JUNTA MONETARIA
RESOLUCIÓN JM-98-2025

Inserta en el punto noveno del acta 46-2025, correspondiente a la sesión celebrada por la Junta Monetaria el 22 de octubre de 2025.

PUNTO NOVENO: Superintendencia de Bancos solicita a Junta Monetaria emitir un nuevo Reglamento para la Administración del Riesgo Tecnológico.

RESOLUCIÓN JM-98-2025. Conocido el oficio número 8810-2025, del 9 de octubre de 2025, del Superintendente de Bancos, al que se adjunta el dictamen número 17-2025, de la Superintendencia de Bancos, por medio del cual solicita a esta junta emitir un nuevo Reglamento para la Administración del Riesgo Tecnológico.

LA JUNTA MONETARIA:

CONSIDERANDO: Que el artículo 55 de la Ley de Bancos y Grupos Financieros establece que los bancos y las empresas que integran grupos financieros deberán contar con procesos integrales que incluyan, entre otros, la administración del riesgo operacional, del cual forma parte el riesgo tecnológico, que contengan sistemas de información y un comité de gestión de riesgos, todo ello con el propósito de identificar, medir, monitorear, controlar y prevenir los riesgos; **CONSIDERANDO:** Que esta junta mediante resolución JM-104-2021, del 26 de noviembre de 2021, emitió el Reglamento para la Administración del Riesgo Tecnológico, a efecto de normar los lineamientos que, como mínimo, deben observar las instituciones para la administración del riesgo tecnológico, incluyendo el establecimiento de políticas y procedimientos; las responsabilidades del Consejo de Administración, del Comité de Gestión de Riesgos y de la Unidad de Administración de Riesgos; aspectos sobre la infraestructura de tecnología de la información, sistemas de información, bases de datos y servicios de tecnología de la información; seguridad de tecnología de la información; ciberseguridad; plan de recuperación ante desastres; así como, lo relativo al procesamiento y/o almacenamiento de información; **CONSIDERANDO:** Que el desarrollo a nivel mundial de la tecnología y las telecomunicaciones han generado mayor rapidez y facilidad para el tratamiento e intercambio de datos, surgiendo nuevos tipos de servicios y modelos, interconectados con Internet o redes externas, que procesan y/o almacenan información, lo cual conlleva un incremento del riesgo tecnológico por la existencia de amenazas cibernéticas que ponen en riesgo los activos de la información; **CONSIDERANDO:** Que para la realización de sus operaciones y prestación de servicios las instituciones del sistema financiero dependen del uso de tecnologías de la información y telecomunicaciones, por lo que se hace necesario regular nuevos aspectos para que estas gestionen su riesgo tecnológico con el propósito de asegurar la integridad, disponibilidad y confidencialidad de la información, así como la continuidad de operaciones y la prestación de sus servicios; **CONSIDERANDO:** Que dada la actualización de los estándares internacionales relacionados a seguridad de la información y ciberseguridad, los cuales brindan un conjunto de mejores prácticas, directrices y procedimientos para garantizar la confidencialidad, integridad y disponibilidad de la información, así como gestionar y mitigar el riesgo tecnológico, es pertinente incorporar al marco normativo tales actualizaciones, con la finalidad de prevenir o reducir el impacto de ataques cibernéticos y proteger los activos de información; **CONSIDERANDO:** Que las instituciones han implementado el uso de sistemas de inteligencia artificial dentro de sus operaciones y servicios, tecnología que tiene la particularidad de transformar el negocio financiero, por un lado, mejorando la eficiencia operativa, y por otro, incrementando el riesgo tecnológico, razón por la cual se hace necesario emitir lineamientos específicos que dichas instituciones deben cumplir para

gestionar este riesgo y garantizar que los referidos sistemas sean utilizados de manera segura, responsable y en función de la protección de los usuarios de servicios y productos financieros, así como de la estabilidad del sistema financiero en su conjunto; **CONSIDERANDO:** Que según se indica en el dictamen número 17-2025, de la Superintendencia de Bancos, luego de la revisión del actual reglamento, del análisis de los estándares internacionales, la normativa internacional y de las mejores prácticas internacionales, se concluye que es pertinente que esta junta emita un nuevo Reglamento para la Administración del Riesgo Tecnológico, que incluya el fortalecimiento en aspectos para la ciberseguridad; análisis de criticidad para servicios tecnológicos que procesan y/o almacenan información; sistemas de inteligencia artificial; ampliación de los mecanismos de intercambio de información; pruebas al plan de recuperación ante desastres; requisitos adicionales para la contratación con terceros de servicios tecnológicos que procesan y/o almacenan información, incluyendo los subcontratistas y subcontratistas en cadena; así como, otras modificaciones que permitan una actualización integral de la norma,

POR TANTO:

Con base en lo considerado, y con fundamento en lo dispuesto en los artículos 26 incisos l y m, y 64 de la Ley Orgánica del Banco de Guatemala; 55, 56, 57 y 129 de la Ley de Bancos y Grupos Financieros; y, tomando en cuenta el oficio número 8810-2025 y el dictamen número 17-2025, ambos de la Superintendencia de Bancos,

RESUELVE:

1. Emitir, conforme Anexo a la presente resolución, el **Reglamento para la Administración del Riesgo Tecnológico**.

2. Derogar la resolución JM-104-2021.

3. Establecer que los expedientes formados y las solicitudes que se encuentren en proceso al amparo de la resolución JM-104-2021, deberán continuar su trámite y ser resueltos con lo establecido en dicha resolución.

4. Autorizar a la secretaría de esta junta para que publique la presente resolución en el diario oficial y en otro periódico, la cual entrará en vigencia el día de su publicación.

Romeo Augusto Archila Navarro
Secretario
Junta Monetaria

Publicada en el Diario de Centro América el 30 de octubre de 2025.

ANEXO A LA RESOLUCIÓN JM-98-2025
REGLAMENTO PARA LA ADMINISTRACIÓN DEL RIESGO TECNOLÓGICO

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto. Este reglamento tiene por objeto establecer los lineamientos mínimos que los bancos, las sociedades financieras y las empresas especializadas en servicios financieros que forman parte de un grupo financiero, deberán cumplir para administrar el riesgo tecnológico.

Artículo 2. Definiciones. Para los efectos de este reglamento se establecen las definiciones siguientes:

Activo de información: es un elemento físico, virtual, tangible o intangible, que tiene valor para la institución y cuya protección es crucial para preservar la seguridad de la información, incluyendo activos en el ciberespacio.

Activos en el ciberespacio: son los sistemas de información, infraestructura de TI, bases de datos, redes, datos, servicios o elementos de la institución que están interconectados a Internet o a otra red externa a la institución.

Administración del riesgo tecnológico: es el proceso que consiste en identificar, medir, monitorear, controlar, prevenir y mitigar el riesgo tecnológico.

Almacenamiento de información: utilización de servicios de cómputo para mantener, conservar y resguardar datos.

Certificado digital: es un identificador único que garantiza la identidad del emisor y del receptor de un mensaje o transacción electrónica, la confidencialidad del contenido del envío, la integridad de la transacción, y el no repudio de los compromisos adquiridos por vía electrónica.

Ciberamenaza: es una circunstancia, situación, evento o acto con el potencial de convertirse en un ciberataque.

Ciberataque: es un evento con la intención de causar daño en uno o varios activos en el ciberespacio de la institución.

Ciberseguridad: políticas, estrategias, recursos, soluciones informáticas, prácticas y competencias para preservar la confidencialidad, integridad y disponibilidad de los activos en el ciberespacio.

Criticidad de la información: se refiere a la clasificación de la información en diferentes niveles considerando la importancia que esta tiene para la operación del negocio, de acuerdo con los manuales de administración de riesgos de la institución.

Diagrama de relación: es la representación gráfica que describe la distribución de datos almacenados en las bases de datos de la institución y la relación entre estos, tales como los diagramas de entidad-relación para el caso de bases de datos del tipo relacional.

Diccionario de datos: es la documentación relativa a las especificaciones de los datos, tales como su identificación, descripción, atributos, el dominio de valores, restricciones de integridad y ubicación dentro de una base de datos.

Incidente cibernético: es un ciberataque que vulneró de forma individual o conjunta la confidencialidad, integridad y/o disponibilidad de la información.

Infraestructura de tecnología de la información o infraestructura de TI: es el hardware, software, redes, instalaciones y otros elementos que se requieren para desarrollar, probar, entregar, monitorear, controlar o dar soporte a los servicios de tecnología de la información. La infraestructura de TI excluye al recurso humano, los procesos y la documentación.

