CIBERSEGURIDAD EN AMÉRICA LATINA Y EL CARIBE: HACIA UNA ARQUITECTURA LEGAL Y UN MARCO COMÚN

Jersain Zadamig Llamas Covarrubias
César Moliné Rodríguez

Este artículo cuestiona una suposición común en los debates sobre políticas de ciberseguridad en América Latina y el Caribe: que el problema principal es la ausencia de legislación. Los autores argumentan, en cambio, que el problema central es la falta de una arquitectura jurídica coherente capaz de facilitar una gobernanza de la ciberseguridad preventiva y basada en riesgos. Si bien la mayoría de los países se basan en normas fragmentadas en materia penal, administrativa o sectorial, solo unos pocos han adoptado una legislación específica en ciberseguridad, lo que genera ambigüedad conceptual, brechas de coordinación y una capacidad operativa desigual.

Mediante un análisis jurídico comparativo basado en estándares internacionales como NIS2, DORA y NIST/ISO, el documento identifica tres brechas sistémicas: la confusión conceptual entre ciberseguridad y ciberdelito, la ausencia de un marco normativo preventivo y la desigualdad en las capacidades para la notificación y respuesta ante incidentes. La contribución clave es un arquetipo legislativo mínimo viable, práctico y basado en diez pilares, diseñado para reducir la incertidumbre regulatoria, apoyar la cooperación público-privada y establecer una base común de cumplimiento.

Es importante destacar que el artículo se concibe como una herramienta de política aplicada. Sirve como base conceptual para un programa de capacitación en políticas cibernéticas, traduciendo el análisis legal en una agenda estructurada que se puede enseñar, probar e implementar en la práctica.

Jersain Zadamig Llamas Covarrubias *es un abogado y estratega tecnológico mexicano que combina el derecho, la política y la ingeniería para abordar los riesgos cibernéticos contemporáneos. Tiene un máster en Derecho, un doctorado en Ciencia de Datos y certificaciones profesionales como CISO, CEH (EC-Council) y CIPP/E (IAPP). Es profesor investigador en la Universidad de Guadalajara, fundador y director ejecutivo de OBEX Cybersecurity y miembro del grupo de expertos CyberNet de la UE.*

César Moliné Rodríguez *es director regional del Centro de Cibercapacidades de Latinoamérica y el Caribe (LAC4). César es un abogado especializado en derecho mercantil y nuevas tecnologías con más de 20 años de experiencia en las áreas de comercio electrónico y firmas digitales, privacidad y ciberseguridad.*

Revisado por ***Juan Pablo González Gutiérrez*** *es abogado de la Universidad Alberto Hurtado. Magíster en Derecho y Nuevas Tecnologías, Universidad de Chile. Cuenta con diversas certificaciones tales como: ISO 27.701, 37.301, DPO, entre otras. Desde noviembre de 2023, Juan Pablo forma parte del Grupo de Expertos EU CyberNet.*

TABLA DE CONTENIDO

RESUMEN 5
GLOSARIO 6
INTRODUCCIÓN 7
METODOLOGÍA 8
PROBLEMA Y POSIBLES SOLUCIONES 9
Países con ley de ciberseguridad 10
Chile 10
El Salvador 11
Países sin ley de ciberseguridad 11
Antigua y Barbuda 12
Argentina 13
Bahamas 13
Barbados 14
Belice 15
Bolivia 15
Brasil 16
Colombia 16
Costa Rica 17
Cuba 18
Dominica 18
Ecuador 19
Granada 20
Guatemala 20
Guyana 20
Haití 21
Honduras 21
Jamaica 22
México 22
Nicaragua 23
Panamá 24
Paraguay 24
Perú 25
República Dominicana 25
San Cristóbal y Nieves 26
San Vicente y las Granadinas 26
Santa Lucía 27
Surinam 27
Trinidad y Tobago 28
Uruguay 28
Venezuela 29
RESULTADOS Y DISCUSIÓN 29
Unión Europea 30
Chile 31
Estados Unidos de América 31

Reino Unido 32
Internacional/Regional 33
Japón 33
Singapur 33
México 33
Francia 33
Estándares Técnicos 33
Hacia un framework normativo homogéneo en ciberseguridad en América Latina y el Caribe. 34
Pilar A – Gobernanza y coordinación nacional 34
Pilar B – Capacidades operativas del Estado 37
Pilar C – Gestión de riesgos e higiene digital 39
Pilar D – Infraestructuras esenciales/sectores críticos 41
Pilar E – Reportes y gestión de incidentes 43
Pilar F – Seguridad de productos digitales y certificación 45
Pilar G – Cooperación internacional y ciberdiplomacia 47
Pilar H – Gobierno, compras públicas y fomento 51
Pilar I – Transparencia, presupuesto y sostenibilidad 53
Pilar J – Responsabilidades y sanciones 55
LIMITACIONES E INVESTIGACIONES FUTURAS 58
CONCLUSIONES 59

RESUMEN

Este artículo sostiene que el principal desafío de América Latina y el Caribe en ciberseguridad no es la ausencia de tutela de bienes jurídicos, sino la falta de una arquitectura legal coherente que habilite una gobernanza preventiva y basada en riesgos. A la fecha, solo Chile y El Salvador cuentan con una *lex specialis* de ciberseguridad; el resto de los países depende de marcos penales, administrativos o sectoriales que generan ambigüedades conceptuales, vacíos de coordinación y obligaciones de reporte heterogéneas. Con un diseño cualitativo de derecho comparado y revisión documental de fuentes primarias, el estudio distingue países con y sin ley especial y triangula sus hallazgos con referentes internacionales (p. ej., NIS2, DORA, CRA, NIST/ISO). Los resultados identifican tres brechas regionales: (i) conceptual (confusión ciberseguridad-cibercrimen), (ii) normativa (ausencia de un marco preventivo con competencias y estándares verificables) y (iii) operativa (capacidades dispares para notificar, responder y aprender de incidentes). Como contribución, se propone un arquetipo legislativo mínimo viable organizado en diez pilares (gobernanza, capacidades estatales, gestión de riesgos, infraestructuras esenciales, reporte de incidentes, seguridad de productos y certificación, cooperación internacional, compras públicas y fomento, transparencia/presupuesto, responsabilidades y sanciones), guiado por proporcionalidad, neutralidad tecnológica y salvaguardas de derechos. El marco busca reducir la incertidumbre regulatoria, facilitar la cooperación público-privada y elevar una base común de cumplimiento para la región. Limitaciones: el análisis se restringe a leyes en sentido formal y no evalúa implementación ni efectividad.

GLOSARIO

Anti-SLAPP: *Anti-Strategic Lawsuit Against Public Participation*/Leyes contra demandas estratégicas contra la participación pública
CRA: *Cyber Resilience Act*/Reglamento de Resiliencia Cibernética
CSF: *Cybersecurity Framework*/Marco de Ciberseguridad
CSIRT: *Computer Security Incident Response Team*/Equipo de Respuesta a Incidentes de Seguridad Informática
CTI: *Cyber Threat Intelligence*/Inteligencia de Amenazas Cibernéticas
CVD: *Coordinated Vulnerability Disclosure*/Divulgación Coordinada de Vulnerabilidades
DORA: *Digital Operational Resilience Act*/Reglamento de Resiliencia Operativa Digital
GovSOC: *Government Security Operations Center*/Centro de Operaciones de Seguridad Gubernamental
ICS: *Industrial Control Systems*/Sistemas de Control Industrial
IEC: *International Electrotechnical Commission*/Comisión Electrotécnica Internacional
IoT: *Internet of Things*/Internet de las Cosas
ISA: *International Society of Automation*/Sociedad Internacional de Automatización
ISMS: *Information Security Management System*/Sistema de Gestión de Seguridad de la Información
ISO: *International Organization for Standardization*/Organización Internacional de Normalización
ISO/IEC 27001: *Information Security Management System requirements standard*/Norma de requisitos para un sistema de gestión de seguridad de la información
ISO/IEC 27002: *Information security controls guidance standard*/Norma guía de controles de seguridad de la información
MSP: *Managed Service Provider*/Proveedor de Servicios Gestionados
MSSP: *Managed Security Service Provider*/Proveedor de Servicios de Seguridad Gestionados
NIS2: *Directive on measures for a high common level of cybersecurity across the Union*/Directiva sobre medidas para un alto nivel común de ciberseguridad en la Unión
NIST: *National Institute of Standards and Technology*/Instituto Nacional de Estándares y Tecnología
OT: *Operational Technology*/Tecnología Operacional
RPO: *Recovery Point Objective*/Objetivo de Punto de Recuperación
RTO: *Recovery Time Objective*/Objetivo de Tiempo de Recuperación
SBOM: *Software Bill of Materials*/Lista de Materiales de Software
SOC: *Security Operations Center*/Centro de Operaciones de Seguridad
SSDF: *Secure Software Development Framework*/Marco de Desarrollo Seguro de Software
STI: *Security/Strategic Threat Intelligence*/Inteligencia de Amenazas de Seguridad/Estratégica
STIX: *Structured Threat Information eXpression*/Expresión Estructurada de Información de Amenazas
TAXII: *Trusted Automated eXchange of Indicator Information*/Intercambio Automatizado Confiable de Información de Indicadores
TLP: *Traffic Light Protocol*/Protocolo del Semáforo
TLPT: *Threat-Led Penetration Testing*/Pruebas de Penetración Guiadas por Amenazas
VDP: *Vulnerability Disclosure Program*/Programa de Divulgación de Vulnerabilidades
VEP: *Vulnerability Equities Process*/Proceso de Equilibrio de Vulnerabilidades

INTRODUCCIÓN

La ciberseguridad en América Latina y el Caribe enfrenta un problema de arquitectura jurídica más que de ausencia de tutela de bienes jurídicos. La región ha avanzado en tipificar conductas de cibercrimen, proteger datos personales y habilitar transacciones electrónicas; sin embargo, dichos bloques resultan insuficientes para una gobernanza preventiva, basada en riesgo y orientada a la resiliencia. A la fecha, solo Chile y El Salvador cuentan con una ley especial de ciberseguridad aprobada por el poder legislativo, mientras que el resto de los países se apoya en marcos dispersos de carácter penal, administrativo o sectorial. Esta heterogeneidad tiende a producir ambigüedades conceptuales, vacíos de coordinación, obligaciones de reporte dispares y costos de cumplimiento asimétricos, con efectos en la interoperabilidad entre sectores y a través de fronteras.

El punto de partida de este artículo es distinguir con nitidez ciberseguridad de cibercrimen: la primera actúa *ex ante* sobre la gestión de riesgos, la continuidad operativa y la mejora continua; el segundo opera *ex post* mediante persecución y sanción penal. Confundir ambos planos diluye responsabilidades, debilita los mecanismos de notificación y aprendizaje postincidente y retrasa la maduración de capacidades nacionales. En este contexto, contar con una *lex specialis* de ciberseguridad no es un mero detalle formal: un instrumento con rango de ley habilita funciones y potestades, define deberes exigibles, establece supervisión y sanción, y asegura continuidad intertemporal con independencia de la alternancia gubernamental. Al fijar objetos, conceptos, roles, competencias y procedimientos comunes – incluidos umbrales y plazos de notificación, coordinación CERT/CSIRT, identificación de servicios esenciales y un régimen sancionador –, la ley crea una plataforma regulatoria compartida que facilita la interoperabilidad jurídica y operativa.

El objetivo del trabajo es doble. Primero, ofrecer una radiografía normativa de la región diferenciando países con y sin ley especial de ciberseguridad, sin equiparar marcos de cibercrimen o inteligencia a ciberseguridad a efectos del

conteo. Segundo, derivado de esa comparación se propone un arquetipo legislativo mínimo viable, organizado en diez pilares y alineado con referentes internacionales y estándares técnicos ampliamente reconocidos, que proporcione un lenguaje común, trazabilidad y una secuencia razonable de adopción adaptable al nivel de madurez de cada país. Con ello, se busca reducir la incertidumbre regulatoria, facilitar la cooperación público-privada y elevar una base común de cumplimiento que permita mejorar prevención, respuesta y aprendizaje postincidente.

El estudio se circunscribe a leyes en sentido formal aprobadas por el poder legislativo. La unidad de análisis es la "ley de ciberseguridad" entendida como norma general – no sectorial – que establece, al menos, principios y definiciones, arquitectura de gobernanza, deberes de gestión de riesgos, régimen de reporte de incidentes y facultades de supervisión y sanción. El análisis se organiza en dos trayectorias – países con ley y países sin ley – para aislar el efecto de un marco habilitante y, a partir de allí, proponer el conjunto mínimo de elementos legislativos recomendables para avanzar hacia un ecosistema normativo más coherente e interoperable en América Latina y el Caribe.

METODOLOGÍA

Metodológicamente, el estudio adopta un diseño cualitativo, descriptivo-analítico y de derecho comparado, basado en revisión documental de fuentes primarias (textos legales publicados en diarios oficiales, repositorios parlamentarios y compilaciones normativas oficiales) y, de apoyo, fuentes secundarias técnicas de autoridades competentes. La unidad de análisis es la "ley de ciberseguridad" entendida como *lex specialis* aprobada por el poder legislativo y de alcance general (no sectorial) que establece, al menos, principios y definiciones, arquitectura de gobernanza, deberes de gestión de riesgos, régimen de reporte de incidentes y facultades de supervisión/sanción. Se excluyen expresamente propuestas de ley, estrategias, políticas, reglamentos, circulares y otros actos ejecutivos, así como normas de cibercrimen e inteligencia, que no se consideran

ciberseguridad a efectos del conteo; éstas últimas solo se utilizan para perfilar la radiografía normativa de países sin ley especial. La región de referencia es América Latina y el Caribe y el corte temporal corresponde a la fecha de cierre del estudio.

El procedimiento siguió cuatro movimientos encadenados: identificación y depuración del universo normativo con los criterios de inclusión/exclusión señalados; extracción estandarizada de contenidos mediante una matriz de lectura dirigida; codificación temática y comparación funcional de disposiciones en torno a categorías analíticas que, iterativamente, se consolidaron en los pilares del *framework* propuesto (gobernanza, capacidades operativas, gestión de riesgos, infraestructuras esenciales, reporte de incidentes, productos y certificación, cooperación internacional, compras públicas y fomento, transparencia/presupuesto y responsabilidades/sanciones); y validación por triangulación con marcos internacionales y estándares técnicos (UE, EE. UU., NIST, ISO/IEC, entre otros) a fin de asegurar coherencia conceptual y trazabilidad. El análisis se organiza en dos subtemas, países con ley y países sin ley, para aislar efectos de la existencia de un marco habilitante y, a partir de esa base comparada, derivar un conjunto mínimo de elementos legislativos recomendables para la región, sin evaluar implementación, capacidades institucionales ni efectividad operativa.

PROBLEMA Y POSIBLES SOLUCIONES

Este apartado diagnostica la situación regional a partir de dos subtemas: países con ley de ciberseguridad (Chile y El Salvador) y países sin ley de ciberseguridad. El análisis se limita a normas con rango de ley aprobadas por el poder legislativo, porque son las que crean puentes jurídicos estables, fijan obligaciones, habilitan supervisión y homogenizan el lenguaje y los principios mínimos en la región; por ello, se excluyen estrategias, políticas y reglamentos que, aunque valiosos, dependen del arbitrio gubernamental y, sin reglas claras, dejan esfuerzos individuales y difícilmente comparables. Con este marco, se identifican brechas (gobernanza, gestión de riesgos, reporte de incidentes,

infraestructura crítica, coordinación CERT/CSIRT y régimen sancionador) y se proponen soluciones orientadas a converger hacia *lex specialis* nacionales que eleven el piso parejo regional.

Países con ley de ciberseguridad

En la región de América Latina y el Caribe, únicamente Chile y El Salvador cuentan hoy con una ley marco de ciberseguridad aprobada por el poder legislativo. Este subtema se limita a instrumentos con rango de ley, excluyendo estrategias, políticas, reglamentos o actos administrativos, porque son las normas que, más allá de la voluntad política coyuntural, fijan obligaciones estables, habilitan supervisión y marcan la pauta. Si bien varias naciones han adoptado estrategias como pasos *ex ante*, los marcos especiales (*lex specialis*) en ciberseguridad siguen siendo excepcionales; su expansión es crucial para cerrar brechas, homogeneizar estándares y fortalecer la resiliencia regional.

Chile

La Ley N.° 21.663 (Ley Marco de Ciberseguridad) establece preceptos nacionales para prevenir, gestionar y sancionar incidentes que afecten a organismos públicos y a privados que prestan servicios esenciales o sean calificados como operadores de importancia vital (OIV): fija principios (seguridad y privacidad por defecto y desde el diseño), impone deberes generales y, a los OIV, exigencias reforzadas (SGSI continuo, planes de continuidad certificados, simulacros, delegado, capacitación y eventual aviso a afectados). Crea la Agencia Nacional de Ciberseguridad (ANCI) con funciones normativas, coordinadoras y fiscalizadoras (protocolos y estándares, Registro Nacional de Incidentes, requerimiento de información y, con control judicial, acceso a redes/sistemas), instaura la gobernanza mediante el CSIRT Nacional, la Red de Conectividad Segura del Estado, un Consejo Multisectorial y un Comité Interministerial, y ordena la coordinación regulatoria con autoridades sectoriales. Establece un régimen de reporte escalonado al CSIRT (alerta en 3 h; actualización en 72 h-24 h si un OIV ve afectada la prestación; informe final en 15 días y plan de acción en 7 días para OIV), refuerza la reserva de

información sensible (matrices de riesgo, planes de continuidad/DRP, etc.), y tipifica infracciones leves, graves y gravísimas, con procedimientos sancionatorios y vía de reclamación judicial; además, ajusta la ley de delitos informáticos para introducir un "puerto seguro" de notificación responsable de vulnerabilidades bajo condiciones estrictas.[1]

El Salvador

La Ley de Ciberseguridad y Seguridad de la Información de El Salvador[2] crea un marco nacional para el sector público, y entidades que administren recursos públicos o incidan en infraestructuras críticas, fijando principios (seguridad por diseño, resiliencia y continuidad, gestión de riesgos, cooperación, control de daños, confidencialidad, integridad y neutralidad tecnológica) y definiciones clave (incidente, servicios esenciales, infraestructuras críticas). Impone obligaciones transversales: implementar un sistema de gestión permanente, estrategia alineada a estándares, registro de acciones, planes de continuidad y ciberseguridad con revisiones periódicas, ejercicios y simulacros, medidas para prevenir/reportar/resolver incidentes, mitigación oportuna, designación de un área responsable, colaboración con auditorías y, cuando lo ordene la autoridad, informar a potenciales afectados. Crea la Agencia de Ciberseguridad del Estado (ACE) con autonomía administrativa y financiera, facultada para dictar política y normativa técnica, requerir información y acciones, llevar un Registro Nacional de Amenazas e Incidentes, calificar operadores de infraestructuras críticas (con ratificación presidencial), coordinar capacitación, apoyar pericia forense e informar al Ministerio Público si advierte posibles delitos. Establece infracciones leves, graves y muy graves, inhabilitación por 10 años para servir en el sector público en casos sancionados, multas coercitivas diarias y un procedimiento sancionador abreviado.

