RESUMEN DE NORMA · CERT.GT

Normativa de la SIB sobre riesgo tecnológico

Versión 1.0 · Revisado el 11 oct 2026 · TLP:CLEAR · Para: Bancos, sociedades financieras y demás entidades supervisadas, y sus proveedores de tecnología.

La Junta Monetaria emitió el Reglamento para la Administración del Riesgo Tecnológico (Resolución JM-102-2011), que la Superintendencia de Bancos supervisa. Establece lo mínimo que las entidades financieras deben hacer para gestionar los riesgos de su tecnología. En 2021 se reformó (Resolución JM-104-2021) para incorporar la ciberseguridad.

A quién aplica

- A las entidades supervisadas por la Superintendencia de Bancos que el reglamento enumera, entre ellas bancos y sociedades financieras.
- De forma indirecta, a sus proveedores: la entidad sigue siendo responsable de los servicios de tecnología que contrata.

Qué pide, en términos generales

Organización	Responsabilidades definidas para el consejo de administración, el comité de gestión de riesgos y la unidad de administración de riesgos.
Políticas y manual	Políticas y procedimientos aprobados por el consejo y reunidos en un manual de administración del riesgo tecnológico.
Infraestructura y sistemas	Inventario, planificación y gestión de la infraestructura de TI, los sistemas de información y las bases de datos.
Seguridad de TI	Gestión de la seguridad de la información: accesos, clasificación, registros, respaldos y seguridad física.
Ciberseguridad	Desde la reforma de 2021: funciones y responsables específicos, monitoreo, y capacidad de respuesta a incidentes cibernéticos.
Continuidad	Plan de continuidad de operaciones de TI, sitio alterno y pruebas periódicas.
Servicios de terceros	Condiciones para contratar servicios y para procesar información fuera de las instalaciones o del país.

Cómo prepararte para una revisión

- Ten a la mano el manual vigente, con la fecha de aprobación del consejo.
- Conserva evidencia de que los controles operan: bitácoras, actas del comité, resultados de pruebas.
- Documenta las pruebas del plan de continuidad y lo que se corrigió después.
- Mantén actualizado el inventario de proveedores de tecnología y sus contratos.
- Registra los incidentes, su análisis y las acciones tomadas.

Cómo se relaciona con otros marcos

- ISO 27001 cubre buena parte de lo que pide el reglamento en seguridad de TI y aporta la estructura del sistema de gestión.
- NIST CSF sirve para ordenar las capacidades de ciberseguridad que incorporó la reforma.
- PCI DSS aplica además a las entidades que emiten o procesan tarjetas.

Advertencia

- Este es un resumen orientativo y no cita artículos. Las obligaciones exactas, los plazos y las entidades alcanzadas están en el texto de las resoluciones.
- Verifica si existen reformas posteriores a la fecha de revisión de este documento.
- Para decisiones de cumplimiento, consulta a tu área legal o directamente a la SIB.

Texto oficial

Resoluciones JM-102-2011 y JM-104-2021 de la Junta Monetaria. Consulta siempre el texto vigente en sib.gob.gt.

cert.gt es una iniciativa privada y comunitaria de Devel Group.

cert.gt · devel.group · Reporta un incidente en cert.gt/reportar o a incidentes@cert.gt

Resumen elaborado por cert.gt con fines educativos; no es el texto oficial de la norma ni sustituye asesoría legal o de cumplimiento. No es un documento de una entidad gubernamental. Puedes copiarlo y adaptarlo citando la fuente (CC BY 4.0).