JUNTA MONETARIA

RESOLUCIÓN JM-42-2020

Inserta en el punto primero del acta 16-2020, correspondiente a la sesión extraordinaria celebrada por la Junta Monetaria el 6 de abril de 2020.

PUNTO PRIMERO: Superintendencia de Bancos eleva a consideración de la Junta Monetaria la propuesta de modificación al Reglamento para la Administración del Riesgo Tecnológico, emitido en resolución JM-102-2011.

RESOLUCIÓN JM-42-2020. Conocido el oficio número 1258-2020 del Superintendente de Bancos, del 24 de marzo de 2020, al que se adjunta el dictamen número 4-2020 de la Superintendencia de Bancos, por medio del cual se eleva a consideración de esta junta la propuesta de modificación al Reglamento para la Administración del Riesgo Tecnológico, emitido en resolución JM-102-2011.

LA JUNTA MONETARIA:

CONSIDERANDO: Que mediante resolución JM-102-2011, del 17 de agosto de 2011, esta junta emitió el Reglamento para la Administración del Riesgo Tecnológico, estableciendo los lineamientos mínimos que los bancos, las sociedades financieras, las entidades fuera de plaza o entidades *off shore* y las empresas especializadas en servicios financieros que forman parte de un grupo financiero, deben observar para administrar el riesgo tecnológico; **CONSIDERANDO:** Que el desarrollo tecnológico en las entidades financieras a nivel mundial ha generado mayor rapidez y facilidad en el intercambio de información y comunicación, eliminando barreras de distancia y tiempo en las operaciones financieras; lo cual conlleva un incremento del riesgo tecnológico por la existencia de amenazas cibernéticas que ponen en riesgo la integridad, disponibilidad, confidencialidad de los activos en el ciberespacio, así como la continuidad de la prestación de sus servicios; **CONSIDERANDO:** Que dada la dinámica del desarrollo tecnológico en el mercado financiero guatemalteco, las mejores prácticas internacionales, así como la gestión del riesgo por parte de las entidades, es conveniente incorporar lo relativo a la gestión de la ciberseguridad, con el objeto que las instituciones puedan detectar, resistir, responder y recuperarse rápidamente de un ciberataque; **CONSIDERANDO:** Que en el dictamen número 4-2020 de la Superintendencia de Bancos se concluye que de la revisión del Reglamento para la Administración del Riesgo Tecnológico, del análisis de los estándares internacionales, la normativa internacional y de las mejores prácticas internacionales es prudente y oportuno modificar el citado reglamento a efecto de incorporar lo relativo a la gestión de la ciberseguridad, la designación de un Oficial de Seguridad de la Información, la implementación de un Centro de Operaciones de Seguridad Cibernética, la organización de un Equipo de Respuestas de Incidentes Cibernéticos y la incorporación de aspectos de ciberseguridad en contratación de proveedores,

POR TANTO:

Con base en lo considerado, y con fundamento en lo dispuesto en los artículos 133 de la Constitución Política de la República de Guatemala; 26, inciso l de la Ley Orgánica del Banco de Guatemala; 55, 56, 57, 113 y 129 de la Ley de Bancos y Grupos Financieros; y tomando en cuenta el oficio número 1258-2020 y el dictamen número 4-2020, ambos de la Superintendencia de Bancos,

RESUELVE:

1. **Modificar los artículos 1, 2, 3, 4, 5, 6, 7, 11, 13, 14, 15, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, y 29; el nombre de los CAPÍTULOS V, VI, VII; así como incorporar los artículos 17 Bis., 19 Bis., 30, 31, 32, 33, 34, 35, 36, 37, 38; y adicionar el CAPÍTULO VIII al Reglamento para la Administración del Riesgo Tecnológico, emitido en resolución JM-102-2011, en el sentido siguiente:**

"Artículo 1. Objeto. Este reglamento tiene por objeto establecer los lineamientos mínimos que los bancos, las sociedades financieras, las entidades fuera de plaza o entidades off shore 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:

Activos en el ciberespacio: son los sistemas de información, infraestructura de TI, bases de datos, redes, datos 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.

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 ésta tiene para la operación del negocio.

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 éstos, 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, las entidades fuera de plaza o entidades off shore y las empresas especializadas en servicios financieros que forman parte de un grupo financiero.

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.

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.

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

"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 de información y tercerización.

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 7 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 párrafo 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) 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; e,

i) 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. 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 ésta 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 11. Inventarios.** Las instituciones deberán mantener inventarios actualizados de su infraestructura de TI, de sus sistemas de información y de sus bases de datos 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.

A la entrada en vigencia de este reglamento, los inventarios de infraestructura de TI, sistemas de información y de bases de datos, a que se refiere este artículo, serán obligatorios para las aplicaciones que soportan los procesos críticos del negocio, especialmente las que permitan a los respectivos depositantes disponer de sus fondos.".

"**Artículo 13. 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 14. 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 15. 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. Gestión de la seguridad de la información.** Las instituciones deberán gestionar la seguridad de su 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 integridad y seguridad de la infraestructura de TI, los sistemas de información y de las bases de datos, 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 17 Bis. Oficial de Seguridad de la Información.** El Oficial de Seguridad de la información tendrá las siguientes funciones:

a) Coordinar el cumplimiento de las políticas, 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 y dirigir el equipo de respuestas de incidentes cibernéticos; y,

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.".

"**Artículo 18. 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.".

"**Artículo 19. 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 19 Bis. Capacitación y concientización.** La institución deberá 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 20. 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) Identificación;

b) Protección;

c) Detección;

d) Repuesta; y,

e) Recuperación.".