Países sin ley de ciberseguridad

En contraste con el apartado anterior, donde se constató que solo Chile y El Salvador poseen una ley marco de ciberseguridad aprobada por el poder legislativo, este apartado mapea los países sin dicha ley especial. Para evitar

[1] Ley 21663, Ley Marco de Ciberseguridad. https://bcn.cl/3isi2
[2] Ley de Ciberseguridad y Seguridad de la Información. http://bit.ly/4gAAD3H

equívocos metodológicos, no se equiparán cibercriminal ni inteligencia a ciberseguridad; se citan únicamente como insumos para ofrecer una radiografía normativa del país analizado. Ello no implica ausencia de tutela de bienes jurídicos vinculados a la seguridad de la información o a la ciberseguridad (p. ej., confidencialidad, integridad, disponibilidad, evidencia y datos personales), sino que carecen de una regulación general, ex ante y de gestión de riesgos que establezca, por ley del poder legislativo, obligaciones de reporte de incidentes, protección de infraestructura crítica, gobernanza y controles mínimos, coordinación CERT/CSIRT y régimen sancionador; en consecuencia, se excluyen decretos, lineamientos o políticas ejecutivas.

Antigua y Barbuda

Antigua y Barbuda organiza su ecosistema de ciberseguridad en torno al *Electronic Crimes Act 2013*[3] y sus reformas de 2018,[4] 2019[5] y 2020,[6] que tipifican el acceso e interferencia a sistemas y datos, prevén agravantes para infraestructuras sensibles y habilitan preservación/producción de datos, allanamiento y exigencia de llaves de descifrado; la *Electronic Evidence Act 2013* asegura admisibilidad y autenticidad de la prueba electrónica;[7] el bloque *Electronic Transactions*[8] y (2013, reformado en 2016)[9] establece equivalencia funcional, firma electrónica y un régimen para prestadores de seguridad de la información; en privacidad, la *Data Protection Act* 2013 impone medidas técnicas y organizativas y diligencia;[10] en pagos, la *Electronic Transfer of Funds Crimes Act* 2007 tipifica fraudes por transferencias electrónicas;[11] y, para criptoactivos, la *Digital Assets Business Act* 2020 crea licenciamiento y *cyber reporting events* para resiliencia y supervisión.[12]

---

[3] *Electronic Crimes Act*, 2013: ss. 3(a)–(j); 11(3)(a)–(d); 16–21; 19(2)(c)–(e); 23–26; 28–30; 32. http://bit.ly/4nIM5wA
[4] *Electronic Crimes (Amendment) Act*, 2018: s. 3; s. 4; ss. 5–8; s. 9 (s. 18). http://bit.ly/421ZY0v
[5] *Electronic Crimes (Amendment) Act*, 2019: Schedule. http://bit.ly/3IevIca
[6] *Electronic Crimes (Amendment) Act*, 2020: ss. 16; 18–21; 19(2)(c); 20; Schedule. http://bit.ly/46yrTq2
[7] *Electronic Evidence Act*, 2013: ss. 5-9; 11; 16–18; 20. http://bit.ly/4nem886
[8] *Electronic Transactions Act*, 2006: ss. 9; 15; 25–27; 29–34. http://bit.ly/4gLpIUX
[9] *Electronic Transactions Act*, 2013: ss. 3-6; Electronic Transactions (Amendment) Act, 2016. http://bit.ly/3VuxwRe; http://bit.ly/4nh77CN
[10] *Data Protection Act*, 2013: s. 8(1)–(2). http://bit.ly/46fpW36
[11] *Electronic Transfer of Funds Crimes Act*, 2007: Pt II, ss. 3–11. http://bit.ly/4pBlLWQ
[12] *Digital Assets Business Act*, 2020: s. 2(1); s. 6; s. 6(3)(a)–(c); s. 23(3)(f). http://bit.ly/4pwBPtb

Argentina

Argentina adopta un enfoque mixto: el Código Penal modernizado por la Ley 26.388 tipifica acceso indebido, interceptación y fraude/daño informático con agravantes sobre servicios públicos y críticos;[13] se penaliza el *grooming*;[14] y la Ley Olimpia (27.736) incorpora la violencia digital con medidas cautelares, remoción de contenidos y preservación probatoria.[15] En protección de datos, la Ley 25.326 impone medidas de seguridad y deberes de confidencialidad y de tratamiento por encargo,[16] reforzados por la adhesión al Convenio 108+ (seguridad del tratamiento y notificación de brechas). La interceptación en inteligencia requiere orden judicial fundada para captar comunicaciones privadas en tareas de inteligencia o contrainteligencia.[17] La firma digital se apoya en certificadores licenciados con obligaciones de seguridad y auditorías.[18] La prevención se articula con el Programa "Mica Ortega" de *grooming*.[19]

Bahamas

Bahamas (Computer Misuse Act, Ch. 107A) penaliza acceso/modificación no autorizados, interceptación de servicios, obstrucción y tráfico de credenciales; prevé agravantes para computadoras protegidas, extraterritorialidad y facultades de preservación/acceso a datos (claves), arresto sin orden y comiso.[20] La interceptación de comunicaciones exige orden judicial y regula su solicitud, autorización, ejecución, confidencialidad, valor probatorio y uso de dispositivos de escucha.[21] El andamiaje de confianza digital se completa con firmas y mensajes electrónicos (*Electronic Communications and Transactions Act*)[22] y con principios de seguridad del tratamiento en la *Data Protection Act*.[23]

---

[13] Ley 26.388 (CP): arts. 77; 128; 153; 153 bis; 155; 157; 157 bis; 173 inc. 16; 183 §2; 184 incs. 5–6; 197; 255. http://bit.ly/3K8mj6y
[14] Ley 26.904 (CP): art. 131 (grooming).http://bit.ly/4gBLs5t
[15] Ley 27.736 (mod. Ley 26.485): arts. 2(h); 4; 6(i); 16(a),(l); 26(a.2),(a.8),(a.9).http://bit.ly/46zq5NJ
[16] Ley 25.326: arts. 9; 10; 21; 25.http://bit.ly/4msLtdi
[17] Ley 25.520 (Inteligencia): art. 18. http://bit.ly/46fq4Q8
[18] Ley 25.506 (Firma digital): arts. 21 incs. s-t; 24-27; 33. http://bit.ly/42DpFEH
[19] Ley 27.590 ("Mica Ortega"): arts. 1-7. http://bit.ly/46rRSRz
[20] *Computer Misuse Act* (Ch. 107A, 2003): ss. 3–8; 9(1)–(3); 10–13; 15(1)–(5); 16(1)(a)–(c),(3)–(4); 17; 11. http://bit.ly/42DpJUX
[21] *Interception of Communications Act*, 2018: ss. 3–13; 14–16; 17–20; 21–23; 24–25; 26–38. http://bit.ly/4nFqPYr
[22] *Electronic Communications and Transactions Act* (Ch. 337A): s. 9(1)–(3); s. 14(1)–(2). http://bit.ly/4nDfKqU
[23] *Data Protection (Privacy of Personal Information) Act (Ch. 324A):* s. 6(1)(a)–(d); 6(3). http://bit.ly/4mxIJvx

En evidencia, el Evidence Act admite datos de monitoreo con certificado y mantiene reglas de exclusión y "banker's books" electrónicos;[24] en niñez, el *Child Protection Act* prevé alertas por redes electrónicas.[25] En pagos, el *Payment Systems Act* blinda la finalidad e irrevocabilidad de liquidaciones y garantías.[26] En mercados, las *Securities Industry (Business Capital) Rules 2021* exigen controles de ciberseguridad, continuidad y protección de datos para plataformas de *crowdfunding*.[27] En criptoactivos, el *Digital Assets and Registered Exchanges Act 2024* eleva requisitos de *fit and proper*, gestión de riesgos tecnológicos y vigilancia de mercado, y ordena divulgación clara a inversores.[28]

Barbados

La *Computer Misuse Act* sanciona acceso no autorizado, interferencia de datos/sistemas, interceptación y uso de herramientas/credenciales; agrava en sistemas restringidos y permite registro, copiado, exigencia de claves/descifrado, órdenes de producción, revelación de tráfico y preservación breve.[29] El *Electronic Transactions Act* asegura la equivalencia jurídica de registros electrónicos, la validez de la firma electrónica y reglas de atribución y admisibilidad probatoria.[30] En telecomunicaciones, puede denegarse interconexión por seguridad/integridad, modificarse temporalmente licencias por seguridad nacional y los carriers pueden rehusar mensajes peligrosos sin responsabilidad.[31] La *Anti-Terrorism Act* define "fondos" en clave amplia – incluidos documentos electrónicos o digitales – para congelamiento/forfeiture.[32] En prueba, la *Evidence Act* facilita la admisión de evidencia producida por máquinas y actualiza los "bankers' books".[33]

---

[24] *Evidence Act*: s. 78E(1)–(2); s. 177(4); s. 178. http://bit.ly/4prB0Sa
[25] *Child Protection Act*: s. 148A(2)(d). http://bit.ly/46LcSTf
[26] *Payment Systems Act (Ch. 351A):* s. 11; s. 15(6). http://bit.ly/3W0IjTh
[27] *Securities Industry (Business Capital) Rules*, 2021: r. 17(1)–(2),(4)(b)–(c),(6). http://bit.ly/3KxZOI6
[28] *Digital Assets and Registered Exchanges Act*, 2024: s. 2(a)–(e)(i)–(iv); s. 39(1)–(7),(3). http://bit.ly/4gBPUkV
[29] Computer Misuse Act (Cap.124B): s.2; s.3; ss.4–8; s.11 & Sch.; ss.15–20; s.21. http://bit.ly/3Ke9mrP
[30] Electronic Transactions Act (Cap.308B): ss.5–6, 8–11, 14, 17–18. http://bit.ly/4nrQIew
[31] Telecommunications Act (Cap.282B): s.28(4); s.44(3)–(7); s.108. http://bit.ly/3Iun6hB
[32] Anti-Terrorism Act (Cap.158): s.2; Pt. IV. http://bit.ly/42KsvYC
[33] Evidence Act (Cap.121): ss.121, 124, 126. http://bit.ly/4nERqEZ

Belice

La *Cybercrime Act* 2020 tipifica acceso e interferencia no autorizados, falsedad y fraude/identidad, y habilita preservación, registro, órdenes de producción y decomiso, con deber de asistencia y confidencialidad.[34] la *Data Protection Act* 2021 impone medidas técnico-organizativas, DPIA y notificación de brechas;[35] la *Digital Government Act* 2022 fija interoperabilidad segura y cifrado en el intercambio de datos y funciones rectoras en seguridad de la información/privacidad;[36] la *Electronic Transactions Act* 2021 reconoce firma (incluida la avanzada) y regula proveedores/procedimientos de seguridad;[37] la Electronic Evidence Act 2021 facilita admisibilidad/autenticidad de prueba electrónica;[38] la *National Security Council Act* 2024 incorpora el dominio cibernético en la arquitectura estratégica;[39] el DPA (Amendment) 2024 crea un *Cybercrime Working Group* regulador-industria;[40] y el sector financiero exige controles de ciber-riesgo y continuidad (FSC, IFSC, banca, FIU).[41]

Bolivia

El Código Penal sanciona la explotación sexual en línea y los delitos informáticos (manipulación para beneficio indebido y acceso/alteración no autorizados);[42] en política pública TIC, la Ley 164 impone seguridad de la información, regula firma/certificación digital y ordena cooperación de operadores en emergencias;[43] en ciudadanía digital, la Ley 1080 limita el uso de datos personales de la plataforma de interoperabilidad a sus fines legales;[44] y en finanzas, la Ley 393 reconoce la equivalencia probatoria de mensajes

[34] Cybercrime Act 2020: ss. 3–7, 9–12, 19–21, 25–30, 37–41, 43. http://bit.ly/4pAKcUh
[35] Data Protection Act 2021: ss. 58, 60–63. http://bit.ly/47VIpCZ
[36] Digital Government Act 2022: ss. 3(1)(l), 8(c)–(d), 15(2)(e)(i)–(ii). http://bit.ly/46P4tya
[37] Electronic Transactions Act 2021: ss. 22–23, 26, 41–42. http://bit.ly/3KfVVrp
[38] Electronic Evidence Act 2021: ss. 3, 5–8. http://bit.ly/42IIUN8
[39] National Security Council Act 2024: s. 2. http://bit.ly/4nDjdFW
[40] Designated Processing Areas (Amendment) Act 2024: s. 23B(1)–(3). http://bit.ly/46ObDTf
[41] FSC Practitioners Code Regs 2023: r. 19(1)–(2). http://bit.ly/47WgTVZ; IFSC Act (Cap. 272s): s. 17(1)–(2). http://bit.ly/47VGePW; Domestic Banks & Financial Institutions (Amendment) No. 2 Act 2023: Annex F(g). http://bit.ly/4ndLFhH; Financial Intelligence Unit (Amendment) Act 2023: s. 12A(a)–(d). http://bit.ly/46GBxr4
[42] Código Penal: arts. 323; 323 bis; 363 bis; 363 ter. http://bit.ly/46um7Wv
[43] Ley 164 (TIC/Telecom): arts. 71; 72; 77; 84; 111. http://bit.ly/46zzncu
[44] Ley 1080 (Ciudadanía Digital): art. 12. http://bit.ly/424irJP

electrónicos y exige controles de seguridad para banca y pagos (integridad, confidencialidad, autenticación, no repudio).[45]

Brasil

Brasil integra un marco robusto y actualizado: en lo penal, se reprime la invasión de dispositivo y se refuerzan el hurto y la estafa por medios electrónicos,[46] con unidades policiales especializadas por ley.[47] El Marco Civil de Internet fija principios, neutralidad, régimen de registros y un "*safe harbor* judicial" con retiro expedito de íntimos no consentidos.[48] La LGPD impone seguridad "desde el diseño", notificación de incidentes y gobernanza, y la reforma crea la ANPD con potestades sancionatorias.[49] En transacciones, la ley de firmas electrónicas clasifica en simple/avanzada/cualificada y el Gobierno Digital exige interoperabilidad con seguridad de la información.[50] Para activos virtuales, el marco de 2022 regula VASPs y tipifica fraude con criptoactivos.[51] En proceso penal, rige cadena de custodia y juez de garantías para medidas intrusivas, clave para evidencia digital.[52] La protección de NNA se refuerza con nuevas figuras de (cyber)bullying y agravantes, sumándose al retiro ágil previsto en el Marco Civil,[53] todo ello con competencias claras para la ANPD y cuerpos especializados.

