UNIVERSIDAD CENTRAL
VICERRECTORÍA ACADÉMICA

ESCUELA DE DERECHO

RETOS PARA EL DERECHO PENAL COSTARRICENSE FRENTE A LA CIBERDELINCUENCIA

MODALIDAD DE TESIS PARA OPTAR POR EL GRADO DE LICENCIATURA EN DERECHO

Estudiante:

ALVARO ANTONIO SOLANO UMAÑA

Tutor:

JOHN BRENES ORTIZ

Sede Central

Diciembre, 2025

CONTENIDO

Índice de tablas 12

Índice de abreviaturas 13

Resumen Ejecutivo 17

INTRODUCCIÓN 19

CAPÍTULO I: PLANTEAMIENTO GENERAL DE LA INVESTIGACIÓN 25

1.1 Planteamiento del problema de investigación 25

1.2 Justificación 26

1.3 Objetivos 27

1.3.1 Objetivo general 27

1.3.2 Objetivos específicos 27

1.4 Antecedentes 27

1.4.1 Antecedentes nacionales 27

1.4.2 Antecedentes internacionales 31

1.5 Alcances y limitaciones 40

1.5.1 Alcances 42

1.5.2 Limitaciones 42

CAPÍTULO II: MARCO TEÓRICO 44

2.1 Delimitaciones conceptuales clave en materia de ciberdelitos 44

2.1.1 Ciberseguridad, privacidad y protección de datos: diferencias desde la perspectiva penal 46

2.1.2 La tríada de la seguridad de la información: Confidencialidad, Integridad, Disponibilidad (CIA) 52

2.1.3 Bienes jurídicos protegidos en el entorno digital 55

2.1.4 Confidencialidad de las comunicaciones.....57
2.1.5 Integridad y funcionamiento de sistemas y datos.....59
2.1.6 Intimidad, privacidad y protección de datos personales.....62
2.1.7 Patrimonio y confianza en entornos digitales.....66
2.2 El marco normativo costarricense.....70
2.2.1 Suplantación de paginas web.....71
2.2.2 Suplantación de identidad.....72
2.2.3 Difusión de información falsa (art. 236 C.P.) y grooming (art. 167 bis C.P.) 72
2.2.4 Facilitación de delito informático.....73
2.2.5 Espionaje informático.....74
2.2.6 El sabotaje informático (art. 229 ter C.P.).....74
2.2.7 Violación de correspondencia o comunicaciones (art. 196 C.P.).....75
2.2.8 Estafa informática.....76
2.2.9 Daño Informático (arts. 229 bis, 229 ter y 232 C.P.).....78
2.3 Delitos informáticos que incluye el Código Penal costarricense.....79
2.3.1 Tenencia de material pornográfico (art. 173 bis C.P.).....79
2.3.2 Difusión de pornografía (art. 174 C.P.).....80
2.3.3 Pornografía virtual y pseudo pornografía (art. 174 bis C.P.).....81
2.3.4 Violación de datos personales (art. 196 bis C.P.).....82
2.3.5 Lo relativo a la pornografía.....83
2.3.6 Extorsión (art. 214 C.P.).....84
2.3.7 Espionaje (art. 295 C.P.).....85
2.3.8 Narcotráfico y crimen organizado.....85
2.3.9 Robo de datos personales por medio de código QR.....86

2.3.10 Bloque constitucional y leyes conexas 86

2.4 Convenio de Europa sobre Ciberdelincuencia (Convenio de Budapest) 91

2.5 Código Penal: catálogo vigente de tipos informáticos y afines 93

2.5.1 Acceso e interceptación ilícita / violación de comunicaciones 93

2.5.2 Fraude/estafa informáticos y falsedad informática 96

2.5.3 Falsedad informática 97

2.5.4 Daño, alteración e interferencia en datos y sistemas (sabotaje informático) 98

2.5.5 Suplantación de identidad digital y abuso de dispositivos 100

2.6 Leyes especiales y normativa complementaria 103

2.6.1 Protección de datos personales (Ley N.° 8968 y reglamentación) 103

2.6.2 Documentos y firma digital (Ley N.° 8454 y reglamentación) 104

2.6.3 Otras normas y estándares complementarios (soft law y sectoriales) 104

2.7 A modo de cierre 105

CAPÍTULO III: MARCO METODOLÓGICO 107

3.1 Enfoque de la investigación 107

3.2 Método de la investigación 107

3.3 Delimitación temporal y espacial 108

3.4 Fuentes 108

3.4.1 Fuentes primarias 109

3.4.2 Fuentes secundarias 109

3.5 Variables o unidades de análisis 110

3.6 Instrumentos 111

3.7 Proceso para la recolección y análisis de datos 111

3.8 Ámbitos de la investigación 113

CAPÍTULO IV: ANÁLISIS DE RESULTADOS 115
4.1 Adecuación a Budapest 115
4.2 Vacíos, solapamientos y ambigüedades del marco costarricense 122
4.3 Otros hallazgos relevantes: análisis por figuras nucleares 123
4.3.1 Acceso ilícito 123
4.3.2 Interceptación de comunicaciones 124
4.3.3 Interferencia en datos y sistemas (daño/sabotaje) 124
4.3.4 Abuso de dispositivos / facilitación 125
4.3.5 Falsificación y fraude informáticos 126
4.3.6 Procesal-probatorio (síntesis) 126
4.3.7 Personas jurídicas (PJ): diagnóstico y llave de política criminal 127
4.3.8 Hacia un modelo costarricense de responsabilidad penal corporativa en ciberseguridad 128
4.4 Cierre del capítulo 130
CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES 135
5.1 Conclusiones 135
5.2 Recomendaciones 143
REFERENCIAS BIBLIOGRÁFICAS 149

