN II.- GESTIÓN DE INCIDENTES Y PROBLEMAS

ARTÍCULO 22.- Gestión de incidentes y problemas. Las entidades de servicios financieros tecnológicos 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 definida por la entidad, de manera que contribuya a la resiliencia operativa de la entidad. Para ello deben implementar como mínimo lo siguiente, pero sin limitarse a:

1. Procedimientos que garanticen que los productos y servicios críticos sean recuperados de manera prioritaria en casos de indisponibilidad, degradación e intermitencia, en un tiempo no mayor a tres (03) horas dentro de las siguientes veinte y cuatro (24) horas consecutivas.

2. Asignar un responsable de la gestión de incidentes, encargado de su registro, trazabilidad y cierre, manteniendo evidencia documentada de las acciones adoptadas. En el caso de entidades que por el tamaño, complejidad o volumen de operaciones no cuenten con responsable de la gestión de incidentes, esta función podrá ser asumida por el responsable de Riesgos.

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. Incorporar en la gestión de problemas el análisis de causa raíz, planes de acción efectivos y la correlación de incidentes recurrentes, asegurando independencia del personal que administra las plataformas afectadas.

5. Mantener una base de conocimiento actualizada sobre incidentes y problemas, que incluya recursos internos y externos, y permita retroalimentar la mejora continua de los controles.

6. Realizar pruebas controladas de los planes de gestión de incidentes y problemas, a fin de evaluar su efectividad y garantizar la resiliencia operativa de la entidad.

7. Activar los planes de contingencia y continuidad del negocio cuando los incidentes tengan un impacto material en los servicios críticos.

8. Las entidades de servicios financieros tecnológicos deben comunicar a la Superintendencia de Bancos los incidentes que afecten a sus servicios críticos y remitir un informe formal del incidente máximo en cinco (5) días plazo siguientes al incidente, y en veinte (20) días plazo el informe de causa raíz del problema.

9. Remitir, mediante oficio hasta máximo el 31 de enero de cada año en curso, el “Plan anual de mantenimientos programados / Pruebas Centro de Datos Alterno”. El “Plan anual de mantenimientos programados” debe incluir al menos la siguiente información:

- **a)** Fecha y hora del inicio del mantenimiento / Pruebas Centro de Datos Alterno (dd/mm/aaaa hh:mm:ss);
- **b)** Objetivo del mantenimiento / Prueba DCA c) Canales de atención al usuario afectados
- **c)** Infraestructura tecnológica que interviene;

d) Detalle de las actividades a desarrollarse que incluya la línea de tiempo; y,
e) Fecha final y hora del mantenimiento / Prueba DCA (dd/mm/aaaa hh:mm:ss)

10. En caso de existir modificaciones al "Plan anual de mantenimientos programados/ Pruebas centro de datos alterno" se deberá notificar a la Superintendencia de Bancos y al canal de reporte con al menos, 5 días de antelación, conforme señala el artículo 201 del Código Orgánico Monetario y Financiero.

11. En caso de presentar incidentes en la ejecución de los mantenimientos programados o pruebas en el DCA, se debe aplicar lo dispuesto para el caso de incidentes.

12. Con relación a los incidentes, notificar al canal de reporte, correspondiente a la Dirección de Evaluación de Riesgos, lo siguiente:

a) Los incidentes o eventos que ocasionen indisponibilidad o intermitencia mayor a treinta (30) minutos en los canales de atención al usuario a través de los cuales se ofrece productos y servicios.

b) Los incidentes o eventos que ocasionen indisponibilidad o intermitencia mayor a treinta (30) minutos en los canales de atención al usuario a través de los cuales se ofrece productos y servicios que fueren ocasionados por un tercero.

c) Las notificaciones deberán ser remitidas en el lapso máximo de cinco (5) minutos posteriores al tiempo límite de indisponibilidad o intermitencia de treinta (30) minutos.

d) La notificación deberá contener la siguiente información:

- Fecha y hora del inicio del incidente (dd/mm/aaaa hh:mm:ss)
- Nivel de criticidad
- Canales de atención al usuario afectados
- Descripción de la indisponibilidad o afectación
- Componentes tecnológicos afectados
- Acciones adoptadas por la entidad para recuperación del servicio, planes de contingencia implementados

e) Reportes, cada treinta (30) minutos, de los avances del incidente hasta que se restablezcan totalmente todos los canales de atención al usuario a través de los cuales se ofrece productos y servicios, especificando la fecha y hora de fin del incidente.

f) Durante o luego de ocurrido un incidente la entidad no deberá establecer como ventanas de mantenimiento programadas los tiempos de interrupción de los canales de atención al usuario a través de los cuales se ofrece productos y servicios.