Colombia

Colombia combina un núcleo penal tecnológico, acceso abusivo, interceptación, daño, malware, violación de datos, *phishing*/DNS, hurto y transferencia no consentida por medios informáticos, incorporado al CP en 2009,[54] con agravantes específicos y una cláusula de mayor punibilidad

---

[45] Ley 393 (Servicios Financieros): arts. 124; 350; 361; 375. http://bit.ly/4mukIFt
[46] Lei 12.737/2012 (CP): art. 154-A; art. 266; art. 298, par. ún. http://bit.ly/4mwbIQm; Lei 14.155/2021 (CP): art. 154-A (penas); art. 155 §4-B, §4-C; art. 171 §2-A, §2-B. http://bit.ly/4mrw2lG
[47] Lei 12.735/2012: art. 4° (unidades especializadas). http://bit.ly/42DtERF
[48] Lei 12.965/2014 (Marco Civil): arts. 7; 9; 10; 13; 15; 19; 21; 22–23. http://bit.ly/4nqTS2j
[49] Lei 13.709/2018 (LGPD): arts. 6(VII); 11; 37; 46–48; 50–52. http://bit.ly/3KgDsuG; Lei 13.853/2019 (LGPD/ANPD): arts. 52; 55-A a 55-K. http://bit.ly/3VripIj
[50] Lei 14.063/2020 (assinaturas): arts. 4–6 (simple/avanzada/cualificada). http://bit.ly/4gxRnsk; Lei 14.129/2021 (Governo Digital): art. 38 (interoperabilidad/seguridad). http://bit.ly/46iL6gS
[51] Lei 14.478/2022 (cripto): arts. 1–4 (diretrizes/VASP); art. 10 → CP art. 171-A. http://bit.ly/4msaHZq
[52] Lei 13.964/2019 (CPP): arts. 158-A a 158-F (cadeia de custódia); arts. 3°-A a 3°-F (juiz de garantias). http://bit.ly/3Ke9W8Z
[53] Lei 14.811/2024: CP art. 146-A (bullying/cyberbullying); agravantes/ECA. http://bit.ly/3Il0ujz
[54] Ley 1273/2009 CP arts. 269A–269J. http://bit.ly/4nNleQ8

cuando se usan medios informáticos;[55] añade un agravante por suplantación con IA/*deepfakes* (2025)[56] y una política de entornos digitales sanos y seguros para NNA (2025).[57] En protección de datos, la ley estatutaria exige medidas técnicas, humanas y administrativas y reporte a la autoridad.[58] La política TIC habilita intervención por seguridad y promueve seguridad de redes (y fue modernizada en 2019);[59] en gobernanza estadística se refuerzan protocolos de seguridad/ciberseguridad y reserva;[60] en inteligencia, el monitoreo de espectro no es interceptación y esta última exige orden judicial.[61] Complementan el reconocimiento de mensajes de datos y firmas digitales.[62]

Costa Rica

Costa Rica opera con: (i) un bloque penal (Ley N.° 9048) que tipifica suplantación, espionaje, malware con agravantes sectoriales, *phishing*, facilitación, y además estafa/daño/sabotaje informáticos y extorsión tecnológica;[63] (ii) reformas que penalizan la violación de comunicaciones y de datos personales con agravantes;[64] (iii) protección de datos con deber de seguridad, confidencialidad, control de transferencias y potestades sancionatorias de PRODHAB;[65] (iv) gobierno digital con ANGD y obligaciones de gestión de riesgos, continuidad y ciberseguridad en el sector público;[66] (v) equivalencia probatoria y firma electrónica para expedientes, contratación y conservación segura; y (vi) actualización en delitos sexuales en línea (*grooming*, pornografía infantil) y coordinación interinstitucional.[67]

---

[55] CP (Ley 599/2000) arts. 269H; 58.17. http://bit.ly/4nhsHHi
[56] Ley 2502/2025 art. 3 (CP 296 agravante IA); arts. 2, 4-6. http://bit.ly/42LfKNt
[57] Ley 2489/2025 arts. 1-3; 5-7; 13-15. http://bit.ly/4pyLoYf
[58] Ley Est. 1581/2012 art. 4(g); arts. 17(d,i,n), 18(b,f,j,k). http://bit.ly/4224vjx
[59] Ley 1341/2009 arts. 2.10; 4.10-4.11; 26.12; 28.14. http://bit.ly/3KmI1DL; Ley 1978/2019 (modernización TIC) arts. 1-3. http://bit.ly/42sow35
[60] Ley 2335/2023 arts. 7; 9; 11; 15-16. http://bit.ly/47V1Bkr
[61] Ley Est. 1621/2013 art. 17. http://bit.ly/46D0fIM
[62] Ley 527/1999 arts. 2; 6-7; 10; 28-29. http://bit.ly/47WKhvs
[63] CP (Ley N.° 9048, Sección VIII): arts. 230-236; 217 bis; 229 bis; 229 ter(a-d); 214 ¶2. http://bit.ly/4ngKWwg
[64] Ley N.° 9135 (reforma CP): arts. 196; 196 bis (agravantes). http://bit.ly/47V1JjV
[65] Ley N.° 8968 (+ Regl. 37554-JP): arts. 10-12; 14; 21; 28-31. http://bit.ly/46zTBmy
[66] Regl. Ley N.° 9943 (ANGD), D.E. 44636-MICITT: art. 9 (riesgos, continuidad, CIA y ciberseguridad). http://bit.ly/3KeKIHw
[67] Ley N.° 10020: art. 167 ¶2; art. 167 bis; arts. 173; 173 bis; 174. http://bit.ly/3VuFXfj

Cuba

El Código Penal (Ley 151) sanciona con penas altas la afectación de datos/sistemas/redes y tutela el secreto de las comunicaciones;[68] el D-L 78/2023 organiza la seguridad de la información clasificada/limitada con habilitaciones, esquemas obligatorios, validaciones y deberes operativos de ciberseguridad (roles MININT, respuesta a incidentes, trazabilidad);[69] la Ley 149 fija principios de protección de datos (seguridad, registro de bases, notificación de incidentes, transferencias internacionales tasadas);[70] el D-L 370 orienta la informatización con objetivos de ciberseguridad y coordinación interministerial;[71] si bien formalmente no es considerado como un instrumento legislativo, cabe destacar que Cuba cuenta con el Decreto 360/2019, que establece el Sistema de Seguridad TIC y defensa del ciberespacio (planes, controles de acceso y trazas con retención mínima, gestión de incidentes/CSIRT, protección de ICI y potestades de inspección y mitigación de spam).[72]

Dominica

La *Electronic Evidence Act* 2010 asegura la admisibilidad de los registros electrónicos, satisface la "mejor evidencia" vía integridad del sistema y reconoce la firma electrónica.[73] La *Electronic Filing Act 2013* autoriza a las autoridades a aceptar/exigir expedientes y pagos electrónicos, fija formato, firma y controles de seguridad, y refuerza el valor probatorio de libros y registros electrónicos públicos.[74] La *Electronic Transactions Act* 2013 otorga equivalencia jurídica a comunicaciones y registros, regula firmas (incluida la "segura") y prevé régimen para intermediarios y remoción de contenidos ilícitos.[75] En pagos, la Electronic Funds Transfer Act 2013 tipifica fraudes con tarjetas y medios electrónicos, crea un delito general para transferencias

[68] Ley 151 (Código Penal): art. 168 (datos/sistemas/redes); arts. 382–383 (secreto comunicaciones). http://bit.ly/4mxyS8O
[69] D-L 78/2023 (info clasificada/limitada): arts. 44–48; 86–88; 154–161; 171; 173; 175–179. http://bit.ly/4nfPcMy
[70] Ley 149 (Protección de Datos Personales): arts. 10; 41; 44–45; 48; 65. http://bit.ly/4nL8nxL
[71] D-L 370/2018 (Informatización): arts. 5; 47; 57. http://bit.ly/4mA7JCd
[72] Decreto 360/2019 (Seguridad TIC y defensa del ciberespacio): arts. 13–21; 24–29; 41–43; 49–53; 55–63; 72–87; 94–106; 107–110. http://bit.ly/46hrcTj
[73] Electronic Evidence Act (2010), ss. 3, 6–7, 12. http://bit.ly/3Vv1eWc
[74] Electronic Filing Act (2013), ss. 4(1)–(2), 11. http://bit.ly/4naVYTT
[75] Electronic Transactions Act (2013), ss. 7–8, 22–28, 34–35. http://bit.ly/3IowWl8

electrónicas y fija reglas de responsabilidad.[76] Como instrumento sectorial, la *Telecommunications Act* 2000 protege el secreto de las comunicaciones y sanciona la interceptación/divulgación sin orden, y prevé órdenes de registro y decomiso.[77]

Ecuador

Ecuador integra datos personales, *telecom*, penal/procesal informático, firma/prueba electrónica, inteligencia y fintech. La LOPDP 2021 define la "vulneración de seguridad", exige seguridad por diseño/defecto y DPIA en alto riesgo, y ordena doble notificación de brechas.[78] La LOT garantiza el secreto de comunicaciones, limita la interceptación a orden judicial y exige seguridad de red y aviso al usuario ante violaciones, bajo supervisión de ARCOTEL.[79] El COIP tipifica acceso/interceptación ilícitos, daño y malware, phishing-DNS, falsificación informática, hurto y transferencias electrónicas, y la responsabilidad penal de personas jurídicas,[80] y en lo procesal prevé interceptación con control judicial, preservación expedita, órdenes de producción, búsqueda/acceso/inhabilitación, cooperación internacional y agente encubierto informático.[81] En lo transaccional, la Ley de Comercio Electrónico reconoce la firma electrónica (y deberes del titular) y la plena validez probatoria de mensajes de datos.[82] La Ley Orgánica de Inteligencia (2025) define ciberinteligencia y habilita requerimientos de información a operadoras con límites de necesidad, proporcionalidad y temporalidad.[83] La Ley FINTECH (2022) fija seguridad como principio, exige trazabilidad pública de incidentes, adopta supervisión basada en riesgo y reconoce servicios auxiliares (ciberseguridad/identidad digital), con salvaguardas para la tercerización pública.[84]

---

[76] Electronic Funds Transfer Act (2013), ss. 9–12, 15–22. http://bit.ly/3KeKPmq
[77] Telecommunications Act (2000), ss. 56, 61–64. http://bit.ly/4gxRSmc
[78] LOPDP 2021: arts. 4; 37; 39–43; 46–47. http://bit.ly/4nIazpA
[79] Ley Orgánica de Telecomunicaciones: arts. 76–79; 82; 85. http://bit.ly/4nrRE2w
[80] COIP (delitos informáticos y conexos): arts. 178–180; 190; 211–212; 230–232; 231; 234–234.4; 234.3. http://bit.ly/47VHkLy
[81] COIP (procesal digital): arts. 69; 476–477.3; 477.4–477.8; 477.10; 483.1–484. http://bit.ly/47WOUFE
[82] Ley de Comercio Electrónico, Firmas y Mensajes de Datos: arts. 17; 54–55. http://bit.ly/4gBRdjP
[83] Ley Orgánica de Inteligencia (2025): arts. 5; 10(l); 43; 51.http://bit.ly/4nlz648
[84] Ley FINTECH (2022): arts. 6.7–6.8; 8.1; 73.1; 439.4 (y reforma al art. 146 LESC). http://bit.ly/4nhclyp

Granada

En la *Electronic Crimes Act* 2013 tipifica acceso/interferencia, identidad, falsedad y fraude; tutela privacidad; protege a NNA; agrava contra sensitive systems y remite a terrorismo electrónico; y habilita preservación, producción, registro, captación en tiempo real y desencriptado bajo orden.[85] La reforma de 2014 suprimió "mensajes ofensivos", acoso y arresto sin orden, manteniendo el núcleo penal.[86] La Electronic Evidence Act 2013 asegura admisibilidad, satisface la "mejor evidencia" por integridad del sistema y reconoce impresos y firma electrónica.[87] La Electronic Transactions Act 2013 presume integridad/autoría de registros y firmas "seguras" y regula proveedores de procedimientos de seguridad.[88] La Data Protection Act 2023 impone seguridad al responsable y al encargado y faculta requerimientos de la autoridad.[89] En resiliencia sectorial, el Payment System Act habilita reglas sobre seguridad, autenticación y contingencia y poderes de directiva del banco central;[90] y la *Terrorism Act* conecta con ataques informáticos que afecten servicios esenciales o la seguridad del Estado.[91]

Guatemala

Opera con: (i) la Ley contra la Delincuencia Organizada (Dec. 21-2006) habilita la interceptación de comunicaciones con control judicial estricto;[92] y (ii) la Ley de Comunicaciones y Firmas Electrónicas exige a los prestadores de certificación seguridad, confidencialidad, continuidad, auditorías y registro público de certificados con revocación por compromiso, más requisitos operativos en el reglamento para repositorios e identificación robusta.[93]

Guyana

La *Cybercrime Act* 2018 tipifica acceso/interceptación ilícitos, injerencia en datos/sistemas, fraude y suplantación, con agravantes para infraestructuras

---

[85] *Electronic Crimes Act* 2013: ss. 5, 7–14; 19–24; 28(2); 31–32. http://bit.ly/3IdDSl3
[86] *Electronic Crimes* (Amendment) Act 2014: s. 3 (deroga ss. 6, 16 y 25). http://bit.ly/4gBTP17
[87] *Electronic Evidence Act* 2013: ss. 5–8; 13–14. http://bit.ly/3Kgntgo
[88] *Electronic Transactions Act* 2013: ss. 26–30. http://bit.ly/48qBLVt
[89] *Data Protection Act* 2023: s. 10(1)–(2); s. 32. http://bit.ly/48e926v
[90] *Payment System Act* (Cap. 227B): s. 33(2)(h); s. 27. http://bit.ly/4mqkCPj
[91] *Terrorism Act* (Cap. 318A): s. 1(2)(f). http://bit.ly/4mxNGV9
[92] Dec. 21-2006: arts. 48–53; 55–57; 58–61; 63–65; 67–70. http://bit.ly/4ngq6NJ
[93] Dec. 47-2008: arts. 33; 42; 47–48 (prestadores, seguridad, continuidad, revocación); Reglamento: arts. 8–9; 13.f; 22 (repositorios, verificación, revocación). http://bit.ly/4mqkGi1

críticas y herramientas procesales (preservación, producción, búsqueda y forensia remota);[94] la Interception of Communications Act 2008 regula la interceptación con orden judicial, asistencia de operadores y claves de descifrado, con ajustes de 2019;[95] la Electronic Communications and Transactions Act 2023 otorga presunciones a registros y firmas electrónicas seguras y crea autoridad certificadora y proveedores acreditados;[96] y la Data Protection Act 2023 consolida principios, derechos y seguridad por diseño, incluida la notificación de brechas.[97]

Haití

La Ley sobre los intercambios electrónicos, ordena la contratación por mensajes de datos y fija reglas de atribución, acuse de recibo y tiempo/lugar de expedición y recepción de mensajes electrónicos.[98] En estricto sentido legal, no hay aún una ley penal de ciberdelitos vigente; el resto del conjunto ha sido desarrollado por decretos/reglamentos, fuera del *corpus de leyes* que aquí reseñamos.

Honduras

La Ley del Sistema Nacional de Bases de Datos de ADN incorpora ciberseguridad/privacidad como principios;[99] en justicia digital, la Ley de Gestión Electrónica de Procesos Judiciales crea el SEJE con integridad, autenticidad, confidencialidad y gestión de riesgos;[100] en transacciones, la Ley sobre Firmas Electrónicas impone deberes estrictos al firmante;[101] la Ley Especial sobre Intervención de las Comunicaciones Privadas sujeta la intervención a orden judicial ejecutada por la UIC;[102] y el Código Penal tipifica *grooming*, revelación de secretos (incluida difusión de íntimos), fraudes y

---

[94] Cybercrime Act 2018, ss. 3–8, 9–12, 13–17, 25, 28, 31–33, 38. http://bit.ly/46ziyOO
[95] Interception of Communications Act 2008, ss. 3, 4–7, 10–13, 16–17; Amendment Act 2019, s. 3(2). http://bit.ly/4pBAsJA; http://bit.ly/3Ke4rHm
[96] Electronic Communications and Transactions Act 2023, ss. 31–34, 35–36, 38–45. http://bit.ly/4nfMgiX
[97] Data Protection Act 2023, ss. 55, 65(1). http://bit.ly/3KmJdad
[98] Loi sur les échanges électroniques (11-abr-2017), arts. 9–13 (atribución del mensaje, acuse de recibo, momento y lugar de envío/recepción). http://bit.ly/3KjH6E2
[99] Ley del Sistema Nacional de Bases de Datos de ADN (D. 57-2023), arts. 3.12–14, 30. http://bit.ly/4nBZgiS
[100] Ley de Gestión Electrónica de Procesos Judiciales (D. 146-2020), arts. 1, 8–10, 18.5–6. http://bit.ly/4nMXQ5e
[101] Ley sobre Firmas Electrónicas (D. 149-2013), art. 9. http://bit.ly/4nhmxab
[102] Ley Especial sobre Intervención de las Comunicaciones Privadas (D. 243-2011, ref. D. 17-2013), art. 24. http://bit.ly/4nNjOVN

accesos electrónicos, espionaje y ciberterrorismo con agravantes sectoriales.[103]

Jamaica

La *Cybercrimes Act* sanciona acceso/alteración/interceptación no autorizados, uso de "herramientas" y comunicaciones maliciosas, agrava contra computadoras protegidas y habilita preservación, órdenes de producción/desencriptado y jurisdicción amplia;[104] la Interception of Communications Act autoriza interceptar solo con orden (o en urgencia, con convalidación), con reglas de minimización, destrucción y acceso a claves y datos de comunicaciones.[105] la *Data Protection Act* exige seguridad "apropiada", notificación de brechas y condiciones para transferencias internacionales;[106] la Evidence (Amendment) Act 2021 equipara copias/imágenes digitales certificadas al original;[107] la Electronic Transactions Act facilita pagos electrónicos al Estado y ofrece remedios por errores en interacciones automatizadas;[108] y la Child Pornography (Prevention) Act define ampliamente la "representación visual", incluyendo datos electrónicos convertibles en imagen.[109]

México

El Código Penal Federal tipifica acceso/manipulación ilícita en sistemas (incluidos Estado y banca) y conductas afines como pornografía infantil y daños a archivos electrónicos;[110] el Código Nacional de Procedimientos Penales habilita medios electrónicos y regula intervención de comunicaciones y extracción de información con control judicial estricto;[111] la Ley Federal de Telecomunicaciones y Radiodifusión impone cooperación 24/7 y conservación de metadatos a concesionarios, reafirmando la inviolabilidad de comunicaciones y límites a bloqueadores;[112] en privacidad, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares exige medidas

---

[103] Código Penal (D. 130-2017), arts. 253, 272, 360, 391, 395, 563, 592-595. http://bit.ly/4nBPayg
[104] *Cybercrimes Act (2015): s*s. 3-11, 13-15, 17-21, 22. http://bit.ly/4pliG7F
[105] *Interception of Communications Act* (2002): ss. 4-7, 11-13, 16-17. http://bit.ly/424knC5
[106] *Data Protection Act* (2020): ss. 21, 30-31. http://bit.ly/46P4Ngj
[107] *Evidence (Amendment) Act* (2021): s. 50 (nueva). http://bit.ly/46ziHlk
[108] *Electronic Transactions Act*: ss. 15, 18. http://bit.ly/424Yz9o
[109] *Child Pornography (Prevention)* Act: s. 2. http://bit.ly/4gBU6RH
[110] Código Penal Federal (CPF): arts. 202, 211 Bis 1-7, 254 Bis 1, 424 Bis II. http://bit.ly/48vA49f
[111] Código Nacional de Procedimientos Penales (CNPP): arts. 51, 71, 291-294. http://bit.ly/4nhmLOz
[112] Ley Federal de Telecomunicaciones y Radiodifusión (LFTR): arts. 182-184. http://bit.ly/4prDtfo

administrativas/técnicas/físicas, aviso de vulneraciones y deber de confidencialidad,[113] mientras la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados obliga a inventarios, análisis de riesgo, bitácoras y avisos de brecha en el sector público;[114] la confianza transaccional se apoya en Código de Comercio y LFEA (infraestructura de certificación, revocación y seguridad de claves);[115] en lo financiero, la Ley Fintech demanda controles de seguridad, continuidad, APIs seguras y supervisión de la CNBV/Banxico;[116] los archivos públicos deben incorporar seguridad y trazabilidad en soportes electrónicos;[117] y la ley del Sistema Nacional de Investigación e Inteligencia obliga a plataformas cifradas y control de accesos para integrar/analizar información.[118]

