

## PUBLICACIONES VARIAS

### 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 1 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 secretaria 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

#### 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.