Institución o instituciones: se refiere a los bancos, las sociedades financieras y las empresas especializadas en servicios financieros que forman parte de un grupo financiero.

Procesamiento de información: utilización de servicios de cómputo para el tratamiento electrónico de datos.

Proveedor de servicios que procesan y/o almacenan información: entidad que de forma directa presta servicios que procesan y/o almacenan información.

Pruebas de penetración: someter un sistema o red a ciberataques simulados o reales que traten de detectar, identificar o explotar vulnerabilidades cibernéticas en condiciones controladas.

Resiliencia cibernética: la capacidad de la institución para adaptarse a las condiciones cambiantes y prepararse para resistir, responder y recuperarse rápidamente de un ciberataque.

Riesgo tecnológico: es la contingencia de que la interrupción, alteración, o falla de la infraestructura de TI, sistemas de información, bases de datos y procesos de TI, provoquen pérdidas a la institución.

Sensibilidad de la información: clasificación de la información según el perjuicio que ocasione a la institución su alteración, destrucción, pérdida o divulgación no autorizada.

Sistemas de información: es el conjunto organizado de datos, procesos y personas, para obtener, procesar, almacenar, transmitir, comunicar y disponer de la información en la institución para un objetivo específico.

Sistema de inteligencia artificial: sistema basado en tecnología de la información que, para la operación y/o los objetivos de la institución, infiere, a partir de los datos de entrada que recibe, cómo generar información de salida, tales como, pronósticos, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales.

Subcontratista de servicios que procesan y/o almacenan información: entidad que es contratada por el proveedor de servicios que procesan y/o almacenan información, para prestar algún servicio o parte del servicio contratado y que derivado de esto, procesa y/o almacena información de la institución.

Tecnología de la información o TI: es el uso de la tecnología para obtener, procesar, almacenar, transmitir, comunicar y disponer de la información, para dar viabilidad a los procesos del negocio.

Vendedor de servicios que procesan y/o almacenan información: entidad que realiza la comercialización de servicios que procesan y/o almacenan información prestados por un tercero de forma directa.

Vulnerabilidad cibernética: debilidad de uno o varios activos en el ciberespacio o control que puede ser explotado por una ciberamenaza.

CAPÍTULO II
ORGANIZACIÓN PARA LA ADMINISTRACIÓN DEL RIESGO TECNOLÓGICO

Artículo 3. Políticas y procedimientos. Las instituciones deberán establecer e implementar políticas y procedimientos que les permitan realizar permanentemente una adecuada administración del riesgo tecnológico de la institución, considerando la naturaleza, complejidad y volumen de sus operaciones.

Dichas políticas y procedimientos deberán comprender, como mínimo, las metodologías, herramientas o modelos de medición del riesgo tecnológico, así como los aspectos que se detallan en los capítulos del III al VII de este reglamento y agruparse en los temas siguientes:

a) Infraestructura de TI, sistemas de información, bases de datos y servicios de TI;

b) Seguridad de tecnología de la información;

c) Ciberseguridad;

d) Plan de recuperación ante desastres; y,

e) Procesamiento y/o almacenamiento de información.

En adición a los aspectos indicados, las instituciones deberán establecer políticas para elaborar, implementar y actualizar el plan estratégico de TI a que se refiere el artículo 8 de este reglamento.

Artículo 4. Responsabilidad del Consejo de Administración. El Consejo de Administración o quien haga sus veces, en lo sucesivo el Consejo, sin perjuicio de las responsabilidades que le asignan otras disposiciones legales aplicables, es el responsable de velar porque se implemente e instruir para que se mantenga en adecuado funcionamiento y ejecución la administración del riesgo tecnológico.

Para cumplir con lo indicado en el párrafo anterior el Consejo como mínimo deberá:

a) Aprobar las políticas y procedimientos a que se refiere el artículo anterior, el plan estratégico de TI, el plan de recuperación ante desastres, así como conocer y resolver sobre las propuestas de actualización y autorizar las modificaciones respectivas;

b) Conocer los reportes que le remita el Comité de Gestión de Riesgos sobre la exposición al riesgo tecnológico, los cambios sustanciales de tal exposición y su evolución en el tiempo, así como las medidas correctivas adoptadas;

c) Conocer los reportes sobre el nivel de cumplimiento de las políticas y procedimientos aprobados, así como las propuestas sobre acciones a adoptar con relación a los incumplimientos. Asimismo, en caso de incumplimiento el Consejo deberá adoptar las medidas que correspondan, sin perjuicio de las sanciones legales que el caso amerite; y,

d) Designar a un Oficial de Seguridad de la Información de la institución, quien formará parte del Comité de Gestión de Riesgos o dependerá directamente de este Consejo.

Lo indicado en este artículo deberá hacerse constar en el acta respectiva.

Artículo 5. Comité de Gestión de Riesgos. El Comité de Gestión de Riesgos, en lo sucesivo el Comité, estará integrado como mínimo por un miembro del Consejo y por las autoridades y funcionarios que dicho Consejo designe. El Comité estará a cargo de la dirección de la administración del riesgo tecnológico, entre otros riesgos, para lo cual deberá encargarse de la implementación, adecuado funcionamiento y ejecución de las políticas y procedimientos aprobados para dicho propósito y tendrá las funciones siguientes:

a) Proponer al Consejo, para su aprobación, las políticas y procedimientos para la administración del riesgo tecnológico, así como el plan estratégico de TI y el plan de recuperación ante desastres;

b) Proponer al Consejo el Manual de Administración del Riesgo Tecnológico y sus actualizaciones;

c) Analizar las propuestas sobre actualización de las políticas, procedimientos, plan estratégico de TI, plan de recuperación ante desastres y su plan de pruebas, y proponer al Consejo las actualizaciones que procedan;

d) Definir la estrategia para la implementación de las políticas y procedimientos aprobados para la administración del riesgo tecnológico y su adecuado cumplimiento;

e) Revisar, al menos anualmente, las políticas y procedimientos y proponer la actualización, cuando proceda;

f) Analizar los reportes que le remita la Unidad de Administración de Riesgos, a que se refiere el artículo 6 de este reglamento, sobre la exposición del riesgo tecnológico de la institución, los cambios sustanciales de tal exposición y su evolución en el tiempo, así como adoptar las medidas correctivas correspondientes;

g) Analizar la información que le remita la Unidad de Administración de Riesgos sobre el cumplimiento de las políticas y procedimientos aprobados, así como evaluar las causas de los incumplimientos que hubieren, y proponer al Consejo acciones a adoptar con relación a dichos incumplimientos;

h) Analizar la información que le remita el Oficial de Seguridad de la Información sobre el desempeño de los indicadores clave de seguridad de la información y ciberseguridad, así como sobre la gestión de incidentes. Asimismo, proponer recomendaciones al Consejo sobre las acciones a adoptar, en relación con dichos indicadores e incidentes, cuando corresponda;

i) Reportar al Consejo, al menos semestralmente y cuando la situación lo amerite, sobre la exposición al riesgo tecnológico de la institución, los cambios sustanciales de tal exposición, su evolución en el tiempo, las principales medidas correctivas adoptadas y el cumplimiento de las políticas y procedimientos aprobados; y,

j) Otras funciones relacionadas que le asigne el Consejo.

Las sesiones y acuerdos del Comité deberán constar en acta suscrita por quienes intervinieron en la sesión.

El Consejo deberá asegurarse que la estructura organizacional para administrar TI permita asesorar al Comité en los aspectos relacionados con el riesgo tecnológico.

Artículo 6. Unidad de Administración de Riesgos. La Unidad de Administración de Riesgos, en lo sucesivo la Unidad, apoyará al Comité en la administración del riesgo tecnológico, para lo cual tendrá las funciones siguientes:

a) Proponer al Comité políticas y procedimientos para la administración del riesgo tecnológico, así como el plan estratégico de TI, el plan de recuperación ante desastres y su plan de pruebas;

b) Revisar, al menos anualmente y cuando la situación lo amerite, las políticas, los procedimientos, el plan estratégico de TI, y para los procesos críticos, el plan de recuperación ante desastres y su plan de pruebas, y proponer su actualización al Comité, atendiendo los cambios en la estrategia o situación de la institución o cuando lo requiera la normativa;

c) Monitorear la exposición al riesgo tecnológico y mantener registros históricos sobre dicho monitoreo, así como medir el riesgo tecnológico, considerando lo establecido en este reglamento;

d) Analizar el riesgo tecnológico inherente de las innovaciones en TI que se implementen en la institución y el que se derive de los nuevos productos y servicios propuestos por las unidades de negocios;

e) Reportar al Comité, al menos trimestralmente y cuando la situación lo amerite, sobre la exposición al riesgo tecnológico de la institución, los cambios sustanciales de tal exposición y su evolución en el tiempo, así como proponer al Comité las medidas correctivas correspondientes;

f) Verificar e informar al Comité, al menos trimestralmente y cuando la situación lo amerite, sobre el nivel de cumplimiento de las políticas y procedimientos aprobados;

g) Identificar las causas del incumplimiento de las políticas y procedimientos aprobados, determinar si los mismos se presentan en forma reiterada e incluir sus resultados en el informe indicado en el inciso f) anterior y proponer las medidas correctivas, debiendo mantener registros históricos sobre tales incumplimientos; y,

h) Otras funciones relacionadas que le asigne el Comité.