Nicaragua

La Ley Especial de Ciberdelitos tipifica acceso, interceptación, interferencia/daño a datos y sistemas, fraude/espionaje/hurto, herramientas y contenidos ilícitos, e incorpora preservación/producción/interceptación con control judicial;[119] su reforma de 2024 amplía alcance (redes sociales/apps y extraterritorialidad), eleva penas, incorpora activos virtuales y responsabilidad de personas jurídicas.[120] La Ley de Protección de Datos Personales garantiza autodeterminación, impone seguridad/confidencialidad y derechos ARCO con régimen sancionador.[121] En la ley de personas consumidoras, se exige seguridad de transacciones y resguardo de datos en servicios financieros y comercio electrónico.[122]

---

[113] LFPDPPP (particulares): arts. 18–20, 38 V, 58 XI, 62. http://bit.ly/47V2UzR
[114] LGPDPPSO (sector público): arts. 3, 6, 25–35, 33–35, 53, 58, 132 X. http://bit.ly/4mvKs4e
[115] Código de Comercio: arts. 20, 102, 112 (soportes/medios electrónicos). http://bit.ly/46QxcT6; Ley de Firma Electrónica Avanzada (LFEA): arts. 13, 19, 25. http://bit.ly/3IDumrr
[116] Ley para Regular las Instituciones de Tecnología Financiera (Ley Fintech): arts. 37 III, 39 VI, 48, 58 III, 76, 83 III, 87 II, 103(b). http://bit.ly/42sqn83
[117] Ley General de Archivos (LGA): arts. 25, 41, 46 IV, 60–63. http://bit.ly/4gxxiCm
[118] Ley del Sistema Nacional de Investigación e Inteligencia en Materia de Seguridad Pública: arts. 12, 31, 34 XI, 41–43. http://bit.ly/4gBUcJ3
[119] Ley 1042, Ley Especial de Ciberdelitos: arts. 1–3, 4–15, 22–35, 36–42. http://bit.ly/46P6L0e
[120] Ley 1219/2024 (reforma Ley 1042): arts. 1–2, 8–10, 10 bis, 11, 12, 15, 30, 11 bis, 15 bis, 30 bis, 34 bis. http://bit.ly/3K8Fm0z
[121] Ley 787, Protección de Datos Personales: arts. 1, 6–15, 16–21, 28–31, 47–52. http://bit.ly/46D1LdW
[122] Ley 842, Protección de los Derechos de las Personas Consumidoras y Usuarias: arts. 6.1, 69, 79–80. http://bit.ly/3Kkbuy5

Panamá

Ley 478/2025: actualiza CP y CPP; define conceptos técnicos; tipifica difusión de íntimos no consentida, grooming, suplantación, interceptación/apoderamiento/alteración de datos y obstrucción, con agravantes por infraestructura crítica; crea capítulo de evidencia digital (preservación rápida, órdenes de suministro y obtención en tiempo real) y moderniza la cooperación internacional (canales electrónicos, equipos conjuntos).[123] En telecomunicaciones, la Ley 51/2009 obliga a conservar y suministrar registros con salvaguardas técnicas y control judicial.[124] La Ley 16/2004 refuerza la persecución de la explotación sexual de menores también en línea.[125] El Código Penal ya contemplaba secreto/intimidad, estafa por medios cibernéticos y delitos contra la seguridad informática.[126] En datos personales, la Ley 81/2019 fija principios, seguridad y notificación de brechas, reglas de transferencia y obligaciones sectoriales.[127]

Paraguay

Paraguay arma un marco donde el MITIC lidera política y respuesta a incidentes (dirección general incluida);[128] las compras públicas exigen estándares de ciberseguridad y cesión de código fuente al Estado para resguardo confidencial;[129]se incorpora cooperación MERCOSUR en ciberseguridad y protección de infraestructuras críticas;[130] la Policía Nacional crea un órgano TIC con seguridad informática propia;[131] el Código Penal actualizado cubre acceso/interceptación, sabotaje, estafa informática y medios de pago, con tutela severa de NNA;[132] los intermediarios deben informar, retener por 6 meses datos mínimos de conexión y retirar contenidos por orden;[133] en datos, aunque no hay ley general, la ley crediticia impone seguridad, secreto y notificación sectorial de brechas;[134] y la ley de servicios de

[123] Ley 478 (2025): CP arts. 151, 166-A, 184, 184-A, 185, 289-A, 289-B, 290, 290-A, 291, 292-A, 428-A; CPP arts. 112.1, 314-A, 338-A–D; L. 11/2015 arts. 4, 6.5, 7–12-J. http://bit.ly/3Iwsz7q
[124] Ley 51/2009 (datos telecom): arts. 7–14. http://bit.ly/3Ib8Eep
[125] Ley 16/2004 (integridad/ libertad sexual): arts. 231-D, 231-E, 16. http://bit.ly/4gyXe0u
[126] Código Penal (texto único 2007): arts. 162–166, 216, 285–288. http://bit.ly/3Iphhly
[127] Ley 81/2019 (protección de datos): arts. 2, 5, 9, 26, 31, 40. http://bit.ly/4muB7tA
[128] Ley N° 6207 (MITIC): art. 7 incs. 4, 5, 13, 23; art. 12. http://bit.ly/4mq3J79
[129] Ley N° 7021 (Contrataciones): art. 35. http://bit.ly/4mxIT6V
[130] Ley N° 7120 (Acuerdo MERCOSUR e-commerce): art. 12.f. http://bit.ly/3KyRk3u
[131] Ley N° 7280 (Reforma Policía): art. 227. http://bit.ly/3KzdnHf
[132] Ley N° 4439 (reforma CP): arts. 146 b–d, 174 b, 175, 175 b, 188, 248 b, 140. http://bit.ly/4mtjv10
[133] Ley N° 4868 (Comercio electrónico): arts. 6, 7, 9 incs. a–c, 10. http://bit.ly/3VrWWiv
[134] Ley N° 6534 (Datos crediticios): arts. 10, 11, 17 inc. a, 21 incs. i, p. http://bit.ly/4pG2ML2

confianza/e-ID fija requisitos de seguridad, niveles de garantía y notificación en 24 h al regulador y al CSIRT del MITIC.[135]

Perú

Tiene un catálogo penal informático (acceso ilícito, daño a datos/sistemas, herramientas, fraude, suplantación, *grooming*, interceptación; con exención para pruebas autorizadas) en la Ley 30096, reforzado por su reforma Ley 30171;[136] técnicas especiales para crimen organizado con control judicial (interceptación, agente encubierto, entrega vigilada, incautación urgente) en la Ley 30077;[137] prevención para NNA en entornos digitales (deber informativo de filtros y acciones intersectoriales) en la Ley 30254;[138] confianza transaccional vía Ley 27269 (firma y certificado digital con trazabilidad y reconocimiento);[139] protección de datos personales con deberes de seguridad y confidencialidad en la Ley 29733;[140] ciberdefensa para amenazas a soberanía/activos críticos en la Ley 30999;[141] y actualización 2025 que incorpora el uso de IA como agravante/figura en CP y en la 30096 (Ley 32314).[142]

República Dominicana

Tipifica el acceso ilícito, la interceptación, el daño de datos y el sabotaje de sistemas, y prevé medidas de preservación, producción, obtención en tiempo real y retención mínima de 90 días, además de unidades especializadas en MP/PN/DNI y alcance extraterritorial moderado;[143] el mercado de valores exige controles internos y de seguridad informática, operación sobre sistemas automatizados con continuidad y resguardo en depósitos centralizados;[144] el comercio electrónico otorga presunciones probatorias a la firma/documento digital y fija deberes de seguridad y revocación para certificadores y

---

[135] Ley N° 6822 (Servicios de confianza y e-ID): arts. 13, 17 incs. 2.a–b, 20.2, 21 incs. 3, 4.f–g, k, 28 incs. 1, 2.b, 2.e-f, 2.h, 3–4, 30–32. http://bit.ly/3ICOfyT
[136] Ley 30096 (delitos informáticos): arts. 2–5, 7–12. http://bit.ly/4ncUIiZ; Ley 30171 (modifica 30096): arts. 2–5, 7–10, 12 (mod.). http://bit.ly/46OdLdH
[137] Ley 30077 (crimen organizado): arts. 7, 9–14, 16–17, 26–30. http://bit.ly/4nETQU5
[138] Ley 30254 (uso seguro TIC NNA): arts. 3–7 (esp. 7). http://bit.ly/3IAF2af
[139] Ley 27269 (firmas/certificados): arts. 1, 3, 6–8, 10–11, 14–15. http://bit.ly/47WQxTM
[140] Ley 29733 (datos personales): arts. 9, 16–17, 30. http://bit.ly/4gBJRwt
[141] Ley 30999 (ciberdefensa): arts. 9–14. http://bit.ly/4pC9Lo5
[142] Ley 32314 (IA en CP y 30096): art. 1 (modifica arts. 46, 129-M, 132, 196-A, 217–220-C CP y la 30096). http://bit.ly/4gzQyPX
[143] Ley 53-07 (sobre Crímenes y Delitos de Alta Tecnología): arts. 1–4, 6–11, 29–41, 43–49, 52–56. http://bit.ly/48vSTt1
[144] Ley 249-17 (Mercado de Valores): arts. 34, 36, 110, 280, 306. http://bit.ly/4mxASxQ

suscriptores;[145] y la ley de datos personales incorpora principios de seguridad y deber de secreto para el tratamiento.[146]

San Cristóbal y Nieves

Electronic Crimes Act: tipifica acceso/injerencia, fraude y arsenal informático; protege sistemas restringidos; habilita registro, producción, preservación, datos de tráfico, interceptación y acceso remoto forense; prevé jurisdicción amplia y define "incautar"/"interceptar";[147] la *Interception of Communications Act* canaliza la interceptación por orden (incluida vía urgente), el "disclosure" de claves y la obtención de metadatos;[148] la *Electronic Transactions Act* consagra original y conservación electrónicos y autoriza a la Administración fijar formatos, firmas y controles de seguridad;[149] la *Data Protection Act* 2018 impone deber de seguridad y verificación a encargados, con poderes de supervisión;[150] la *Virtual Asset Act* exige políticas de ciberseguridad y protección de datos a VASPs;[151] y, en seguridad nacional, la *Anti-Terrorism Act* crea una *Electronic Crime Task Force* y autoriza interceptaciones prolongadas en casos de terrorismo.[152]

San Vicente y las Granadinas

Cybercrime Act tipifica acceso/injerencia/interceptación, fraude e identidad; agrava en infraestructura crítica; habilita preservación/producción de datos, obtención de tráfico, bloqueo de contenidos y, excepcionalmente, forense remoto; prevé jurisdicción amplia y puertos seguros para intermediarios.[153] La *Electronic Transactions Act* reconoce la equivalencia funcional de registros y firmas electrónicas, presume válidas las versiones "seguras" y faculta fijar estándares y reconocer certificados extranjeros (interoperabilidad).[154] La

---

[145] Ley 126-02 (Comercio Electrónico, Documentos y Firmas Digitales): arts. 32–34, 40, 49, 51–53. http://bit.ly/4gyXvR4
[146] Ley 172-13 (Protección de Datos Personales): arts. 1 y 5. http://bit.ly/46ieh3F
[147] Electronic Crimes Act: ss.2–3; ss.4–7, 8–11, 12–17; ss.18–25. http://bit.ly/46iNh42
[148] Interception of Communications Act: ss.4–7; ss.12–13; ss.16–17. http://bit.ly/46wn0Oh
[149] Electronic Transactions Act: ss.8–9, 15. http://bit.ly/3W8jKUt
[150] Data Protection Act 2018: ss.10, 28. http://bit.ly/47VKWNv
[151] Virtual Asset Act: s.6(2)(i)–(j). http://bit.ly/3IAyXKY
[152] Anti-Terrorism Act: ss.2(1), 67(1)–(4). http://bit.ly/47XdImw
[153] Cybercrime Act 2016: defs., conductas, agravantes, investigación (preservación/producción/tráfico/bloqueo), acceso remoto, jurisdicción, safe harbors (ss.2; 3–12, 14–21; 22–26, 29, 35–36; 33; 40–45). http://bit.ly/47VJydS
[154] Electronic Transactions Act 2015: firma/registro "seguros", presunciones, estándares y reconocimiento transfronterizo (ss.23–30). http://bit.ly/3W2wxI5

Electronic Evidence Act elimina barreras probatorias: admite registros electrónicos y satisface la "mejor prueba" vía integridad del sistema o impresos usados como registros, con presunciones técnicas y declaraciones juradas.[155]

Santa Lucía

La *Computer Misuse Act* tipifica acceso/interceptación/modificación-daño, herramientas y fraude; agrava en "computadoras protegidas" y habilita preservación, producción y registro con control judicial.[156] La *Interception of Communications Act* limita la interceptación a orden judicial (con renovaciones tasadas), prevé asistencia técnica y confidencialidad, y permite ordenar la revelación de claves y la obtención de datos de tráfico con límites.[157] El Evidence Act admite registros electrónicos, sustituye la "mejor prueba" por integridad/autenticidad y reconoce la firma electrónica cuando el método es fiable.[158] En lo transaccional, la Electronic Transactions Act consagra equivalencia funcional y safe harbors para intermediarios, presume válidas firmas/registros "seguros" y habilita reconocimiento transfronterizo.[159] La Data Protection Act exige medidas técnicas/organizativas, notificación de brechas y salvaguardas para transferencias internacionales, con régimen sancionatorio.[160]

Surinam

WTv/TAS (telecom): la ley crea y faculta a la TAS como regulador del sector (licencias, espectro, numeración, estándares y supervisión). Hablar de "seguridad de redes/servicios" es razonable como función regulatoria vinculada a estándares y calidad de servicio;[161] WER (transacciones electrónicas): establece el marco de actos por vía electrónica y sustenta la equivalencia funcional (firmas/contratos/notificaciones), con procedimientos para intermediarios;[162] y WMTF 2024 (AML/CFT): es tangencial a

[155] Electronic Evidence Act 2004: admisibilidad, autenticación, mejor prueba por integridad del sistema/printouts, presunciones y affidavits (ss.3, 5–9, 11–12). http://bit.ly/423eGEC
[156] Computer Misuse Act: ss.5, 7–12, 13, 15–21. http://bit.ly/42LimuL
[157] Interception of Communications Act: ss.3–7, 16–17, 21–22, 24(12)–(18). http://bit.ly/4o4beCf
[158] Evidence Act: ss.136C, 136E–136G. http://bit.ly/426FALF
[159] Electronic Transaction Act: ss.20–21, 23, 34, 47. http://bit.ly/3W6yDXm
[160] Data Protection Act: ss.32, 42, 45, 71+. http://bit.ly/4nH37ei
[161] Wet Telecommunicatievoorzieningen: arts. 2–3, 122–125, 131. http://bit.ly/4nhnWxt
[162] Wet Elektronisch Rechtsverkeer: arts. 1, 15–16, 77–78. http://bit.ly/4nfNMSb

ciberseguridad; la conexión es principalmente vía ciberfraude/finanzas ilícitas.[163]

Trinidad y Tobago

La *Computer Misuse Act* penaliza acceso/modificación/obstrucción ilícitos, uso/interceptación no autorizados y divulgación de credenciales; tipifica severamente el "cese" de un computador, agrava en equipos protegidos y habilita órdenes de registro/acceso con deber de asistencia técnica.[164] La *Evidence (Amendment) Act* 2021 admite sin distinción los registros electrónicos en lo penal y civil y presume su fiabilidad cuando provienen de procesos habitualmente exactos.[165] La *Data Protection Act* crea al *Information Commissioner* y obliga a los organismos públicos a medidas de seguridad y reglas estrictas para divulgar con fines de investigación.[166] La *Electronic Transactions Act* regula a los proveedores de autenticación y refuerza la equivalencia funcional de firmas y registros electrónicos.[167] La *Children Act* tipifica la pornografía infantil por medios electrónicos.[168] En seguridad del Estado, la *Anti-Terrorism (Amendment) Act* 2018 prevé entrenamiento por medios electrónicos y órdenes con alcance expreso a dispositivos.[169]

Uruguay

Uruguay adopta un esquema integrado: bloque penal moderno (acceso/vigilancia ilícita, daño y fraude informático, suplantación y "arsenales" digitales) y medidas preventivas (educación, intercambio interbancario, inmovilización rápida de fondos) contra estafas.[170] el antilavado incorpora el fraude informático como delito precedente y regula la obtención de evidencia electrónica bajo control judicial;[171] la tutela de datos impone principios y medidas de seguridad, registro y potestades de la autoridad;[172] y la confianza

---

[163] WMTF (reforma 2024): Art. I (defs; art. 29(2); remite CP arts. 489a-489b), art. 38(1), arts. 41-43; Art. II. http://bit.ly/4gxUel2
[164] Computer Misuse Act 2000: ss.2 (def. "damage"), 3-7, 8, 10-11, 14, 16. http://bit.ly/3Ke62gk
[165] Evidence (Amendment) Act 2021: ss.14B, 40. http://bit.ly/46u9IC0
[166] Data Protection Act 2011: ss.8-9, 35, 43. http://bit.ly/4pSBj95
[167] Electronic Transactions Act 2011: s.35. http://bit.ly/46PQN5V
[168] Children Act 2012: Part VIII, s.40. http://bit.ly/4pANtD3
[169] Anti-Terrorism (Amendment) Act 2018: s.13A; ss.22BC, 24. http://bit.ly/46yyOQ2
[170] Ley 20.327: arts. 288 bis-ter, 277 ter, 297 bis-ter-quater, 347 bis-ter, 348 bis-ter, 358 quater-quinquies, 359 ter, 9-11. http://bit.ly/3IeCP4m
[171] Ley 19.574: arts. 34.34, 62 y 17 (según modif. Ley 20.327 art. 4). http://bit.ly/3IozsrA
[172] Ley 18.331: arts. 5, 10, 20, 28-29, 34. http://bit.ly/46u9KK8

transaccional descansa en firmas y prestadores acreditados.[173] En paralelo, toda operación especial que afecte comunicaciones o sistemas exige autorización judicial en el Sistema de Inteligencia.[174]

Venezuela

La Ley Especial contra los Delitos Informáticos concentra la tipificación—acceso/interceptación ilícita, daño/sabotaje (incluido malware), herramientas, fraude, datos personales, comunicaciones y medios de pago.[175] La Ley sobre Protección a la Privacidad de las Comunicaciones sujeta la intervención a orden judicial con canal urgente y estricta confidencialidad;[176] la Ley de Infogobierno fija principios de seguridad (confidencialidad-integridad-disponibilidad), crea órganos rectores y el Sistema Nacional de Protección y Seguridad Informática;[177] y la Ley Orgánica de Telecomunicaciones acopla el sector imponiendo reservas y obligaciones de seguridad y calidad al operador público y privado.[178]

RESULTADOS Y DISCUSIÓN

En América Latina y el Caribe (ALC) solo se han identificado dos leyes específicas de ciberseguridad (Chile y El Salvador), mientras que la mayoría de los ordenamientos se apoyan en marcos de cibercrimen, delitos informáticos, protección de datos personales, comercio electrónico, *fintech*, inteligencia o procesal. Esta configuración normativa heterogénea produce tres brechas distinguibles: (i) conceptual, por la confusión entre ciberseguridad (gestión de riesgos y resiliencia) y cibercrimen (persecución penal); (ii) normativa, por la ausencia de un marco preventivo que asigne competencias, obligaciones y estándares verificables; y (iii) operativa, por capacidades insuficientes y reglas dispares para notificar, responder y aprender de incidentes. Sus efectos conllevan a que la región sufra de fragmentación regulatoria, costos de

[173] Ley 18.600: arts. 16–18, 25. http://bit.ly/46QK0Ji
[174] Ley 19.696: art. 20. http://bit.ly/4gFuwey
[175] Ley Especial contra los Delitos Informáticos: arts. 1–3, 6–12, 13–22, 5, 27, 29–31. http://bit.ly/47VLEKF
[176] Ley sobre Protección a la Privacidad de las Comunicaciones: arts. 1–9. http://bit.ly/4gHbFjo
[177] Ley de Infogobierno: arts. 1, 5.15, 23, 37, 41, 54–59, 66, 74, 81.10. http://bit.ly/4gzRzHL
[178] Ley Orgánica de Telecomunicaciones: arts. 8 y 2.8. http://bit.ly/4gBPlHO

cumplimiento asimétricos, baja interoperabilidad y protección desigual de infraestructuras esenciales y cadenas de suministro.

