Boletín Fiscal
Noviembre 2026, No. 23-2026



LEY MARCO DE CIBERSEGURIDAD

Con fecha 17 de noviembre de 2026, fue publicada en el Diario Oficial la Ley Marco de Ciberseguridad, Decreto No. 26-2026 del Congreso de la República de Guatemala. A continuación, un breve resumen:

La ley tiene como finalidad crear el marco institucional, administrativo, penal y procesal para prevenir, detectar, responder e investigar amenazas, incidentes y delitos informáticos en Guatemala. Asimismo, establece mecanismos de coordinación nacional e internacional y fortalece las capacidades del Estado en materia de ciberseguridad.

➢ Objetivos principales

La ley declara la ciberseguridad como asunto de interés nacional y busca:

- Crear la institucionalidad especializada en ciberseguridad.
- Proteger infraestructuras críticas y servicios esenciales.
- Regular la gestión de incidentes cibernéticos.
- Establecer delitos informáticos y sus sanciones.
- Fortalecer la cooperación internacional.
- Desarrollar capacidades técnicas y de investigación en el Estado.

➢ Nueva institucionalidad

La ley crea una estructura nacional integrada por:

- Consejo Nacional de Ciberseguridad (CONCIBER) como órgano rector estratégico.
- Ministerio de Gobernación como ente rector sectorial.
- Dirección Nacional de Ciberseguridad (DICIBER) como órgano técnico-operativo especializado.

Además, se crea el Centro de Respuesta a Incidentes de Ciberseguridad de Guatemala (CRIC-GT), encargado de monitorear, detectar y responder a incidentes y ataques cibernéticos.

➢ Coordinación nacional de respuesta

La ley establece un sistema nacional de respuesta a incidentes mediante:

- CRIC-GT.
- Equipos institucionales de respuesta en entidades públicas.
- Equipos de respuesta en sectores estratégicos privados.
- Oficiales de Seguridad de la Información.

Se impone la obligación de reportar incidentes significativos:

- En 3 horas cuando afecten infraestructura crítica.
- En 6 horas para otros incidentes relevantes.
- Presentar informe completo en un máximo de 72 horas.

➢ Niveles de respuesta ante incidentes

La ley establece cuatro niveles de actuación:

- Nivel 1: incidente institucional.
- Nivel 2: incidente crítico institucional.
- Nivel 3: incidente crítico nacional con impacto multisectorial.
- Nivel 4: incidente que afecte la soberanía nacional.

En los niveles 3 y 4, el Consejo Nacional de Ciberseguridad actúa como Comité de Crisis.

➢ Ciberdefensa

Se asignan funciones específicas al Ministerio de la Defensa Nacional para:

- Proteger infraestructuras críticas vinculadas a la defensa nacional.
- Elaborar el Catálogo de Infraestructuras Críticas Digitales.
- Desarrollar protocolos de acciones defensivas y ofensivas de ciberdefensa.
- Cooperar con DICIBER y CRIC-GT.

La ley establece expresamente que estas funciones deben respetar las garantías constitucionales.

➢ Régimen administrativo sancionador

Se establecen obligaciones para operadores de servicios esenciales y administradores de sistemas críticos, entre ellas:

- Implementar medidas de protección de datos y sistemas.
- Gestionar adecuadamente los riesgos cibernéticos.
- Cumplir estándares internacionales y buenas prácticas.

Las infracciones se clasifican en: leves, graves y gravísimas.

➢ Delitos informáticos creados por la ley

La ley tipifica varios ciberdelitos:

Delito	Pena de prisión
Acceso ilícito	4 a 6 años
Interceptación ilícita	5 a 8 años
Ataque a la integridad de datos	5 a 7 años
Ataque a la integridad de sistemas	5 a 8 años
Falsificación informática	2 a 6 años
Apropiación de identidad ajena	2 a 4 años (hasta 6 años en casos agravados)
Fraude informático	4 a 8 años
Abuso de dispositivos	3 a 6 años

Las penas aumentan cuando los hechos afectan información sensible, generan beneficios ilícitos o perjudican infraestructuras críticas digitales.

➢ Responsabilidad de personas jurídicas

Las empresas utilizadas para cometer ciberdelitos podrán recibir:

- Multas entre Q100,000 y Q300,000.
- Suspensión de patentes y permisos.
- Inhabilitación para contratar con el Estado.
- Comiso de bienes.
- Publicación de la sentencia.
- Cancelación de personalidad jurídica en caso de reincidencia.

➢ Investigación y prueba digital

La ley regula:

- Conservación urgente de datos.
- Órdenes judiciales para acceso a información.
- Registros informáticos.
- Aseguramiento digital de evidencia.
- Interceptación de comunicaciones bajo control judicial.
- Cadena de custodia y pruebas digitales.

➢ Cooperación internacional

Se fortalece la cooperación internacional mediante:

- Extradición por ciberdelitos.
- Preservación transfronteriza de datos.
- Intercambio de información.
- Asistencia jurídica internacional.
- Reconocimiento de pruebas digitales obtenidas en el extranjero.

➢ Fortalecimiento institucional

La ley ordena:

- Crear una Fiscalía Especializada en ciberdelitos en el Ministerio Público.
- Implementar la Red 24/7 de cooperación internacional.
- Fortalecer al INACIF, Policía Nacional Civil, Defensa Pública Penal y Ministerio de la Defensa.
- Crear órganos jurisdiccionales especializados.

➢ Educación y cultura de ciberseguridad

El Ministerio de Educación deberá incorporar contenidos de ciberseguridad en el sistema educativo nacional y promover una cultura de uso seguro del entorno digital.

La Ley Marco de Ciberseguridad constituye el primer marco integral de Guatemala para la gestión de riesgos digitales, protección de infraestructuras críticas, persecución de los ciberdelitos y fortalecimiento institucional. Su eje central es la creación del sistema nacional de ciberseguridad liderado por el Consejo Nacional de Ciberseguridad, la Dirección Nacional de Ciberseguridad y el CRIC-GT, complementado con un catálogo de delitos informáticos, mecanismos de cooperación internacional y normas especiales para la investigación y obtención de evidencia digital.

La Ley entrará en vigencia el 17 de diciembre de 2026

Para mayor información puede comunicarse a nuestras oficinas

Mario Salazar mario.salazar@gt.Andersen.com
Evelyn Guerra evelyn.guerra@gt.Andersen.com
Fernando Pérez fernando.perez@gt.Andersen.com