El Consejo deberá asegurarse que la estructura organizacional para administrar TI permita apoyar a la Unidad en los aspectos relacionados con el riesgo tecnológico.

Artículo 7. Funciones de la auditoría interna. Sin perjuicio de las funciones establecidas en el Reglamento de Gobierno Corporativo, la auditoría interna verificará, como mínimo una vez al año, el cumplimiento de lo establecido en este reglamento, debiendo realizar principalmente auditorías para evaluar la eficacia de los procesos en la administración del riesgo tecnológico, incluyendo las medidas de seguridad de la información, ciberseguridad y la evaluación de la relación con proveedores de servicios de TI.

Artículo 8. Plan estratégico de TI. Las instituciones, como parte de su plan estratégico general, deberán tener un plan estratégico de TI alineado con la estrategia de negocios, para gestionar la infraestructura de TI, los sistemas de información, la base de datos y al recurso humano de TI.

El plan estratégico de TI debe incluir, como mínimo, los aspectos siguientes:

a) Objetivos de TI alineados con la estrategia de negocios en función del análisis e impacto de factores internos y externos en esta materia, tales como oportunidades, limitaciones y desempeño de la infraestructura de TI, los sistemas de información, la base de datos, el recurso humano relacionado y los activos en el ciberespacio de la institución;

b) Estrategias de TI, para la consecución de los objetivos;

c) Proyectos y actividades específicas; y,

d) El presupuesto financiero para su ejecución.

Las instituciones deberán poner a disposición de la Superintendencia de Bancos el plan estratégico de TI y sus modificaciones, cuando esta lo requiera.

Las nuevas instituciones que se constituyan o se autorice su funcionamiento deberán remitir una copia del plan estratégico de TI a que se refiere este artículo, a la Superintendencia de Bancos, antes del inicio de sus operaciones.

Artículo 9. Organización de TI. Las instituciones deberán contar con una estructura organizacional de TI que esté alineada con el plan estratégico, asegurándose que el recurso humano de TI tenga las capacidades necesarias mediante programas de entrenamiento y capacitación, una adecuada separación de funciones, delegación de autoridad, definición de roles y asignación de responsabilidades, todo esto soportado con un marco de trabajo estructurado en procesos, los cuales deberán estar debidamente identificados.

Artículo 10. Manual de Administración del Riesgo Tecnológico. Las políticas y procedimientos a que se refiere el artículo 3 de este reglamento deberán constar por escrito en un Manual de Administración del Riesgo Tecnológico que será aprobado por el Consejo.

El Consejo conocerá y resolverá sobre las propuestas de actualización del Manual de Administración del Riesgo Tecnológico y autorizará las modificaciones al mismo, las que deberán ser comunicadas a la Superintendencia de Bancos, dentro de los diez (10) días hábiles siguientes a su aprobación.

Las nuevas instituciones que se constituyan o se autorice su funcionamiento deberán remitir una copia del manual a que se refiere este artículo a la Superintendencia de Bancos antes del inicio de sus operaciones.

CAPÍTULO III
INFRAESTRUCTURA DE TI, SISTEMAS DE INFORMACIÓN, BASES DE DATOS Y SERVICIOS DE TI

Artículo 11. Esquema de la información del negocio. Las instituciones deberán contar con un esquema actualizado de la información del negocio que represente la interrelación entre la infraestructura de TI, los sistemas de información, los servicios de TI y los procesos de las principales líneas de negocio.

Artículo 12. Inventarios de activos de información. Las instituciones deberán mantener inventarios actualizados que incluyan, como mínimo, lo siguiente:

a) De infraestructura de TI:

1. Especificaciones técnicas de sus elementos:

i. Tipo;

ii. Nombre;

iii. Función; y,

iv. Identificar si el mantenimiento es propio o realizado por terceros, en este último caso deberá identificarse al proveedor.

2. Ubicación física de sus elementos.

b) De sistemas de información:

1. Características de los sistemas de información:

i. Nombre;

ii. Función;

iii. Lenguaje de programación;

iv. Versión;

v. Estructura del sistema y las relaciones entre sus componentes;

vi. Nombre y versión de los manejadores de bases de datos con las cuales interactúan;

vii. Nombre de las bases de datos con las cuales interactúan;

viii. Identificar si es desarrollo propio o realizado por terceros, en este último caso deberá identificarse al proveedor; y,

ix. Identificar si el mantenimiento es propio o realizado por terceros, en este último caso deberá identificarse al proveedor.

2. Documentación técnica; y,

3. Documentación para el usuario final.

c) De bases de datos:

1. Nombre;

2. Descripción general de la información que contiene;

3. Manejador de base de datos o sistema de gestión de archivos, y su versión;

4. Nombre de los servidores en los que reside;

5. Diccionario de datos;

6. Diagramas de relación; y,

7. Nombre del administrador de la base de datos.

d) De activos en el ciberespacio:

1. Nombre;

2. Categoría del activo;

3. Criticidad del activo;

4. Descripción general de la información que contiene;

5. Descripción del servicio que soporta;

6. Responsable del activo;

7. Nombre de la infraestructura en la que reside;

8. Nombre del proveedor; y,

9. Esquema de conectividad.

Artículo 13. Administrador de base de datos. Las instituciones deberán designar uno o más administradores de base de datos para gestionar los controles de accesos, la integridad, disponibilidad y confidencialidad de los datos, así como los procesos de creación, actualización o eliminación de estructuras en las bases de datos, entre otros.

Artículo 14. Evaluación de capacidades y desempeño. Las instituciones deberán realizar evaluaciones periódicas de la capacidad y desempeño de la infraestructura de TI, de los sistemas de información y de las bases de datos, con el objeto de determinar necesidades de ampliación de capacidades o actualizaciones.

Las instituciones deberán documentar y llevar registro de las evaluaciones periódicas a que se refiere este artículo y realizar análisis de tendencias para determinar capacidades futuras.

Artículo 15. Adquisición, mantenimiento e implementación de infraestructura de TI, sistemas de información y bases de datos. Las instituciones deberán contar con procesos documentados y planes operativos para la adquisición, mantenimiento e implementación de la infraestructura de TI, los sistemas de información y las bases de datos. Dichos procesos deberán incluir, como mínimo, los aspectos siguientes:

a) En lo referente a adquisición y mantenimiento:

1. Selección de proveedores, considerando factibilidad tecnológica y económica;

2. Contratación, considerando la suscripción y ejecución; y,

3. Uso de herramientas controladas previamente certificadas por el proveedor, así como verificadas y aprobadas por la institución.

b) En lo referente a implementación:

1. Realización de pruebas; y,

2. Registro y monitoreo de la implementación.

Artículo 16. Gestión de servicios de TI. Las instituciones deberán realizar una adecuada gestión de los servicios de TI de acuerdo con las prioridades del negocio estableciendo, como mínimo, los aspectos siguientes:

a) Un catálogo que comprenda la definición de cada uno de los servicios de TI.

b) Acuerdos de niveles de servicio de TI establecidos entre las áreas del negocio y las áreas de TI. Dichos acuerdos deben comprender:

1. Los compromisos de las áreas de negocios;

2. Los compromisos de las áreas de TI;

3. Los requerimientos de soporte para el servicio de TI;

4. Las condiciones del servicio de TI; y,

5. El registro, monitoreo y actualización para la mejora de los servicios de TI.

c) Procesos de gestión de incidentes y de problemas, los cuales deben comprender:

1. La clasificación, registro, atención, análisis de tendencias y monitoreo de los eventos reportados por los usuarios o por el Centro de Operaciones de Seguridad Cibernética;

2. El escalamiento de incidentes para su atención y resolución, cuando aplique; y,

3. La identificación, análisis, registro y monitoreo de la causa raíz de los problemas y su posterior resolución.

d) Procesos de gestión de cambios en infraestructura de TI, sistemas de información y bases de datos, los cuales deben comprender:

1. La evaluación del impacto, priorización y autorización del cambio;

2. Los cambios de emergencia; y,

3. Realización de pruebas, registro y monitoreo del cambio.

Artículo 17. Ciclo de vida de los sistemas de información. Las instituciones deberán implementar metodologías adecuadamente documentadas para el análisis, diseño, desarrollo, pruebas, puesta en producción, mantenimiento, control de versiones y control de calidad de los sistemas de información.