Partiendo de este diagnóstico, el problema central no es la falta de bienes jurídicos relacionados a la seguridad de la información y ciberseguridad, sino la inexistencia de una ley especial habilitante que establezca definiciones, distribuya funciones y sirva como fundamento habilitante de instrumentos ejecutivos y administrativos. Tomando las mejores prácticas de la industria, estándares y regulaciones, se logró crear una propuesta de *framework* con elementos proporcionales, adaptativos y basado en riesgos, tecnológicamente neutro, con garantías de derechos y métricas de desempeño, para reducir la incertidumbre regulatoria y mejorar la coordinación público-privada.

En consecuencia, se propone un arquetipo legislativo mínimo viable, como núcleo común regional para América Latina y el Caribe. El *framework* propuesto se organiza en diez pilares y se tomaron como referencias los siguientes instrumentos normativos más prominentes en el ámbito de ciberseguridad:

Unión Europea

- Directiva (UE) 2022/2555 (NIS2).[179]
- Reglamento (UE) 2022/2554 (DORA)[180]
- UE DORA normas técnicas (para que no quede genérico "RTS/ITS 2024") – RTS/ITS criterios de notificación de incidentes (EBA/ESMA/EIOPA).[181]
- Directiva (UE) 2022/2557 (CER).[182]
- Reglamento (UE) 2019/881 (Cybersecurity Act - CSA).[183]
- Reglamento (UE) 2025/38 (Cyber Solidarity Act).[184]
- Reglamento (UE) 2024/2847 (Cyber Resilience Act - CRA).[185]

[179] http://bit.ly/4my1Aq6
[180] http://bit.ly/46hx9jb
[181] http://bit.ly/46NqOMu
[182] http://bit.ly/4gycRp0
[183] http://bit.ly/3IuQx35
[184] http://bit.ly/425pSjW
[185] http://bit.ly/46gwgay

- Directiva 2014/53/UE (RED).[186]
- Reglamento Delegado (UE) 2022/30.[187]
- Reglamento de Ejecución (UE) 2024/482 (EUCC).[188]
- Reglamento (UE) 2016/679 (RGPD).[189]
- Directiva (UE) 2019/1937 (Whistleblowers).[190]
- Decisión (PESC) 2019/797.[191]
- Reglamento (UE) 2019/796.[192]
- Reglamento (UE) 2021/694.[193]
- Regulation (EU) 2023/1543[194].
- Product Liability Directive Directive (EU) 2024/2853.[195]
- Anti-SLAPP Directive Directive (EU) 2024/1069.[196]
- Commission Implementing Regulation (EU) 2024/2690.[197]

Chile

- Ley 21.663 - Ley Marco de Ciberseguridad.[198]
- Decreto Supremo N.° 295/2024 – Reglamento de Reporte de Incidentes.[199]

Estados Unidos de América

- CIRCIA – Propuesta de reglamentación (NPRM), 6 CFR Parte 226. [Cybersecurity and Infrastructure Security Agency (CISA). Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA).][200]
- CISA 2015 – Cybersecurity Information Sharing Act (6 U.S.C. §§ 1501–1510).[201]

---

186 http://bit.ly/4pGtH9y
187 http://bit.ly/46OAI0h
188 http://bit.ly/3Kh6MkK
189 http://bit.ly/4gDPpXp
190 http://bit.ly/4pAi9ob
191 http://bit.ly/46QrTTK
192 http://bit.ly/4nIg47R
193 http://bit.ly/46sXuJW
194 http://bit.ly/42KRISI
195 http://bit.ly/3K9ok2p
196 http://bit.ly/3IyEf9Q
197 http://bit.ly/4pyWcpq
198 https://bcn.cl/3isi2
199 https://bcn.cl/4Do2DD
200 http://bit.ly/3ImKSft
201 http://bit.ly/4n9HsM6

- DOJ - Política 2022 sobre casos bajo la CFAA (investigación de buena fe).[202]
- OFAC – Aviso 2021 actualizado sobre riesgos de sanciones por facilitar pagos de ransomware.[203]
- FinCEN – 2020 *Advisory* sobre *ransomware*.[204]
- OMB M-22-18; OMB M-23-16; OMB M-22-16. [Office of Management and Budget. M-22-18[205]; M-23-16[206]; M-22-16.][207]
- Executive Order 14028 – 2021 Improving the Nation's Cybersecurity.[208]
- Executive Order 13694 – 2015 Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities.[209]
- FedRAMP Authorization Act (44 U.S.C. cap. 36, subch. II).[210]
- SEC – Form 8-K, Ítem 1.05 (Divulgación de incidentes de ciberseguridad). [U.S. Securities and Exchange Commission. Form 8-K. [211]
- VEP Framework Vulnerabilities Equities Policy and Process for the United States Government.[212]
- US Cyber Diplomacy Act 22 U.S.C. Chapter 110.[213]
- DMCA §1201[214]
- CLOUD Act[215]

Reino Unido

- PSTI Regulations 2023 – The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products.)[216]
- Product Security and Telecommunications Infrastructure Act 2022, Chapter 46.[217]

---

[202] http://bit.ly/46OANB7
[203] http://bit.ly/48tsrjC
[204] http://bit.ly/46gwr5I
[205] http://bit.ly/46OLVxU
[206] http://bit.ly/4nAeVjf
[207] http://bit.ly/46th20F
[208] http://bit.ly/4mFcZ7O
[209] http://bit.ly/4gVyDU5
[210] http://bit.ly/3K8Sym6
[211] http://bit.ly/4gz0vgh
[212] http://bit.ly/4nkFCZ0
[213] http://bit.ly/46zFVYA
[214] http://bit.ly/4gz0xVr
[215] http://bit.ly/4pC7wRG
[216] http://bit.ly/47RBZEY
[217] http://bit.ly/47WaBWl

- The Cyber (Sanctions) Regulations 2020.[218]

Internacional/Regional

- Convenio de Budapest sobre Ciberdelincuencia (ETS 185). [Council of Europe. Convention on Cybercrime (Budapest Convention).[219]
- OSCE – Decisión N° 1202 (CBMs TIC).[220]
- UN Special Rapporteur Report on encryption and anonymity, A/HRC/29/32, May 22, 2015.[221]

Japón

- Basic Act on Cybersecurity (Act No. 104 of 2014). Translation. [222]

Singapur

- Cybersecurity Act 2018. [Singapore. Cybersecurity Act 2018. Singapore Statutes Online.] [223]

México

- CNBV – Disposiciones de carácter general aplicables a las instituciones de crédito (CUB).[224]

Francia

- LOI n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur.[225]

Estándares Técnicos

- NIST CSF 2.0. [National Institute of Standards and Technology. Cybersecurity Framework 2.0.] [226]

---

[218] http://bit.ly/3IqqBpm
[219] http://bit.ly/46wzOUX
[220] http://bit.ly/46LGakF
[221] http://bit.ly/46zG3aw
[222] http://bit.ly/3IzTW0p
[223] http://bit.ly/3IzUoM9
[224] http://bit.ly/46D7OPz
[225] http://bit.ly/4gHVySI
[226] http://bit.ly/3I9tCu8

- NIST SP 800-218 (SSDF). [National Institute of Standards and Technology. SP 800-218, Secure Software Development Framework.][227]
- NTIA – Minimum Elements for an SBOM. [U.S. Department of Commerce, NTIA. The Minimum Elements for a Software Bill of Materials (SBOM).][228]
- ISO/IEC 27001:2022.[229]
- ISO/IEC 27002:2022.[230]
- ISO/IEC 29147:2018.[231]
- ISO/IEC 30111:2019.[232]
- ISA/IEC 62443 (serie).[233]
- FIRST – Traffic Light Protocol (TLP) v2.0. [FIRST. Traffic Light Protocol (TLP).][234]
- OASIS – STIX 2.1 y TAXII 2.1. [OASIS. STIX Version 2.1.;[235] TAXII Version 2.1.][236]

Hacia un *framework* normativo homogéneo en ciberseguridad en América Latina y el Caribe.

Pilar A – Gobernanza y coordinación nacional

Este pilar establece la arquitectura institucional mínima de la ley y sus reglas de coordinación. Primero, fija definiciones comunes para evitar ambigüedades (A1) y delimita el ámbito material y subjetivo, entidades esenciales e importantes, sectores y exclusiones penal/procesal, así como criterios proporcionados de extraterritorialidad frente a riesgos transfronterizos (A2). Prevé una autoridad nacional con mandato claro, facultades de inspección y sanción, presupuesto propio y mecanismos de coordinación (A3). Establece una estrategia nacional con políticas, planes, indicadores país, revisión periódica y consulta pública (A4) y asigna roles institucionales (dirección

[227] http://bit.ly/4mtip5q
[228] http://bit.ly/4gFuKSX
[229] http://bit.ly/3W1m5k2
[230] http://bit.ly/3VZRzqS
[231] http://bit.ly/4mtKA4a
[232] http://bit.ly/4mFdbny
[233] http://bit.ly/3IB0Z9a
[234] http://bit.ly/4nFkTP7
[235] http://bit.ly/3IbzGlT
[236] http://bit.ly/481Hjpv

ejecutiva de ciberseguridad, CISO en el sector público y POC 24/7 donde corresponda) para asegurar responsabilidad y continuidad operativa (A5). Incorpora un consejo multiactor que provea asesoría permanente y participación informada (A6). Integra salvaguardas de derechos, incluida la protección del cifrado de extremo a extremo y unas reglas como la de no-retroceso (A7). Exige métricas y rendición de cuentas mediante KPIs, informes anuales y revisiones entre pares (A8). Para la coordinación regulatoria, instituye un punto único de contacto y reglas anti-duplicidad que armonicen reportes entre autoridades (A9). Finalmente, establece un Proceso de Equidades de Vulnerabilidades (VEP) público y trazable para la ponderación estatal sobre la retención o divulgación de 0-days (A10). Se debe hacer hincapié en que, para el presente pilar, se tomaron fuentes normativas adicionales de Europa, EE. UU. y Latinoamérica; específicamente de Japón y Singapur.

Pilar A – Gobernanza y coordinación nacional			
Elemento	**Descripción**	**¿Por qué debe estar?**	**Fuentes (art./sección)**
A1. Definiciones	Describir conceptos que se emplearán en el instrumento normativo.	Evita ambigüedad regulatoria y alinea terminología con estándares y otras leyes.	- Chile: Art. 2 (definiciones) en Ley 21.663. - NIS2 definiciones Art. 6; - Japón en *Basic Act on Cybersecurity*, definiciones Art. 2.
A2. Ámbito y extraterritorialidad	Entidades esenciales e importantes; sectores; exclusiones (penal/procesal) y extraterritorialidad.	Define sujetos obligados y coherencia sectorial; permite exclusiones específicas y coordinación con derecho penal/procesa.	-NIS2: Ámbito y Anexos I-II; exclusiones Art. 2 y 4; - Singapur - Ámbito (s.3) y alcance material: CII (Part 3), respuesta a incidentes (Part 4), licencias (Part 5). Extraterritorialidad: efectos limitados y funcionales

A3. Autoridad/Agencia nacional (mandato/inspección/sanciones/presupuesto/coordinación)	Mandato, independencia, inspección, sanciones, presupuesto, coordinación; mecanismos interinstitucionales y sectoriales.	Garantiza rectoría, potestad sancionadora y coordinación nacional.	- Chile: creación y atribuciones de la ANCI (Arts. 10-19); en Ley 21.663. - NIS2: autoridades competentes y punto único de contacto (Art. 8).
A4. Estrategia, políticas, planes, indicadores y consulta	Anclaje legal; revisión periódica; plan de implementación; indicadores país; consulta pública.	Integra políticas de Estado, con KPIs y revisiones cíclicas.	- NIS2: Estrategia nacional Art. 7 (KPIs y revisión al menos 5 años). - Japón, Basic Act on cybersecurity: estrategia y cuartel general Arts. 12, 25-37. - Chile: Política Nacional de Ciberseguridad (Arts. 11, 48) en Ley 21.663.
A5. Roles institucionales	Director ejecutivo de ciberseguridad; CISO en entidades públicas; POCs 24/7 (incluye sector privado crítico).	Clarifica responsabilidades y continuidad operativa 24/7.	- NIS2: gobernanza y formación de directivos (Art. 20); CSIRTs y POC 24/7 (Arts. 8, 10, 11). - México: Disposiciones de carácter General Aplicables a las Instituciones de Crédito, Artículo 168 Bis 13 (CISO/dir. ciberseguridad)
A6. Consejo/Comité multiactor	Sector privado, academia, sociedad civil.	Asegura participación y asesoría continua.	- Chile: Consejo Multisectorial (Art 20). Ley 21.663. - UE Cybersecurity Act (Reg. 2019/881): crea el Stakeholder Cybersecurity Certification Group (SCCG), un comité multiactor que asesora a la Comisión/ENISA en certificación (art. 22).
A7. Transparencia y derechos	Salvaguardas derechos fundamentales; protección del cifrado extremo a extremo; no-retroceso.	Equilibra seguridad con derechos y preserva cifrado robusto.	- NIS2: cumplimiento con derechos y *state-of-the-art encryption* (considerando 51). - ONU: Relator Especial, cifrado y anonimato (A/HRC/29/32).
A8. Métricas, evaluación y rendición de cuentas	KPIs país; informes anuales; revisión independiente.	Permite medir madurez y ajustar políticas.	- NIS2: KPIs y revisión periódica de la estrategia (Art. 7, *peer-reviews* Art. 19); obligaciones de información y cooperación (Arts. 18, 23, 30 y tareas de autoridades/ENISA). - UE Cyber Solidarity Act (Reg. (UE) 2025/38): Art. 21 crea el European Cybersecurity Incident Review Mechanism (mecanismo de revisión de incidentes a escala UE)
A9. Armonización multi-agencia (one-stop),	Regla de ventanilla única; evitar reportes duplicados.	Reduce carga regulatoria y mejora calidad de datos.	- NIS2: Single Point of Contact (Art. 8). - DORA (arts. 19 y 21), reporting de incidentes TIC y coordinación inter-autoridades. Mandato a las

evitar duplicidades			ESAs para estudiar la centralización mediante un "single EU Hub".
A10. VEP (*Vulnerability Equities Process*)	Proceso estatal para retener/divulgar *0-days* con salvaguardas.	Asegura trazabilidad y ponderación de impactos.	EE. UU.: VEP 2017 (carta pública).

Pilar B – Capacidades operativas del Estado

Este pilar define las capacidades mínimas y continuas para prevenir, detectar, responder y recuperarse de incidentes a nivel país. Establece CSIRT/CERT nacionales y sectoriales con operación 24/7, competencias mínimas, portal y canales de alerta e intercambio, como núcleo técnico y punto de articulación con el sector privado y con otros Estados (B1). Institucionaliza la gestión de crisis y la continuidad de gobierno/negocio mediante comité, umbrales de severidad comunes, ejercicios periódicos y protocolos de comunicación pública, integrados con marcos de resiliencia operacional en sectores sistémicos (B2). Habilita la inteligencia de amenazas y la compartición (CTI) bajo TLP 2.0 y con salvaguardas de responsabilidad y competencia (*safe harbor*/antimonopolio), incluyendo cooperación transfronteriza mediante redes 24/7 (B3). Crea un GovSOC/Centro Nacional para el monitoreo continuo del sector público, la correlación de telemetría y el canal técnico directo con el CSIRT, elevando la detección temprana y la coordinación operativa (B4). Finalmente, define lineamientos de respuesta comunicacional coordinados con protección civil y reguladores, incluidos avisos al público cuando proceda, y prevé mecanismos de auxilio/solidaridad para crisis de gran escala (B5).

