JUNTA MONETARIA
RESOLUCIÓN JM-102-2011

Inserta en el Punto Cuarto del Acta 32-2011, correspondiente a la sesión celebrada por la Junta Monetaria el 17 de agosto de 2011.

PUNTO CUARTO: Superintendencia de Bancos eleva a consideración de la Junta Monetaria el proyecto de Reglamento para la Administración del Riesgo Tecnológico.

RESOLUCIÓN JM-102-2011. Conocido el Oficio No. 3881-2011 del Superintendente de Bancos, del 10 de agosto de 2011, mediante el cual eleva a consideración de esta Junta el proyecto de Reglamento para la Administración del Riesgo Tecnológico.

LA JUNTA MONETARIA:

CONSIDERANDO: Que para el desarrollo normal de sus actividades, las entidades del sistema financiero supervisado dependen en alto grado del uso de tecnología de la información por lo que se hace necesario gestionar adecuadamente el riesgo tecnológico para asegurar la integridad, disponibilidad, confidencialidad de la información, así como la continuidad de la prestación de sus servicios; **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 de conformidad con buenas prácticas a nivel internacional es conveniente que los bancos, las sociedades financieras, las entidades fuera de plaza o entidades off shore, así como las empresas especializadas en servicios financieros que forman parte de grupos financieros, cuenten con lineamientos mínimos que deben observar a fin de llevar a cabo una adecuada administración del riesgo tecnológico, con el objetivo de mitigar el riesgo de pérdidas financieras ocasionadas por la materialización de dicho riesgo,

POR TANTO:

Con fundamento en lo dispuesto en los artículos 132 y 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, así como tomando en cuenta el Oficio No. 3881-2011 del Superintendente de Bancos, del 10 de agosto de 2011,

RESUELVE:

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

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 el 1 de septiembre de 2011.

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

Armando Felipe García Salas Alvarado
Secretario
Junta Monetaria

ANEXO A LA RESOLUCIÓN JM-102-2011

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, 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:

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.

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.

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.

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, provoque pérdidas financieras 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.

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 VI 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) Continuidad de operaciones de tecnología de la información; y,

d) 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 continuidad de operaciones de TI, 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; y,

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.

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 continuidad de operaciones de TI;

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 continuidad de operaciones de TI 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 continuidad de operaciones de TI a que se refiere el artículo 20 de este reglamento y su plan de pruebas descrito en el artículo 21;

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 continuidad de operaciones de TI 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;

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 y el recurso humano relacionado;

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 8. 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 9. 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 10. 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 11. Inventarios de infraestructura de TI, sistemas de información y de bases de datos. 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 12. 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 13. Monitoreo de la infraestructura de TI, sistemas de información y bases de datos. 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; y,

2. Contratación, considerando la suscripción y ejecución.

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 incidentes presentados por los usuarios;

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 16. 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 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 los sistemas de información y de los 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. Pruebas periódicas para detectar vulnerabilidades en la infraestructura de TI, los sistemas de información y las bases de datos.

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 la estrategia institucional para la continuidad de operaciones; 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;

b) Medidas de seguridad en el intercambio de información a través de los canales electrónicos. Cualquier intercambio de información sensible debe estar respaldado por un certificado digital, cifrado de datos u otro mecanismo que permita garantizar la transferencia de información;

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

d) Registro y bitácoras de las transacciones efectuadas.

CAPÍTULO V
CONTINUIDAD DE OPERACIONES DE TECNOLOGÍA DE LA INFORMACIÓN

Artículo 20. Plan de continuidad de operaciones de TI. Las instituciones deberán contar con un plan de continuidad de operaciones de TI, que esté alineado a las necesidades de la institución, para recuperar los procesos críticos de las principales líneas de negocio soportados por TI, así como la información asociada en caso de una interrupción.

El plan de continuidad de operaciones de TI deberá incluir, como mínimo, los aspectos siguientes:

a) Objetivo y alcance del plan;

b) Identificación de los procesos críticos de las principales líneas de negocio;

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

d) Procedimientos y canales de comunicación;

e) Procedimientos de recuperación y restauración de operaciones y procesos críticos;

f) Identificación y descripción de responsabilidades del personal clave para la continuidad de operaciones de TI y listado de proveedores;

g) Recursos necesarios para la recuperación;

h) Convenios documentados con terceros; e,

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.

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

Las modificaciones al plan de continuidad de operaciones de TI deberán ser comunicadas a la Superintendencia de Bancos dentro de los diez (10) días hábiles siguientes a su aprobación.

Artículo 21. Pruebas al plan de continuidad de operaciones de TI. Las instituciones deberán elaborar como parte del plan de continuidad de TI 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 continuidad de operaciones de TI en función de los resultados obtenidos.

Artículo 22. Capacitación del personal clave para la continuidad de operaciones de TI. Las instituciones deberán mantener capacitado al personal clave, a que se refiere el inciso f) del artículo 20 de este reglamento, para activar o probar el plan de continuidad de operaciones de TI y sus modificaciones.

Artículo 23. 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 VI
PROCESAMIENTO DE INFORMACIÓN Y TERCERIZACIÓN

Artículo 24. 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 capacitado 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, capacitados 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 25. Tercerización. 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 y continuidad de operaciones de tecnología de la información; y,

e) Acuerdos de niveles de servicio.

Lo establecido en este artículo, es sin perjuicio del cumplimiento de lo indicado en los artículos 23 y 24 de este reglamento.

CAPÍTULO VII
DISPOSICIONES TRANSITORIAS Y FINALES

Artículo 26. Transitorio. Las instituciones que al momento del inicio de vigencia de este reglamento se encuentren operando, deberán presentar a la Superintendencia de Bancos un plan de implementación aprobado por el Consejo, para ajustarse a las disposiciones de esta normativa, dentro de los seis (6) meses siguientes a la fecha en que cobre vigencia el mismo.

La ejecución del plan indicado en el párrafo anterior, no deberá exceder de veinticuatro (24) meses contados a partir de vencido el plazo para la entrega de dicho plan.

Artículo 27. Transitorio. Las instituciones deberán enviar a la Superintendencia de Bancos el manual de administración del riesgo tecnológico y el plan de continuidad de operaciones de TI, dentro de los cinco (5) días siguientes de vencido el plazo para la ejecución del plan indicado en el artículo 26.

Artículo 28. 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.

Artículo 29. Casos no previstos. Los casos no previstos en este reglamento serán resueltos por la Junta Monetaria, previo informe de la Superintendencia de Bancos.

(195474-2)-26-agosto