Las actividades de desarrollo y producción deberán realizarse en ambientes distintos.

CAPÍTULO IV
SEGURIDAD DE TECNOLOGÍA DE LA INFORMACIÓN

Artículo 18. Gestión de la seguridad de la información. Las instituciones deberán gestionar la seguridad de sus activos de información con el objeto de garantizar la confidencialidad, integridad y disponibilidad de los datos, así como mitigar los riesgos de pérdida, extracción indebida y corrupción de la información, debiendo considerar, como mínimo, los aspectos siguientes:

a) Identificación y clasificación de la información de acuerdo a criterios de sensibilidad y criticidad;

b) Roles y responsabilidades para la gestión de la seguridad de la información;

c) Monitoreo de la seguridad de la información;

d) Seguridad física que incluya controles y medidas de prevención para resguardar adecuadamente la infraestructura de TI de acuerdo a la importancia definida por la institución conforme al riesgo a que esté expuesta, considerando:

   1. Ubicación física y sus controles de acceso;

   2. Acondicionamiento del espacio físico que considere factores tales como temperatura, humedad y prevención de incendios;

   3. Vigilancia, que incluya factores tales como personal de seguridad, sistemas de video y sensores;

   4. Suministro ininterrumpido de energía eléctrica; y,

   5. Adecuado manejo del cableado de red y de energía eléctrica.

e) Seguridad lógica que incluya controles y medidas de prevención para resguardar la confidencialidad, integridad y disponibilidad de los activos de información, considerando:

   1. Administración de los permisos a los sistemas de información, datos y elementos de la infraestructura de TI, que incluya registro y bitácoras del proceso y revisiones periódicas de los permisos;

   2. Revisión del uso de permisos para detectar actividades no autorizadas;

   3. Bitácoras de las transacciones realizadas en los sistemas de información críticos; y,

   4. Mecanismos y recursos técnicos para la identificación y detección de vulnerabilidades a través de escaneo, evaluaciones y pruebas de penetración, internas y externas, debiendo consignarse el resultado en un informe técnico.

      La frecuencia de las pruebas de penetración deberá realizarse, como mínimo, de forma anual o en función de la exposición de riesgo tecnológico de la institución, los cambios significativos en la institución, infraestructura tecnológica, sistemas de información y bases de datos.

f) Lo establecido en el Capítulo V Ciberseguridad.

Artículo 19. Oficial de Seguridad de la Información. El Oficial de Seguridad de la Información tendrá, como mínimo, las siguientes funciones:

a) Coordinar el cumplimiento de las políticas, procesos, procedimientos y mecanismos de seguridad de la información y ciberseguridad para preservar la confidencialidad, integridad y disponibilidad de la información de la institución;

b) Convocar, coordinar y dirigir el equipo de respuestas de incidentes cibernéticos;

c) Gestionar los incidentes de seguridad de la información considerando lo establecido en este reglamento, en las políticas, procesos y procedimientos de la institución, así como en el plan de recuperación ante desastres y el plan de continuidad de negocio de la institución;

d) Establecer y supervisar indicadores clave que permitan medir y evaluar la efectividad de los controles de seguridad de la información y ciberseguridad, asegurando que dichos indicadores y controles sean revisados, como mínimo una vez al año o cuando la situación lo amerite, y de ser necesario deberán ser ajustados para mitigar los riesgos asociados; y,

e) Presentar informes, como mínimo una vez al año o cuando la situación lo amerite, al Comité de Gestión de Riesgos o al Consejo, según corresponda, sobre el estado de la seguridad de la información y ciberseguridad, incluyendo el desempeño de indicadores clave, la gestión de incidentes y recomendaciones para la mejora continua de las políticas, procesos y procedimientos de seguridad de la información y ciberseguridad. Dichos informes deberán estar a disposición de la Superintendencia de Bancos, cuando esta lo requiera.

En caso la institución contrate con un tercero los servicios de apoyo a las funciones del Oficial de Seguridad de la Información deberá cumplir con lo establecido en el Reglamento para la Administración del Riesgo Operacional, con respecto a la contratación de servicios con terceros. Asimismo, la institución deberá, como mínimo, constatar la vigencia de las certificaciones relacionadas con seguridad de la información y ciberseguridad del tercero contratado, otorgadas por una empresa u organización de reconocido prestigio y documentar las competencias técnicas y la experiencia necesaria que respalden la contratación de estos servicios.

Artículo 20. Copias de respaldo. Las instituciones deberán tener copias de la información de la infraestructura de TI, sistemas de información y bases de datos, para lo cual deberán considerar, como mínimo, los aspectos siguientes:

a) Información a respaldar, periodicidad y validación de las copias de respaldo;

b) Procedimientos de restauración de las copias de respaldo;

c) Congruencia con el plan de continuidad del negocio y el plan de recuperación ante desastres de la institución; y,

d) Ubicación de las copias de respaldo y de la documentación de los procedimientos de restauración.

En caso de la información crítica, se deberá contar con copias de respaldo, como mínimo, realizadas de forma diaria, debiendo considerar los aspectos señalados en las anteriores literales de este artículo. Estas copias deberán encontrarse en

infraestructura dentro del territorio nacional y estar a disposición de la Superintendencia de Bancos cuando le sea solicitada.

Artículo 21. Operaciones y servicios financieros a través de canales electrónicos. Las instituciones que realicen operaciones y presten servicios financieros a través de canales electrónicos deberán implementar, como mínimo, lo siguiente:

a) Mecanismos para la protección y control de la infraestructura de TI, los sistemas de información y las bases de datos considerando la gestión de la ciberseguridad;

b) Medidas de seguridad en el intercambio de información, respaldadas por un certificado digital, cifrado de datos u otro mecanismo que permita garantizar la autenticidad, confidencialidad, integridad y disponibilidad de la información;

c) Programas de educación y divulgación de información para clientes; y,

d) Registro y bitácoras de las transacciones efectuadas.

Artículo 22. Uso de sistemas de inteligencia artificial. Las instituciones que utilicen sistemas de inteligencia artificial, adicionalmente a lo establecido en este reglamento, deberán gestionar los riesgos asociados a estas tecnologías considerando los estándares y mejores prácticas internacionales y, como mínimo, los aspectos siguientes:

a) Gobierno de los sistemas de inteligencia artificial que incluya políticas y procedimientos, organización y gestión de riesgos;

b) Identificación y comprensión del contexto, riesgos e impactos asociados a los sistemas de inteligencia artificial;

c) Medición y monitoreo del rendimiento y la efectividad de los sistemas de inteligencia artificial, que incluyan, entre otros controles, la supervisión humana sobre las decisiones tomadas por estos sistemas; y,

d) Implementación y mantenimiento de prácticas efectivas de gestión de riesgos, alineadas con los objetivos y estrategia de la institución, para el uso de los sistemas de inteligencia artificial, considerando la mejora continua de estos.

Las instituciones deberán garantizar, como mínimo, la seguridad, resiliencia, privacidad, confianza, transparencia e imparcialidad de los sistemas de inteligencia artificial que utilicen.

Artículo 23. Capacitación y concientización. Las instituciones deberán tener políticas y procedimientos para promover una cultura de seguridad de la información, incluyendo un programa continuo de capacitación a todo su recurso humano y concientización a los usuarios de la institución, debiendo llevar un registro de la realización de estos programas.

CAPÍTULO V
CIBERSEGURIDAD

Artículo 24. Gestión de la Ciberseguridad. Las instituciones deberán establecer e implementar políticas y procedimientos para gestionar efectivamente la ciberseguridad, debiendo considerar, como mínimo, las funciones siguientes:

a) Gobernanza;

b) Identificación;

c) Protección;

d) Detección;

e) Respuesta; y,

f) Recuperación.

