Estudio de legislación comparada sobre ciberseguridad

GUATEMALA
GUATEMALA NO SE DETIENE

“Estudio de legislación comparada sobre Ciberseguridad”

6 de junio 2025

Presentado por
Sylvia Maria Campos Verdesia

Contenido

Listado de Acrónimos y Significados

Acrónimo	Significado
AGESIC	Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (Uruguay)
ANCI	Agencia Nacional de Ciberseguridad (Chile)
ANTD	Agencia Nacional de Transformación Digital
CCN-CERT	Centro Criptológico Nacional – Equipo de Respuesta a Incidentes de Seguridad (España)
CEPAL	Comisión Económica para América Latina y el Caribe
CERT	Computer Emergency Response Team
CERT-EE	Computer Emergency Response Team de Estonia
CERT-MX	Centro de Respuesta a Incidentes Cibernéticos de México
CNI	Centro Nacional de Inteligencia (México)
CNPIC	Centro Nacional para la Protección de las Infraestructuras Críticas (España)
CSIRT	Computer Security Incident Response Team
CSIRT-CR	Centro de Respuesta a Incidentes de Seguridad Informática de Costa Rica
EEUU	Estados Unidos
INCIBE	Instituto Nacional de Ciberseguridad de España
INCIBE-CERT	CSIRT nacional para ciudadanos y empresas (España)
INCIBE-GT	Instituto Nacional de Ciberseguridad de Guatemala (INCIB-GT)
MICITT	Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Costa Rica)
NIS	Network and Information Security (Directiva NIS de la UE)
OCDE	Organización para la Cooperación y el Desarrollo Económicos
OEA	Organización de los Estados Americanos
ONU	Organización de las Naciones Unidas
PIC	Protección de Infraestructuras Críticas
RGPD	Reglamento General de Protección de Datos (UE)
RIA	Autoridad del Sistema de Información (Estonia)
SEDENA	Secretaría de la Defensa Nacional (México)
SIT	Superintendencia de Telecomunicaciones (Guatemala)
TIC	Tecnologías de la Información y la Comunicación
UE	Unión Europea
UIT	Unión Internacional de Telecomunicaciones

1. Resumen Ejecutivo

Este estudio ofrece un análisis técnico y comparado de marcos legales, modelos de gobernanza y prácticas institucionales en materia de ciberseguridad en países seleccionados, con el fin de proporcionar insumos sustantivos para la formulación de una Ley Marco de Ciberseguridad en Guatemala. A través del examen de los casos de España, Chile, México, Colombia, Uruguay, Costa Rica y Estonia -así como de los lineamientos de organismos internacionales (OCDE, OEA, UIT, Unión Europea)-, se identifican elementos comunes de éxito, riesgos frecuentes y principios estructurales para una gobernanza eficaz.

Los hallazgos muestran que los países con leyes específicas o estrategias nacionales robustas, entes rectores especializados, CSIRTs funcionales, coordinación interinstitucional efectiva y mecanismos de cooperación público-privada han logrado mayores niveles de resiliencia y protección de sus activos digitales. En contraste, los modelos fragmentados, sin jerarquía institucional ni recursos sostenibles, presentan graves debilidades frente a amenazas cibernéticas complejas.

Entre los países analizados, algunos han optado por leyes marco de ciberseguridad (como España, Chile y Estonia), mientras que otros operan bajo estrategias nacionales (como Uruguay, Colombia y México), con distintos niveles de consolidación institucional y eficacia operativa. La existencia de un marco normativo no garantiza por sí sola la resiliencia cibernética: la articulación institucional, el financiamiento sostenido, la supervisión efectiva y la participación multisectorial son condiciones decisivas para su implementación exitosa.

En función de estas lecciones, se recomienda que Guatemala adopte una ley integral que defina principios rectores como legalidad, responsabilidad compartida, cooperación multisectorial, prevención, resiliencia y flexibilidad tecnológica. Esta ley debe establecer obligaciones diferenciadas para entidades públicas y operadores críticos, crear un sistema de notificación y respuesta a incidentes, y proteger legalmente las infraestructuras críticas digitales.

Se propone la creación de una **Instituto Nacional de Ciberseguridad de Guatemala (INCIB-GT)**, con autonomía técnica, mandato legal, presupuesto propio y capacidad de coordinación estratégica. También se sugiere establecer un **Consejo Nacional de Ciberseguridad** de carácter consultivo e intersectorial, así como un **Sistema Nacional de Respuesta a Incidentes** liderado por un CSIRT nacional y complementado por CSIRT sectoriales bajo un modelo federado.

Además, se plantea la necesidad de articular la ciberseguridad con la transformación digital del Estado, la protección de datos personales, la defensa nacional, las telecomunicaciones y la gestión de infraestructuras críticas, a través de mecanismos de cooperación formalizados y protocolos operativos. La legislación deberá también garantizar un equilibrio entre la protección de infraestructuras críticas y el respeto de los derechos fundamentales en el entorno digital.

Finalmente, se enfatiza que el éxito normativo dependerá de la voluntad política, la asignación presupuestaria, la formación de capacidades técnicas, la participación multisectorial y la evaluación continua. El documento incluye además un análisis preliminar de costos de implementación y una evaluación de riesgos estratégicos, con propuestas de mitigación adaptadas al contexto guatemalteco.

La ciberseguridad no es únicamente un reto tecnológico, sino una política pública de Estado que debe integrarse al desarrollo nacional y a la confianza digital del país.

2. Introducción

En el contexto actual de acelerada transformación digital, la ciberseguridad se ha convertido en un componente estratégico para la protección del funcionamiento del Estado, la economía, los derechos fundamentales y la seguridad nacional. Las crecientes amenazas cibernéticas -desde el robo de información hasta los ataques a infraestructuras críticas- afectan por igual a gobiernos, empresas y ciudadanos, y demandan respuestas normativas integrales, coordinadas y actualizadas.

Guatemala avanza en procesos de digitalización del Estado, incorporación de servicios públicos en línea, interconexión de datos y adopción de sistemas electrónicos de pago. Sin embargo, esta evolución tecnológica incrementa la exposición del país a incidentes cibernéticos que podrían comprometer sectores clave como salud, justicia, energía, telecomunicaciones y seguridad pública. Esta situación revela una necesidad urgente: contar con un marco legal robusto en materia de ciberseguridad, alineado con estándares internacionales y adaptado a las particularidades institucionales y sociales del país.

Actualmente, Guatemala no cuenta con una ley integral de ciberseguridad. Las normativas existentes, como la Ley de Acceso a la Información Pública (Decreto 57-2008) y regulaciones de la Superintendencia de Telecomunicaciones (SIT), abordan aspectos parciales relacionados con la protección de datos y la infraestructura de telecomunicaciones, pero no establecen un marco sistemático para la prevención, detección y respuesta a ciberincidentes. Además, la falta de coordinación entre instituciones como el Ministerio de Gobernación, el Ministerio de la Defensa Nacional y la Secretaría de Planificación y Programación de la Presidencia (SEGEPLAN), entre otras instituciones, genera vacíos operativos y limitaciones en la capacidad de respuesta ante amenazas cibernéticas. Este contexto subraya la necesidad de una ley marco que articule esfuerzos y fortalezca la resiliencia digital del país.

Este estudio tiene como propósito brindar un análisis comparado de legislaciones y marcos normativos de ciberseguridad, con énfasis en tres aspectos fundamentales: los conceptos clave que deben estar presentes en cualquier ley de ciberseguridad, el contenido normativo mínimo, y los modelos institucionales de gobernanza adoptados por distintos países. Su objetivo es proporcionar insumos técnicos y jurídicos que respalden la toma de decisiones legislativas bien fundamentadas, tanto para la formulación de una nueva ley como para la mejora del marco vigente.

El análisis incluye la revisión de marcos legales y estrategias nacionales en países seleccionados por su diversidad institucional y nivel de avance digital -como España, Chile, México, Colombia, Uruguay, Costa Rica y Estonia-, así como lineamientos de organismos internacionales como la OCDE, la OEA, la Unión Europea, la UIT y las Naciones Unidas. El estudio incorpora también el análisis del contexto guatemalteco, sus instituciones, capacidades actuales y desafíos específicos.

Este documento no busca imponer un modelo único, sino presentar alternativas viables, buenas prácticas y elementos esenciales que deben considerarse al legislar sobre ciberseguridad, con miras a fortalecer la resiliencia del país y avanzar hacia una Guatemala más segura y preparada ante los desafíos del entorno digital.

2.1 Contexto de ciberseguridad en Guatemala

Guatemala enfrenta un entorno de creciente digitalización, con avances en servicios públicos en línea, interconexión de datos gubernamentales y adopción de sistemas electrónicos en sectores como salud, justicia y finanzas. Sin embargo, esta transformación incrementa la exposición a riesgos cibernéticos, en un contexto donde las capacidades institucionales y normativas son limitadas. Actualmente, el país no cuenta con una ley integral de ciberseguridad, y las normativas existentes, como la Ley de Acceso a la

Información Pública (Decreto 57-2008) y regulaciones de la Superintendencia de Telecomunicaciones (SIT), solo abordan aspectos parciales, como la protección de datos o la seguridad de redes de telecomunicaciones.

Entre los desafíos identificados se encuentran:

- **Fragmentación institucional**: La ausencia de un ente rector especializado genera descoordinación entre instituciones clave, como el Ministerio de Gobernación, el Ministerio de la Defensa Nacional y la Secretaría de Planificación y Programación de la Presidencia (SEGEPLAN).
- **Brecha digital**: Según datos de la Unión Internacional de Telecomunicaciones (UIT, 2023), solo el 51% de la población guatemalteca tiene acceso a internet, con disparidades significativas entre áreas urbanas y rurales, lo que limita la adopción de prácticas de ciberseguridad.
- **Capacidades técnicas limitadas**: La falta de personal especializado en ciberseguridad en el sector público y privado, junto con una infraestructura tecnológica heterogénea, reduce la capacidad de respuesta ante incidentes.
- **Incidentes cibernéticos**: Aunque no se han reportado públicamente ataques de la magnitud del ransomware Conti en Costa Rica (2022), Guatemala ha enfrentado incidentes como intentos de phishing dirigidos a instituciones públicas y filtraciones de datos en plataformas gubernamentales, lo que evidencia vulnerabilidades estructurales.