13. Remitir mediante oficio el informe del incidente en los cinco (5) días plazo una vez superado el incidente. Este deberá contener el ciclo de vida del incidente con al menos lo siguiente: Registro del incidente, priorización en función de la gravedad, análisis, escalamiento, solución, monitoreo, lecciones aprendidas, reporte a las partes interesadas tanto internas como externas y planes de contingencia implementados; y, en el plazo de veinte (20) días el informe de causa raíz del problema una vez cerrado el incidente.

14. Remitir al ente de control un informe trimestral hasta el quince (15) del mes posterior con el detalle de todos los incidentes o eventos que generaron indisponibilidad o intermitencias, menores o iguales a treinta (30) minutos, en los canales de atención al usuario que considere los aspectos del numeral 12 literal d) y numeral 13.

15. En cualquiera de los casos en los que se presenten indisponibilidades en los canales de atención al usuario las entidades controladas deben comunicar de manera oportuna a los usuarios.

16. Remitir al ente de control el nombre, cargo, correo electrónico y teléfono de contacto de la persona responsable en la entidad de la gestión de incidentes que pueda proporcionar la información técnica del avance de la resolución de estos, en el plazo de cinco (5) días a partir de su calificación, se deberá actualizar esta información en caso de que haya cambios del delegado en la entidad.

Las entidades de servicios financieros tecnológicos deberán notificar los incidentes conforme lo previsto en esta norma al canal de reporte sb_monitoreo@superbancos.gob.ec, asegurando que la información sea suficiente, oportuna y confiable para la toma de decisiones y la supervisión de la Superintendencia de Bancos.

SUBSECCIÓN III.- GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

ARTÍCULO 23.- Sistema de gestión de continuidad del negocio. Las entidades de servicios financieros tecnológicos deberán establecer, implementar, mantener y mejorar un sistema de gestión de la continuidad del negocio, con el fin de garantizar su capacidad de operar de forma continua y limitar las pérdidas en caso de una interrupción grave. Este sistema deberá alinearse a estándares internacionales reconocidos, como la norma ISO 22301 o la que la sustituya, y considerar tanto eventos internos como externos que pudieran afectar la prestación de servicios críticos.

El sistema de continuidad del negocio deberá contemplar, como mínimo:

1. **Gobernanza y responsabilidad.** La entidad deberá designar un responsable de continuidad del negocio, acorde a su tamaño y complejidad, que dirija el establecimiento, implementación y mantenimiento del sistema. Con base en el tamaño, complejidad y volumen de operaciones, la Superintendencia de Bancos podrá requerir la conformación de un comité especializado en continuidad del negocio, encargado de evaluar y supervisar el sistema y proponer su aprobación al órgano de gobierno;

2. **Marco de referencia.** El sistema deberá incluir políticas, estrategias, objetivos, metodologías y planes de continuidad revisados periódicamente y aprobados por el órgano de gobierno, en concordancia con el sistema de gestión de riesgos;

3. **Análisis de impacto al negocio (BIA).** Identificación de procesos críticos, dependencias internas y externas, recursos de soporte y tiempos y puntos de recuperación objetivo (RTO/RPO), revisados al menos una vez al año o cuando existan cambios significativos en la organización o su entorno;

4. **Estrategias de continuidad.** Definición y selección de alternativas que permitan mantener la operatividad de los procesos críticos dentro de los tiempos objetivo de recuperación, considerando seguridad del personal, infraestructura alterna, proveedores y aplicativos relacionados; y,

5. **Pruebas y mejora continua.** Realización periódica de pruebas del plan de continuidad y planes de contingencia, incluyendo la participación de proveedores críticos y validación de sitios alternos, cuyos resultados deberán documentarse e incorporarse al proceso de mejora continua con responsables y plazos.