Pilar B – Capacidades operativas del Estado			
Elemento	**Descripción**	**¿Por qué debe estar?**	**Fuentes (art./sección)**

B1. CSIRT/CERT nacionales o sectoriales	Competencias mínimas; intercambio; alertas; portal; 24/7.	Núcleo operativo para manejo de incidentes y alerta temprana.	- NIS2: CSIRTs (Arts. 10-12), creación de CSIRTs. - Chile: CSIRT Nacional/Defensa en la Ley 21.663 (Arts. 24, 27, 29, 30, 31) (CSIRT Nacional, CSIRT de la Defensa Nacional y CSIRT institucionales; funciones y coordinación)
B2. Gestión de crisis y continuidad de gobierno o negocio	Comité; umbrales; ejercicios; comunicación pública.	Coordina respuesta nacional y resiliencia.	- NIS2 (cooperación y crisis: Arts. 9-11, 15, 16). - DORA UE (resiliencia operacional), Arts. 5 Comité (gobernanza de crisis), 11(7) función de gestión de crisis con procedimientos de comunicación interna y externa, 14, 18-21 Umbrales (clasificación y reporte), 49 ejercicios de gestión de crisis y contingencia a nivel UE.
B3. CTI y compartición (TLP; antimonopolio/*safe harbor*)	TLP; salvaguardas de responsabilidad/antimonopolio.	Comparte inteligencia con protección legal.	- FIRST TLP 2.0, Definiciones y reglas de compartición de TLP. - CISA 2015 (protecciones de responsabilidad) Arts. 6 U.S.C. § 1503(c)(e), § 1505. - NIS2 Cap. VI (acuerdos de intercambio), Art. 29. - Convenio de Budapest Ciberdelincuenia (red 24/7), Art 35.
B4. GovSOC/Centro Nacional	Monitoreo 24/7 sector público; telemetría; canal con CSIRT.	Unifica detección/correlación estatal.	- Chile: ANCI - acceso a registros y Red Segura del Estado (RCSE) Ley 21.663, Arts 23, 24. - NIS2 habilita soporte operativo/asesoría (Arts. 10, 11). - UE Cyber Solidarity Act (Art. 3), European Cybersecurity Alert System con National Cyber Hubs y Cross-Border Cyber Hubs (SOC nacionales y transfronterizos)
B5. Respuesta comunicacional	Lineamientos; coordinación con protección civil y reguladores.	Minimiza daño reputacional y desinformación.	- Chile, Ley 21.663 Art 7: deber de informar a potenciales afectados. - NIS2 (información al público cuando sea necesario, Art. 9, 16, 23(7)). - EU Cybersecurity Act, Arts 7 (Cooperación operativa), 10 (Sensibilización y educación). - EU Cyber Solidarity Act (mecanismos de emergencia), Arts 3, 10, 14.

Pilar C – Gestión de riesgos e higiene digital

Este pilar fija la capa mínima y continua de gestión del riesgo que deben implementar las entidades para reducir exposición, acelerar la detección y estandarizar la respuesta. Exige un ISMS (Sistema de Gestión de Seguridad de la Información/SGSI) con política, análisis de riesgos, controles mínimos, registro de eventos (*logging*) y gestión de parches, como base de mejora continua y de adopción de controles "*state-of-the-art*" (C1). Establece deberes de diligencia en la cadena de suministro, incluidos MSP/MSSP, con SBOM de elementos mínimos, derecho de auditoría y cooperación con CSIRTs, para mitigar riesgos de terceros y habilitar trazabilidad técnica y legal (C2). Define requisitos para nube y servicios gestionados respecto de disponibilidad de datos operativos de seguridad, portabilidad y notificación de fallos, considerando su carácter transfronterizo y su papel en servicios críticos (C3). Institucionaliza programas de concienciación y formación por rol, desde directivos hasta operativos, como control determinante frente al error humano y para cimentar la cultura de seguridad (C4). Finalmente, activa mecanismos de divulgación coordinada de vulnerabilidades (CVD/VDP) con safe harbor nacional, lineamientos para pruebas autorizadas, plazos y canales estandarizados, a fin de maximizar hallazgos tempranos sin criminalizar la investigación de buena fe (C5).

Pilar C – Gestión de riesgos e higiene digital			
Elemento	**Descripción**	**¿Por qué?**	**Fuentes (art./sección)**
C1. ISMS	Política; análisis de riesgo; controles mínimos; logging; parches.	Base de gestión continua y controles "*state-of-the-art*".	- NIS2: lista mínima de medidas (Art. 21(2)). - NIST CSF 2.0: gobernanza y funciones PR/DE/RS/RR. - Familia ISO 27000: ISO/IEC 27001:2022 (requisitos del ISMS) e ISO/IEC 27002:2022 (guía de controles)

C2. Cadena de suministro/MSP/MSSP; *SBOM*; derecho de auditoría; registro/coop. con CSIRT	Diligencia a terceros/MSP/MSSP; cláusulas; SBOM; derecho de auditoría; registro/notificación MSP/MSSP.	Los ataques de cadena son vector principal; SBOM otorga trazabilidad.	- NIS2 (supply chain; MSP/MSSP, rec. 84-86; Art. 21(2)-(5)), cadena de suministro, MSP/MSSP, registro y cooperación con CSIRT. - NTIA SBOM (elementos mínimos). - UE Cyber Resilience Act. Arts. 3(39), Anexo I, Parte II. Requisitos esenciales y manejo de vulnerabilidades, documentación técnica, proceso y evaluación de riesgos, reporte y coordinación.
C3. Nube/servicios gestionados (soberanía operativa y notificación)	Requisitos mínimos; localización/portabilidad de datos operativos de seguridad; notificación de fallos.	Cloud/MSP son "esenciales" y transfronterizos.	- NIS2 (Art 6(30), Art. 21(5) Anexos I-II (Clasificación como esenciales); obligaciones y reporte de incidentes, Art. 23; rec. 84-86). - EU Cybersecurity Act, esquemas de certificación cloud (EUCS). - Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. (considerando 74) - CLOUD Act (EE. UU.)
C4. *Awareness* y formación por rol	Competencias mínimas de seguridad por rol.	Las habilidades del personal son control clave.	- NIS2 (formación de directivos y personal, Art. 20; 21(2)(g)). - EU DORA. Art. 13(6), exige programas obligatorios de concienciación y formación en resiliencia digital. - EU Cybersecurity Act. Art. 10, sensibilización/educación y guías de ciberhigiene.
C5. Divulgación responsable e investigación de buena fe (pruebas autorizadas - safe harbor)	*Safe harbor* nacional; lineamientos para pruebas autorizadas.	Proceso técnico-legal para reportes de vulnerabilidades. Incentiva hallazgos tempranos sin criminalizar investigación de buena fe.	- EE. UU.: DOJ - política de no perseguir investigación de buena fe. - UE Cyber Resilience Act (CRA) Art. 13: gestión de vulnerabilidades del fabricante, Art. 14: notificación ≤ 24 h de vulnerabilidades explotadas/incidentes. - ISO/IEC 29147, pauta la política y el proceso de divulgación y la ISO 30111, gestión interna del reporte. - EU Cyber Resilience Act, Art. 13 (obligaciones del fabricante: evaluación de riesgos, procesos de gestión de vulnerabilidades/CVD durante todo el ciclo)

Pilar D – Infraestructuras esenciales/sectores críticos

Este pilar concentra obligaciones reforzadas y coordinación sectorial sobre los operadores con mayor impacto sistémico por ataques informáticos en infraestructura o sistemas críticos. Establece, primero, criterios objetivos y un registro nacional con revisión periódica para identificar sectores/operadores esenciales (y, cuando corresponda, entidades críticas) y mantener actualizado este catálogo (D1). Segundo, dispone requisitos avanzados proporcionales al riesgo, incluyendo evaluaciones periódicas, pruebas de *red team* tipo TLPT y continuidad operativa con metas RTO/RPO, a fin de validar resiliencia real y no solo de papel (D2). Tercero, define autoridades competentes por sector y su coordinación con la autoridad nacional mediante un punto único de contacto, evitando solapamientos y clarificando la supervisión y la ejecución (D3). Cuarto, incorpora evaluaciones coordinadas de riesgos de interdependencia, con pruebas conjuntas y de cadena de suministro, para anticipar y mitigar efectos en cascada entre sectores críticos (D4). Por último, prevé un tratamiento específico para OT/ICS, alineado con la serie ISA/IEC 62443 y en congruencia con la seguridad física, definiendo roles y controles a lo largo del ciclo de vida (D5).

En la región, leyes recientes en ciberseguridad como la de Chile (Ley N.° 21.663), ya introducen servicios esenciales y operadores de importancia vital con procedimiento administrativo específico para su aprobación y revisión periódica, lo que ilustra la viabilidad jurídica del enfoque propuesto. No obstante, hay que recordar que Chile como pionero en la región en el ámbito de ciberseguridad regulatoria, comenzó su proyecto de ley con un título de "Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información"[237], y concluyó su promulgación con el nombre oficial de "Ley Marco de Ciberseguridad", y aunque esto pareciera un asunto de forma, es de fondo, toda vez que como la infraestructura crítica contempla también seguridad física, otros poderes del Estado tienen competencia sobre los activos y genera problemas de competencia; como resultado únicamente se acotó a servicios esenciales y operadores de importancia vital.

Por su parte, en la UE, la NIS 2 regula las entidades esenciales y entidades importantes, mientras que la CER (Directiva relativa a la resiliencia de las

[237] Véase http://bit.ly/47WkmUv

entidades críticas), regula las entidades críticas. Esto quiere decir, que, al momento de aplicar este apartado, el legislador debe hacer un análisis respecto a si debe separar las entidades esenciales e importantes como la UE, y los servicios esenciales y operadores de importancia vital como Chile, dejando el marco jurídico de infraestructuras o entidades críticas fuera del objeto de la ley de ciberseguridad, o regularlas en un mismo instrumento. Para efectos prácticos, en el presente apartado se considerarán tanto entidades esenciales, importantes y críticas.

Pilar D – Infraestructuras esenciales/sectores críticos			
Elemento	**Descripción**	**¿Por qué?**	**Fuentes (art./sección)**
D1. Sectores/operadores esenciales	Criterios; registro nacional; revisión periódica de listados.	Focaliza esfuerzos en servicios con mayor externalidad; actualiza el universo obligado.	- NIS2: Arts. 2(1)(2), 3(1)-(3) (lista y revisión bienal); Anexos I–II (sectores). - Chile: Ley 21.663, Arts. 4-6 (Servicios esenciales y operadores de importancia vital). - UE CER (Dir. (UE) 2022/2557), Arts. 5, 6 y 7.
D2. Obligaciones reforzadas	Evaluaciones periódicas; TLPT; RTO/RPO y planes de continuidad.	Requisitos avanzados proporcionados al riesgo sistémico; valida resiliencia real.	- NIS2: Art. 21 (2)(c) (medidas de gestión). - DORA: Art. 11 (respuesta/recuperación, BIA, pruebas de continuidad), 26 (TLPT). - UE CER (Dir. (UE) 2022/2557), Art. 11 (evaluación de riesgos periódica) y Art. 13 (medidas de resiliencia + plan de resiliencia).
D3. Supervisión sectorial y coordinación	Autoridades por sector; coordinación con autoridad nacional y punto único de contacto.	Alinea competencias y evita solapamientos regulatorios.	- NIS2: Art. 8(1)-(5) (autoridades competentes y single point of contact); Cap. VII Arts.31-36 (supervisión y ejecución); Art. 14, 15 y 16 (Cooperation Group, CSIRT Network, EU-CyCLONe). - UE CER (Dir. (UE) 2022/2557), Arts. 9 (Autoridades competentes y single point of contact) y 11 (Cooperación entre Estados miembros), 19 (Critical Entities Resilience Group). - Chile: Ley 21.663, Arts. 26 (normativa sectorial).
D4. Interdependencias/efecto cascada	Evaluación de riesgos entre sectores; pruebas conjuntas y de	Evita dominó entre sectores críticos y dependencias ocultas.	- NIS2: Art. 22 (evaluaciones coordinadas de cadenas críticas); Recital 30 (coherencia con seguridad física y coordinación inter-autoridades). - UE CER (Dir. (UE) 2022/2557), Arts. 5 (evaluación nacional de riesgos), 12 (evaluación de riesgos por la entidad crítica).

	cadena de suministro.		- UE Cyber Solidarity Act Art. 3 (European Cybersecurity Alert System) y Art. 5 (Cross-Border Cyber Hubs), Art. 21 (Incident Review Mechanism)
D5. OT/ICS (físico-lógico)	Coordinación con seguridad física; roles y controles por la serie ISA/IEC 62443.	ICS/OT requieren salvaguardas y responsabilidades específicas por rol.	- ISA/IEC 62443: partes 1-1, 2-1, 3-2, 3-3, 4-1/4-2 (roles, programa de seguridad, requisitos de sistema y componentes). - NIS2 (Considerando 30 liga con CER y pide coherencia institucional, Coordinación seguridad física). - UE CER (Dir. (UE) 2022/2557), Art. 5 (evaluación nacional de riesgos) y Art. 12–13 (evaluación y plan de resiliencia de la entidad crítica)

Pilar E – Reportes y gestión de incidentes

Este pilar define un ciclo completo de notificación y aprendizaje con umbrales y plazos perentorios y un canal único para asegurar alerta temprana, coordinación efectiva y trazabilidad (E1). Estandariza el contenido mínimo del reporte (IoC, impacto/severidad y medidas de contención/mitigación) y exige acuse y guía inicial del CSIRT tras la alerta, cerrando el bucle operativo (E2). Dada la naturaleza sistémica del *ransomware*, incorpora reporte de cifrado/exfiltración, reporte de pagos cuando aplique y coordinación con regímenes de sanciones y AML/CFT, incluyendo comunicación pública cuando proceda (E3). Protege a víctimas e informantes de buena fe: la mera notificación no incrementa responsabilidad, habilitas canales confidenciales y reconoce notificación voluntaria y *near-misses* (E4). Para priorizar y habilitar coordinación interagencia, adopta una clasificación nacional de severidad con disparadores claros, incluyendo el registro de *near-misses* (E5). Consolida la mejora continua mediante *post-mortems* con acciones correctivas y plazos (E6). Finalmente, asegura interoperabilidad técnica (por ejemplo, STIX 2.1/TAXII 2.1), campos obligatorios y retroalimentación del CSIRT, evitando reportes duplicados y facilitando el intercambio automatizado entre autoridades y operadores (E7).

Pilar E – Reportes y gestión de incidentes			
Elemento	**Descripción**	**¿Por qué?**	**Fuentes (art./sección)**

E1. Umbrales y plazos	≤ 24 h aviso temprano; ≤ 72 h detalle; final ≤ 1 mes; canal único	Da visibilidad temprana y trazabilidad.	- NIS2: Art. 23(4) (a)-(e) (24 h/72h/informe final ≤ 1 mes; progreso si sigue abierto); Art. 23(5) (acuse/guía el CSIRT) - DORA - Art. 19–21 + RTS/ITS (2024) fijan plazos armonizados. - UE RGPD: Art. 33 (72 h brecha de datos personales).
E2. Contenido del reporte	IoC; impacto; mitigación; contención.	Estandariza análisis y respuesta coordinada.	- NIS2: Art. 23(4)(b)-(d) (severidad/impacto; IoC; mitigación/causas). - EE. UU. CIRCIA: (NPRM, 6 CFR Parte 226).
E3. *Ransomware* (cifrado/exfiltración, pagos, sanciones)	Reporte de cifrado/exfiltración; reporte de pagos; coordinación sanciones/AML; comunicación pública cuando proceda.	Desincentiva pagos, alinea con sanciones y apoya recuperación.	- CIRCIA (EE. UU.) - regla propuesta (NPRM, 6 CFR Parte 226): § 226.5(b): 24 h para el Ransom Payment Report (desde que se desembolsa el pago). - NIS2: Art. 23(7) (información al público cuando sea necesario). - OFAC Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (21-sep-2021)
E4. Protección informante/víctima	No penalización extra por notificar; confidencialidad; notificación voluntaria.	Incentiva reporte temprano sin represalias.	- UE Directiva de Whistle blowers 2019/1937, Art. 16 (deber de confidencialidad: no revelar identidad del informante); Art. 21(1)-(3) (protección contra represalias y no incurrir en responsabilidad por reportar de buena fe)- - NIS2: Art. 23(1) ("la mera notificación no incrementa la responsabilidad") y Art. 30(1)-(2) (notificaciones voluntarias; *near-misses*; tratamiento conforme al Art. 23). - EE. UU. CISA 2015, 6 U.S.C. § 1505 (no cause of action/protección de responsabilidad por compartir indicadores)
E5. Clasificación de severidad	Taxonomía (alto/medio/bajo; near-miss); disparadores.	Priorización y coordinación inter-agencia.	- NIS2: Art. 23(3) (criterios de "incidente significativo" para el umbral de notificación). - Chile: Ley 21.663 (Art. 27) + DS 295/2024 (Reglamento de reporte, arts. 3 y 5) - DORA. Arts. 18 y 19 (Clasificación de incidentes relacionados con las TIC y ciberamenazas y Notificación de incidentes importantes relacionados con las TIC)
E6. Lecciones aprendidas / Post-mortem	Acciones correctivas; plazos.	Mejora continua post-incidente.	- NIS2: Art. 21(2) (gestión de incidentes/continuidad) y Art. 23(4)(d) (causas y mitigación en el informe final). - DORA, Arts. 13 (revisiones posteriores al incidente. - EU Cyber Solidarity Act (Art. 21 crea el Mecanismo Europeo de Revisión de Incidentes de Ciberseguridad).

E7. Interoperabilidad de reportes	Formatos mínimos (STIX/TAXII); campos obligatorios; acuse y *feedback* CSIRT.	Automatiza ingestión y compartición.	- OASIS: STIX 2.1 y TAXII 2.1 (estándares). - NIS2: Art. 23(5) (acuse/guía del CSIRT) y Cap. V-VI (cooperación/compartición).