Estos factores subrayan la necesidad de un marco normativo que no solo adopte estándares internacionales, sino que también considere las particularidades del contexto guatemalteco, como la heterogeneidad tecnológica, las limitaciones presupuestarias y la necesidad de fortalecer la alfabetización digital. Este análisis busca proporcionar a los legisladores un punto de partida para evaluar cómo los modelos internacionales podrían adaptarse a estas realidades.

2.2 Importancia estratégica de la ciberseguridad

La ciberseguridad se ha consolidado como un pilar esencial para el desarrollo sostenible, la estabilidad institucional y la protección de los derechos fundamentales en la era digital. En un entorno global marcado por la creciente interdependencia tecnológica, las amenazas cibernéticas no solo afectan la infraestructura digital, sino también la economía, la seguridad nacional, la democracia y la confianza ciudadana.

Ataques dirigidos a servicios públicos, filtraciones de datos personales, ciberextorsión, desinformación y sabotaje digital son manifestaciones de un fenómeno complejo, en expansión y con implicaciones estructurales. En este contexto, contar con un marco normativo integral no es una medida opcional, sino una condición para garantizar la continuidad institucional, la soberanía digital y la protección efectiva de la población.

2.3 Referentes internacionales

Diversos organismos multilaterales han establecido principios y estándares para orientar la formulación de políticas y marcos normativos de ciberseguridad. Entre ellos destacan la OCDE, la OEA, la Unión Europea (a través de las Directivas NIS y NIS2), la UIT y las Naciones Unidas. Estos coinciden en la necesidad de promover marcos legales claros, instituciones especializadas, mecanismos de cooperación público-privada y una cultura nacional de ciberseguridad.

Asimismo, países como España, Chile, Colombia, Estonia y Uruguay han adoptado modelos normativos que integran dimensiones técnicas, organizativas y estratégicas. Sus experiencias ofrecen lecciones valiosas que pueden ser adaptadas por países en desarrollo como Guatemala.

2.4 Justificación de una ley nacional

Guatemala no cuenta actualmente con una ley integral de ciberseguridad que regule de forma sistemática la prevención, detección, respuesta y recuperación frente a incidentes cibernéticos. Aunque existen esfuerzos institucionales y normas sectoriales en ámbitos específicos, el país carece de un marco legal que defina competencias claras, articule a los actores públicos y privados, establezca estándares de seguridad, y asegure la protección de infraestructuras críticas digitales.

La creciente digitalización de servicios y la dependencia tecnológica de sectores estratégicos amplifican esta vulnerabilidad estructural. En este escenario, una ley nacional de ciberseguridad permitiría fortalecer la resiliencia del país, clarificar responsabilidades institucionales, promover la confianza digital y cumplir con compromisos internacionales en la materia.

2.5 Enfoque metodológico del estudio

Este estudio realiza un análisis comparado de marcos normativos y modelos de gobernanza en materia de ciberseguridad, tomando como referencia una muestra de países que representan distintos niveles de madurez institucional y digital. La revisión comprende leyes, estrategias nacionales, estructuras institucionales y experiencias de implementación.

El análisis se organiza en torno a tres ejes: a) los conceptos clave y definiciones comunes en los marcos legales; b) el contenido mínimo que debe contemplar una ley moderna de ciberseguridad; y c) los modelos de gobernanza institucional, incluyendo entes rectores, centros de respuesta a incidentes (CSIRT o CERT) y esquemas de coordinación interinstitucional. La finalidad es proporcionar una base técnica comparada que oriente la formulación de una legislación eficaz, pertinente y coherente con las necesidades nacionales y los estándares internacionales.

3. Marco Teórico

3.1 Definición

La ciberseguridad se entiende como el conjunto de políticas, medidas técnicas, organizativas y legales orientadas a proteger los sistemas de información, redes digitales, servicios electrónicos, y los datos que en ellos se procesan o almacenan, frente a accesos no autorizados, daños, interrupciones o manipulaciones. Su finalidad es garantizar la **confidencialidad, integridad, disponibilidad y resiliencia** de los activos digitales, especialmente aquellos esenciales para el funcionamiento del Estado y la sociedad.

La Unión Internacional de Telecomunicaciones (UIT) define la ciberseguridad como "*la preservación de la disponibilidad, integridad y confidencialidad de la información en el ciberespacio*"[1]. La OCDE[2] y la OEA[3] han señalado que la ciberseguridad requiere un enfoque multiactor y multisectorial, que no se limita a la tecnología, sino que abarca gobernanza, cooperación y políticas públicas.

[1] UIT (2014). *Glosario de Ciberseguridad*.
[2] OCDE (2015). *Recomendación del Consejo sobre la seguridad digital para la prosperidad económica y social*.
[3] OEA (2020). *Guía de estrategias nacionales de ciberseguridad en las Américas*.

3.2 Activos críticos y sistemas esenciales

Los activos críticos son aquellos sistemas, infraestructuras o procesos cuya interrupción o destrucción tendría un impacto significativo en la seguridad, la economía o los servicios esenciales de un país. Estos activos incluyen los sectores de salud, energía, transporte, agua, telecomunicaciones, finanzas y los servicios gubernamentales digitales.

La Directiva NIS de la Unión Europea (2016/1148) y su versión actualizada NIS2 (2022/2555)4 introducen el concepto de entidades esenciales que prestan servicios fundamentales para la sociedad, y establecen obligaciones específicas de seguridad y notificación de incidentes. El Modelo de Madurez en Ciberseguridad de la OEA también destaca la necesidad de identificar y proteger infraestructuras críticas como parte de una estrategia nacional[5].

3.3 Amenazas y riesgos cibernéticos (tipología y actores)

Las amenazas cibernéticas son acciones o condiciones que pueden explotar vulnerabilidades en los sistemas digitales y generar impactos negativos. Entre las más frecuentes están:

- Malware (software malicioso)
- Ransomware (secuestro de datos a cambio de rescate)
- Ataques DDoS (denegación de servicios)
- Phishing (suplantación de identidad para robar información)
- Intrusiones a sistemas críticos por actores estatales o no estatales

Según el Informe de Riesgos Globales del Foro Económico Mundial 20236 , los ciberataques se ubican entre las amenazas más probables y con mayor impacto para los próximos años. La creciente sofisticación de los actores maliciosos -incluyendo organizaciones criminales, hacktivistas[7] y actores estatales- exige respuestas normativas y operativas proporcionales y coordinadas.

3.4 Impacto de tecnologías emergentes en la ciberseguridad

El panorama de la ciberseguridad está evolucionando rápidamente debido a la adopción de tecnologías emergentes como la inteligencia artificial (IA), el internet de las cosas (IoT), la computación en la nube y el blockchain. Estas tecnologías ofrecen oportunidades para la innovación, pero también introducen nuevos riesgos que requieren marcos normativos adaptativos. Los países analizados han comenzado a abordar estos desafíos de manera diferenciada:

- **Estonia**: Su Ley de Ciberseguridad (2018) incluye disposiciones para evaluar riesgos asociados con tecnologías disruptivas, como el uso de blockchain en servicios de identidad digital (e-Residency). El CSIRT nacional (CERT-EE) realiza análisis periódicos de amenazas emergentes, incluyendo ataques basados en IA.
- **España**: La Estrategia Nacional de Ciberseguridad 2023 incorpora lineamientos para mitigar riesgos en IoT y computación en la nube, con énfasis en la seguridad de dispositivos conectados en sectores críticos como salud y energía.

[4] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo (NIS2).
[5] OEA (2021). *Modelo de madurez en ciberseguridad*
[6] Foro Económico Mundial (WEF) (2023). *Global Risks Report 2023*.
[7] El hacktivista es aquella persona que se aprovecha de sus conocimientos en la rama de la tecnología y la informática para detectar vulnerabilidades en equipos y sistemas, con el objetivo de penetrar en ellos y reivindicar alguna causa social o política.

- **Chile**: La Ley Marco de Ciberseguridad (2023) establece principios de flexibilidad tecnológica, permitiendo al ente rector actualizar estándares técnicos para abordar amenazas emergentes, como el uso malicioso de IA en ataques de ingeniería social.
- **Unión Europea (Directiva NIS2)**: Exige a los operadores críticos implementar medidas de seguridad para dispositivos IoT y servicios en la nube, además de fomentar la investigación en ciberseguridad para anticipar riesgos futuros.
- **Costa Rica, Colombia y México**: Aunque sus marcos normativos no abordan explícitamente estas tecnologías, han iniciado programas de capacitación para preparar a sus CSIRT ante amenazas relacionadas con IA y big data.

La experiencia internacional sugiere que los marcos legales deben ser tecnológicamente neutros y prever mecanismos de actualización periódica para adaptarse a la evolución de las amenazas. Esto incluye la colaboración con el sector privado y la academia para identificar riesgos emergentes y desarrollar estándares técnicos adecuados.

3.5 Relación con transformación digital, protección de datos y defensa nacional

La ciberseguridad está conectada con otras dimensiones estratégicas del desarrollo estatal:

- **Transformación digital**: Un entorno digital seguro es condición habilitante para procesos de gobierno electrónico, identidad digital, servicios en línea y plataformas interoperables. La CEPAL[8] ha subrayado que sin confianza digital no es posible una transformación digital sostenible.
- **Protección de datos personales**: La ciberseguridad garantiza que los datos personales sean almacenados y tratados de forma segura, reduciendo los riesgos de fuga, robo o manipulación. Esto es clave para la efectividad de leyes de protección de datos y derechos digitales[9].
- **Infraestructura crítica**: Las infraestructuras esenciales para el funcionamiento del país -como la energía, las telecomunicaciones, la salud, el transporte o el suministro de agua- dependen cada vez más de sistemas digitales[10]. Su vulnerabilidad ante ataques cibernéticos las convierte en un foco prioritario para las políticas de ciberseguridad. La identificación, protección y resiliencia de estos activos debe ser un componente central de cualquier marco normativo moderno.
- **Defensa nacional**: Algunos ciberataques pueden tener impactos estratégicos comparables a amenazas militares. Por ello, países como EE. UU., Francia y Estonia integran la ciberseguridad en sus doctrinas de seguridad nacional y defensa, con participación de sus fuerzas armadas o inteligencia civil en escenarios específicos[11].