El alcance y nivel de detalle del sistema de gestión de continuidad del negocio se ajustará al tamaño, naturaleza, complejidad y volumen de operaciones de cada entidad.

ARTÍCULO 24.- Plan de continuidad del negocio. Las entidades de servicios financieros tecnológicos deberán contar con un plan de continuidad del negocio que operacionalice el sistema de gestión de continuidad del negocio y que, como mínimo, considere:

1. Escenarios de riesgo y procesos críticos cubiertos por el plan;

2. Tiempos y puntos de recuperación objetivo (RTO/RPO) de cada proceso crítico;

3. Estrategias de continuidad para cada proceso crítico, detallando personal responsable, infraestructura y ubicaciones alternas, proveedores y aplicativos necesarios;

4. Procedimientos operativos para la reanudación urgente de procesos críticos, incluidos protocolos de traslado a sitios alternos que no estén expuestos a los mismos riesgos que la sede principal;

5. Protocolos de comunicación interna y externa, incluyendo comunicación con empleados, proveedores, usuarios y autoridades competentes;

6. Procedimientos de emergencia para preservar la seguridad del personal;

7. Plan de recuperación tecnológica y de desastres, que contemple restauración en ubicaciones remotas seguras;

8. Roles y responsabilidades de los encargados de la ejecución del plan;

9. Criterios claros de activación e invocación del plan; y,

10. En caso de entidades de servicios financieros tecnológicos dependientes de matrices en el exterior, el plan local deberá estar alineado y coordinado con el plan de continuidad de la casa matriz, garantizando la resiliencia de las operaciones en Ecuador.

El plan deberá ser revisado, probado y actualizado al menos con periodicidad anual, y mantenerse a disposición de la Superintendencia de Bancos.

SUBSECCIÓN IV.- RIESGO LEGAL

ARTÍCULO 25.- Riesgo legal. Las entidades de servicios financieros tecnológicos deberán identificar, medir, controlar, mitigar y monitorear los riesgos legales que pudieran afectar sus operaciones y derivar en pérdidas financieras, reputacionales o sanciones regulatorias. Estos riesgos pueden originarse, entre otros, en actos societarios, estipulaciones contractuales, incumplimiento normativo, relaciones con proveedores, uso de tecnologías y/o algoritmos, así como en operaciones vinculadas al giro del negocio.

En función de su tamaño, naturaleza y complejidad de operaciones, las entidades de servicios financieros tecnológicos deberán contar con mecanismos adecuados de asesoría

jurídica, interna o externa, que permitan gestionar los riesgos legales de manera eficaz, también contemplará cumplimiento de Ley Orgánica de Protección de Datos Personales.

Como parte de su gestión, las entidades de servicios financieros tecnológicos deberán mantener matrices de riesgo legal actualizadas, que identifiquen los principales escenarios de exposición, medidas de mitigación y responsables de su control.

SUBSECCIÓN V.- SERVICIOS PROVISTOS POR TERCEROS

ARTÍCULO 26.- Administración de proveedores de servicios terceros. Las entidades de servicios financieros tecnológicos deberán implementar un proceso integral para la gestión de proveedores externos que soporten sus operaciones, en especial aquellos vinculados con procesos críticos o con servicios tecnológicos. Este proceso deberá abarcar la evaluación previa a la contratación, la suscripción de contratos, el monitoreo del servicio y su eventual renovación o terminación, con el fin de garantizar la continuidad, seguridad y calidad de los servicios prestados.

Para el efecto, las entidades de servicios financieros tecnológicos deberán observar, como mínimo, lo siguiente:

1. **Evaluación previa**. Antes de la contratación, la entidad deberá realizar una evaluación proporcional a la criticidad del servicio, que considere la experiencia del proveedor, su capacidad técnica, financiera y operativa, así como los riesgos asociados en materia de seguridad de la información, ciberseguridad, continuidad del negocio y cumplimiento normativo;

2. **Contratos**. Los contratos deberán contener cláusulas claras sobre: niveles de servicio, medidas de seguridad de la información y protección de datos personales, continuidad del negocio, derechos de auditoría por parte de la entidad y de la Superintendencia de Bancos, y mecanismos de sanción o terminación en caso de incumplimiento;