Pilar F – Seguridad de productos digitales y certificación

Este pilar traslada la seguridad durante todo el ciclo de vida al nivel del producto y sus componentes, fijando deberes claros para fabricantes y proveedores. Define requisitos mínimos de soporte y actualización, gestión/divulgación de vulnerabilidades (VDP/VHD), y fin de vida/soporte (EoL) con comunicación comprensible al usuario (F1). Establece un régimen de conformidad y certificación proporcional al riesgo, apoyado en procedimientos de evaluación y marcado reconocidos y en esquemas de certificación interoperables (por ejemplo, como en la UE el CSA/EUCC) para favorecer confianza y comparabilidad (F2). Ordena etiquetado e información al usuario sobre período de soporte y canales de reporte como condición de transparencia y toma de decisiones informada (F3). Alinea seguros cibernéticos con marcos de gestión de riesgo ampliamente utilizados, de modo que pólizas y exigencias reflejen buenas prácticas verificables (F4). Prevé reconocimiento de esquemas/equivalencias, vigilancia de mercado y retiros/*recalls* cuando exista riesgo grave, evitando barreras innecesarias y acelerando la mitigación (F5). Finalmente, incorpora deberes de diligencia y responsabilidad por vulnerabilidades graves, con sanciones proporcionales, para incentivar *secure-by-design*/default y parcheo oportuno como estándar de la industria (F6).

Cabe señalar que este pilar podría no formar parte directa del núcleo normativo de una ley de ciberseguridad, sino constituir un fundamento habilitante para desarrollos regulatorios específicos. La UE, por ejemplo, optó por separar estas materias del marco general de NIS2, desarrollando el *Cyber Resilience Act* como instrumento normativo independiente, reconociendo la especificidad técnica y la necesidad de marcos de conformidad diferenciados

para productos digitales. Sin embargo, se incluye aquí dado que las leyes de ciberseguridad contemporáneas frecuentemente establecen mandatos o bases habilitantes para que las autoridades competentes desarrollen estos marcos complementarios.

Es importante distinguir que mientras los productos digitales (*hardware, software, IoT*) requieren enfoques centrados en el ciclo de vida, actualizaciones y conformidad técnica, los servicios en ciberseguridad (auditorías, *pentesting*, consultoría) demandan marcos de responsabilidad profesional, competencia técnica y seguros por mala praxis. Aunque el componente de seguros cibernéticos no es determinante para la efectividad de una ley de ciberseguridad, las regulaciones actuales tienden a abordarlo como elemento complementario que incentiva la adopción de buenas prácticas a través de mecanismos de mercado, alineando las exigencias aseguradoras con estándares verificables de gestión de riesgo cibernético.

Pilar F – Seguridad de productos digitales, servicios en ciberseguridad y certificación			
Elemento	**Descripción**	**¿Por qué?**	**Fuentes (art./sección)**
F1. Productos/IoT (soporte, actualizaciones, VHD, EoL). Fin de vida/soporte	Soporte y actualizaciones; gestión de vulnerabilidades; EoL; "secure-by-default". Comunicación y mitigaciones de fin de soporte.	Reduce el riesgo a lo largo de todo el ciclo de vida del producto. Evita exposición por equipos sin soporte.	- Cyber Resilience Act: Anexo I (requisitos esenciales); Art. 13(17) (punto de contacto para vulnerabilidades), Art. 13(19) (información al usuario y fin de soporte), Art. 14(1)-(6) (notificación ≤ 24 h vulnerabilidades explotadas/incidentes). - PSTI Regs 2023: Schedule 1, 1-3 (contraseñas, canal de reporte, período mínimo de actualizaciones). - RED (UE) 2014/53/EU + Reglamento Delegado (UE) 2022/30: impone requisitos de ciberseguridad a equipos radio/IoT (Art. 3(3)(d)-(f):
F2. Conformidad/ certificación proporcional al riesgo	Esquemas aceptados; proporcionalidad por riesgo.	Facilita mercado, confianza y comparabilidad.	- Cyber Resilience Act (CRA): Art. 30 (marcado CE), Art. 32 (procedimientos de evaluación); posibilidad de apoyarse en esquemas de certificación del CSA (Art. 27(9)). - Cybersecurity Act (CSA) 2019/881: Título III (Arts. 46, 52-58). - EUCC: Reglamento de Ejecución 2024/482.

F3. Etiquetado/Información al usuario	Período de soporte; canal de reporte.	Informa riesgos y ciclo de vida; mejora la tomada de decisión.	- Cyber Resilience Act (CRA): Art. 13(17)(19) (información al usuario, fin de soporte). - Reino Unido PSTI Regulations 2023 (Schedule 1, 2-3 (cómo reportar; período mínimo y fecha fin de actualizaciones).
F4. Seguro cibernético	Reconocimiento de marcos de riesgo.	Alinea pólizas y exigencias con buenas prácticas.	- UE DORA Arts. 27(1)(e): los *testers* deben estar cubiertos por seguros de responsabilidad profesional (por ejemplo, por mala *praxis* o negligencia). Nota: Esto es para el proveedor de *pentesting*, no un seguro cibernético de la entidad. Además, aquí es para un servicio, no para un producto per se. - Francia, *LOI n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur*[238] Art. 5, asegurabilidad de daños por ciberataques.
F5. Reconocimiento de esquemas / vigilancia de mercado / retiros	Aceptación de certificados/equivalencias; vigilancia; retiros por riesgo grave.	Evita barreras y permite retirada rápida ante peligro.	- Cyber Resilience Act (CRA): Art. 27(9) (uso de esquemas UE), Art. 30 (marcado CE), Art. 53 (medidas de vigilancia/retirada). -Cybersecurity Act (CSA) Arts 46, 52, 54, 56-58/EUCC: Reglamento de Ejecución como base de certificación.
F6. Responsabilidad por vulnerabilidades graves (deber de diligencia)	Deber de diligencia del fabricante/proveedor y sanciones asociadas.	Incentiva "*secure-by-design*" y parches oportunos.	- Cyber Resilience Act (CRA): Art. 64(2)-(4) (régimen de multas administrativas por incumplimientos de Anexo I y Arts. 13-14; hasta 2.5 %/15 M€). - Directiva de Responsabilidad por Productos (PLD) – Dir. (UE) 2024/2853. Arts Art. 4(1): "producto" incluye software; Art. 7(2)(f): al valorar defectuosidad se consideran los requisitos de seguridad pertinentes, incluidos los de ciberseguridad, entonces fallo en seguridad/correcciones puede ser defecto, Art. 7(2)(c),(e): contempla aprendizaje/actualizaciones y control del fabricante, cubriendo deberes post-venta (no parchear puede generar responsabilidad)

Pilar G – Cooperación internacional y ciberdiplomacia

Este pilar convierte la cooperación exterior en una capacidad operativa para prevenir, detectar, responder y recuperarse de incidentes transfronterizos. Establece mecanismos formales de cooperación con canales 24/7, CBMs y redes regionales de CSIRTs alineadas con foros/grupos de coordinación (G1). Distingue y habilita la asistencia mutua no penal (operativa/civil) entre autoridades de ciberseguridad y CSIRTs (alertas, apoyo técnico y

[238] véase http://bit.ly/3VxnbnB

coordinación) independiente de la cooperación penal clásica (G2). Define gestión de crisis y mando transfronterizo, con autoridades competentes, reglas de escalamiento y coordinación internacional para incidentes de gran escala (G3). Incorpora medidas restrictivas y respuesta diplomática coordinada (por ejemplo, regímenes de sanciones selectivas) basadas en procedimientos de atribución y actuación conjunta (G4). Asegura interoperabilidad y confidencialidad del intercambio (como TLP) mediante protocolos estandarizados y salvaguardas para proteger fuentes y datos sensibles (G5). Finalmente, institucionaliza la ciberdiplomacia mediante puntos focales Ministerio o Secretaría de Relaciones Exteriores (o Cancillería) y, cuando proceda, agregadurías/adjuntos digitales en misiones prioritarias, para traducir obligaciones internacionales en coordinación sostenida y disuasión creíble (G6). Finalmente, establece un mandato legislativo explícito para que el Estado desarrolle y publique una posición nacional sobre la aplicación del derecho internacional en el ciberespacio, dotando de legitimidad democrática y coherencia jurídica a la participación del país en foros multilaterales y procesos de construcción normativa internacional (G7).

Si bien la cooperación internacional y la ciberdiplomacia constituyen materias de política exterior que, por su naturaleza, corresponden al poder ejecutivo y se instrumentan típicamente a través de actos presidenciales, decretos o directivas ejecutivas, resulta conveniente establecer fundamentos habilitantes en la ley de ciberseguridad para evitar actuaciones arbitrarias o vacíos competenciales que impidan una respuesta coordinada efectiva. La experiencia regional demuestra la importancia de estas bases legales: República Dominicana, por ejemplo, designó mediante Decreto núm. 729-22 de diciembre de 2022 a un asesor del Ministerio de Relaciones Exteriores para asuntos de ciberseguridad con rango de embajador, actuando bajo las atribuciones constitucionales del artículo 128 y la Ley núm. 630-16 Orgánica del Ministerio de Relaciones Exteriores[239]. Este tipo de designaciones y la creación de capacidades diplomáticas especializadas requieren no solo voluntad política, sino también marcos jurídicos claros que definan competencias, procedimientos y alcances de la cooperación internacional en ciberseguridad, evitando que la ausencia de mandatos específicos limite la capacidad estatal de respuesta ante amenazas transfronterizas o genere incertidumbre sobre las

[239] Véase http://bit.ly/3Iye6Ie

facultades para suscribir acuerdos operativos con contrapartes internacionales.

Un precedente particularmente relevante en este contexto es el caso de los Países Bajos, donde, a raíz de un debate parlamentario sobre ciberseguridad y de la moción Verhoeven/Bruins Slot, la Cámara de Representantes solicitó formalmente al gobierno que tomara la iniciativa para promover la aplicación del derecho internacional en el dominio digital e informara al Parlamento al respecto. En respuesta, el Ministerio de Asuntos Exteriores, en coordinación con los Ministerios de Defensa, Justicia y Seguridad, e Interior y Relaciones del Reino, remitió en 2019 una carta al Parlamento con un anexo[240] que expone la interpretación neerlandesa de las principales normas de derecho internacional aplicables al ciberespacio, que hoy se reconoce como la posición nacional de los Países Bajos en la materia. Este caso, recogido entre las buenas prácticas compiladas por UNIDIR[241], ilustra un modelo de legitimación democrática de la política exterior digital en el que la posición nacional se formula desde el ejecutivo, pero en cumplimiento de una solicitud explícita del órgano legislativo. Para los países de América Latina y el Caribe, la inclusión de un mandato legislativo similar en sus respectivas leyes de ciberseguridad permitiría institucionalizar este proceso de consulta y rendición de cuentas, asegurando que el Ministerio o Secretaría de Relaciones Exteriores (o Cancillería), en coordinación con las autoridades competentes en materia de ciberseguridad, defensa y justicia, elabore una posición nacional que refleje no sólo criterios técnicos y diplomáticos, sino también un consenso político legitimado por el poder legislativo, fortaleciendo así la coherencia del Estado en negociaciones internacionales sobre normas de comportamiento responsable en el ciberespacio, aplicación del derecho internacional humanitario, legítima defensa, atribución de responsabilidad estatal y otras cuestiones jurídicas críticas.

Pilar G – Cooperación internacional y ciberdiplomacia			
Elemento	**Descripción**	**¿Por qué?**	**Fuentes (art./sección)**

[240] Véase https://bit.ly/43DVkGK
[241] Véase https://bit.ly/3JYAR92

G1. Mecanismos de cooperación (canales, CBMs, redes regionales)	Canales 24/7, CBMs interestatales, y redes regionales de CSIRTs; alineación con grupos/registros y foros de cooperación.	Mejora la confianza y el flujo oportuno de información transfronteriza para prevención, detección y respuesta.	- Budapest Art. 35 (red 24/7); - OSCE Decisión N° 1202 (CBMs; punto de contacto); - OEA/CICTE, CSIRT Americas (red regional); - NIS2 Art. 14 (Cooperation Group), Art. 15 (CSIRTs network), Art. 16 (EU-CyCLONe), Art. 17 (cooperación internacional).
G2. Asistencia mutua no penal (operativa/civil)	Procedimientos para auxilio técnico entre autoridades nacionales de ciberseguridad/CSIRTs (alertas, apoyo, coordinación), independientes de la cooperación penal.	Acelera contención y recuperación ante incidentes transfronterizos sin judicializar la respuesta operativa.	- NIS2 Art. 11 (tareas de CSIRTs, incluida asistencia mutua), Art. 15(2) (asistencia mutua en la red de CSIRTs) Art. 17 (cooperación con terceros países). - OEA/CICTE – CSIRTAmericas (mecanismos de apoyo regional).
G3. Gestión de crisis y mando (nacional/transfronterizo)	Coordinar respuesta a incidentes cibernéticos de gran escala que excedan capacidades nacionales individuales, incluyendo designación de autoridades competentes, protocolos de escalamiento y mecanismos de coordinación transfronteriza.	La coordinación institucionalizada permite respuesta rápida, evita duplicación de esfuerzos y facilita compartir recursos técnicos y de inteligencia durante crisis.	- UE NIS2: crea y articula autoridades/CSIRTs, Grupo de Cooperación y EU-CyCLONe para gestión de crisis a nivel de la UE (arts. 14-17; recitals sobre coordinación con IPCR)
G4. Medidas restrictivas y respuesta diplomática coordinada	Marco jurídico para imponer sanciones selectivas contra individuos y entidades responsables de ciberataques significativos, incluyendo procedimientos de atribución y respuesta diplomática coordinada.	Proporciona herramientas legales para responder proporcionalmente a amenazas cibernéticas estatales sin recurrir a medidas militares.	- UE Decisión (PESC) 2019/797 y Reglamento (UE) 2019/796 (régimen de sanciones cibernéticas); - UK Cyber Sanctions Regime (2020); - US Executive Order 13694 del 2015 sobre sanciones por actividades cibernéticas maliciosas.
G5. Interoperabilidad y confidencialidad (p. ej., TLP), intercambio seguro	Protocolos estandarizados para el intercambio seguro de información de amenazas cibernéticas entre autoridades nacionales, CSIRTs y socios internacionales, incluyendo sistemas de clasificación de información (como Traffic Light Protocol) y requisitos de confidencialidad.	El intercambio efectivo de información sobre amenazas requiere confianza mutua y protección de fuentes sensibles.	- UE NIS2 art. 29 (Arreglos de intercambio de información) y reglas para la red de CSIRTs con referencia expresa al Traffic Light Protocol.

G6. Ciberdiplomacia institucionalizada (puntos focales y operadores diplomáticos digitales)	Mandatar que la Cancillería designe puntos focales de ciberdiplomacia y, cuando proceda, agregados/adjuntos digitales en misiones prioritarias.	Traduce obligaciones y marcos internacionales en capacidad permanente del Estado; acelera la coordinación técnica-operativa-diplomática, refuerza la coherencia externa y mejora la disuasión y la gestión de crisis transfronterizas.	- EE. UU.: 22 U.S.C. ch. 110, §10301 (política internacional de ciberespacio) y §10302 (estrategia de ciber y política digital) - UE: Decisión (PESC) 2019/797 y Reglamento (UE) 2019/796 (régimen de sanciones cibernéticas y "toolbox" diplomática)
G7. Posición nacional sobre derecho internacional en ciberespacio (mandato legislativo)	Mandato legislativo que ordena al poder ejecutivo desarrollar, actualizar y publicar una posición nacional sobre aplicación del derecho internacional en ciberespacio (uso de la fuerza, legítima defensa, responsabilidad estatal, diligencia debida, soberanía, DIH, DDHH en operaciones cibernéticas), mediante proceso interinstitucional coordinado por Cancillería. Plazo: 12-24 meses; incluir mecanismos de consulta.	Legitima democráticamente la política exterior digital; facilita participación informada en negociaciones internacionales; proporciona guía operativa para respuesta nacional; refuerza transparencia y rendición de cuentas; contribuye a estabilidad internacional mediante claridad jurídica sobre "líneas rojas" y conducta estatal esperada.	Países Bajos: Carta Ministerio RREE al Parlamento (5 julio 2019, Kamerstuk 33 694, nr. 47) en respuesta a moción parlamentaria, con anexo sobre DI en ciberespacio

Pilar H – Gobierno, compras públicas y fomento

Este pilar convierte el poder de compra y de fomento del Estado en una palanca directa para elevar la seguridad del ecosistema. Establece que la contratación pública incorpore atestaciones de desarrollo seguro (SSDF), *SBOM* con elementos mínimos y políticas CVD/VDP exigibles en RFP y contratos, incluyendo certificaciones cuando proceda (H1). Refuerza la gestión de riesgo en servicios gestionados mediante cláusulas específicas para MSP/MSSP, derecho de auditoría, métricas/SLA, planes de remediación, cooperación con CSIRT y deberes de registro/notificación, para internalizar dependencias críticas en los contratos (H2). Alinea incentivos con mecanismos de preferencia e inhabilitación: prioriza proveedores con madurez mínima

verificable y sanciona incumplimientos graves, disciplinando el mercado público (H3). Profesionaliza el sector mediante un plan nacional de fuerza laboral con perfiles por rol, certificaciones aceptadas y rutas de carrera para el servicio público y su cadena de suministro (H4). Atiende las brechas estructurales con apoyos a PYMES (guías, plantillas y *sandbox* regulatorios) para elevar su ciberhigiene y su capacidad de cumplir requisitos estatales (H5). Finalmente, prevé asistencia a víctimas críticas (bonos o servicios) tras incidentes significativos, como instrumento de contención sistémica y recuperación acelerada complementario a la respuesta operativa (H6).