Índice de tablas

Tabla 1 Matriz inicial de adecuación a Budapest 96
Tabla 2 Matriz de adecuación a Budapest 117
Tabla 3 Matriz con detalle artículos 4 y 5 119
Tabla 4 Matriz de adecuación a Budapest (bloque de art. 6) 121
Tabla 5 Matriz de adecuación al Convenio de Budapest (síntesis ejecutiva) 132

Índice de abreviaturas

APA	American Psychological Association (estilo de citación APA)
CIA	Confidencialidad, Integridad y Disponibilidad (tríada de seguridad de la información)
CP	Código Penal
CR	Costa Rica
CSWP	Cybersecurity White Paper (documento técnico del NIST)
DOI	Digital Object Identifier
DPEJ	Diccionario panhispánico del español jurídico
EDR	Endpoint Detection and Response (respuesta y detección en el endpoint)
EE. UU.	Estados Unidos de América
ETS	European Treaty Series (serie de tratados europeos del Consejo de Europa)
EU	European Union (Unión Europea)
IA	Inteligencia artificial
ICS	Industrial Control Systems (sistemas de control industrial)
IEC	International Electrotechnical Commission
IP	Internet Protocol (dirección IP)
ISO	International Organization for Standardization
MFA	Multi-Factor Authentication (autenticación multifactor)
MIDEPLAN	Ministerio de Planificación Nacional y Política Económica (Costa Rica)
MP	Ministerio de la Presidencia (Costa Rica)
NHS	National Health Service (Servicio Nacional de Salud del Reino Unido)
NIST	National Institute of Standards and Technology (Estados Unidos)
OTP	One-Time Password (contraseña de un solo uso)
OWASP	Open Web Application Security Project

PJ	Personas Jurídicas
PRODHAB	Agencia de Protección de Datos de los Habitantes (Costa Rica)
RIDCA	Revista de Investigación, Derecho, Cultura y Ambiente
RREE	Ministerio de Relaciones Exteriores y Culto (Costa Rica)
SCADA	Supervisory Control and Data Acquisition (sistemas de supervisión, control y adquisición de datos)
SCIJ	Sistema Costarricense de Información Jurídica
SIEM	Security Information and Event Management (gestión de eventos e información de seguridad)
SIM	Subscriber Identity Module (tarjeta SIM de telefonía móvil)
SLA	Service Level Agreement (acuerdo de nivel de servicio)
TFG	Trabajo Final de Graduación
TI	Tecnologías de la Información
UC	Universidad Central
UCR	Universidad de Costa Rica
UE	Unión Europea
ULACIT	Universidad Latinoamericana de Ciencia y Tecnología
UNIR	Universidad Internacional de La Rioja
UNODC	United Nations Office on Drugs and Crime (Oficina de las Naciones Unidas contra la Droga y el Delito)

Dedicatoria

A mis padres

Este logro es un testimonio de su inmenso amor y dedicación. Valoro mucho las lecciones de vida que me han impartido y por el cariño que siempre me han brindado. Mi gratitud hacia ustedes es imposible de expresar completamente.

Esta tesis está dedicada con profundo agradecimiento a mis queridos padres, cuyo ejemplo de esfuerzo, disciplina y compromiso han guiado mi formación personal y académica. A lo largo de sus vidas, me han inculcado los valores del trabajo y el estudio, brindándome, con dedicación y constancia, las oportunidades necesarias para alcanzar mis metas.

Su sacrificio, amor incondicional y apoyo permanente representan un legado invaluable que ha marcado mi camino. Esta tesis constituye un testimonio de ese legado y una expresión sincera de mi admiración y gratitud hacia ustedes.

Álvaro Solano Umaña

Agradecimiento

Deseo iniciar expresando mi más sincero agradecimiento a mi tutor de tesis, el máster Jonh Brenes Ortiz, cuya experiencia, paciencia y guía constante resultaro fundamentales para la culminación de este trabajo académico.

A mi familia, en especial, a mis padres y a mi hermana Paula, les extiendo mi más profundo agradecimiento por su amor incondicional y su apoyo permanente. Su confianza en mí ha sido el motor que impulsó cada etapa de este proceso. Este logro no habría sido posible sin ustedes.

A mi esposa Yansy y a mi hijo Sebastián, les expreso mi gratitud por su comprensión, paciencia y motivación diaria, que me brindaron la fuerza necesaria para avanzar. Extiendo también mi agradecimiento a la Universidad Central por brindarme el espacio y las herramientas para crecer tanto académica como profesionalmente.

A mi coach, Juan Carlos, le agradezco su asesoría y su aporte en mi desarrollo profesional. A mis amigos y compañeros de clase, les agradezco su compañía, apoyo y solidaridad durante los momentos de mayor exigencia y también en los de alegría.

A todos ustedes, gracias por acompañarme en este camino y por contribuir de manera esencial en la realización de este logro académico.

Álvaro Solano Umaña.

Resumen Ejecutivo

La tesis analiza los retos que enfrenta el Derecho Penal Costarricense ante la expansión de la ciberdelincuencia y, en particular, frente a las exigencias del Convenio de Budapest. La investigación parte de la constatación de que actividades esenciales para la vida económica y social —como la banca, el comercio electrónico, la gestión de datos personales o la provisión de servicios públicos— dependen hoy de infraestructuras digitales vulnerables a ataques cada vez más sofisticados. En este contexto, el ordenamiento penal costarricense ha incorporado diversas figuras informáticas en las últimas décadas, pero lo ha hecho de forma parcial, dispersa y con problemas de técnica legislativa que afectan la seguridad jurídica y la eficacia de la respuesta estatal.