3. **Monitoreo y control**. La entidad deberá establecer procedimientos para monitorear periódicamente el cumplimiento de los niveles de servicio y demás obligaciones contractuales, utilizando mecanismos propios de validación cuando sea posible, y no únicamente la información reportada por el proveedor;

4. **Dependencia de proveedores críticos**. Cuando la entidad dependa de un único proveedor para un servicio crítico, deberá asegurarse de que este cuente con planes de contingencia y continuidad de negocio probados y actualizados, y documentar las medidas de mitigación de riesgos;

5. **Servicios en la nube y tecnológicos.** En caso de contratar servicios de infraestructura, plataforma o software en la nube, la entidad deberá elaborar informes técnicos, legales y de seguridad de la información que identifiquen y mitiguen los riesgos asociados. La Superintendencia de Bancos podrá establecer lineamientos específicos sobre estándares mínimos aplicables a estos servicios; y,

6. **Notificación al órgano de control**. Las entidades de servicios financieros tecnológicos deberán notificar a la Superintendencia de Bancos sobre la contratación de proveedores que soporten procesos críticos, proporcionando la documentación que respalde la gestión de riesgos realizada.

El alcance y nivel de detalle de estas obligaciones se ajustará al tamaño, naturaleza, complejidad y volumen de operaciones de la entidad.

SUBSECCIÓN VI. - SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

ARTÍCULO 27.- Sistema de gestión de seguridad de la información. Las entidades de servicios financieros tecnológicos deberán establecer, implementar, mantener y mejorar de forma continua un **Sistema de Gestión de Seguridad de la Información**, alineado a estándares internacionales (ISO 27001, ISO 27017, ISO 27018, NIST Cybersecurity Framework, o los que los sustituyan), que permita:

1. Proteger la confidencialidad, integridad y disponibilidad de la información;
2. Prevenir accesos, usos, revelaciones, modificaciones, daños o pérdidas no autorizadas; y,
3. Procurar la resiliencia tecnológica y operativa de sus procesos y servicios.

ARTÍCULO 28.- Funciones y responsables. Las entidades de servicios financieros tecnológicos deberán:

1. Definir formalmente las funciones y responsabilidades relacionadas con la seguridad de la información, incluyendo la gestión de ciberseguridad;

2. Designar un **responsable de seguridad de la información**, con conocimientos y experiencia suficientes en la materia, acorde al tamaño y complejidad de la entidad;

3. En entidades de servicios financieros tecnológicos de mayor complejidad, contar con una unidad especializada de seguridad de la información, la cual sea independiente de las unidades de negocio, riesgos, tecnología y auditoría, en caso de existirlas; y,

4. Diseñar e implementar programas de capacitación periódica en seguridad de la información y ciberseguridad, con alcance a todo el personal y refuerzos para funciones críticas

ARTÍCULO 29.- Requisitos del sistema de gestión de seguridad de la información. Las entidades de servicios financieros tecnológicos deberán contar con un Sistema de Gestión de Seguridad de la Información que contemple, sin limitarse, a lo siguiente:

1. **Políticas y procedimientos documentados** de seguridad de la información y ciberseguridad, revisados y actualizados al menos una vez al año o cuando existan cambios significativos;

2. **Controles de acceso físico y lógico,** que incluyan autenticación robusta, segregación de funciones y gestión de usuarios privilegiados;

3. **Inventario y clasificación de activos de información**, considerando su criticidad, valor, requisitos legales y de protección de datos personales;

4. **Gestión de incidentes de seguridad de la información y ciberseguridad**, que incluya mecanismos de detección, registro, análisis de causa raíz, respuesta, recuperación y notificación a la Superintendencia de Bancos conforme la normativa vigente;

5. **Evaluaciones periódicas de riesgos de seguridad de la información y ciberseguridad**, alineadas a la metodología de gestión de riesgos de la entidad, que permitan identificar, medir, controlar y monitorear amenazas y vulnerabilidades;

6. **Capacitación y concienciación del personal**, orientada a la prevención de riesgos de seguridad de la información, ciberseguridad y protección de datos;