3.6 Principios rectores de la legislación en ciberseguridad

En la legislación comparada, varios principios aparecen de forma recurrente como guías para el diseño y aplicación de leyes de ciberseguridad:

- **Seguridad y resiliencia:** Capacidad del sistema nacional para prevenir, resistir y recuperarse eficazmente ante incidentes cibernéticos, garantizando la continuidad operativa de servicios esenciales.
- **Legalidad y proporcionalidad:** Toda medida en materia de ciberseguridad debe respetar el Estado de derecho, los principios democráticos y los derechos fundamentales de las personas, aplicándose con criterios de necesidad y proporcionalidad.

[8] CEPAL (2022). *Digitalización en América Latina: desafíos de la ciberseguridad*.
[9] Red Iberoamericana de Protección de Datos (2020). *Lineamientos sobre ciberseguridad y protección de datos*.
[10] De acuerdo con OEA y BID: "La protección de infraestructuras críticas debe ser parte integral de cualquier estrategia nacional de ciberseguridad, en particular ante la creciente digitalización de sectores estratégicos como energía, agua y salud."
[11] NATO (2021). *Cyber Defence Policy Update*.

- **Responsabilidad compartida:** La ciberseguridad es una responsabilidad común de los sectores público y privado, que deben asumir funciones diferenciadas[12] pero complementarias conforme a sus competencias, capacidades y niveles de exposición al riesgo.
- **Cooperación público-privada:** La colaboración entre el Estado, las empresas, la academia y la sociedad civil es esencial para la detección, prevención y respuesta efectiva frente a amenazas cibernéticas, así como para el fortalecimiento de una cultura nacional de ciberseguridad.
- **Prevención y educación:** Se debe fomentar una cultura de prevención, ciberhigiene y uso responsable de las tecnologías digitales desde la educación formal, el sector público, las empresas y la ciudadanía en general.
- **Flexibilidad tecnológica:** El marco legal y las políticas públicas deben ser adaptables a la evolución constante de las amenazas cibernéticas, los avances tecnológicos y las transformaciones del entorno digital.

Estos principios están recogidos, entre otros, en las Directrices de Buenas Prácticas de la OCDE en Seguridad Digital[13], en la Declaración de Principios de Ciberseguridad de la OEA[14], y en marcos nacionales como la Ley de Ciberseguridad de Chile 2023[15] o la Estrategia Nacional de España[16].

4. Componentes esenciales de una Ley de Ciberseguridad

Una legislación moderna en materia de ciberseguridad debe establecer con claridad el marco normativo general que regirá la protección de los sistemas digitales del Estado y de los sectores estratégicos del país. Si bien los modelos varían según el contexto institucional, existen componentes comunes que deben estar presentes para asegurar efectividad, coordinación y seguridad jurídica. A continuación se presentan los principales elementos que, con base en el derecho comparado, deberían considerarse al momento de formular una ley nacional de ciberseguridad.

4.1 Objeto, ámbito de aplicación y definiciones

Toda ley debe comenzar por precisar su objeto, es decir, la finalidad que persigue: proteger los sistemas de información, garantizar la seguridad digital, y establecer mecanismos de coordinación y respuesta frente a incidentes. Debe incluir un ámbito de aplicación claro, que normalmente cubre: entidades del sector público, operadores de servicios esenciales o infraestructuras críticas y proveedores de servicios digitales relevantes.

Además, se recomienda incorporar un glosario de definiciones clave (por ejemplo: ciberincidente, infraestructura crítica, ciberresiliencia, riesgo cibernético), a fin de evitar ambigüedades en su aplicación y asegurar una comprensión común por parte de todos los actores involucrados[17].

4.2 Principios y fines

[12] La ciberseguridad requiere una corresponsabilidad entre el sector público y el privado, cuyas funciones son complementarias pero diferenciadas. El sector público tiene el rol de establecer el marco legal y regulatorio, coordinar la gobernanza nacional, operar centros de respuesta a incidentes (CSIRT/CERT), supervisar el cumplimiento normativo, proteger infraestructuras críticas y fomentar la cooperación internacional. Además, es responsable de promover la educación y la cultura de ciberseguridad en la sociedad. Por su parte, el sector privado debe implementar medidas técnicas y organizativas para proteger sus sistemas y servicios, desarrollar soluciones tecnológicas, garantizar la continuidad operativa y la protección de datos personales, así como colaborar activamente con las autoridades mediante el reporte de incidentes, el intercambio de información y la participación en mecanismos de gobernanza multiactor. Esta colaboración público-privada es esencial para construir un ecosistema de ciberseguridad robusto, resiliente y alineado con los estándares internacionales.
[13] OCDE (2015). *Recomendación del Consejo sobre la seguridad digital para la prosperidad económica y social*.
[14] OEA (2019). *Declaración de principios de ciberseguridad*.
[15] Ley Marco de Ciberseguridad de Chile, Ley N.º 21.635 (2023).
[16] Estrategia Nacional de Ciberseguridad de España (2023).
[17] OCDE (2015). *Recomendación del Consejo sobre la Seguridad Digital para la Prosperidad Económica y Social.* Organización para la Cooperación y el Desarrollo Económicos. https://www.oecd.org/sti/ieconomy/digital-security-recommendation.htm

La ley debe fundamentarse en **principios rectores**, antes mencionados, como proporcionalidad, responsabilidad compartida, cooperación, legalidad, flexibilidad y prevención. Estos principios orientan la interpretación y aplicación de la norma y sirven de marco para la actuación de las autoridades.

En cuanto a los **fines**, se suelen incluir los siguientes: a) Proteger la integridad, disponibilidad y confidencialidad de los sistemas; b) Fortalecer la resiliencia nacional frente a amenazas cibernéticas; c) Establecer mecanismos de coordinación entre sectores; y d) Promover una cultura de ciberseguridad.

4.3 Obligaciones del sector público

La ley debe establecer obligaciones específicas para las entidades públicas, con la idea de fortalecer el comportamiento institucional y reducir vulnerabilidades dentro del propio Estado[18], como lo exige la mayoría de los estándares internacionales. Dentro de estas obligaciones se incluyen:

- Implementar políticas internas de seguridad digital.
- Designar responsables institucionales de ciberseguridad.
- Reportar incidentes de forma oportuna.
- Participar en ejercicios y auditorías nacionales.

4.4 Obligaciones del sector privado

Dado que buena parte de la infraestructura digital y de los servicios críticos está en manos del sector privado, la ley debe establecer obligaciones diferenciadas según el tipo de operador, por ejemplo: implementar medidas técnicas y organizativas adecuadas al riesgo, notificar ciberincidentes a la autoridad competente y colaborar en investigaciones o respuestas coordinadas. Estas obligaciones deben aplicarse principalmente a operadores de servicios esenciales (ej. energía, telecomunicaciones, finanzas) y a empresas con exposición digital significativa, definidas por criterios como el volumen de usuarios, el impacto potencial de un ciberincidente o la criticidad de los datos manejados. Para pequeñas y medianas empresas, se recomienda un enfoque escalonado con requisitos mínimos para no imponer cargas desproporcionadas, siguiendo el modelo de la Directiva NIS2 de la Unión Europea.

En España o Chile, estas obligaciones se aplican a entidades consideradas “esenciales” o “importantes” bajo criterios definidos por ley (por ejemplo: sector, volumen de usuarios, impacto potencial)[19].

4.5 Mecanismos de notificación y respuesta a incidentes

Un elemento clave es el establecimiento de **protocolos obligatorios de notificación** de incidentes relevantes, con plazos, canales y formatos definidos. Asimismo, debe preverse:

- La creación o fortalecimiento de un Centro Nacional de Respuesta a Incidentes (CSIRT/CERT).
- La articulación con centros sectoriales o regionales.
- Procedimientos de alerta temprana, análisis forense y recuperación de servicios.

Estos mecanismos permiten coordinar respuestas rápidas, minimizar daños y generar aprendizaje institucional ante ciberamenazas[20].

---

[18] OEA (2020). *Guía para la formulación de estrategias nacionales de ciberseguridad en las Américas.* Comité Interamericano contra el Terrorismo (CICTE), Organización de los Estados Americanos. https://www.oas.org/es/sms/cicte/documentos/GuiaCiberseguridad2020.pdf

[19] Unión Europea (2022). *Directiva (UE) 2022/2555 sobre medidas para un alto nivel común de ciberseguridad en toda la Unión (Directiva NIS2).* Diario Oficial de la UE, 14 de diciembre de 2022.

[20] ENISA (2021). *Incident Reporting in the EU: Overview of Practices.* Agencia de la Unión Europea para la Ciberseguridad. https://www.enisa.europa.eu/publications/incident-reporting-in-the-eu

4.6 Protección de infraestructuras críticas digitales

La ley debe establecer un régimen especial de **protección de infraestructuras críticas**, es decir, aquellas cuya afectación puede generar un grave impacto social, económico o institucional. Esto implica: a) Identificación y clasificación de activos críticos; b) Requisitos de seguridad reforzados; c) Auditorías periódicas y coordinación entre los operadores y el ente rector de ciberseguridad. Este enfoque está presente en países como Alemania, Chile, Colombia y México, bajo distintos modelos de gobernanza[21].

4.7 Régimen sancionatorio y responsabilidades

Toda legislación eficaz debe prever un **régimen de consecuencias** por incumplimiento de las obligaciones establecidas, que pueden incluir: a) Multas económicas proporcionales a la gravedad y reincidencia; b) Medidas correctivas u órdenes de cumplimiento; y c) Inhabilitación temporal en casos extremos. También es clave establecer claramente las **responsabilidades administrativas, civiles o incluso penales**, según corresponda. Sin sanción, no hay incentivo suficiente para cumplir, ni garantía de seguridad jurídica.