El objetivo general del estudio es analizar la adecuación del marco penal costarricense frente a la ciberdelincuencia, a partir del Convenio de Budapest y del derecho comparado, poniendo especial atención a la tipificación de las conductas, la protección de los bienes jurídicos y la proporcionalidad de las sanciones. Para ello, se definieron cuatro objetivos específicos: clarificar el concepto de ciberdelincuencia y los bienes jurídicos protegidos; examinar el catálogo vigente de delitos informáticos y sus lagunas; contrastar la legislación costarricense con los estándares de Budapest y revisar experiencias comparadas que sirvan de base para formular propuestas de reforma.

Metodológicamente, se trata de una investigación jurídica de carácter dogmático y propositivo, basada en el análisis sistemático de normas nacionales e internacionales, doctrina especializada y estudios comparados. El trabajo organiza el corpus en torno a unidades de análisis (conceptualización, catálogo de delitos, adecuación a Budapest, responsabilidad penal de las personas jurídicas y política criminal) y emplea matrices de

adecuación para evaluar, figura por figura, el nivel de cumplimiento de los requerimientos del Convenio. No se recurre a técnicas empíricas, pues el problema abordado es predominantemente normativo.

Los principales hallazgos muestran que, si bien Costa Rica ha avanzado en la tipificación de conductas como el acceso ilícito, la interferencia en datos y sistemas, el fraude informático o ciertos delitos vinculados a la pornografía infantil, subsisten zonas de solapamiento entre tipos tradicionales e informáticos, definiciones ambiguas y vacíos frente a nuevas modalidades delictivas. Asimismo, el país presenta un rezago significativo en materia de responsabilidad penal de las personas jurídicas por incidentes de ciberseguridad: pese a la existencia de un régimen corporativo limitado para delitos de corrupción, no se ha extendido aún un modelo de imputación penal a los ciberdelitos, a pesar de lo previsto en el artículo 12 de Budapest y de las tendencias comparadas más recientes.

A partir de este diagnóstico, la tesis propone lineamientos de reforma orientados a consolidar y modernizar la legislación penal sobre ciberdelincuencia, ya sea mediante una ley especial o mediante un capítulo sistemático en el Código Penal; introducir de forma expresa la responsabilidad penal de las personas jurídicas en los principales ciberdelitos, con un catálogo sancionatorio adecuado y reconocer el papel de los programas de cumplimiento en ciberseguridad como criterios relevantes para la imputación y la graduación de la respuesta penal. Con ello, el trabajo busca aportar insumos concretos para la construcción de un modelo costarricense de política criminal en ciberseguridad que sea coherente, garantista y alineado con los compromisos internacionales del país.

INTRODUCCIÓN

La acelerada transformación digital de las últimas décadas ha modificado de manera profunda la forma en que las personas, las empresas y el propio Estado se relacionan, producen y se comunican. Hoy actividades tan diversas como la banca, el comercio, la prestación de servicios públicos esenciales, la gestión de datos personales o la propia administración de justicia dependen de infraestructuras informáticas y redes de comunicación interconectadas. Este nuevo escenario ha traído consigo importantes ventajas en términos de eficiencia, acceso a la información y creación de oportunidades, pero también ha abierto un campo fértil para la aparición y expansión de la ciberdelincuencia en todas sus manifestaciones.

Costa Rica no es ajena a esta realidad: el país ha experimentado en los últimos años un aumento sostenido de incidentes que comprometen la confidencialidad, integridad y disponibilidad de datos y sistemas, así como afectaciones patrimoniales, a la intimidad y a la confianza en los entornos digitales.

En este contexto, el Derecho Penal costarricense se enfrenta al reto de reaccionar frente a un fenómeno delictivo que, por su naturaleza tecnológica, desborda los moldes tradicionales de tipificación y exige repensar tanto los bienes jurídicos protegidos como las formas de atribución de responsabilidad. No se trata únicamente de incorporar nuevos delitos al catálogo, sino de hacerlo de manera sistemática, coherente con los estándares internacionales y respetuosa de los principios de legalidad, culpabilidad y proporcionalidad. La adhesión de Costa Rica al Convenio de Budapest sobre Ciberdelincuencia en 2017 marcó un punto de inflexión en este camino, al fijar un parámetro claro sobre qué conductas deben ser sancionadas —acceso ilícito, interferencia en datos y sistemas, abuso de dispositivos,

fraude y falsificación informáticos, entre otras— y al exigir, además, que los Estados prevean la responsabilidad de las personas jurídicas por los delitos contemplados en dicho instrumento.

El ordenamiento costarricense ha dado pasos relevantes en esta dirección. A las reformas del Código Penal para introducir o actualizar figuras como la violación de comunicaciones, el fraude informático, el daño o sabotaje informático y la suplantación de identidad digital, se suman leyes especiales como la de firma y documentos electrónicos (Ley N.º 8454) y la de protección de datos personales (Ley N.º 8968), así como la Ley N.º 9699 de 2019, que incorpora por primera vez un régimen de responsabilidad penal de las personas jurídicas.

Sin embargo, la doctrina nacional ha señalado que estos avances conviven con problemas de técnica legislativa, dispersión normativa, vacíos y solapamientos entre tipos penales, así como con un desarrollo aún incipiente de la responsabilidad penal corporativa en materia de ciberseguridad. En particular, persiste un rezago a la hora de articular una respuesta penal clara frente a incidentes de ciberseguridad que se producen en el seno de organizaciones y que, de una u otra forma, las benefician o se ven facilitados por defectos de organización interna.