7. **Controles de movilidad y acceso remoto,** implementar, según la naturaleza, complejidad y volumen de operaciones de la entidad, controles de seguridad para el uso de dispositivos móviles y el acceso remoto (incluyendo, de ser el caso, redes privadas virtuales - VPN y esquemas de confianza cero - Zero Trust), así como la gestión de parches de software y firmware, la protección de redes mediante firewalls y sistemas de detección y prevención de intrusos (IDS/IPS), la gestión de identidades y accesos (IAM), la gestión de privilegios (PAM), y mecanismos de control de identidad para prevenir la suplantación de terceros;

8. **Condiciones ambientales y emplazamiento seguro,** gestionar condiciones ambientales y localización segura de equipos críticos;

9. **Gestión de amenazas cibernéticas,** definir procedimientos para phishing, malware, ransomware e inyección de código, con campañas simuladas y métricas de mejora; y,

10. **Auditorías internas y externas** que verifiquen la efectividad del **Sistema de Gestión de Seguridad de la Información** y el cumplimiento de la normativa aplicable. Las entidades en función de su tamaño podrán realizar estas auditorías de manera proporcional a su naturaleza y complejidad.

SUBSECCIÓN VII.- SEGURIDADES EN CANALES ELECTRÓNICOS

ARTÍCULO 30.- Seguridad en canales electrónicos. Las entidades de servicios financieros tecnológicos deberán establecer políticas, procesos y controles para garantizar la seguridad en las transacciones realizadas a través de canales electrónicos, de ser el caso, asegurando la confidencialidad, integridad y disponibilidad de la información, así como la protección de los recursos de sus usuarios.

En función del tamaño, complejidad y volumen de operaciones, las entidades de servicios financieros tecnológicos deberán, como mínimo:

1. Implementar **mecanismos de autenticación fuerte** en el acceso y ejecución de transacciones electrónicas;

2. Asegurar la **transmisión y almacenamiento cifrado de datos sensibles**, conforme a estándares internacionales vigentes;

3. Contar con **sistemas de monitoreo y detección de fraudes** que permitan identificar y alertar sobre transacciones inusuales o no autorizadas, estableciendo procedimientos para su bloqueo y resolución;

4. Mantener **registros históricos suficientes** de las transacciones electrónicas, para fines de auditoría, control interno y atención de reclamos; y,

5. Desarrollar e implementar programas de información y capacitación periódica dirigidos a los usuarios sobre los riesgos asociados al uso de canales electrónicos y las medidas de seguridad disponibles.

Cuando las entidades operen canales electrónicos tradicionales (cajeros automáticos, puntos de venta, corresponsales no bancarios u otros), deberán sujetarse a las disposiciones específicas emitidas por la Superintendencia de Bancos.

DISPOSICIONES GENERALES

PRIMERA.- La Superintendencia de Bancos con base en los resultados de sus evaluaciones in situ y/o extra situ, podrá disponer a las entidades de servicios financieros tecnológicos la implementación de controles adicionales o complementarios, para lo cual se podrá considerar lo detallado en la "Norma de control para la gestión del riesgo operativo", así como en las mejores prácticas internacionales.

SEGUNDA.- La Superintendencia de Bancos podrá disponer a las entidades controladas la contratación de empresas auditoras externas debidamente calificadas para llevar a cabo procesos de evaluación especializada relacionados con el cumplimiento de lo detallado en la presente norma.

TERCERA.- Los casos de duda en la aplicación de la presente norma serán resueltos por la Superintendencia de Bancos.