4.8 Coordinación interinstitucional

La ciberseguridad es un tema transversal que involucra a múltiples instituciones: telecomunicaciones, defensa, justicia, inteligencia, gobernanza digital, protección de datos, entre otras. Por tanto, se requiere:

- La creación de un **ente rector o coordinador nacional**.
- La definición de **mecanismos formales de coordinación** interinstitucional, como consejos nacionales, comités o redes.
- Establecer **canales de cooperación con gobiernos locales**, cuando corresponda.

La experiencia internacional demuestra que sin coordinación efectiva, los esfuerzos se fragmentan y los recursos se desperdician[22].

4.9 Participación internacional y cooperación técnica

Dado que las amenazas cibernéticas trascienden fronteras, la ley debe habilitar:

- La cooperación con organismos regionales e internacionales (OEA, UIT, Interpol, ONU).
- La adhesión a instrumentos multilaterales, convenios y mecanismos de asistencia técnica.
- La posibilidad de intercambiar información y buenas prácticas con otros países o actores relevantes.

Esto refuerza la capacidad nacional de anticipar, prevenir y responder ante amenazas complejas y coordinadas.

4.10 Medidas preventivas y de fomento de la cultura de ciberseguridad

Finalmente, una buena ley no solo reacciona ante los riesgos, sino que también **fomenta una cultura nacional de ciberseguridad** a través de:

---

[21] CEPAL (2022). *Ciberseguridad y transformación digital: desafíos y oportunidades para América Latina y el Caribe.* Comisión Económica para América Latina y el Caribe, Naciones Unidas. https://www.cepal.org/es/publicaciones/48194

[22] OCDE (2019). *Good Governance for Critical Infrastructure Protection: The Role of Risk Governance.* https://www.oecd.org/gov/risk/good-governance-critical-infrastructure.htm

- Programas de capacitación y sensibilización para funcionarios, empresas y ciudadanía.
- Inclusión de la ciberseguridad en la educación.
- Apoyo a la investigación, innovación y talento en seguridad digital.

Países como Estonia, Uruguay o España han invertido en estos componentes como parte integral de su estrategia nacional[23].

4.11 Participación ciudadana y legitimidad social

La participación ciudadana y de la sociedad civil es un componente esencial para garantizar la legitimidad y eficacia de las políticas de ciberseguridad. Los países analizados han implementado diversas estrategias para involucrar a estos actores y mitigar preocupaciones relacionadas con la privacidad y los derechos fundamentales:

- **España**: El Instituto Nacional de Ciberseguridad (INCIBE) lidera campañas de sensibilización dirigidas a ciudadanos, empresas y escuelas, como el programa “Internet Segura”. Además, se realizan consultas públicas para actualizar la Estrategia Nacional de Ciberseguridad, incorporando perspectivas de organizaciones civiles sobre protección de datos.
- **Uruguay**: AGESIC promueve la inclusión digital mediante talleres y programas educativos que integran la ciberseguridad en la alfabetización digital, con un enfoque en comunidades marginadas. La Ley de Protección de Datos Personales (18.331) refuerza la participación ciudadana al garantizar derechos digitales.
- **Estonia**: La alta digitalización del país se acompaña de una cultura de ciberseguridad promovida a través de la educación formal y campañas públicas. Organizaciones no gubernamentales participan en foros consultivos para debatir el equilibrio entre seguridad y privacidad.
- **Chile**: La Ley Marco de Ciberseguridad (2023) establece canales formales para la participación de la sociedad civil en el Consejo Nacional de Ciberseguridad, asegurando que las políticas reflejen necesidades sociales y protejan derechos fundamentales.
- **Costa Rica**: La Estrategia Nacional de Ciberseguridad incluye programas de concienciación dirigidos a ciudadanos y pequeñas empresas, con énfasis en prevenir phishing y otros ataques comunes. El proyecto de Ley 23.254 propone un consejo consultivo con representación civil.

Estas experiencias destacan la importancia de: a) campañas educativas adaptadas a diferentes públicos, b) consultas públicas para legitimar políticas, c) inclusión de organizaciones civiles en consejos asesores, y d) estrategias para equilibrar la seguridad con la protección de derechos fundamentales. Los parlamentarios pueden considerar estas prácticas al evaluar cómo fomentar la confianza ciudadana en un marco normativo de ciberseguridad.

5. Modelos de gobernanza de la Ciberseguridad

5.1 Entes rectores

Todo sistema nacional de ciberseguridad necesita un ente rector o autoridad coordinadora, encargado de liderar la formulación de políticas públicas, establecer estándares técnicos, coordinar a los actores clave, y supervisar el cumplimiento normativo. Este ente puede adoptar diversas formas, según el país:

- Una **agencia o instituto autónomo especializado** (como en Chile, bajo la nueva Ley Marco de Ciberseguridad de 2023).

[23] ENISA (2022). *National Cybersecurity Strategies: Practical Guide 2022.*

- Una **dependencia ministerial con mandato legal claro** (como el MICITT en Costa Rica o el Ministerio del Interior en España).
- Una **unidad interinstitucional de alto nivel**, en modelos más incipientes o en transición.

Sus funciones suelen incluir:

- Elaborar y actualizar la Estrategia Nacional de Ciberseguridad.
- Definir políticas de seguridad digital para el sector público.
- Coordinar la gestión de incidentes críticos.
- Representar al país en foros y acuerdos internacionales.

La independencia funcional, el respaldo político y el financiamiento sostenible son factores decisivos para el éxito de este ente rector[24].

5.2 Centros de Respuesta a Incidentes (CSIRT/CERT nacionales y sectoriales)

Los CSIRT (Computer Security Incident Response Team), también conocidos como CERT, son estructuras técnicas operativas encargadas de **detectar, analizar, contener y mitigar incidentes cibernéticos** a nivel nacional o sectorial.

Un CSIRT nacional: coordina la respuesta ante incidentes críticos; emite alertas tempranas y boletines técnicos; colabora con otros CSIRT internacionales; y apoya a entidades públicas y operadores clave ante eventos de seguridad.

Muchos países han complementado el CSIRT nacional con: CSIRT sectoriales (financiero, salud, energía) y redes federadas[25] con centros universitarios o municipales. Por ejemplo, en España, el INCIBE-CERT es el CSIRT nacional para ciudadanos y empresas, y se articula con otros centros bajo el Sistema Nacional de Ciberseguridad; y en Costa Rica, el CSIRT-CR opera bajo el MICITT, pero el proyecto de Ley 23.254 prevé fortalecerlo institucionalmente. Contar con marcos legales claros que respalden su funcionamiento, y asegurar recursos humanos y tecnológicos adecuados, es clave para su efectividad[26].

5.3 Mecanismos de coordinación público-privada

Dado que gran parte de la infraestructura digital está en manos del sector privado (telecomunicaciones, servicios financieros, tecnologías de la información), una buena gobernanza en ciberseguridad debe fomentar la cooperación estructurada con empresas y operadores críticos. Los mecanismos más comunes incluyen:

- Consejos asesores multisectoriales.
- Convenios de cooperación e intercambio de información.
- Sistemas nacionales de notificación de incidentes.
- Participación del sector privado en ejercicios nacionales de simulación.

---

[24] OCDE (2019). *Good Governance for Critical Infrastructure Protection: The Role of Risk Governance.* Organización para la Cooperación y el Desarrollo Económicos.
https://www.oecd.org/gov/risk/good-governance-critical-infrastructure.htm

[25] Una red federada de CSIRTs es un sistema distribuido y colaborativo de equipos de respuesta que, sin estar subordinados jerárquicamente entre sí, trabajan de forma coordinada y estandarizada para reforzar la ciberseguridad nacional en todos los niveles: nacional, regional, sectorial e institucional.

[26] ENISA (2021). *Incident Reporting in the EU: Overview of Practices.* Agencia de la Unión Europea para la Ciberseguridad. https://www.enisa.europa.eu/publications/incident-reporting-in-the-eu

En Chile, la ley exige a los operadores esenciales colaborar con el ente rector y notificar incidentes; en Colombia, la colaboración público-privada es parte integral de su Estrategia Nacional de Ciberseguridad; y en Uruguay, AGESIC coordina estrechamente con proveedores TIC para asegurar estándares mínimos.

5.4 Consejos nacionales o comités interinstitucionales

Para facilitar la articulación de políticas y evitar la dispersión institucional, muchos países han creado **Consejos Nacionales de Ciberseguridad**, con representación de:

- Ministerios clave (interior, defensa, tecnologías, relaciones exteriores).
- Entidades de inteligencia y seguridad.
- Organismos reguladores.
- Sector privado y sociedad civil (en algunos casos).

Estos consejos tienen funciones como: definir prioridades estratégicas, coordinar acciones en crisis cibernéticas y aprobar planes nacionales o emitir recomendaciones al ente rector.

En España, el Consejo Nacional de Ciberseguridad forma parte del Consejo de Seguridad Nacional y es presidido desde el más alto nivel político. En Costa Rica, el proyecto de ley propone un Consejo Nacional como instancia de coordinación superior con funciones consultivas y de articulación.

5.5 Supervisión, auditoría y rendición de cuentas

Una buena gobernanza requiere mecanismos de control y evaluación periódica, que aseguren el cumplimiento de obligaciones por parte de los actores públicos y privados. Las leyes suelen prever:

- Auditorías de seguridad obligatorias para entidades críticas.
- Informes anuales del ente rector al parlamento o al poder ejecutivo.
- Protocolos de evaluación de capacidades y madurez.
- Mecanismos de denuncia, monitoreo y fiscalización.

Esto permite al Estado no solo actuar frente a incidentes, sino anticiparse y corregir vulnerabilidades estructurales antes de que sean explotadas.

5.6 Financiamiento y sostenibilidad institucional

Sin recursos financieros y humanos adecuados, ninguna estructura de ciberseguridad es viable. Una gobernanza efectiva requiere prever:

- Asignaciones presupuestarias específicas.
- Fondos de emergencia ante incidentes críticos.
- Inversión continua en formación y tecnología.
- Modelos de cooperación con organismos internacionales o donantes técnicos.