Artículo 25. Gobernanza. Las instituciones deberán desarrollar e implementar políticas, procesos y procedimientos para una adecuada gobernanza en materia de ciberseguridad, considerando, como mínimo, lo siguiente:

a) Definición de objetivos de la gestión de riesgos de ciberseguridad consistentes con los procesos generales de gestión de riesgos de la organización;

b) Asignación de roles y responsabilidades específicas para la gestión de la ciberseguridad;

c) Mecanismos de monitoreo y revisión periódica de la ciberseguridad, lo cual deberá realizarse, como mínimo, una vez al año o cuando la situación lo amerite; y,

d) Gestión de riesgos de ciberseguridad de los servicios de TI, que incluya la cadena de suministro.

Artículo 26. Identificación. Las instituciones deberán tomar en cuenta su contexto tecnológico, los activos en el ciberespacio que soportan los servicios críticos de sus operaciones y el riesgo tecnológico asociado, de conformidad con su Manual de Administración de Riesgo Tecnológico, considerando como mínimo lo siguiente:

a) Gestión de activos en el ciberespacio: deberán ser identificados, clasificados por su criticidad, documentados, esquematizados a nivel lógico y gestionados en forma consistente durante todo su ciclo de vida;

b) Evaluación: la institución deberá identificar, analizar, clasificar y documentar sus vulnerabilidades cibernéticas, ciberamenazas, ciberataques, incidentes cibernéticos y los efectos de estos, considerando:

    1. El potencial impacto en la institución y la probabilidad de ocurrencia de estas;

    2. Priorizar las respuestas a las mismas;

    3. Procedimientos para recibir, registrar, analizar y responder ante información y alertas por parte de grupos y fuentes especializadas externas;

    4. Los cambios y excepciones, evaluando su impacto en el riesgo, así como el registro y seguimiento de estos;

    5. La autenticidad e integridad del hardware y software antes de su contratación, adquisición o utilización; y,

6. Efectuar la debida diligencia a los proveedores antes de la adquisición de activos de información y/o contratación de servicios con estos.

Artículo 27. Protección. Las instituciones deberán desarrollar e implementar políticas, procesos y procedimientos para proteger la confidencialidad, integridad y disponibilidad de sus activos en el ciberespacio, con el objeto de prevenir, limitar o contener el impacto de un ciberataque, considerando, como mínimo, lo siguiente:

a) Controles de seguridad para la adquisición, desarrollo y mantenimiento de sistemas y aplicaciones;

b) Gestión de cambios en las configuraciones de los activos en el ciberespacio;

c) Gestión de control y autorización de acceso, implementando medidas para emitir, registrar, administrar, verificar, revocar y auditar las identidades y credenciales, de usuarios, servicios y activos en el ciberespacio;

d) Prueba y mantenimiento de copias de respaldo de información;

e) Cumplimiento de regulaciones de la ubicación donde se encuentran los activos en el ciberespacio;

f) Proceso de eliminación de datos y destrucción de dispositivos;

g) Cifrado de datos en tránsito y reposo, así como protección de datos en uso, utilizando estándares y mejores prácticas en la materia. En situaciones excepcionales, debidamente justificadas y técnicamente documentadas por parte de las instituciones, estas podrán aplicar mecanismos alternos para proteger los datos en reposo. En todos los casos, se debe garantizar la integridad y confidencialidad de la información;

h) Protección y restricción del uso de medios extraíbles y de dispositivos móviles;

i) Documentación, implementación y revisión de los registros de auditoría de los activos en el ciberespacio;

j) Mecanismos para asegurar la resiliencia de sus activos en el ciberespacio, en situaciones normales y adversas, manteniendo una capacidad de recursos adecuada para garantizar la disponibilidad de los activos en el ciberespacio, de acuerdo a su criticidad; y,

k) Programas de capacitación de ciberseguridad dirigido al personal que desempeña funciones especializadas, a efecto de que posea los conocimientos y aptitudes necesarios para realizar las tareas pertinentes teniendo en cuenta los riesgos de seguridad cibernética.

Artículo 28. Detección. Las instituciones deberán monitorear sus activos en el ciberespacio, accesos, conexiones, las acciones que realizan los usuarios internos o externos, aplicaciones y acciones de los proveedores de servicios externos en la institución, para detectar vulnerabilidades cibernéticas, ciberamenazas, ciberataques e incidentes cibernéticos a través de la implementación, de forma interna o a través de la contratación, de un Centro de Operaciones de Seguridad Cibernética (*Security Operations Center*) con el objeto de proporcionar una visibilidad centralizada, monitoreo continuo y emisión de alertas.

Las instituciones deberán llevar un registro, de al menos los últimos doce (12) meses, de las vulnerabilidades cibernéticas, ciberamenazas, ciberataques e incidentes cibernéticos detectados en ese período de tiempo.

Artículo 29. Respuesta. Las instituciones deberán contar con procesos y procedimientos para garantizar una respuesta oportuna, durante y después de un incidente cibernético, considerando, como mínimo, lo siguiente:

a) Mecanismos de convocatoria e integración del equipo de respuesta a incidentes cibernéticos y de terceros pertinentes;

b) Mecanismos para analizar, documentar y atender las alertas recibidas de fuentes internas y externas;

c) Metodología de evaluación del impacto del incidente cibernético para su clasificación y categorización;

d) Actividades de mitigación de incidentes cibernéticos y sus efectos, documentando las mismas; y,

e) Análisis forense digital de los incidentes cibernéticos, debiendo elaborarse un informe técnico de los resultados obtenidos. Asimismo, deberán mantener un registro de las acciones realizadas durante dicho análisis forense digital.

Artículo 30. Recuperación. Las instituciones deberán establecer y mantener mecanismos para resistir, responder y recuperarse de un incidente cibernético, con el objeto de restaurar cualquier activo en el ciberespacio o servicios relacionados a este, que haya sido afectado debido a un incidente cibernético, de conformidad con lo establecido en el plan de recuperación ante desastres.

Estos mecanismos, deberán estar integrados con el plan de recuperación del grupo financiero.

Artículo 31. Equipo de respuesta de incidentes cibernéticos. Las instituciones deberán organizar un equipo de respuesta de incidentes cibernéticos (*Computer Security Incident Response Team*) que se reunirá de forma periódica y actuará ante la existencia de un incidente cibernético, con el objeto de contener y mitigar el impacto, así como promover los procesos de recuperación y resiliencia cibernética, el cual actuará en línea con el plan de recuperación ante desastres y el plan de continuidad del negocio de la institución.

El equipo de respuesta estará conformado por personal multidisciplinario de distintas áreas de la institución y será dirigido por el Oficial de Seguridad de la Información de la institución.

Las instituciones podrán integrar al equipo de respuesta de incidentes cibernéticos personas externas que, por su conocimiento técnico apoyen a lo establecido en este artículo. En este caso, las instituciones deberán garantizar la confidencialidad de la información a la que puedan tener acceso dichos externos.

Artículo 32. Aspectos de ciberseguridad en contratación de proveedores. Cuando las instituciones contraten operaciones o servicios de terceros que tengan relación con sus activos en el ciberespacio, deberán incluir en el contrato a suscribir, como mínimo, lo siguiente:

a) Obligación del proveedor de contar con políticas, procedimientos y mecanismos para la gestión de su ciberseguridad;

b) Mecanismos específicos, durante el plazo del contrato, que garanticen la protección de los activos en el ciberespacio, autorizando a la institución poder realizar revisiones periódicas de dichos mecanismos o de los certificados de seguridad de la información reconocidos internacionalmente extendidos al proveedor;

c) Acuerdos de nivel de servicio que incluya la gestión de incidentes cibernéticos que ponga en riesgo los activos en el ciberespacio, definiendo responsabilidades de la institución y del proveedor, así como la obligación de este último de informar a la institución de forma oportuna la ocurrencia de dicho incidente cibernético; y,

d) Acuerdos de recuperación ante desastres y resiliencia cibernética que garanticen la confidencialidad, integridad y disponibilidad de la información.

Artículo 33. Intercambio de información y comunicación. Las instituciones deberán establecer mecanismos de intercambio de información y comunicación entre ellas; asimismo, podrán establecer dichos mecanismos con otras entidades del sistema financiero nacional y con equipos de respuesta a incidentes de seguridad informática nacional y de otros países, con el objeto de que los ciberataques e incidentes cibernéticos sean comunicados a las demás instituciones, para que puedan implementar los mecanismos de gestión de ciberseguridad que consideren pertinentes.