Sobre este trasfondo se ubica la presente investigación, cuyo eje central es analizar en qué medida el marco penal costarricense vigente resulta adecuado, suficiente y sistemático para enfrentar la ciberdelincuencia conforme al Convenio de Budapest, con especial atención al tratamiento de los bienes jurídicos afectados, a la proporcionalidad de las sanciones y, de forma particular, a la responsabilidad penal de las personas jurídicas en incidentes de ciberseguridad.

A partir de ese diagnóstico, el trabajo busca identificar los vacíos, solapamientos y ambigüedades del sistema actual y formular pautas de técnica legislativa que permitan proponer un modelo normativo más coherente y alineado con las tendencias comparadas.

La pregunta que guía el estudio puede resumirse, en términos sencillos, en dos planos: por un lado, si el catálogo actual de delitos informáticos costarricenses cubre de manera adecuada las conductas que el Convenio de Budapest exige sancionar —acceso ilícito, interferencia en datos y sistemas, abuso de dispositivos, falsificación y fraude informáticos, entre otras—; y, por otro, si el régimen de responsabilidad penal de las personas jurídicas, tal como hoy está configurado, resulta apto para hacerse cargo de los incidentes de ciberseguridad que se producen en el ámbito corporativo. Se trata, en definitiva, de evaluar hasta qué punto el Derecho Penal Costarricense está realmente preparado para enfrentar una ciberdelincuencia cada vez más compleja, organizada y muchas veces vinculada a estructuras empresariales.

Los objetivos específicos de la investigación se orientan, en primer lugar, a delimitar conceptualmente la ciberdelincuencia y los bienes jurídicos protegidos en el entorno digital, clasificando las principales conductas previstas en el ordenamiento penal costarricense. En segundo lugar, se propone examinar el marco normativo vigente —Código Penal y leyes especiales— para identificar vacíos, solapamientos y ambigüedades en los tipos informáticos.

En tercer lugar, se pretende contrastar la legislación costarricense con los estándares del Convenio de Budapest, a fin de determinar criterios de adecuación normativa. Finalmente, se busca revisar experiencias de derecho comparado y formular pautas de técnica legislativa que puedan ser aplicadas al contexto nacional para fortalecer la respuesta penal

frente a la ciberdelincuencia y, en particular, frente a la responsabilidad penal corporativa por incidentes de ciberseguridad.

Metodológicamente, el trabajo adopta un enfoque cualitativo de carácter jurídico-dogmático y propositivo, apoyado en un diseño no experimental y documental. El análisis se centra en el estudio de normas penales, doctrina especializada, instrumentos internacionales y legislación comparada, complementado con una lectura de política criminal que permita valorar la proporcionalidad y coherencia del catálogo de delitos informáticos. Se recurre también al derecho comparado funcional —en particular, a experiencias europeas y latinoamericanas— para identificar modelos de imputación penal de personas jurídicas y buenas prácticas normativas que puedan servir de referencia a la realidad costarricense. No se utilizan técnicas empíricas como encuestas o entrevistas, por cuanto la naturaleza del problema es fundamentalmente normativa y dogmática.

En cuanto a su alcance, la investigación se concentra en los incidentes de ciberseguridad que comprometen la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos, así como en aquellos supuestos en que estas afectaciones se traducen en perjuicios patrimoniales, vulneraciones a la intimidad o quiebras de la confianza en los entornos digitales. El período de análisis se extiende desde la adhesión de Costa Rica al Convenio de Budapest en 2017 hasta la actualidad, lo que permite incorporar las reformas legales más recientes y los debates doctrinales que se han desarrollado en torno a la responsabilidad penal de las personas jurídicas y la ciberseguridad. Deliberadamente, el estudio se limita al ámbito penal, dejando fuera un examen exhaustivo de las dimensiones civil y administrativa, aunque estas se mencionen cuando resulte necesario para contextualizar el problema.

El trabajo reconoce varias limitaciones. Por un lado, se circunscribe al ordenamiento costarricense, utilizando el derecho comparado únicamente como marco ilustrativo y no como objeto de análisis exhaustivo. Por otro, se desarrolla en un contexto en el que la jurisprudencia nacional específica sobre delitos informáticos y responsabilidad penal corporativa en ciberseguridad es aún escasa, lo que obliga a formular propuestas de lege ferenda apoyadas principalmente en la doctrina y en experiencias legislativas extranjeras. A ello, se suma la propia dinámica del fenómeno: la rápida evolución de las tecnologías y de las modalidades delictivas implica que cualquier propuesta normativa debe entenderse como un punto de partida flexible, susceptible de revisión y actualización conforme cambian las amenazas y las prácticas en el ciberespacio.

La estructura de la tesis responde a estos propósitos. El capítulo I presenta la introducción, el planteamiento del problema, la justificación, los objetivos, los antecedentes, los alcances y limitaciones, así como el diseño metodológico seguido. El segundo capítulo desarrolla el marco conceptual, en el que se abordan las principales delimitaciones en materia de ciberdelitos, la relación entre ciberseguridad, privacidad y protección de datos, la tríada de seguridad de la información (confidencialidad, integridad, disponibilidad) y los bienes jurídicos protegidos en el entorno digital. El siguiente capítulo III examina el marco normativo costarricense, incluye el bloque constitucional, las leyes especiales y el catálogo vigente de tipos informáticos y afines. El capítulo IV realiza el análisis crítico de adecuación al Convenio de Budapest, identifica vacíos, solapamientos y ambigüedades del sistema y explora los desafíos específicos en materia de responsabilidad penal de las personas jurídicas. Finalmente, el capítulo V recoge las conclusiones y recomendaciones, y ofrece lineamientos de reforma y propuestas de técnica legislativa que buscan aportar insumos concretos al debate jurídico nacional.