La experiencia internacional muestra que muchos países han subestimado este componente, generando estructuras débiles o simbólicas. Por eso, vincular la ley de ciberseguridad con el sistema nacional de presupuesto o mecanismos de financiamiento sostenido es fundamental para su éxito operativo[27].

De acuerdo con lo mencionado en esta sección un buen modelo de gobernanza no es aquel que centraliza todo el poder en una sola entidad, sino el que define con claridad quién hace qué, cómo se coordina, qué mecanismos existen para responder, y cómo se asegura el cumplimiento y la mejora continua. Para Guatemala, esto implica no solo pensar en una ley bien estructurada, sino en una arquitectura institucional que:

- Sea realista en función de las capacidades actuales.
- Evolucione con el tiempo.
- Promueva cooperación, transparencia y confianza entre actores.
- Esté respaldada política y presupuestariamente.

6. Comparación internacional de legislaciones seleccionadas

Para garantizar una comparación útil y orientada a la toma de decisiones legislativas, se utiliza los siguientes criterios transversales:

1. Existencia y tipo de marco legal principal (ley específica, estrategia, decreto).
2. Ente rector de la ciberseguridad (tipo, ubicación institucional y nivel de jerarquía).
3. Obligaciones del sector privado y operadores críticos.
4. Gestión de incidentes y funcionamiento de CSIRT nacionales.
5. Protección de infraestructuras críticas digitales.
6. Mecanismos de coordinación interinstitucional.
7. Cooperación internacional y régimen sancionatorio.
8. Nivel de madurez institucional (capacidades, recursos y sostenibilidad).

Los países seleccionados combinan modelos avanzados y contextos regionalmente relevantes: España, Chile, México, Colombia, Uruguay, Estonia y Costa Rica.

6.1 Análisis comparado por país

España

- **Marco legal principal:** Ley 36/2015 de Seguridad Nacional; Ley 6/2021 sobre seguridad de las redes y sistemas de información; Estrategia Nacional de Ciberseguridad 2023, Directiva NIS2 (transpuesta en 2024).
- **Tipo de gobernanza:** Mixta. La Dirección General de Seguridad Nacional coordina políticamente y el Instituto Nacional de Ciberseguridad (INCIBE) ejerce funciones técnicas.
- **Obligaciones del sector privado:** Elevadas. Las entidades críticas deben aplicar medidas de seguridad, someterse a auditorías y notificar incidentes.
- **Regulación de incidentes y CSIRT:** Establecida por ley. Existen múltiples CSIRT (INCIBE-CERT para ciudadanos y empresas; CCN-CERT para el sector público).
- **Protección de infraestructura crítica:** Amparada en la Ley 8/2011. Gestión a cargo del Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC).

[27] CEPAL (2022). *Ciberseguridad y transformación digital: desafíos y oportunidades para América Latina y el Caribe.* Comisión Económica para América Latina y el Caribe, Naciones Unidas.
https://www.cepal.org/es/publicaciones/48194

- **Rol de defensa y seguridad nacional:** Integrado mediante el Sistema de Seguridad Nacional; participación del Ministerio del Interior y Ministerio de Defensa.
- **Participación ciudadana y derechos fundamentales:** Enfocada en campañas de sensibilización, inclusión digital y protección de datos personales (Ley Orgánica 3/2018).
- **Nivel de madurez institucional:** Alto. Existe financiamiento sostenido y capacidad técnica consolidada.

Chile

- **Marco legal principal:** Ley Marco de Ciberseguridad N.º 21.635 (2023).
- **Tipo de gobernanza:** Centralizada. La Agencia Nacional de Ciberseguridad (ANCI) es un órgano autónomo de alto nivel.
- **Obligaciones del sector privado:** Altas. Los operadores de servicios esenciales y relevantes tienen deberes de prevención, reporte y respuesta.
- **Regulación de incidentes y CSIRT:** Obligatoria por ley. Funciona un CSIRT nacional y se prevén CSIRT sectoriales.
- **Protección de infraestructura crítica:** Reconocida explícitamente en la ley, con regulaciones específicas.
- **Rol de defensa y seguridad nacional:** Coordinación operativa mediante protocolos interinstitucionales. Las Fuerzas Armadas no dirigen, pero participan.
- **Participación ciudadana y derechos fundamentales:** La ley promueve derechos digitales y establece canales de participación.
- **Nivel de madurez institucional:** En proceso de consolidación. Alta proyección futura.

México

- **Marco legal principal:** No existe ley específica. Se cuenta con la Estrategia Nacional de Ciberseguridad 2017.
- **Tipo de gobernanza:** Descentralizada y fragmentada. Intervienen múltiples entidades sin un ente rector legalmente definido.
- **Obligaciones del sector privado:** Débiles. No hay disposiciones generales vinculantes, solo normativas sectoriales dispersas.
- **Regulación de incidentes y CSIRT:** No estandarizada. Opera el Centro de Respuesta a Incidentes Cibernéticos de México (CERT-MX) bajo la Guardia Nacional.
- **Protección de infraestructura crítica:** No existe regulación específica.
- **Rol de defensa y seguridad nacional:** Predominante. Participación directa de la Secretaría de la Defensa Nacional (SEDENA) y el Centro Nacional de Inteligencia (CNI).
- **Participación ciudadana y derechos fundamentales:** Limitada. No está integrada formalmente en el marco estratégico.
- **Nivel de madurez institucional:** Intermedia-baja. Faltan articulación normativa y capacidades técnicas suficientes.

Colombia

- **Marco legal principal:** Estrategia Nacional de Ciberseguridad; leyes sectoriales; Decreto 1649/2021; normas sectoriales
- **Tipo de gobernanza:** Mixta. El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) lidera técnicamente, pero sin un marco unificado.
- **Obligaciones del sector privado:** Parciales. Regulación por sectores (financiero, telecomunicaciones, salud).
- **Regulación de incidentes y CSIRT:** Establecida a nivel sectorial. Existen CSIRT nacionales y sectoriales en operación.
- **Protección de infraestructura crítica:** Ausente de regulación específica.

- **Rol de defensa y seguridad nacional:** Coordinación a través de la Comisión Intersectorial de Seguridad Digital; participación de Policía Nacional y organismos de inteligencia.
- **Participación ciudadana y derechos fundamentales:** Presente en estrategias de confianza digital y protección de datos personales.
- **Nivel de madurez institucional:** Intermedia. Con buenas prácticas, pero con margen de mejora normativa y operativa.

Uruguay

- **Marco legal principal:** No cuenta con ley específica. Se basa en la Estrategia Nacional de Ciberseguridad 2024–2030, emitida por la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC).
- **Tipo de gobernanza:** Centralizada en el ámbito público. AGESIC lidera política y técnicamente.
- **Obligaciones del sector privado:** Limitadas. El foco está en instituciones públicas.
- **Regulación de incidentes y CSIRT:** Se aplica mediante directrices técnicas. El CSIRT nacional (CERTuy) actúa con autonomía técnica.
- **Protección de infraestructura crítica:** No contemplada normativamente.
- **Rol de defensa y seguridad nacional:** Coordinación débil; bajo nivel de integración operativa con defensa nacional.
- **Participación ciudadana y derechos fundamentales:** Fuerte énfasis en inclusión digital, gobierno abierto y protección de datos personales (Ley 18.331).
- **Nivel de madurez institucional:** Alta. Modelo técnico avanzado y gobernanza digital robusta, aunque sin base legal específica.

Estonia

- **Marco legal principal:** Ley de Ciberseguridad (Cybersecurity Act, 2018); complementada por leyes de servicios esenciales y defensa.
- **Tipo de gobernanza:** Centralizada con fuerte integración civil-militar.
- **Ente rector:** Autoridad del Sistema de Información (RIA) bajo el Ministerio de Asuntos Económicos y Comunicaciones.
- **Obligaciones del sector privado:** Elevadas. Empresas que prestan servicios esenciales deben cumplir requisitos técnicos, notificar incidentes y someterse a supervisión.
- **Regulación de incidentes y CSIRT:** Regulación avanzada y obligatoria. El CSIRT nacional (CERT-EE) actúa con autonomía técnica.
- **Protección de infraestructura crítica:** Integrada al marco legal con enfoque de riesgo sectorial.
- **Rol de defensa y seguridad nacional:** Coordinación directa entre el Ministerio de Defensa, RIA y entidades civiles.
- **Participación ciudadana y derechos fundamentales:** Alta. Amplia cultura digital, protección constitucional de derechos en entornos digitales.
- **Nivel de madurez institucional:** Muy alta. Es referente global en gobernanza cibernética.

Costa Rica

- **Marco legal principal:** Proyecto de Ley Marco de Ciberseguridad (expediente 23.254); Decreto Ejecutivo N.º 43770-MICITT; Estrategia Nacional de Ciberseguridad.
- **Tipo de gobernanza:** En transición. El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) actúa como rector provisional.
- **Obligaciones del sector privado:** Propuestas en el proyecto de ley. Incluyen medidas técnicas, planes de contingencia y notificación obligatoria.
- **Regulación de incidentes y CSIRT:** Prevista en el proyecto. Actualmente operado por el CSIRT nacional (CSIRT-CR).
- **Protección de infraestructura crítica:** Reconocida en el proyecto de ley como eje estratégico.

- **Rol de defensa y seguridad nacional:** Participación prevista mediante coordinación interinstitucional. Aún sin consolidación.
- **Participación ciudadana y derechos fundamentales:** Abordada en la Estrategia Nacional mediante programas de concienciación y protección de datos personales (Ley 8968).
- **Nivel de madurez institucional:** En desarrollo. Se fortaleció significativamente tras el ataque de ransomware Conti en 2022, que afectó a múltiples instituciones públicas, incluyendo el Ministerio de Hacienda, lo que evidenció la necesidad de un marco normativo robusto y una mejor coordinación interinstitucional.