CAPÍTULO VI
PLAN DE RECUPERACIÓN ANTE DESASTRES

Artículo 34. Plan de recuperación ante desastres. Las instituciones deberán contar con un plan de recuperación ante desastres, que esté alineado con el plan de continuidad del negocio de la institución, con el objeto de recuperar los servicios tecnológicos críticos que apoyan los procesos críticos de las principales líneas de negocio, sus activos en el ciberespacio, así como la información asociada en caso de una interrupción.

El plan de recuperación ante desastres deberá incluir, como mínimo, los aspectos siguientes:

a) Objetivo y alcance del plan;

b) Identificación de los servicios tecnológicos críticos, procesos críticos y activos en el ciberespacio de las principales líneas de negocio;

c) Identificación de los procesos que son necesarios para soportar los procesos identificados en el inciso b) anterior;

d) Procedimientos y canales de comunicación, internos y externos;

e) Procedimientos y tiempos de recuperación y restauración de operaciones y procesos críticos, así como de los activos en el ciberespacio posterior a un incidente cibernético;

f) Identificación y descripción de roles, así como de responsabilidades del personal clave para la recuperación y listado de proveedores críticos;

g) Recursos necesarios para la recuperación y restauración;

h) Convenios documentados con terceros y proveedores críticos;

i) Identificación de factores de dependencia interna y externa de la institución, tales como proveedores, personal de la entidad u otros, y las acciones para mitigar el riesgo de dicha dependencia, que incluya la contratación con terceros de servicios críticos que procesan y/o almacenan información; y,

j) Identificación de prioridades de recuperación y restauración.

En caso de que la institución contrate con terceros servicios tecnológicos críticos que procesan y/o almacenan información, deberá incluir dentro de su plan de recuperación ante desastres, consideraciones específicas para recuperarse ante eventos que afecten estos servicios. Asimismo, la institución deberá incluir mecanismos de salida ante un incumplimiento de los términos y condiciones de los servicios contratados, que considere el término anticipado de la relación contractual y que permitan retomar la operación, ya sea por cuenta propia o mediante otro proveedor de este tipo de servicios.

Las nuevas instituciones que se constituyan o se autorice su funcionamiento deberán remitir una copia del plan de recuperación ante desastres a que se refiere este artículo a la Superintendencia de Bancos antes del inicio de sus operaciones. Las modificaciones al plan de recuperación ante desastres deberán ser comunicadas a la Superintendencia de Bancos dentro de los diez (10) días hábiles siguientes a su aprobación.

Artículo 35. Pruebas al plan de recuperación ante desastres. Las instituciones deberán elaborar como parte del plan de recuperación ante desastres un plan de pruebas que incluya, como mínimo, lo siguiente:

a) Alcance;

b) Escenarios con diferentes niveles de severidad que consideren la adaptación y evolución de la tecnología, así como las amenazas relacionadas con el entorno tecnológico; y,

c) Cronograma que establezca al menos actividades, responsables y sus respectivas fechas de ejecución.

Las pruebas al plan de recuperación ante desastres deberán realizarse como mínimo de forma anual o cuando la situación lo amerite. Asimismo, los resultados de las pruebas realizadas deberán documentarse y, cuando corresponda, adecuar el plan de recuperación ante desastres en función de los resultados obtenidos.

Artículo 36. Capacitación del personal clave para la recuperación ante desastres. Las instituciones deberán mantener capacitado al personal clave, a que se refiere el inciso f) del artículo 34 de este reglamento, para activar o probar el plan de recuperación ante desastres y sus modificaciones.

Artículo 37. Centro de cómputo alterno. Las instituciones deberán contar con un centro de cómputo alterno con las características físicas y lógicas necesarias para dar continuidad a las operaciones y los procesos críticos de negocios, cumpliendo con los requisitos establecidos en este reglamento referentes a seguridad de tecnología de la información, ciberseguridad, infraestructura de TI, sistemas de información y bases de datos.

El centro de cómputo alterno deberá estar en una ubicación geográfica distinta del centro de cómputo principal, de tal forma que no se vean expuestos a un mismo nivel de riesgo ante la ocurrencia de un mismo evento, de acuerdo con los manuales de administración de riesgo de la institución. Se entenderá por evento toda situación que interrumpa las operaciones normales de un negocio.

Las instituciones deberán realizar réplica de toda la información crítica, de acuerdo con su plan de continuidad de negocio y su plan de recuperación ante desastres, al centro de cómputo alterno.

En caso de servicios críticos que procesan y/o almacenan información, fuera del territorio nacional, el centro de cómputo principal y centro de cómputo alterno deberán estar en países distintos. Asimismo, en el caso de servicios críticos, que procesan y/o almacenan información, contratados con un tercero fuera del territorio nacional, el servicio contingente de este deberá ubicarse en un país distinto.

En caso el centro de cómputo alterno esté ubicado fuera del territorio nacional, las instituciones deberán permitir a la Superintendencia de Bancos el libre acceso a su infraestructura de TI, sistemas de información y bases de datos, y proporcionar a esta la información que les requiera.

En el caso que la institución tenga su centro de cómputo alterno contratado con un proveedor de servicios de procesamiento y/o almacenamiento de información deberá permitir que la Superintendencia de Bancos tenga libre acceso a los sistemas de información, registros, bases de datos y todos los servicios contratados, así como proporcionar a esta la información que les requiera.

CAPÍTULO VII
PROCESAMIENTO Y/O ALMACENAMIENTO DE INFORMACIÓN

Artículo 38. Procesamiento y/o almacenamiento de información. Las instituciones podrán procesar y/o almacenar su información dentro o fuera del territorio nacional debiendo disponer para el efecto con la infraestructura de TI, sistemas de información, bases de datos y personal técnico con el propósito de asegurar la disponibilidad, integridad, confidencialidad y accesibilidad de la información.

Adicionalmente, a lo establecido en el Reglamento para la Administración del Riesgo Operacional con respecto a la contratación de servicios con terceros, las instituciones, en caso de contratar con terceros servicios que procesan y/o almacenan información, deberán establecer e implementar políticas y procedimientos para la administración de los riesgos asociados, de conformidad a lo indicado en el artículo 3 de este reglamento, debiendo contar con, al menos, las políticas siguientes:

a) Gobierno y gestión de la información;

b) Selección y contratación de proveedores de servicios que procesan y/o almacenan información;

c) Disponibilidad y acuerdos de niveles de servicios a contratar; y,

d) Cifrado de la información.

Artículo 39. Obligaciones de la institución al procesar y/o almacenar su información fuera del territorio nacional. Las instituciones, en caso de procesar y/o almacenar información fuera del territorio nacional, deberán cumplir, como mínimo, lo siguiente:

a) Que la infraestructura tecnológica y sistemas que se utilizarán para la comunicación, procesamiento y/o almacenamiento de información cumplan con aspectos de seguridad de la información y ciberseguridad para resguardar la confidencialidad, integridad y disponibilidad de la información, con al menos, lo establecido en este reglamento;

b) Contar con enlaces de comunicación cifrados de extremo a extremo, asegurando la confidencialidad, integridad y disponibilidad de la información, gestionando todas las medidas necesarias para la transmisión;

c) Cifrado de toda la información en reposo y en tránsito, así como la protección de la información en uso, utilizando estándares reconocidos internacionalmente que garanticen la confidencialidad e integridad de la información de la institución, manteniendo las llaves de cifrado bajo control y administración de la institución;

d) Tener bajo su único control y responsabilidad la administración de usuarios y privilegios de acceso;

e) Contar con controles de autenticidad y no repudio en el acceso, procesamiento y transmisión de la información;

f) Que no existan limitaciones legales para los accesos a la información, auditorías y para las actividades de supervisión realizadas por la Superintendencia de Bancos;

g) En caso de infraestructura propia, permitir a la Superintendencia de Bancos, cuando esta lo requiera, el libre acceso a la infraestructura de TI, sistemas de información, registros, bases de datos e instalaciones y proporcionar a esta la información que le requiera;

h) Disponer en el territorio nacional de personal técnico y capacitado para administrar la infraestructura, servicios, sistemas y bases de datos, teniendo accesos y controles a estos; e,

i) Establecer las medidas administrativas necesarias para que, en caso de suspensión de operaciones resuelta por Junta Monetaria de un banco o una sociedad financiera, la Junta de Exclusión de Activos y Pasivos, así como el Representante Legal de la institución suspendida, puedan tener acceso a la información, servicios, sistemas y bases de datos en los servicios contratados.