Como se observa, esta investigación se inscribe en un momento clave para la reflexión sobre la política criminal en materia de ciberdelincuencia en Costa Rica. La creciente dependencia de infraestructuras digitales, sumada al incremento de ataques que afectan tanto a personas como a organizaciones públicas y privadas, exige que el Derecho penal responda de manera clara, proporcionada y respetuosa de las garantías. Al analizar la adecuación del marco penal costarricense frente a los estándares del Convenio de Budapest y al proponer ajustes específicos —en particular, en lo relativo a la responsabilidad penal de las personas jurídicas—, el trabajo aspira a contribuir a la construcción de un sistema más coherente y eficaz, capaz de proteger los bienes jurídicos en juego sin caer en expansiones punitivas injustificadas y ofrece, a la vez, herramientas normativas que acompañen la consolidación de una cultura de ciberseguridad en el país.

CAPÍTULO I: PLANTEAMIENTO GENERAL DE LA INVESTIGACIÓN

1.1 Planteamiento del problema de investigación

La aceleración de la transformación digital ha multiplicado las modalidades de ciberdelincuencia en Costa Rica: acceso ilícito a sistemas, interceptación y violación de comunicaciones, violación de datos personales, estafa informática, daño o sabotaje informático, espionaje, extorsión mediante tecnologías, entre otras figuras que hoy conviven con los tipos tradicionales del Código Penal. Aunque en la última década, se han introducido reformas relevantes y se han creado o actualizado varios tipos penales informáticos, la literatura nacional advierte problemas de técnica legislativa, dispersión normativa y zonas de solapamiento u omisión que dificultan una persecución penal eficaz y coherente con los estándares internacionales (Esquivel & Romero, 2021; Elizondo Alfaro, 2020).

Desde 2017, Costa Rica es Estado Parte del Convenio sobre la Ciberdelincuencia (Budapest), cuyo Título I exige a los países tipificar —con rangos claros de culpabilidad y sanción— conductas como el acceso ilícito, la interferencia en sistemas y datos, el abuso de dispositivos y el fraude y la falsificación informáticos, entre otras, además de prever la punibilidad de la tentativa y la participación (Consejo de Europa, 2001). Sin embargo, diversos estudios señalan que la recepción interna ha sido parcial y fragmentada: subsisten definiciones ambiguas, dificultades para delimitar bienes jurídicos y duplicidades con figuras no informáticas, lo que afecta la seguridad jurídica y la proporcionalidad de la respuesta penal (Elizondo Alfaro, 2020; Esquivel & Romero, 2021).

A ello, se suma la escasez de criterios jurisprudenciales específicos en la materia y la necesidad de alinear el catálogo penal con la evolución técnico-criminal de las conductas digitales. En términos de política criminal, el desafío no es “penalizar la ciberseguridad” —

que es un conjunto de prácticas preventivas en organizaciones—, sino depurar y actualizar el inventario de delitos informáticos y sus elementos típicos para que la persecución penal se concentre en conductas lesivas y no en fallas de gestión o estándares técnicos (Esquivel & Romero, 2021).

En este contexto, la pregunta de investigación que orienta el estudio es:

¿En qué medida el marco penal costarricense vigente resulta adecuado, suficiente y sistemático para enfrentar la ciberdelincuencia conforme al Convenio de Budapest, y qué ajustes normativos y de técnica legislativa se requieren para superar vacíos, solapamientos y ambigüedades en los tipos penales informáticos?

1.2 Justificación

Relevancia jurídica y política criminal. La ausencia de reglas claras para atribuir responsabilidad penal a entes colectivos en incidentes que comprometen la seguridad de la información incentiva la infraprotección de bienes supraindividuales y dificulta la prevención mediante programas de cumplimiento eficaces. La adopción de un modelo costarricense de responsabilidad penal corporativa —compatible con los principios de culpabilidad, legalidad y proporcionalidad— permitiría alinear el ordenamiento con Budapest (arts. 12 y 13) y homologar estándares con comparables regionales (de lege ferenda).

Pertinencia académica y social. En el país, hay antecedentes valiosos sobre delitos informáticos y política criminal, pero no se identifica una propuesta legislativa integral centrada específicamente en responsabilidad penal de personas jurídicas por incidentes de ciber delitos y su ingeniería normativa (tipicidad de organización, deberes de prevención, modelos de atribución y catálogo sancionatorio). Este trabajo busca llenar ese vacío con una propuesta articulada y contextualizada al sistema constitucional costarricense (articulación con el CP y leyes especiales).

1.3 Objetivos

1.3.1 Objetivo general

Analizar la adecuación del marco penal costarricense frente a la ciberdelincuencia, a partir del Convenio de Budapest y del derecho comparado, con especial atención a la tipificación, la protección de bienes jurídicos y la proporcionalidad de las sanciones.

1.3.2 Objetivos específicos

1. Definir el concepto de ciberdelincuencia y los bienes jurídicos protegidos, clasificando las principales conductas previstas en el ordenamiento penal costarricense.

2. Examinar el marco normativo vigente (Código Penal y leyes especiales) e identificar vacíos, solapamientos y ambigüedades en los tipos penales informáticos.

3. Contrastar la legislación costarricense con los estándares del Convenio de Budapest para determinar criterios de adecuación normativa.