Cuadro comparativo consolidado de legislación y gobernanza en ciberseguridad (2024)

País	Ley específica	Gobernanza	Obligaciones sector privado	Regulación de incidentes / CSIRT	Protección de infraestructuras críticas	Rol defensa / seguridad nacional	Participación ciudadana / derechos	Madurez institucional
España	✓ Ley 8/2011, Real Decreto 43/2021, Directiva NIS2 (2024)	Mixta (INCIBE + Seguridad Nacional)	✓ Alta, incluye sectores de menor criticidad	✓ Establecida por ley / múltiples CSIRT	✓ Ley 8/2011	✓ Integrada al sistema de seguridad nacional	✓ Alta (protección de datos, inclusión)	Alta
Chile	✓ Ley 21.635 (2023)	Centralizada (ANCI)	✓ Alta	✓ CSIRT nacional y sectoriales	✓ Regulada, en implementación	✓ Coordinación operativa	✓ Promoción de derechos digitales	Alta proyección
México	✗ Sólo estrategia Proyecto en fase avanzada	Descentralizada	✗ Limitada	✗ CERT-MX con marco parcial	✗ No definida	✓ Participación predominante de SEDENA y CNI	✗ Limitada	Intermedia-baja
Colombia	✗ No hay ley específica, sólo estrategia	Mixta (MinTIC+CSIRT sectoriales)	✓ Parcial	✓ Sectorial / múltiples CSIRT	✗ No regulada (Proyecto de Ley 245/19)	✓ Coordinación intersectorial	✓ Enfocada en confianza digital/protección de datos	Intermedia
Uruguay	✗ No hay ley, sino Estrategia Nacional de Ciberseguridad 2024-2030	Centralizada (AGESIC)	✗ Limitada	✓ CERTuy nacional (Decreto 92/014	✗ No regulada	✗ Participación débil	✓ Inclusión digital y gobierno abierto	Alta técnica
Estonia	✓ Ley de 2018	Centralizada civil-militar (RIA)	✓ Alta	✓ Avanzada / CERT-EE	✓ Integrada por sectores	✓ Coordinación defensa + civil	✓ Alta protección de derechos	Muy alta
Costa Rica	✗ No hay ley, Proyecto 23.254 en discusión	En transición (MICITT)	✓ Limitada	✓ Prevista en proyecto / CSIRT-CR	✓ Reconocida en proyecto	✓ Prevista en coordinación	✓ Programas de sensibilización	En desarrollo

6.2 Elementos comunes de la experiencia internacional

Después de analizar la legislación de diferentes países se logró identificar los siguientes elementos comunes:

1. Existencia de una ley marco clara, una propuesta legislativa en curso o una estrategia nacional institucionalizada como en el caso de Uruguay
2. Ente rector con jerarquía, mandato legal y capacidad técnica.
3. CSIRT nacionales operativos, respaldados por normativa específica.
4. Obligaciones diferenciadas para operadores críticos.
5. Coordinación interinstitucional efectiva y formalizada.
6. Inclusión de protección de infraestructuras críticas como prioridad nacional.
7. Integración progresiva de actores de defensa, sin militarización.
8. Promoción de derechos digitales y participación ciudadana.
9. Evaluación constante y sostenibilidad institucional como condición de éxito.

Debe anotarse que algunos países, como Uruguay, aunque sin ley específica, han desarrollado modelos técnicos sólidos apoyados en estrategias nacionales vigentes (2024–2030). En contraste, otros como México carecen aún de articulación normativa y de un ente rector formal.
Estos elementos deben orientar la construcción de una ley de ciberseguridad y una gobernanza adaptada al contexto guatemalteco, alineada con estándares internacionales pero adecuada a sus capacidades institucionales.

6.3 Comparación de estrategias de financiamiento en los países analizados

La sostenibilidad de los marcos de ciberseguridad depende de una asignación adecuada de recursos financieros y humanos. Los países analizados han adoptado diversas estrategias para financiar sus estructuras de ciberseguridad, adaptadas a sus capacidades económicas y prioridades nacionales:

- **España**: El Instituto Nacional de Ciberseguridad (INCIBE) y el Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC) cuentan con asignaciones presupuestarias anuales directas del gobierno central, complementadas por fondos de la Unión Europea para proyectos específicos. Además, se han establecido asociaciones público-privadas para financiar programas de capacitación y simulacros conjuntos.
- **Chile**: La Ley Marco de Ciberseguridad (2023) establece un presupuesto específico para la Agencia Nacional de Ciberseguridad (ANCI), financiado mediante el presupuesto nacional y contribuciones de organismos internacionales como el BID.
- **Estonia**: La Autoridad del Sistema de Información (RIA) recibe una partida fija del presupuesto estatal, reforzada por fondos europeos y cooperación técnica internacional. Estonia invierte en formación de talento local a través de programas universitarios y alianzas con el sector privado.
- **Costa Rica**: El proyecto de Ley 23.254 prevé un fondo específico para el CSIRT nacional, financiado parcialmente por el presupuesto público y donaciones internacionales. Tras el ataque de ransomware Conti (2022), el país incrementó su inversión en ciberseguridad, priorizando la cooperación con organismos como la OEA.
- **México y Colombia**: La falta de una ley específica limita la asignación de recursos centralizados. Ambos países dependen de presupuestos sectoriales (por ejemplo, defensa o telecomunicaciones) y cooperación internacional, lo que genera desafíos de sostenibilidad.
- **Uruguay**: AGESIC opera con un presupuesto público asignado, pero su enfoque en gobernanza digital ha permitido aprovechar economías de escala al integrar la ciberseguridad con otros proyectos tecnológicos.

Estos ejemplos muestran que el financiamiento efectivo requiere: a) asignaciones presupuestarias recurrentes, b) mecanismos de emergencia para incidentes críticos, c) cooperación internacional para países con limitaciones fiscales, y d) alianzas con el sector privado para optimizar recursos. Los parlamentarios pueden considerar estas estrategias al evaluar opciones para garantizar la viabilidad económica de un marco nacional de ciberseguridad.

6.4 Cronogramas de implementación en los países analizados

La implementación de marcos normativos e institucionales de ciberseguridad requiere plazos que varían según el contexto político, económico e institucional de cada país. A continuación, se presenta una comparación de los tiempos y factores clave en los países analizados:

- **España**: La Ley 6/2021 sobre seguridad de las redes y sistemas de información se aprobó tras dos años de consultas y debates legislativos, impulsada por la transposición de la Directiva NIS de la UE. La consolidación del Sistema Nacional de Ciberseguridad, liderado por INCIBE y el CNPIC, tomó aproximadamente cinco años (2016-2021), apoyada por un fuerte consenso político y financiamiento europeo.
- **Chile**: La Ley Marco de Ciberseguridad (21.635) fue aprobada en 2023 tras tres años de discusión legislativa, acelerada por incidentes cibernéticos regionales. La creación de la Agencia Nacional de Ciberseguridad (ANCI) está en curso, con un plazo estimado de dos años para su plena operatividad (2023-2025).

- **Estonia**: La Ley de Ciberseguridad (2018) se desarrolló en un año, gracias a una alta madurez institucional y experiencia previa en digitalización. La Autoridad del Sistema de Información (RIA) y el CSIRT nacional (CERT-EE) se consolidaron en menos de tres años, apoyados por una fuerte voluntad política.
- **Costa Rica**: El proyecto de Ley 23.254 lleva más de dos años en discusión legislativa (2022-2025), impulsado por el ataque de ransomware Conti. La implementación de un CSIRT nacional fortalecido podría tomar entre tres y cinco años, dependiendo de la aprobación legislativa y el financiamiento.
- **México y Colombia**: La ausencia de leyes específicas ha prolongado los procesos de consolidación institucional, con estrategias nacionales que han tomado entre dos y tres años en formularse, pero con implementación fragmentada debido a la falta de coordinación.
- **Uruguay**: AGESIC desarrolló su modelo de gobernanza digital en aproximadamente cinco años (2008-2013), integrando la ciberseguridad progresivamente sin una ley específica, lo que refleja un enfoque técnico pero con limitaciones normativas.

Los factores que aceleran la implementación incluyen: a) consenso político, b) eventos críticos que generan urgencia, c) financiamiento asegurado, y d) cooperación internacional. Por otro lado, la fragmentación institucional, la resistencia política o la falta de recursos pueden extender los plazos significativamente. Esta información puede orientar a los legisladores en la planificación de cronogramas realistas.

7. Lecciones aprendidas y buenas prácticas

7.1 Factores de éxito en la implementación normativa

El análisis comparado permite identificar varios factores clave que explican el éxito de la implementación normativa en ciberseguridad:

- **Marco legal integral y claro:** La existencia de una ley marco que delimita competencias, define obligaciones, y establece mecanismos de coordinación reduce ambigüedades y refuerza la ejecución institucional[28] (caso de España y Chile), o al menos una estrategia nacional integral con respaldo institucional (como Uruguay)
- **Ente rector especializado y con autonomía técnica:** Modelos como el de Estonia (Autoridad del Sistema de Información, RIA) y Chile (Agencia Nacional de Ciberseguridad, ANCI) muestran que contar con un organismo técnico y políticamente respaldado facilita la articulación nacional[29].
- **Financiamiento sostenible y recursos humanos calificados:** Países con presupuestos asignados a ciberseguridad y programas de formación permanente han logrado mayor resiliencia operativa[30] (España, Uruguay).
- **Sistema funcional de notificación y respuesta a incidentes:** La existencia de Centros de Respuesta a Incidentes de Seguridad Informática (CSIRT) nacionales respaldados por ley y articulados en red permite una respuesta más eficaz ante amenazas[31].
- **Actualización continua de normas y estrategias:** Los países con procesos regulares de revisión normativa, como Estonia y España, se adaptan mejor a nuevas amenazas y tecnologías[32].