"**Artículo 21. 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, documentados y gestionados en forma consistente, en relación con los objetivos y la estrategia de riesgo de la institución;

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; y,
3. Procedimientos para recibir información y alertas por parte de grupos y fuentes especializadas externas.".

"**Artículo 22. 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;

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) Protección por medio de encriptación o cifrado de datos;

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

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

"**Artículo 23. 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 Operation 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 meses, de las vulnerabilidades cibernéticas, ciberamenazas, ciberataques e incidentes cibernéticos detectados en ese período de tiempo.".

"**Artículo 24. 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 respuestas a incidentes cibernéticos;

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.".

"Artículo 25. 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 26. Equipo de Respuesta de Incidentes Cibernéticos. La institución deberá 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, 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.".

"Artículo 27. Aspectos de ciberseguridad en contratación de proveedores. Cuando la institución contrate 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 28. Intercambio de información y comunicación. Las instituciones podrán establecer mecanismos de intercambio de información y comunicación entre ellas, con el objeto de que los incidentes cibernéticos sufridos sean comunicados a las demás instituciones, con el fin exclusivo de que puedan implementar los mecanismos que consideren pertinentes para gestionar su ciberseguridad.".

"CAPÍTULO VI
PLAN DE RECUPERACIÓN ANTE DESASTRES"

"Artículo 29. 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, para recuperar 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 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 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; y,

j) Identificación de prioridades de recuperación y restauración.

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 30. 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: alcance, escenarios y periodicidad.

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 31. 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 29 de este reglamento, para activar o probar el plan de recuperación ante desastres y sus modificaciones.".

"Artículo 32. 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, infraestructura de TI, sistemas de información y bases de datos.

El centro de cómputo alterno deberá estar en una ubicación 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 desastre. Se entenderá por desastre todo evento que interrumpa las operaciones normales de un negocio.

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 ésta la información que les requiera.".

"CAPÍTULO VII
PROCESAMIENTO DE INFORMACIÓN"

"Artículo 33. Procesamiento de la información. Las instituciones podrán procesar su información dentro o fuera del territorio nacional debiendo contar 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.

En el caso de procesamiento fuera del territorio nacional, previamente deberán contar con autorización de la Superintendencia de Bancos y cumplir con los requisitos siguientes:

a) Contar con un centro de cómputo alterno, conforme lo establecido en el artículo anterior, ubicado en el territorio nacional;

b) Disponer de personal técnico y uno o más administradores de bases de datos, en el territorio nacional, con las capacidades para operar el centro de cómputo alterno;

c) Replicación en tiempo real hacia servidores locales de su información procesada fuera del territorio nacional; y,

d) Permitir a la Superintendencia de Bancos el libre acceso a su infraestructura de TI, sistemas de información, bases de datos e instalaciones ubicadas fuera del territorio nacional, y proporcionar a ésta la información que le requiera.

Asimismo, las instituciones deberán contar con la autorización previa de la Superintendencia de Bancos para cambiar el sitio donde se procesa la información hacia otro país.".

"Artículo 34. Contratación de servicios de procesamiento de información. Cuando se contraten servicios de terceros para el procesamiento de su información, las instituciones serán las responsables de cumplir con lo establecido en este reglamento. En los contratos que se suscriban deberán incluir, como mínimo, lo siguiente:

a) Que la Superintendencia de Bancos tendrá libre acceso a las instalaciones de los contratados, infraestructura de TI, sistemas de información y bases de datos, relacionadas con el servicio contratado por la institución;

b) Que el contratado tiene obligación de proporcionarle a la Superintendencia de Bancos, cuando ésta se lo requiera, toda la información y/o documentos relacionados con las operaciones y servicios de tercerización prestados a la institución por el contratado;

c) Que el contratado guardará la confidencialidad de las operaciones y servicios que realizare y demás información a que tenga acceso con motivo de su relación con la institución contratante;

d) Que el contratado se compromete a cumplir con la institución lo establecido en este reglamento, relativo a la infraestructura de TI, sistemas de información, bases de datos, servicios de TI, seguridad de tecnología de la información, ciberseguridad y el plan de recuperación ante desastres; y,

e) Acuerdos de niveles de servicio.

Lo establecido en este artículo, es sin perjuicio del cumplimiento de lo indicado en los artículos 32 y 33 de este reglamento.".

"CAPÍTULO VIII
DISPOSICIONES TRANSITORIAS Y FINALES"

"Artículo 35. Transitorio. Las instituciones deberán enviar a la Superintendencia de Bancos el manual de administración del riesgo tecnológico actualizado y su plan de recuperación ante desastres, dentro de los cinco (5) días siguientes a la entrada en vigencia de la presente modificación.".

"Artículo 36. Transitorio. La designación del Oficial de Seguridad de la Información establecida en la literal d) del artículo 4; la implementación del Centro de Operaciones de Seguridad Cibernética establecida en el artículo 23; y, la organización del Equipo de Respuesta de Incidentes Cibernéticos establecido en el artículo 26, de este reglamento, deberá realizarse a más tardar el 4 de enero de 2021.".

"Artículo 37. 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 la institución de cumplir con otras disposiciones legales o normativas aplicables.".

"Artículo 38. Casos no previstos. Los casos no previstos en este reglamento serán resueltos por la Junta Monetaria, previo informe de la Superintendencia de Bancos.".

2. 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 seis meses después de su publicación.

BANCO DE GUATEMALA - Junta Monetaria - GUATEMALA, C. A.

Romeo Augusto Archila Navarro
Secretario
Junta Monetaria

(192864-2)-24-abril