4. Revisar experiencias de derecho comparado y proponer pautas de técnica legislativa aplicables al contexto nacional.

1.4 Antecedentes

1.4.1 Antecedentes nacionales

En Costa Rica, se han desarrollado diversas investigaciones que abordan, desde distintos ángulos, los retos que plantea la ciberdelincuencia y la regulación penal. La tesis de Esquivel Alpízar y Romero Salmerón (2021) constituye por ejemplo uno de los aportes más recientes en la literatura nacional sobre ciberdelincuencia. El trabajo tuvo como objetivo analizar la legislación penal costarricense en materia de delitos informáticos, identificar vacíos y proponer soluciones. Para ello, empleó una metodología descriptivo-analítica con

razonamiento deductivo, sustentada en la revisión de normativa, doctrina y derecho comparado.

En su diagnóstico, las autoras señalan que Costa Rica no cuenta con una ley penal especial integral que regule de manera suficiente los delitos informáticos, pese a la adhesión al Convenio de Budapest en 2017. De ahí que persistan zonas de impunidad y dificultades en la persecución penal de estas conductas. Entre las recomendaciones principales, proponen mejorar la técnica legislativa en la redacción de tipos penales y crear figuras nuevas, con el fin de ofrecer mayor claridad y seguridad jurídica.

El aporte más relevante de este trabajo es su propuesta de reconceptualización de diversas figuras, tales como la difusión de información falsa, el espionaje informático, el sabotaje o daño informático y la violación de correspondencia, entre otras. Cada categoría se desarrolla a partir del análisis del bien jurídico tutelado, los elementos del tipo y su correspondencia con los estándares de Budapest. El estudio concluye con un conjunto de recomendaciones normativas orientadas a armonizar la legislación nacional con compromisos internacionales.

Esta tesis ofrece un panorama tipológico y conceptual sólido sobre los delitos informáticos en el país y la necesidad de modernizar la legislación. No obstante, no aborda de manera específica la responsabilidad penal de las personas jurídicas frente a incidentes de ciberseguridad, aspecto central del artículo 12 de Budapest.

Destaca además la tesis de Elizondo (2021), uno de los primeros estudios que examinan de forma sistemática las implicaciones penales de la incorporación del Convenio de Budapest al ordenamiento nacional, que culmina con propuestas de *lege ferenda* para armonizar los tipos penales con los estándares internacionales. En términos sustantivos, el autor plantea como hipótesis que el sistema penal presenta insuficiencias frente a la adhesión

de Costa Rica al Convenio, generando inseguridad jurídica para los imputados, hipótesis que considera demostrada tras un examen bibliográfico y comparado de fuentes doctrinales y jurisprudenciales.

Asimismo, documenta vacíos de adecuación legislativa —incluida la ausencia de reservas en el proceso de ratificación y la necesidad de clarificar conceptos— a partir del análisis de figuras como acceso e interceptación ilícita, ataques a la integridad de datos y sistemas, abuso de dispositivos, falsificación y fraude informático y delitos vinculados a pornografía infantil y propiedad intelectual.

En lo histórico-normativo, reconstruye el derrotero de la adhesión y entrada en vigor del Convenio en Costa Rica —3 de julio de 2017—, lo que enmarca la urgencia de reformas internas coherentes con los compromisos asumidos. En conjunto, este antecedente robustece la base nacional para la presente investigación, que se centra en la responsabilidad penal de las personas jurídicas por incidentes de ciberseguridad y propone cerrar el vacío costarricense conforme al artículo 12 del Convenio de Budapest.

En la misma línea de reflexión sobre la adecuación del ordenamiento nacional, Bolaños Jaimes (s. f.), en su tesis Los ciberdelitos: retos que enfrenta el Código Penal en Costa Rica, realizó un análisis crítico de las reformas introducidas al Código Penal frente a los delitos informáticos. Su investigación resalta la insuficiencia de los mecanismos tradicionales de persecución penal frente a los desafíos del entorno digital y propone una actualización más integral que incorpore las nuevas formas de criminalidad tecnológica.

Por otra parte, investigaciones más recientes se han centrado en la figura de la responsabilidad penal de las personas jurídicas. La tesis de Alfaro Ulate y Rojas Rodríguez (2022): La imputación de la responsabilidad penal de la persona jurídica: un análisis crítico de la regulación costarricense, examina la Ley N.° 9699 de 2019, que introdujo la

responsabilidad penal de las personas jurídicas en casos de corrupción. El trabajo discute los modelos doctrinales de imputación (vicarial y autorresponsabilidad) y analiza comparativamente las experiencias de países como España, Italia y Argentina. Los autores concluyen que la regulación costarricense es limitada y requiere ser ampliada a otros ámbitos delictivos.

En la misma dirección, Fernández (2024) publicó el artículo La responsabilidad penal de la persona jurídica en Costa Rica, en el cual revisa los fundamentos de la Ley N.° 9699, la génesis internacional de estas reformas y la función que cumplen los programas de cumplimiento como posibles atenuantes. Su análisis muestra cómo Costa Rica ha dado un primer paso hacia el reconocimiento de la responsabilidad penal corporativa, pero todavía mantiene un catálogo reducido de delitos aplicables, lo que limita su eficacia y su alcance.

Finalmente, desde una perspectiva distinta, Jiménez Mora y Merayo Ramírez (2017), en su tesis Los ciberataques en el marco de la responsabilidad internacional de los Estados en tiempos de paz, abordaron la cuestión de los ciberataques en clave de derecho internacional. Aunque no se centra en el ámbito penal interno, este estudio aporta elementos sobre la debida diligencia estatal y las obligaciones internacionales que pueden derivarse de ataques cibernéticos, lo que enriquece la comprensión de la problemática de la seguridad digital en un plano más amplio.