[28] OCDE (2015). *Recomendación del Consejo sobre la Seguridad Digital para la Prosperidad Económica y Social*. ttps://www.oecd.org/sti/ieconomy/digital-security-recommendation.htm
[29] ENISA (2022). *National Cybersecurity Strategies: Practical Guide 2022*. https://www.enisa.europa.eu/publications/ncss-practical-guide-2022
[30] OEA (2020). *Guía para la formulación de estrategias nacionales de ciberseguridad en las Américas*. https://www.oas.org/es/sms/cicte/documentos/GuiaCiberseguridad2020.pdf
[31] ENISA (2021). *Incident Reporting in the EU: Overview of Practices*. https://www.enisa.europa.eu/publications/incident-reporting-in-the-eu
[32] OCDE (2015). *Recomendación del Consejo sobre la Seguridad Digital para la Prosperidad Económica y Social*. https://www.oecd.org/sti/ieconomy/digital-security-recommendation.htm

- **Participación multisectorial formalizada:** La inclusión del sector privado, sociedad civil y la academia en consejos consultivos o estructuras de gobernanza mejora la legitimidad y la eficacia de las políticas[33] (caso España y Costa Rica).
- **Enfoque estratégico en protección de infraestructuras críticas:** Definir y priorizar activos esenciales en el marco legal ha sido determinante en los modelos exitosos[34] (Chile, Estonia).

7.2 Riesgos comunes de diseño institucional

El estudio revela riesgos frecuentes en el diseño e implementación de marcos normativos e institucionales:

- **Fragmentación de competencias:** La dispersión de responsabilidades entre múltiples entidades sin coordinación efectiva (como en México o Colombia, donde múltiples entidades actúan sin un marco legal unificado) genera vacíos, duplicidades o bloqueos operativos[35].
- **Falta de liderazgo político o jerarquía institucional:** En algunos casos, el bajo perfil del ente rector o su ubicación subordinada dentro de estructuras administrativas débiles reduce su capacidad de actuación[36] (Colombia, México).
- **Exclusión del sector privado:** La ausencia de mecanismos formales de cooperación con operadores críticos debilita la capacidad preventiva y de respuesta[37].
- **Subestimación de la infraestructura crítica:** Cuando la normativa no distingue ni prioriza activos esenciales, se compromete la seguridad nacional[38].
- **Débil articulación con los sistemas de defensa o protección civil:** La falta de interoperabilidad entre actores civiles y militares limita la respuesta a amenazas complejas[39] (Uruguay, Colombia).
- **Escasa protección de derechos y participación ciudadana:** Ignorar estos elementos puede afectar la legitimidad social de las políticas y generar resistencias[40] (México, algunos modelos en transición).
- **Ausencia de mecanismos de evaluación y actualización normativa:** Modelos sin esquemas de revisión periódica tienden a quedar obsoletos ante nuevas tecnologías y amenazas[41] (Colombia, Uruguay).

7.3 Elementos necesarios para asegurar el cumplimiento y evolución normativa

Para que una ley de ciberseguridad no solo exista formalmente, sino que tenga efecto práctico sostenido, se requiere considerar:

- **Supervisión efectiva y mecanismos de cumplimiento:** Deben incluirse auditorías, sanciones proporcionales, procedimientos de verificación técnica y mecanismos de seguimiento público[42].

---

[33] CEPAL (2022). *Ciberseguridad y transformación digital: desafíos y oportunidades para América Latina y el Caribe*. https://www.cepal.org/es/publicaciones/48194
[34] OEA (2021). *Modelo de Madurez en Ciberseguridad (CMM)*. https://www.oas.org/es/sms/cicte/cmm.html
[35] CEPAL (2022). *Ciberseguridad y transformación digital: desafíos y oportunidades para América Latina y el Caribe*. https://www.cepal.org/es/publicaciones/48194
[36] OEA (2020). *Guía para la formulación de estrategias nacionales de ciberseguridad en las Américas*. https://www.oas.org/es/sms/cicte/documentos/GuiaCiberseguridad2020.pdf
[37] OCDE (2015). *Recomendación del Consejo sobre la Seguridad Digital para la Prosperidad Económica y Social*. https://www.oecd.org/sti/ieconomy/digital-security-recommendation.htm
[38] OEA (2021). *Modelo de Madurez en Ciberseguridad (CMM)*. https://www.oas.org/es/sms/cicte/cmm.html
[39] ENISA (2022). *National Cybersecurity Strategies: Practical Guide 2022*. https://www.enisa.europa.eu/publications/ncss-practical-guide-2022
[40] CEPAL (2022). *Ciberseguridad y transformación digital: desafíos y oportunidades para América Latina y el Caribe*. https://www.cepal.org/es/publicaciones/48194
[41] OCDE (2019). *Good Governance for Critical Infrastructure Protection*. https://www.oecd.org/gov/risk/good-governance-critical-infrastructure.htm
[42] ENISA (2021). *Incident Reporting in the EU: Overview of Practices*. https://www.enisa.europa.eu/publications/incident-reporting-in-the-eu

- **Evaluación periódica del marco normativo:** Los países más exitosos realizan revisiones técnicas y actualizaciones legales cada 3 a 5 años para adaptarse a nuevos riesgos y tecnologías[43].
- **Formación continua y desarrollo de capacidades:** Programas nacionales de capacitación en ciberseguridad, tanto en sector público como privado, son clave para reducir la vulnerabilidad estructural[44].
- **Gobernanza adaptativa y participativa:** El marco debe permitir la incorporación de nuevas tecnologías, amenazas y actores, sin requerir reformas constantes que ralenticen su aplicación[45].
- **Participación multisectorial y transparencia:** Consejos asesores, consultas públicas, foros técnicos y la colaboración abierta con academia y sector privado refuerzan legitimidad y eficacia[46].
- **Cooperación internacional sistemática:** La adhesión a marcos como los de la Organización de Estados Americanos (OEA), la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la Unión Europea (UE) o la Unión Internacional de Telecomunicaciones (UIT), y la colaboración con CSIRT internacionales, potencian la capacidad nacional y alinean a los países con estándares globales[47].
- **Asignación presupuestaria específica:** La sostenibilidad de las estructuras, formación, respuesta y prevención en ciberseguridad requiere financiamiento público recurrente y, en algunos casos, fondos de emergencia ante ciberincidentes de alto impacto[48].
- **Inclusión de principios rectores en la ley:** La legislación debe incluir principios como legalidad, proporcionalidad, responsabilidad compartida, enfoque preventivo, protección de derechos fundamentales y resiliencia[49].

8. Recomendaciones para Guatemala

8.1 Necesidades normativas

Guatemala carece actualmente de un marco legal integral y específico en materia de ciberseguridad. Las normativas existentes son dispersas y parciales, lo que impide una respuesta coordinada, preventiva y eficaz ante amenazas cibernéticas. Las principales necesidades normativas identificadas incluyen:

- Contar con una ley marco de ciberseguridad que defina principios, competencias, obligaciones y mecanismos de coordinación.
- Establecer un régimen de protección de infraestructuras críticas digitales.
- Formalizar la obligación de notificación y respuesta ante incidentes cibernéticos.
- Regular la función y operatividad de los Centros de Respuesta a Incidentes (CSIRT).
- Incorporar la ciberseguridad como un componente estructural de la transformación digital del Estado.
- Promover la inclusión de perspectivas de género y equidad, mediante programas de capacitación en ciberseguridad dirigidos a mujeres y comunidades marginadas, y estrategias para cerrar la

[43] OCDE (2019). *Good Governance for Critical Infrastructure Protection*. https://www.oecd.org/gov/risk/good-governance-critical-infrastructure.htm
[44] OEA (2020). *Guía para la formulación de estrategias nacionales de ciberseguridad en las Américas*. https://www.oas.org/es/sms/cicte/documentos/GuiaCiberseguridad2020.pdf
[45] OCDE (2015). *Recomendación del Consejo sobre la Seguridad Digital para la Prosperidad Económica y Social*. https://www.oecd.org/sti/ieconomy/digital-security-recommendation.htm
[46] CEPAL (2022). *Ciberseguridad y transformación digital: desafíos y oportunidades para América Latina y el Caribe*. https://www.cepal.org/es/publicaciones/48194
[47] ENISA (2022). *National Cybersecurity Strategies: Practical Guide 2022*. https://www.enisa.europa.eu/publications/ncss-practical-guide-2022
[48] OEA (2020). *Guía para la formulación de estrategias nacionales de ciberseguridad en las Américas*. https://www.oas.org/es/sms/cicte/documentos/GuiaCiberseguridad2020.pdf
[49] OCDE (2015). *Recomendación del Consejo sobre la Seguridad Digital para la Prosperidad Económica y Social*. https://www.oecd.org/sti/ieconomy/digital-security-recommendation.htm

brecha digital en zonas rurales, garantizando que la ley beneficie a todos los sectores de la población.

8.2 Posibles modelos institucionales

A partir del análisis comparado, se recomienda que Guatemala adopte un modelo de gobernanza centralizada especializada, basado en la creación de un ente rector con autonomía administrativa y funcional, garantizada mediante un mandato legal explícito, con competencias técnicas y de coordinación estratégica. Su presupuesto debe estar protegido por una asignación anual fija en el Presupuesto General de la Nación, con mecanismos de auditoría transparente para garantizar su independencia. Este organismo podría denominarse **Instituto Nacional de Ciberseguridad de Guatemala (INCIB-GT)**[50].

Funciones principales de la INCIB-GT:

- Formular y actualizar la Estrategia Nacional de Ciberseguridad.
- Coordinar el sistema nacional de respuesta a incidentes, incluyendo el CSIRT nacional.
- Emitir estándares técnicos vinculantes para entidades públicas y operadores críticos.
- Supervisar el cumplimiento normativo y aplicar medidas correctivas.
- Cooperar con organismos internacionales y con otros CSIRT del mundo.

Además, se sugiere la creación de un **Consejo Nacional de Ciberseguridad**, como instancia superior de coordinación interinstitucional, multisectorial y consultiva.

8.3 Articulación con leyes existentes (protección de datos, transformación digital, defensa, telecomunicaciones)

Una futura ley de ciberseguridad debe integrarse coherentemente con el resto del marco jurídico vigente o en desarrollo. Se recomienda lo siguiente:

- **Protección de Datos Personales:** Coordinar con la autoridad de datos (actual o futura), especialmente en aspectos de prevención de incidentes que afecten la privacidad y la integridad de la información personal (Ley 8968 o propuesta de nueva ley).