ANEXO 1. EVENTOS DE RIESGO OPERATIVO DE ACUERDO CON BASILEA

Categoría de Tipo de Eventos (nivel 1)	Definición	Categoría (nivel 2)	Ejemplos de actividades (Nivel 3)
Fraude interno	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad / discriminación) en las que se encuentra implicada, al menos, una parte interna a la empresa	Actividades no autorizadas	i) Operaciones no reveladas intencionalmente; ii) Operaciones no autorizadas con pérdidas monetarias; y iii) Valoración errónea intencional de posiciones
		Hurto y fraude	i) Fraude/fraude crediticio/ depósitos sin valor Hurto/extorsión/malversación / robo; ii) Apropiación indebida de activos; iii) Destrucción dolosa de activos; iv) Falsificación; v) Utilización de cheques sin fondos; vi) Contrabando; vii) Apropiación de cuentas, de identidad, etc.; viii) Incumplimiento/evasión intencional de impuestos; ix) Soborno/cohecho; y x) Abuso de información privilegiada
Fraude externo	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte un tercero	Hurto y fraude	i) Hurto/robo; ii) Falsificación; y, iii) Utilización de cheques sin fondos
		Seguridad de los sistemas	i) Daños por ataques informáticos; y, ii) Robo de información con pérdidas monetarias
Relaciones laborales y seguridad en el puesto de trabajo	Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones por daños personales, o sobre casos relacionados con la discriminación	Relaciones laborales	i) Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos; y, ii) Organización laboral
		Higiene y seguridad en el trabajo	i) Imposibilidad en general (resbalones, caídas, etc.); ii) Casos relacionados con las normas de higiene y seguridad en el trabajo; y, iii) Indemnización a los trabajadores
		Diversidad y discriminación	Todo tipo de discriminación
Incidencias en el negocio y fallos en los sistemas	Pérdidas derivadas de interrupción en los negocios o por fallas en los sistemas	Sistemas	i) Hardware; ii) Software; iii) Telecomunicaciones; y; iv)Interrupción / incidencias en el suministro

Categoría de Tipo de Eventos (nivel 1)	Definición	Categoría (nivel 2)	Ejemplos de actividades (Nivel 3)
Daños a activos materiales	Pérdidas derivadas por daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros eventos	Desastres otros acontecimientos	i) Pérdidas por desastres naturales; ii) Pérdidas humanas por causas externas (terrorismo, vandalismo)
Clientes, productos y prácticas empresariales	Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto	Adecuación, divulgación de información y confianza	i) Abusos de confianza / incumplimiento de pautas; ii) Apropiamiento / divulgación de información; iii) Violación de la privacidad de clientes minoristas; iv) Quebrantamiento de privacidad; v) Ventas agresivas; vi) Pérdidas de cuentas; vii) Mal uso de información confidencial; y ii) Responsabilidad del prestamista
		Prácticas empresariales o de mercado impropias	i) Prácticas anticompetencia; ii) Prácticas impropias comerciales y de mercado; iii) Manipulación del mercado; iv) Comercialización de información privilegiada a favor de la empresa; v) Actividades no autorizadas; y, vi) Lavado de dinero
		Productos defectuosos	i) Defectos del producto; y, ii) Error de modelo
		Selección, patrocinio y riesgos	i) Fallida investigación a clientes según los protocolos; y, ii) Superación de los límites de exposición frente a clientes
		Actividades de asesoramiento	Litigios sobre resultados de las actividades de asesoramiento
Ejecución, entrega y gestión de procesos	Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores	Recepción, ejecución y mantenimiento de operaciones	i) Comunicación defectuosa; ii) Errores de introducción de datos, mantenimiento o descarga; iii) Incumplimiento de plazos o de responsabilidades; iv) Ejecución errónea de modelos / sistemas; v) Error contable / atribución a entidades erróneas; vi) Errores en otras tareas; vii) Fallo en la entrega; viii) Fallo en la gestión del colateral; y ix) Mantenimiento de datos de referencia

Categoría de Tipo de Eventos (nivel 1)	Definición	Categoría (nivel 2)	Ejemplos de actividades (Nivel 3)
		Seguimiento y monitoreo	i) Incumplimiento en la obligación reportar; y, ii) Inexactitud de informes externos (incurriendo en pérdidas)
		Aceptación de clientes y documentación	i) Extravío de autorizaciones / rechazos de clientes; y, ii) Documentos jurídicos inexistentes / incompletos
		Gestión de cuentas de clientes	i) Acceso no autorizado a cuentas; ii) Registros incorrectos de clientes (incurriendo en pérdidas); y, iii) Pérdida o daño de activos de clientes por negligencia
		Contrapartes comerciales	i) Fallos con contrapartes no-clientes; y ii) Otros litigios con contrapartes distintas de clientes
		Distribuidores y proveedores	i) Subcontratación; y, ii) Litigios con distribuidores