Estos antecedentes muestran que la literatura costarricense ha explorado tanto la necesidad de modernizar los tipos penales en materia informática como los primeros pasos hacia la responsabilidad penal de las personas jurídicas. Sin embargo, ninguno de los estudios se ha enfocado de manera específica en la responsabilidad penal corporativa por incidentes de ciberseguridad bajo el estándar del artículo 12 del Convenio de Budapest. Precisamente

allí radica la originalidad del presente trabajo, que busca llenar ese vacío mediante una propuesta normativa concreta.

Los estudios nacionales existentes ofrecen un valioso marco doctrinal y normativo sobre ciberdelincuencia (Bolaños Jaimes), responsabilidad penal corporativa (Alfaro Ulate & Rojas Rodríguez; Fernández) y responsabilidad estatal internacional (Jiménez Mora & Merayo Ramírez). Sin embargo, ninguno aborda directamente la responsabilidad penal de personas jurídicas por incidentes de ciberseguridad conforme al artículo 12 del Convenio de Budapest.

1.4.2 Antecedentes internacionales

La discusión sobre la responsabilidad penal de las personas jurídicas en materia de ciberdelincuencia y ciberseguridad ha recibido atención creciente en distintos ordenamientos y ámbitos académicos. A continuación, se presentan varias tesis y artículos académicos internacionales relevantes que abordan la responsabilidad penal de las personas jurídicas en incidentes de ciberseguridad. Se incluyen trabajos sobre modelos de imputación corporativa (vicarial, autorresponsabilidad, deberes de organización), fundamentos jurídicos, experiencias legislativas comparadas (UE, EE.UU., Latinoamérica) y propuestas de reforma:

1. Březinová, K. (2017). *Company Criminal Liability for Unlawful Attacks against Information Systems within the Scope of EU Law*. Charles University in Prague, Faculty of Law Research Paper No. 2017/II/3. Esta tesis de investigación examina la responsabilidad penal de las personas jurídicas por ciberdelitos en el ámbito de la Unión Europea, con especial atención a los ataques contra sistemas informáticos. Březinová analiza la evolución normativa europea, en particular la Directiva 2013/40/UE sobre ataques contra los sistemas de información, y cómo esta

exige a los Estados miembros establecer la responsabilidad penal de las personas jurídicas por delitos de acceso ilícito o interferencia informática. El trabajo describe el régimen sancionatorio aplicable a entes corporativos bajo la legislación de la UE y de la República Checa, evaluando críticamente su eficacia. La autora concluye que el modelo europeo combina elementos vicariales y de autorresponsabilidad, pues la directiva europea obliga a imputar a la empresa los ataques informáticos cometidos "por su cuenta" por individuos vinculados a ella, a la vez que exige incorporar programas de cumplimiento (*compliance*) para prevenir tales delitos. Este estudio ofrece una perspectiva comparada valiosa sobre los fundamentos legales y retos prácticos de atribuir responsabilidad penal corporativa en materia de ciberataques, señalando lagunas y proponiendo mejoras a la implementación nacional de estas normas.

2. Rote, N., Bhardwaj, S., & Sebastian, A. (2025). *Corporate Criminal Liability for AI-Induced Cybersecurity Failures in Healthcare Systems*. Lex Localis – Journal of Local Self-Government, 23(S1), 95–106. – *Artículo académico reciente que explora la responsabilidad penal corporativa frente a incidentes de ciberseguridad ligados al uso de inteligencia artificial (IA) en el sector sanitario, con un enfoque filosófico-jurídico y comparativo.* Los autores evalúan casos de brechas de seguridad célebres (como el ataque *ransomware* a Colonial Pipeline en EE.UU. o el incidente *WannaCry* en el NHS del Reino Unido) para evidenciar la renuencia de las legislaciones actuales a criminalizar a las empresas incluso ante negligencias graves en ciberseguridad. Se destaca que en jurisdicciones como EE.UU., Reino Unido, India y la UE, los vacíos legales llevan a canalizar las consecuencias de grandes incidentes hacia sanciones civiles o administrativas, eludiendo la vía penal.

Este trabajo critica la inadecuación de los conceptos clásicos del derecho penal (como el *mens rea* individual) frente a amenazas tecnológicas emergentes. Propone por ello, reformas jurídicas "adaptativas", incluyendo la adopción de un *"mens rea organizacional"* y nuevos paradigmas de imputación basados en el diseño y la cultura corporativa. En síntesis, Rote et al. abogan por actualizar el marco legal para hacer efectivamente imputables penalmente a las corporaciones cuando fallas de seguridad (p. ej. falta de controles sobre sistemas de IA) causen graves riesgos sociales, especialmente, en sectores sensibles como la salud. La propuesta subraya la necesidad de reforzar la obligación jurídica de organización en materia de ciberseguridad corporativa como elemento de responsabilidad penal y no solo de responsabilidad civil.