- **Transformación Digital:** Articulación formal con la Agencia Nacional de Transformación Digital (ANTD) para asegurar que todo desarrollo digital del Estado integre desde su diseño los principios de ciberseguridad.

- **Infraestructura Crítica:** Vinculación directa con el ente responsable de proteger activos físicos y digitales estratégicos del país, mediante protocolos de seguridad, simulacros y auditorías.

- **Defensa Nacional y Seguridad Pública:** Definir mecanismos de coordinación con el Ministerio de la Defensa Nacional y el Ministerio de Gobernación para compartir alertas, inteligencia técnica

[50] Los modelos más avanzados (como Estonia, España, Chile o la Unión Europea en la Directiva NIS2) establecen que: i) La ciberseguridad debe operar como una función transversal y especializada, que se articula con otras políticas, sin depender subordinadamente de ellas; ii) La transformación digital lidera los procesos de cambio tecnológico del Estado, pero debe incorporar la ciberseguridad como componente obligatorio, no como superior o inferior jerárquicamente; iii) La protección de infraestructuras críticas (PIC) puede tener su propio ente rector, pero en la práctica requiere coordinación con el organismo de ciberseguridad, especialmente cuando esas infraestructuras incluyen sistemas digitales; iv) Protección de datos personales y datos abiertos son ámbitos de gobernanza de la información. La ciberseguridad colabora con ambos, respetando sus marcos legales propios (como el RGPD en la UE o las leyes de protección de datos en América Latina).

y actuar ante amenazas complejas, limitando su participación a ciberamenazas de alto impacto o de origen estatal, para evitar una militarización excesiva de la ciberseguridad.

En este sentido, para garantizar una gobernanza efectiva, la ciberseguridad debe articularse con el ámbito de la defensa nacional bajo un liderazgo civil claro, evitando una militarización excesiva que podría generar desconfianza social o solapamientos institucionales. En Chile, la Ley Marco de Ciberseguridad (2023) asigna la coordinación a la Agencia Nacional de Ciberseguridad (ANCI), un ente civil autónomo, mientras que las Fuerzas Armadas participan solo en ciberamenazas de alto impacto mediante protocolos interinstitucionales. De manera similar, Estonia centraliza la gestión en la Autoridad del Sistema de Información (RIA), un organismo civil, con el Ministerio de Defensa apoyando únicamente en escenarios estratégicos. Estos modelos demuestran que un liderazgo civil, respaldado por mecanismos formales de colaboración con el sector militar, fortalece la resiliencia nacional sin comprometer la transparencia ni los derechos fundamentales.

- **Telecomunicaciones:** Coordinar con el ente regulador del sector (SIT) para asegurar que los operadores implementen medidas de ciberseguridad en redes e infraestructuras de conectividad.

- **Datos Abiertos:** Establecer criterios mínimos de seguridad para plataformas de apertura de datos públicos, garantizando la integridad y confidencialidad donde corresponda.

8.4 Propuesta de líneas de acción legislativa y política pública

- Redacción y presentación de un proyecto de Ley Marco de Ciberseguridad, que recoja los elementos analizados en este estudio. (prioridad: 1-2 años)
- Creación legal del Instituto Nacional de Ciberseguridad de Guatemala (INCIB-GT), con independencia técnica y presupuesto propio. (prioridad: 2-3 años)
- Establecimiento de un Sistema Nacional de Respuesta a Incidentes, liderado por un CSIRT nacional, complementado por CSIRT sectoriales y respaldado legalmente con protocolos técnicos estandarizados. (prioridad: 1-3 años)
- Conformación del Consejo Nacional de Ciberseguridad, con participación del sector público, operadores críticos, academia, sociedad civil y sector privado, asegurando paridad de género y representación territorial. (prioridad: 2-4 años)
- Definición legal de infraestructura crítica digital, y su protección como asunto de interés nacional. (prioridad: 1-2 años)
- Integración obligatoria de la ciberseguridad en toda estrategia digital del Estado, a través de la ANTD y otras entidades. (prioridad: continuo)
- Formación y certificación de capacidades nacionales en ciberseguridad, con apoyo de cooperación internacional, universidades y centros técnicos. (prioridad: continuo)
- Adopción de estándares internacionales y alianzas multilaterales, especialmente con la OEA, OCDE, UIT y redes latinoamericanas de ciberseguridad. (prioridad: 2-5 años)
- Implementar campañas de sensibilización dirigidas a tomadores de decisión y actores políticos para superar resistencias institucionales y garantizar el respaldo político necesario (prioridad: 1-2 años).

8.5 Escenarios de implementación en Guatemala

Para lograr una aplicación efectiva de la ley de ciberseguridad, se recomienda un enfoque gradual con etapas claramente definidas:

- **Corto plazo**: Aprobación legislativa, creación de la INCIB, establecimiento del CSIRT nacional y definición de protocolos mínimos.
- **Mediano plazo**: Implementación de CSIRT sectoriales, consolidación del Consejo Nacional de Ciberseguridad y vinculación efectiva con el ente encargado de la Transformación Digital..
- **Largo plazo**: Evaluaciones periódicas, desarrollo de talento nacional, integración regional y actualización normativa basada en nuevas amenazas.

8.6 Marco presupuestario y financiamiento

Se sugiere que la ley incluya disposiciones específicas para asignar una partida presupuestaria anual para la ANCIB en el Presupuesto General de la Nación, establecer un fondo de contingencia ante ciberincidentes de alto impacto (Fondo Nacional de Ciberseguridad), promover acuerdos de cooperación con organismos internacionales (como BID, AECID, OEA) para financiar formación, infraestructura y asistencia técnica, así como incentivar acuerdos público-privados en fortalecimiento de capacidades tecnológicas y de formación de talento nacional.

Para una implementación gradual de la Instituto Nacional de Ciberseguridad de Guatemala (INCIB-GT) y del Sistema Nacional de Respuesta a Incidentes, se estiman los siguientes costos anuales preliminares, basados en experiencias internacionales adaptadas al contexto guatemalteco:

Concepto	Costo aproximado por año (en millones de quetzales)
ANCIB (operación y fortalecimiento institucional)	15–25
CSIRT Nacional (equipamiento y operación)	5
Campañas de formación y sensibilización	3–5
Desarrollo de CSIRT sectoriales (por sector)	2–4

Nota: Las cifras presentadas son aproximadas y sujetas a validación mediante estudios específicos de factibilidad.)

Estas estimaciones fueron elaboradas con el apoyo de inteligencia artificial, utilizando datos de presupuestos reportados en legislaciones de ciberseguridad de países como España, Chile, Uruguay y Costa Rica, y ajustados proporcionalmente al Producto Interno Bruto, tamaño poblacional y nivel de desarrollo digital de Guatemala[51].

8.7 Indicadores de evaluación y seguimiento

Se recomienda establecer indicadores clave para monitorear el avance de la ley, tales como:

- Porcentaje de entidades públicas con responsables de ciberseguridad designados.
- Tiempo promedio de respuesta ante incidentes reportados al CSIRT.
- Número de ejercicios de simulación realizados anualmente.
- Nivel de cumplimiento normativo de operadores críticos en auditorías periódicas.
- Porcentaje de operadores críticos con planes de continuidad ante ciberincidentes implementados.
- Número de profesionales certificados en ciberseguridad formados anualmente.

[51] Las estimaciones financieras fueron generadas con apoyo de un modelo de inteligencia artificial que procesó datos de presupuesto y gasto público reportados en legislaciones comparadas de ciberseguridad (España: INCIBE, Chile: Ley 21.635/2023, Uruguay, Costa Rica), ajustados por PIB, población y nivel de digitalización de Guatemala. Estas cifras son orientativas y preliminares, sujetas a validación mediante estudios de factibilidad específicos.

- Tasa de adopción de estándares internacionales (ej. ISO27001) por entidades públicas y privadas.

Estas líneas de acción buscan dotar a Guatemala de un marco legal, institucional y operativo robusto, coherente con estándares internacionales y adaptado a su realidad institucional. De su implementación dependerá la capacidad del Estado para proteger sus activos digitales, generar confianza en su transformación digital y asegurar el bienestar de su población frente a riesgos cibernéticos emergentes.

8.8 Evaluación de riesgos y estrategias de mitigación

La implementación de un marco normativo integral en ciberseguridad conlleva desafíos inherentes que es necesario anticipar para maximizar sus probabilidades de éxito. La identificación temprana de riesgos permite diseñar estrategias de mitigación adecuadas y fortalece la resiliencia institucional.

Entre los principales riesgos potenciales se encuentran factores internos como el financiamiento sostenido, la autonomía de las nuevas entidades, la disponibilidad de talento especializado y la transparencia en los procesos de adquisición pública. Asimismo, se reconocen riesgos asociados a la resistencia institucional al cambio, la descoordinación interinstitucional y la creciente complejidad de los ciberataques.

La siguiente tabla resume los principales riesgos identificados y las estrategias sugeridas para su mitigación:

Tabla de riesgos y acciones de mitigación

Riesgo	Impacto Potencial	Estrategia de Mitigación
Falta de financiamiento sostenido	Debilitamiento institucional	Asignaciones presupuestarias específicas y creación de fondo.
Captura política de la ANCIB	Pérdida de autonomía técnica	Autonomía legal y auditorías públicas periódicas.
Déficit de talento especializado	Vulnerabilidad operativa	Programas nacionales de formación continua y certificación.
Corrupción en adquisiciones públicas	Ineficiencia y desvío de recursos	Procesos transparentes de compra y control social.
Ciberataques complejos	Disrupción de servicios esenciales	Sistema nacional de respuesta rápida y ejercicios de simulación.
Resistencia institucional y cultural	Retardo en la implementación de políticas	Sensibilización a tomadores de decisión; capacitación en cultura de seguridad.
Descoordinación interinstitucional	Fragmentación de esfuerzos y respuesta ineficiente	Fortalecimiento de mecanismos de coordinación multisectorial.