Artículo 40. Obligaciones de la institución al contratar con terceros servicios que procesan y/o almacenan información. Las instituciones, en caso de contratar con terceros, dentro o fuera del territorio nacional, servicios que procesan y/o almacenan información, adicionalmente a los requerimientos del artículo anterior, deberán cumplir lo siguiente:

a) Verificar que el proveedor con el que se desee procesar y/o almacenar información aplique políticas de seguridad de información y ciberseguridad, considerando estándares internacionales y cumpliendo, como mínimo, con lo establecido en este reglamento, asimismo, que el proveedor posea certificaciones vigentes relacionadas con tecnología, seguridad de la información, ciberseguridad, continuidad de negocio y/o gestión de servicios tecnológicos;

b) Verificar, en el caso de servicios críticos que procesan y/o almacenan información, los informes de auditorías independientes relacionadas con tecnología, del último año, a las que se somete el proveedor del servicio, con objeto de determinar la factibilidad técnica de contratación de dicho proveedor de procesamiento y/o almacenamiento de información;

c) Establecer procedimientos para verificar el cumplimiento de los acuerdos de niveles de servicio definidos, según sea el caso, con el proveedor o vendedor. Asimismo, procedimientos para verificar que dicho proveedor o vendedor se asegure de que los subcontratistas y subcontratistas en cadena de los servicios que procesan y/o almacenan información de la institución, cumplan con los referidos niveles de servicio establecidos;

d) En caso de contratar servicios que procesan y/o almacenan información confidencial, en una jurisdicción extranjera, dicha jurisdicción debe contar con un marco normativo de protección y seguridad de datos personales;

e) Establecer los roles y responsabilidades de la institución, del proveedor, del vendedor del servicio y subcontratistas de los servicios que procesan y/o almacenan información;

f) Independencia lógica o física de su información con la de otros usuarios que procesan y/o almacenan información con el mismo proveedor;

g) Aplicar métodos seguros de autenticación para acceder a los servicios contratados;

h) Permitir a la Superintendencia de Bancos, cuando esta lo requiera, el libre acceso a la información, registros, sistemas, bases de datos, servicios contratados, y proporcionar a esta la información que le requiera;

i) Establecer e implementar mecanismos para verificar que el proveedor se asegure que los subcontratistas y subcontratistas en cadena relacionados al servicio, que procesan y/o almacenan información de la institución, se sujeten y cumplan las mismas condiciones y obligaciones que le son aplicables a dicho proveedor en virtud de este reglamento; y,

j) En caso las instituciones contraten, a través de un vendedor, servicios tecnológicos que procesan y/o almacenan información, estas deberán establecer e implementar mecanismos para verificar que el vendedor se asegure que los proveedores, subcontratistas y subcontratistas en cadena relacionados al servicio, se sujeten y cumplan con las mismas condiciones y obligaciones que le son aplicables al proveedor en virtud de este reglamento.

Artículo 41. Análisis de criticidad de los servicios. Las instituciones, previo a la contratación de servicios de procesamiento y/o almacenamiento de información con terceros, deberán realizar, para cada servicio, un análisis de criticidad, conforme a su metodología, basándose en estándares y mejores prácticas internacionales, para determinar si estos servicios son críticos.

En adición a lo anterior, se deberá considerar, entre otros criterios, si la potencial ocurrencia de cualquiera de los eventos que se indican a continuación pudiera causar uno o más de los impactos siguientes:

a) Eventos:

   1. Falta de disponibilidad de los servicios a contratar;

   2. Pérdida de la confidencialidad, integridad o disponibilidad de su información; o,

   3. Imposibilidad de sustituir al proveedor de los servicios en el corto plazo.

b) Impactos:

1. Afectación en la continuidad del negocio;

2. Interrupción significativa en el otorgamiento de productos y/o la prestación de servicios financieros;

3. Afectación sustancial en la situación financiera, la estrategia o prestigio de la institución;

4. Afectación sustancial en el funcionamiento del sistema de pagos; o,

5. Limitación en la capacidad de cumplir con obligaciones legales y reglamentarias.

Asimismo, posterior a la contratación de dichos servicios, al menos durante el primer trimestre de cada año, así como cuando exista una situación que lo amerite, las instituciones deberán realizar el análisis anteriormente indicado para determinar si la clasificación de criticidad de los servicios ha cambiado, a efecto de aplicar lo establecido en el artículo 42 de este reglamento.

Las instituciones deberán realizar un informe que desarrolle el análisis indicado en el presente artículo y los resultados correspondientes, el cual podrá ser requerido en cualquier momento por la Superintendencia de Bancos.

Artículo 42. Cambio en la criticidad de servicios de procesamiento y/o almacenamiento de información. Si las instituciones, con base en lo establecido en el artículo 41, determinan que la clasificación del servicio cambió de no crítico a crítico, en un plazo no mayor a seis (6) meses, deberán:

a) Cumplir con lo establecido en los artículos 38, 39 y 40, así como con los incisos a); b); c); y, d) del artículo 44 y b); c); d); y, e) del artículo 45, todos de este reglamento, lo cual deberá hacer constar en un informe aprobado por el Consejo; y,

b) Adecuar el contrato suscrito a los requisitos establecidos en los artículos 46 o 47, según corresponda.

Artículo 43. Registro de servicios contratados con terceros que procesan y/o almacenan información. Las instituciones deberán conservar un registro actualizado de los servicios contratados con terceros que procesan y/o almacenan información de estas. Dicho registro deberá considerar, como mínimo, lo siguiente:

a) Nombre del vendedor que comercializa los servicios de procesamiento y/o almacenamiento de información de la institución, si aplica;

b) Nombre del proveedor que procesa y/o almacena información de la institución;

c) Breve descripción del servicio que procesa y/o almacena información;

d) Clasificación de la criticidad del servicio contratado;

e) Fecha de vencimiento del contrato con el proveedor o vendedor del servicio; y,

f) Ubicaciones geográficas en las cuales se procesa y/o almacena la información.

Por cada proveedor o vendedor, se deberá contar con un expediente que incluya los informes indicados en los artículos 41 y 42, así como el contrato, adendas, anexos y cualquier documento legal relacionado con el servicio.

Artículo 44. Autorización para procesar y/o almacenar información fuera del territorio nacional. En caso de servicios tecnológicos que procesan y/o almacenan información, en infraestructura propia ubicada fuera del territorio nacional, la institución, adicional al cumplimiento de lo establecido en los artículos 38 y 39 de este reglamento, deberá solicitar autorización previa a la Superintendencia de Bancos, remitiendo para el efecto la información siguiente:

a) Autorización expresa, del Consejo de Administración o quien haga sus veces, para procesar y/o almacenar su información fuera del territorio nacional;

b) Identificación y descripción de la información a procesar y/o almacenar, así como un plan de migración;

c) El país o países donde se procesará y/o almacenará la información; y,

d) Opinión legal de un abogado de la jurisdicción donde se procesará y/o almacenará la información, respecto a la existencia de un marco normativo de protección y seguridad de datos personales en dicha jurisdicción; el mecanismo a que quedarán sujetas las contingencias legales que pudieran surgir; y, la no existencia de limitaciones normativas para que la Superintendencia de Bancos pueda tener acceso a la información, servicios, sistemas y bases de datos procesadas y/o almacenadas.

La autorización de la Superintendencia de Bancos es sin perjuicio de la responsabilidad de la institución de cumplir en forma integral con los aspectos atinentes contenidos en este reglamento, a efecto que la decisión adoptada por dicha institución respecto al procesamiento y/o almacenamiento de información, fuera del territorio nacional, no comprometa la confidencialidad, integridad y disponibilidad de la información, así como el plan de recuperación ante desastres que garantice la continuidad de operaciones de esta.

Artículo 45. Autorización para contratar servicios críticos que procesan y/o almacenan información. En caso de contratar con terceros servicios tecnológicos que procesan y/o almacenan información que, según el análisis realizado por la institución, de conformidad con lo establecido en el artículo 41 de este reglamento, sean considerados como críticos, la institución deberá cumplir con lo indicado en los artículos 38, 39 y 40, asimismo, debe solicitar autorización previa a la Superintendencia de Bancos, remitiendo para el efecto la información requerida en el artículo 44 y la siguiente:

a) El nombre o razón social del vendedor y proveedor de servicios que procesan y/o almacenan información;

b) Las certificaciones vigentes del proveedor del servicio, relacionadas con tecnología, seguridad de la información, ciberseguridad, continuidad de negocio y/o gestión de servicios tecnológicos;

c) Informes de auditorías independientes relacionadas con tecnología, del último año, a las que se somete el proveedor del servicio;

d) La información sobre el modelo de servicio y tipo de implementación a contratar;

e) El esquema de los servicios contratados, incluyendo los enlaces de comunicación para transferencia de información;

f) Proyecto del contrato a suscribir y proyecto de los acuerdos de niveles de servicio con el vendedor y proveedor final de los servicios que procesan y/o almacenan información;

g) Informe del análisis de la criticidad del servicio que se pretende contratar, a que se refiere el artículo 41 de este reglamento, debidamente aprobado por el Consejo; y,

h) Autorización expresa por parte del Consejo para la contratación del servicio que procesa y/o almacena información correspondiente.