Pilar H – Gobierno, compras públicas y fomento			
Elemento	**Descripción**	**¿Por qué?**	**Fuentes (art./sección)**
H1. Requisitos en contratación pública (SSDF/SBOM/CVD)	Incluir en RFP/contratos atestaciones de desarrollo seguro, SBOM conforme a formatos mínimos y evidencias de VDP/CVD.	Eleva la barrera de seguridad de la cadena de suministro del Estado y genera señales de mercado.	- OMB M-22-18 (secs. I-III; Apéndice A); - OMB M-23-16 (actualización de plazos); - EO 14028 (§4(e)); NTIA SBOM (mínimos elementos cadena de suministro de software); - NIST SP 800-218 (SSDF), marco de desarrollo seguro. - NIS2 art. 7(2)(b) (ciberseguridad en contratación pública) - UE Cybersecurity Act (Reg. 2019/881) y NIS2 art. 24-25, base para exigir certificaciones UE (EUCC/EUCS, etc.) como criterio técnico en la compra pública de TIC. - EE. UU. – FedRAMP Authorization Act (44 U.S.C. cap. 36), obligatorio en compras cloud federales.
H2. Clausulados MSP/MSSP	Derecho de auditoría, métricas/SLA, planes de remediación, cooperación con CSIRT y registros/notificaciones.	MSP/MSSP concentran riesgo sistémico; contratos deben internalizar la gestión de cadena y dependencias.	- NIS2 definiciones de MSP/MSSP (puntos (39)-(40)); art. 21(2) (seguridad de cadena de suministro); considerandos 84-85. - Reglamento de Ejecución NIS2 (UE) 2024/2690. Específica técnicamente qué deben implementar, entre otros, MSP/MSSP (control de acceso, registro, gestión de vulnerabilidades, criptografía, continuidad, etc.) - DORA (Reg. (UE) 2022/2554), mejores prácticas contractuales aplicables. Arts. 28 y 30.
H3. Preferencia/inhabilitación	Preferencias a proveedores con madurez mínima; inhabilitación por	Alinea incentivos y disciplina el	- NIS2 arts. 31-36 (supervisión, medidas y multas); - Chile Ley 21.663 art. 11 letra v) (estándares para proveedores del Estado)

	incumplimientos graves.	mercado público.	
H4. Fuerza laboral (perfiles, certificaciones, trayectorias)	Plan nacional por roles, certificaciones aceptadas y rutas de carrera para sector público y proveedores.	Cierra brechas críticas de talento y profesionaliza el ecosistema.	- NIS2 Arts. 7(2)(f)(i), 20, 21(2)(g): educación y formación en ciberseguridad, apoyo específico a PYMES, formación obligatoria para órganos de dirección. - DORA Art. 13(6): programas obligatorios de concienciación para personal y alta dirección financiera. - Chile Ley 21.663. Art. 11, letra i): facultad de diseñar e implementar planes de formación, capacitación y promoción de cultura en ciberseguridad
H5. Apoyos a PYMES (guías, plantillas, sandbox)	Programas de asistencia técnica, materiales listos para usar y pilotos regulatorios.	PYMES son eslabones vulnerables y proveedoras del Estado.	- NIS2 art. 7(2)(i) y considerandos 56-57 (apoyo específico a PYMES) - Cybersecurity Act (Reg. (UE) 2019/881) – art. 10 "Awareness-raising and education".
H6. Fondo/Asistencia a víctimas críticas	Bonos o servicios para operadores pequeños/estratégicos tras incidentes significativos.	Acelera recuperación y reduce contagio sistémico.	- Chile Ley 21.663 art. 11 letra m) (asesoría técnica a afectados) - NIS2, Arts. 11(3)(a), (c), (f) tareas de los CSIRTs: asistencia a entidades esenciales/importantes. - Cyber Solidarity Act (Reg. UE 2025/38) Arts. 10-12: Cybersecurity Emergency Mechanism para respuesta y recuperación inicial con financiación del Programa Europa Digital; Art. 11(b): EU Cybersecurity Reserve (proveedores precontratados); Art. 11(c) y 18: apoyo a asistencia mutua entre Estados. - UE Programa Europa Digital (Reg. 2021/694). Art. 6 (Objetivo específico 3: "Ciberseguridad y confianza"): base financiera para acciones, equipos y servicios de ciberseguridad (incluye los del Mecanismo de Emergencia/Reserva del Acta de Solidaridad).

Pilar I – Transparencia, presupuesto y sostenibilidad

Este pilar asegura la viabilidad en el tiempo de la política de ciberseguridad mediante reglas de financiamiento, rendición de cuentas, revisión periódica y estímulos económicos. Establece presupuesto etiquetado con partidas verificables para la autoridad nacional, la red de CSIRTs y programas de apoyo a PYMES, garantizando trazabilidad, continuidad operativa y priorización de capacidades críticas (I1). Dispone la publicación periódica de estadísticas agregadas y anonimizadas (incidentes significativos, tiempos de respuesta,

sectores afectados) para transparencia, *benchmarking* y aprendizaje sistémico, sin exponer información sensible (I2). Ordena una revisión quinquenal de la política, con KPIs y ajuste por cambio tecnológico (p. ej., IA, PQC), a fin de evitar obsolescencia y mantener el enfoque en riesgos reales (I3). Finalmente, incorpora estímulos fiscales dirigidos a inversiones en ciberseguridad (con especial foco en PYMES), como palanca para movilizar capital privado, elevar ciberhigiene y reducir barreras de adopción (I4).

Cabe precisar que el componente de estímulos fiscales (I4) corresponde típicamente a leyes tributarias especializadas y podría constituir una medida temporal (tipo *sunset*) diseñada para impulsar el ecosistema de ciberseguridad durante sus etapas iniciales de desarrollo. Se incluye en este pilar reconociendo que sólo resulta viable en los primeros pasos de consolidación de las capacidades nacionales de un país, cuando el mercado de ciberseguridad aún requiere incentivos adicionales para alcanzar masa crítica. En jurisdicciones con ecosistemas maduros, estos estímulos pierden justificación económica y tienden a eliminarse progresivamente. No obstante, el establecimiento de fundamentos habilitantes en la ley de ciberseguridad puede facilitar que las autoridades fiscales desarrollen posteriormente estos instrumentos mediante reformas tributarias específicas, proporcionando un marco de referencia para vincular beneficios fiscales con métricas verificables de mejora en ciberseguridad y cumplimiento de estándares reconocidos.

Pilar I – Transparencia, presupuesto y sostenibilidad			
Elemento	**Descripción**	**¿Por qué?**	**Fuentes (art./sección)**
I1. Presupuesto etiquetado (autoridad/CSIRT/PYMES)	Presupuesto con partidas identificables para la autoridad nacional, red CSIRT y	Asegura financiamiento estable, trazabilidad y continuidad de capacidades públicas.	- OMB M-22-16 (prioridades ciberseguridad en el ciclo presupuestario); - NIS2: Art. 7(1)-(3) (estrategia con recursos), Art. 8(5) (autoridades), Arts. 10-12 (CSIRTs/cooperación). - Cyber Solidarity Act (Reg. UE 2025/38) Arts. 10-12: Cybersecurity Emergency Mechanism para respuesta y recuperación inicial con financiación del Programa Europa Digital; Art. 11(b): EU Cybersecurity Reserve

	programas de apoyo a PYMES.		(proveedores precontratados); Art. 11(c) y 18: apoyo a asistencia mutua entre Estados. - Chile Ley 21.663 - crea la ANCI y su marco de funciones; la asignación presupuestaria se materializa vía Ley de Presupuestos anual
I2. Publicación de estadísticas (agregadas/anonimizada)	Difusión periódica de métricas país: incidentes significativo, tiempos de respuesta, sectores (en agregado y anonimizado).	Crea transparencia y aprendizaje sistémico; habilita benchmarking e investigación aplicada.	- Chile: Ley 21.663, Art. 11(f) (Registro Nacional de Incidentes), Art. 24(h) (pedir información anonimizada). - NIS2: Art. 18 (informe bienal UE). - Cyber Security Act (CSA) (Reg. 2019/881), Art. 10 (concienciación y educación): mandato para publicar guías, análisis y panoramas.
I3. Revisión quinquenal (actualización tecnológica)	Revisión al menos cada 5 años, con KPIs y ajuste por cambio tecnológico (IA, PQC, etc.).	Mantiene vigencia normativa y enfoque en riesgo; evita obsolescencia.	- NIS2: Art. 7(4) (evaluación de la estrategia al menos cada cinco años), Art. 19 establece *peer reviews* coordinadas; tras una revisión, el mismo aspecto no se vuelve a revisar por 2 años. - CER (Dir. (UE) 2022/2557), Art. 5(5) (evaluación nacional de riesgos: revisión "al menos cada cuatro años"), Art. 12(1) (las entidades críticas deben reevaluar sus riesgos "al menos cada cuatro años").
I4. Estímulos fiscales para el ecosistema de ciberseguridad	Incentivos tributarios para inversiones en ciberseguridad: deducciones, créditos fiscales para PYMES y beneficios por participación en programas de intercambio de amenazas.	Moviliza la inversión privada y reduce barreras económicas para adopción de ciberseguridad.	- Maryland (EE. UU.) – crédito fiscal específico en ciberseguridad (estatal). El programa Buy Maryland Cybersecurity (BMC)[242] otorga 50 % de crédito sobre el precio neto de tecnologías/servicios de ciberseguridad adquiridos a vendedores certificados, hasta USD 50 000 por año (compras elegibles hasta USD 100 000). Es el ejemplo más directo y "sectorial". - Trinidad y Tobago – Cybersecurity Investment Tax Allowance (nacional). El Presupuesto 2024 introdujo una deducción de hasta 500 000 $ para empresas que inviertan en software y equipos de monitoreo de seguridad de red (vigente 2024-2025)[243].

Pilar J – Responsabilidades y sanciones

Este pilar define una base coercitiva y garantista que ordena la ejecución sin desalentar el reporte responsable. Establece una escalera de cumplimiento proporcional (advertencia, plan/auditoría, instrucciones de implementación, infracciones, multa, limitación/cesa, publicación) con criterios objetivos y

[242] Véase http://bit.ly/46CIGbH
[243] Véase http://bit.ly/4munTwT

debido proceso para graduar la respuesta regulatoria y asegurar disuasión efectiva (J2). Blinda la investigación de seguridad de buena fe en el marco de CVD/VDP mediante definición operativa, regla de no incriminación por la mera notificación y protecciones anti-SLAPP (inadmisión temprana, cauciones, costas y sanciones a demandas abusivas) para evitar el enfriamiento de la divulgación coordinada (J1). Positiviza el procedimiento sancionador con plazos, autoridad competente, medidas cautelares proporcionales y vías de apelación ante instancia independiente, garantizando el derecho de defensa y la seguridad jurídica (J3). Finalmente, prevé publicidad proporcional de medidas o sanciones bajo criterios de gravedad/interés público y coordinación con regímenes sectoriales (por ejemplo, valores), a fin de promover aprendizaje sistémico sin re-victimizar (J4). En conjunto, el pilar reduce la arbitrariedad, alinea incentivos y protege ecosistemas de reporte responsable.

Pilar J – Responsabilidades y sanciones			
Elemento	**Descripción**	**¿Por qué?**	**Fuentes (art./sección)**
J1. Protecciones anti-SLAPP para investigación de buena fe	Blindaje procesal frente a demandas abusivas contra investigadores/divulgadores; reglas de inadmisión temprana, caución y costas; reconocimiento expreso de investigación de buena fe en CVD/VDP.	Evita "enfriar" el reporte responsable; reduce el abuso del sistema judicial y alinea incentivos con divulgación coordinad.	- Directiva (UE) 2024/1069: arts. 11-15 (inadmisión, costas, sanciones) - DOJ JM 9-48.000 (CFAA): sección B.3, definición y no persecución de "*good-faith security research*" - NIS2, Art. 23(1): "la mera notificación no incrementa la responsabilidad", Art 30 notificación voluntaria. - Directiva de denunciantes (UE) 2019/1937. Arts. 16 y 21: confidencialidad y protección frente a represalias.

J2. Escalera de cumplimiento (advertencia-plan-instrucciones - multas, infracciones - limitación/cesa-publicación)	Catálogo gradual de medidas: requerimientos, auditorías/planes, órdenes de implementación, infracciones, multas y, en casos graves, publicación o restricciones temporales.	Asegura proporcionalidad y disuasión efectiva, evitando tanto la inacción como la sobrerreacción regulatoria.	- NIS2: Art. 31 (aspectos generales de supervisión y ejecución), art. 32(4) (a-h) (medidas), art. 32(5-8) (criterios/garantías), art. 34 (multas). - DORA (Reg. 2022/2554), Art. 50–51: catálogo de potestades correctivas y sancionatorias, Art. 54: publicación de sanciones. - Chile Ley 21.663. Sistema escalonado con infracciones leves, graves y gravísimas (Art. 38) y categoría especial para OIV (Art. 39). Multas para OIV (Art. 40). Procedimientos: simplificado para leves (Art. 41) y administrativo con descargos (Art. 42). Recursos y pronto pago (Arts. 43-46). Competencia: ANCI vs. autoridad sectorial (Art. 37). - El Salvador, Ley Ciberseguridad: Arts. 18-21 (clasificación leves/graves/muy graves con catálogo), Arts. 22-24 (multas 1-10, 11-50, 51-100 salarios mínimos según gravedad), Art. 17 (principios proporcionalidad y culpabilidad), Art. 27 (multas coercitivas diarias)
J3. Procedimiento sancionador y apelación	Procedimiento con plazos, autoridad competente, medidas cautelares proporcionales y recursos ante instancia independiente.	Garantiza debido proceso y seguridad jurídica; legitima la ejecución.	- NIS2: art. 32(7) (derechos de defensa) y considerandos 127-131 (remedios y proporcionalidad). - Chile, Ley 21.663. Art. 41 (procedimiento simplificado) y Art. 42 (procedimiento sancionatorio con formulación de cargos, descargos, prueba y resolución). Art. 43-46 (recursos, pago, pronto pago, reclamación judicial).
J4. Publicidad proporcional de incumplimientos	Posibilidad de revelar medidas o sanciones bajo criterios de gravedad/interés público y coordinación con regímenes sectoriales (por ejemplo, valores).	Incrementa disuasión y aprendizaje sistémico sin revictimizar.	- NIS2: art. 32(4)(g) (orden de publicar aspectos de la infracción); - SEC: Form 8-K, ítem 1.05 (divulgación de incidentes materiales en 4 días hábiles). - DORA Art. 54: publicación de sanciones administrativas en los sitios web oficiales

LIMITACIONES E INVESTIGACIONES FUTURAS

El alcance de este trabajo es deliberadamente acotado a leyes aprobadas por el poder legislativo que configuran una ley especial de ciberseguridad. Se excluyen propuestas de ley, estrategias, políticas, reglamentos, circulares y demás actos políticos o administrativos, así como la normativa de cibercrimen e inteligencia (mencionadas únicamente en el apartado de países sin ley para trazar la radiografía normativa). La clasificación "con ley/sin ley" no evalúa la existencia de bienes jurídicos en seguridad de la información, sino la ausencia o presencia de un marco legal específico. El estudio no analiza la implementación ni la capacidad institucional, tampoco jurisprudencia, presupuestos a nivel económico en la implementación de la misma, costos de cumplimiento o efectividad operativa; además, depende de textos públicos disponibles a la fecha de corte, con los sesgos que ello conlleva.

De cara a la investigación futura, conviene realizar un inventario exhaustivo del bagaje normativo, administrativo, judicial y legislativo de cada país, con verificación de la implementación y de los resultados; construir indicadores comparables – tiempos de notificación, severidad e incorporación de lecciones aprendidas – y un índice de madurez por pilares; desarrollar estudios sectoriales en OT/ICS, salud y financiero con evaluaciones costo-beneficio; pilotear el marco propuesto mediante modelos de texto legislativo y guías de implementación para probar su viabilidad regulatoria; e incorporar frentes emergentes como la IA, la criptografía post-cuántica, la certificación de productos y los seguros cibernéticos, junto con el fortalecimiento de la cooperación internacional operativa. Las propuestas de ley y otros instrumentos de naturaleza política permanecerán fuera del análisis comparado hasta su aprobación legislativa; a partir de entonces, podrán integrarse para refinar las conclusiones y favorecer la convergencia hacia un lenguaje y principios comunes en la región.

CONCLUSIONES

El análisis comparado muestra que, a la fecha únicamente Chile y El Salvador han adoptado una ley especial de ciberseguridad aprobada por el poder legislativo. En el resto de América Latina y el Caribe predominan instrumentos normativos apoyados en cibercrimen, protección de datos personales, comercio electrónico, regulación sectorial o inteligencia: útiles, pero insuficientes para una gobernanza preventiva y basada en riesgos. Esta asimetría se asocia con ambigüedades conceptuales, vacíos de coordinación, obligaciones heterogéneas de reporte y costos de cumplimiento dispares, con efectos en la interoperabilidad regional y en la protección desigual de infraestructuras esenciales y sus cadenas de suministro. Se debe subrayar que la clasificación "con ley/sin ley" no desconoce la tutela de bienes jurídicos vinculados a la seguridad de la información; más bien, constata la ausencia de una *lex specialis* que ordene competencias, fije mínimos verificables y habilite con estabilidad en punto de equilibrio, funciones de supervisión y sanción.

Sobre esa base, se propone un arquetipo legislativo mínimo viable articulado en diez pilares (gobernanza; capacidades operativas; gestión de riesgos; infraestructuras esenciales; reporte de incidentes; seguridad de productos; cooperación internacional; compras públicas y fomento; transparencia/presupuesto; y responsabilidades/sanciones) guiado por proporcionalidad, enfoque en riesgos, neutralidad tecnológica y salvaguardas de derechos. Alineado con referentes internacionales y estándares técnicos, el marco ofrece un lenguaje común y una secuencia de adopción graduable, acompañada de notas que permiten interpretar su implementación según la madurez de cada país. En síntesis, su ejecución tiene como fin reducir la incertidumbre jurídica, facilitar la cooperación público-privada y elevar una plataforma regulatoria compartida en América Latina y el Caribe.

Asimismo, el estudio consideró exclusivamente leyes en sentido formal, sin evaluar implementación, capacidades institucionales, presupuestos, jurisprudencia ni efectividad operativa, y dependió de textos públicos disponibles al cierre. Este recorte es sustantivo, toda vez que, a diferencia de

los instrumentos políticos o administrativos, una norma con rango de ley habilita competencias, define deberes exigibles, establece mecanismos de supervisión y sanción y asegura continuidad más allá de la alternancia gubernamental. Al fijar objetos, conceptos, roles, competencias y procedimientos comunes, incluidos umbrales y plazos de notificación, coordinación CSIRT/CERT, identificación de servicios esenciales y régimen sancionador, una *lex specialis* en ciberseguridad crea un marco regulatorio compartido que favorece la interoperabilidad jurídica y operativa entre sectores y fronteras.

© EU CyberNet 2025

Las opiniones y puntos de vista expresados son responsabilidad exclusiva de los autores y no reflejan necesariamente los de la Unión Europea ni de LAC4. Ni la Unión Europea ni LAC4 se responsabilizan de ellas.