La autorización de la Superintendencia de Bancos es sin perjuicio de la responsabilidad de la institución de cumplir en forma integral con los aspectos atinentes contenidos en este reglamento, a efecto que la decisión adoptada por dicha institución respecto al procesamiento y/o almacenamiento de información, contratado con terceros, no comprometa la confidencialidad, integridad y disponibilidad de la información, así como el plan de recuperación ante desastres que garantice la continuidad de operaciones de esta.

Artículo 46. Contratación de servicios tecnológicos críticos con proveedores de servicios que procesan y/o almacenan información. En caso las instituciones contraten servicios tecnológicos críticos con proveedores que procesan y/o almacenan información, en los contratos suscritos con estos, deberán incluir, como mínimo, lo siguiente:

a) Acuerdo de disponibilidad de al menos 99.90% en los servicios contratados;

b) Las condiciones referentes a capacidad, tiempos de recuperación y horarios de atención del proveedor del servicio, estableciendo niveles de servicio que permitan cumplir, cuando menos, con lo establecido en este reglamento;

c) Las condiciones de seguridad de la información y ciberseguridad de los servicios contratados, así como, las condiciones establecidas para proteger la confidencialidad de la información, considerando cuando menos, con lo establecido en este reglamento;

d) Que la institución mantiene la propiedad de toda la información procesada y/o almacenada y que esta conserva todos los derechos sobre la misma;

e) Prohibición al proveedor de utilizar la información para algún propósito diferente al establecido en el contrato, durante la vigencia y posterior a la terminación de este;

f) Confidencialidad de la información procesada y/o almacenada por el proveedor durante la vigencia y posterior a la terminación del contrato, estableciendo que el proveedor y subcontratados en cadena guardarán la confidencialidad de las operaciones y servicios que realizaren;

g) El borrado seguro de los datos existentes en los medios de almacenamiento cuando finalice el contrato, o cuando el proveedor de servicios reemplace dichos medios;

h) Acceso a informes y certificaciones anuales que demuestran la efectividad en la gestión de los servicios contratados;

i) Las condiciones y limitaciones bajo las cuales el proveedor de servicios que procesan y/o almacenan información puede subcontratar parte del servicio;

j) Que únicamente la institución podrá seleccionar en qué países y/o regiones se podrá procesar y/o almacenar la información, estableciendo prohibición al proveedor de transferir la información a otros países o regiones sin autorización previa de la institución;

k) Los derechos y obligaciones de cada una de las partes en el contrato. En caso de existir subcontratistas y subcontratistas en cadena de servicios que procesan y/o almacenan información de la institución, el contrato deberá estipular que el proveedor tendrá la responsabilidad ante la institución de asegurar que dichos subcontratistas se sujeten y cumplan, respecto del servicio subcontratado, con las mismas condiciones y obligaciones que dicho proveedor adquiere en virtud de este reglamento y del respectivo contrato;

l) La obligación del proveedor del servicio que procesa y/o almacena información de comunicar a la institución sobre cualquier evento o situación que pudiera afectar la prestación del servicio y la afectación a los servicios prestados por la institución, así como la corrección oportuna y eficaz de las vulnerabilidades de seguridad de la información detectadas;

m) Las causales de terminación del contrato por parte de la institución, incluyendo el incumplimiento de los acuerdos o niveles de servicio o el cambio de las condiciones que generen impacto negativo al servicio contratado;

n) Que la Superintendencia de Bancos, cuando esta lo requiera, tendrá libre acceso a la información, registros, sistemas, bases de datos y servicios contratados;

o) Estipulación que, en caso de suspensión de operaciones resuelta por Junta Monetaria, de un banco o una sociedad financiera, el proveedor de los servicios contratados otorgará todos los accesos a los servicios, recursos, información y componentes del servicio contratado a la Junta de Exclusión de Activos y Pasivos y al Representante Legal de la institución suspendida, para el cumplimiento de sus respectivas atribuciones legales y reglamentarias; y,

p) El plazo no podrá ser superior a un período de cinco (5) años.

En caso de finalización del contrato por plazo o de forma anticipada, ante un cambio o modificación, así como ante un cambio de proveedor, la institución deberá proceder conforme lo establecido en este capítulo.

Artículo 47. Contratación de servicios tecnológicos críticos a través de un vendedor de servicios que procesan y/o almacenan información. Ante la imposibilidad de celebrar el contrato de forma directa con el proveedor de servicios que procesan y/o almacenan información, las instituciones deberán, como mínimo, establecer en el contrato con el vendedor lo siguiente:

a) Que el vendedor acredita tener las facultades legales necesarias y válidas en Guatemala para la comercialización de los servicios de procesamiento y/o almacenamiento de información del proveedor; y,

b) Que el vendedor tiene un contrato con el proveedor, en el cual este último, como responsable de prestar el servicio contratado que procesa y/o almacena información, se compromete a dar cumplimiento a los requisitos establecidos

en el artículo 46 de este reglamento, durante todo el tiempo de vigencia del servicio contratado para la institución.

Las instituciones, previamente a celebrar el contrato con el vendedor, deberán obtener de este los documentos que sustenten los requisitos establecidos en este artículo, así como conservarlos. Asimismo, deberán verificar que en los términos y condiciones ofrecidos por el proveedor de servicios que procesan y/o almacenan información de la institución, se establezca lo relacionado al debido cumplimiento de lo indicado en el artículo 46 de este reglamento.

Artículo 48. Contratación con terceros de servicios no críticos que procesan y/o almacenan información. Cuando las instituciones contraten con terceros servicios que procesan y/o almacenan información que, bajo su entera responsabilidad y conforme el análisis indicado en el artículo 41 de este reglamento, clasifiquen como no críticos, adicionalmente al cumplimiento de lo establecido en los artículos 38, 39 y 40 de este reglamento, estas deberán cerciorarse que los contratos y/o términos y condiciones que se suscriban, reúnan los requisitos mínimos que aseguren la disponibilidad, integridad y confidencialidad de la información que se procesará y/o almacenará.

CAPÍTULO VIII
DISPOSICIONES TRANSITORIAS Y FINALES

Artículo 49. Transitorio. Las instituciones deberán actualizar sus inventarios de activos de información, dentro de los tres (3) meses siguientes a la entrada en vigencia de este reglamento.

Artículo 50. Transitorio. Las instituciones deberán actualizar el Manual de Administración del Riesgo Tecnológico y su plan de recuperación ante desastres, dentro de los doce (12) meses siguientes a la entrada en vigencia de este reglamento.

Artículo 51. Transitorio. Las instituciones que, a la entrada en vigencia de este reglamento, tengan contratados con terceros servicios que procesan y/o almacenan información deberán adecuar los contratos a lo establecido en este reglamento de la forma siguiente:

a) Si la vigencia del contrato es de plazo determinado, se efectuará la adecuación al realizar alguna modificación y/o renovación; o,

b) Si la vigencia del contrato es de plazo indeterminado, se realizará la adecuación dentro de los doce (12) meses siguientes a la entrada en vigencia de este reglamento.

Artículo 52. Transitorio. A más tardar el 31 de enero de 2027, las instituciones deberán realizar el análisis de criticidad indicado en el artículo 41 respecto de todos los servicios de procesamiento y/o almacenamiento de información que hubieren sido contratados antes de la vigencia de este reglamento, para que los mismos sean clasificados, según correspondan, en críticos y no críticos, asimismo, en el caso de los servicios que cambiaron de no crítico a crítico deberán cumplir con lo establecido en el artículo 42.

Artículo 53. Envío de información a la Superintendencia de Bancos. Las instituciones deberán enviar a la Superintendencia de Bancos información relacionada con el riesgo tecnológico conforme a las instrucciones generales que el órgano supervisor les indique.

El envío de información establecido en el párrafo anterior no exime a las instituciones de cumplir con otras disposiciones legales o normativas aplicables.

Artículo 54. Casos no previstos. Los casos no previstos en este reglamento serán resueltos por la Junta Monetaria, previo informe de la Superintendencia de Bancos.