3. Moreno-Piedrahíta Hernández, C. (2019). *El ocaso de los modelos de responsabilidad penal de las personas jurídicas en la jurisprudencia y doctrina españolas*. Política Criminal, 14(28), 323–354. Este es un artículo doctrinal que revisa críticamente los modelos teóricos de imputación penal corporativa *(heterorresponsabilidad vs. autorresponsabilidad) a la luz de la experiencia española.* El autor expone que tradicionalmente la doctrina distinguía entre un modelo vicarial (o *heterorresponsabilidad*), donde la empresa responde por el delito cometido por su empleado y un modelo de autorresponsabilidad, donde la persona jurídica es culpable por sus defectos de organización o "cultura corporativa" que propician el delito. Cita, por ejemplo, a Gómez-Jara, quien desarrolla la noción de *culpabilidad por cultura empresarial de irrespeto al Derecho*, con la posibilidad de eximir a la empresa si tenía programas de compliance penal eficaces. No obstante, Moreno-Piedrahíta argumenta que en la práctica reciente del Tribunal Supremo

español estas categorías se han entremezclado hasta el punto de volverse difusas o inexistentes. La jurisprudencia ha incorporado elementos de ambos enfoques: exige un "hecho de conexión" (delito cometido por un individuo ligado a la empresa, como en el modelo vicarial) pero al mismo tiempo evalúa la falta de prevención o defectos organizativos de la empresa (elemento propio del modelo de autorresponsabilidad). El trabajo concluye que esta convergencia implica la superación del debate dicotómico entre modelos puros, consolidándose en cambio un modelo mixto coherente con una teoría del delito específica para personas jurídicas. Este análisis es relevante pues sitúa los fundamentos jurídicos de la responsabilidad penal corporativa (especialmente aplicable a delitos tecnológicos o de ciberseguridad) en una base teórica unificada, donde tanto la acción delictiva individual como la falla de organización son considerandos esenciales para imputar a la empresa.

4. Santana Grimaldi, G. (2022). *Distintos modelos de imputación penal de las personas jurídicas (I)*. Acento (República Dominicana), 20 de julio de 2022. Santana identifica tres vías de imputación: *(i) Modelo vicarial o por transferencia*, *(ii) Modelo de autorresponsabilidad*, y *(iii) Modelo mixto o ecléctico*. En el modelo vicarial, la persona jurídica responde *por traslación* del acto ilícito cometido por uno de sus empleados, representantes o agentes en el seno de la empresa y en su beneficio. En esta concepción, el delito del individuo se atribuye directamente a la empresa como si fuera propio, de modo que la compañía tiene la obligación de controlar la actuación de sus integrantes y resulta penalmente responsable si alguno comete un delito en su nombre. La autora señala dos variantes de este modelo en el derecho comparado: la teoría de la identificación inglesa (que solo considera los actos de la alta dirección) versus el amplio *respondeat superior* estadounidense (que abarca los

actos de cualquier empleado cometido en el ámbito de sus funciones y en beneficio de la empresa). Santana también discute las críticas al modelo vicarial, como la que lo tilda de *responsabilidad objetiva por hecho ajeno* en aparente contradicción con el principio de culpabilidad, aunque aclara que la doctrina mayoritaria defiende su constitucionalidad al considerar que los actos de un órgano o directivo no son realmente "ajenos" a la persona jurídica.

Finalmente, se adelanta que los modelos de autorresponsabilidad enfatizan la culpabilidad propia de la empresa (por ejemplo, un defecto organizativo o falta de supervisión), mientras que modelos mixtos combinan elementos de ambos. Aunque esta publicación es de tipo divulgativo, proporciona una excelente síntesis doctrinal, útil para entender los fundamentos teóricos con los que distintos países (common law vs. civil law) abordan la imputación penal de personas jurídicas, lo cual es aplicable al análisis de incidentes de ciberseguridad corporativos.

5. Riffo, F. (2023). *Ciberseguridad: cuando la responsabilidad depende de la jurisdicción*. Idealex Press, 14 de septiembre de 2023. El autor señala que en Latinoamérica no existe uniformidad en cuanto a la responsabilidad (penal o regulatoria) de las empresas por brechas de seguridad digital. Países como Argentina, Perú y Chile han promulgado leyes para incentivar que las empresas fortalezcan su seguridad digital, aunque con resultados dispares. En el caso de Chile, se destacan dos nuevas normas de 2022: la Ley de Delitos Informáticos (inspirada en la Convención de Budapest) y la Ley de Delitos Económicos, que en conjunto refuerzan la responsabilidad penal de las personas jurídicas e imponen a las compañías el deber de gestionar proactivamente sus riesgos cibernéticos. Un experto citado explica que estas leyes chilenas son muy severas con las empresas, indicándoles que

la ciberseguridad "es un tema muy importante" y obligándolas implícitamente a implementar protocolos de prevención. Incluso se advierte que la falta de medidas adecuadas puede traducirse en que la filtración de datos o la afectación de la confidencialidad e integridad de la información constituya en sí misma un delito imputable a la empresa por omisión. El artículo también menciona el caso de Colonial Pipeline en EE.UU., cuyo ataque de *ransomware* en 2021 llevó a una sanción propuesta de casi un millón de dólares por parte de una agencia federal debido a fallas en su plan de contingencia. Sin embargo, dicha sanción fue de carácter administrativo, subrayando que en EE.UU. la respuesta tiende a venir por vía de reguladores (como el Departamento de Transporte) más que por condenas penales directas a la empresa. En suma, Riffo evidencia que la responsabilidad corporativa en ciberseguridad "depende de la jurisdicción", contrastando la aproximación proactiva de algunos países latinoamericanos –que combinan deberes legales de ciberseguridad, *enforcement* regulatorio y posibilidad de sanción penal– con la situación en otras jurisdicciones donde prevalecen medidas civiles o incentivos voluntarios de cumplimiento. Esta panorámica comparada sirve como referencia de las diferentes experiencias legislativas en el mundo hispanoamericano y EE.UU. respecto de la imputación corporativa en materia de ciberseguridad.

6. Millán López, E. (2023). *Delitos informáticos: situación actual, acceso ilícito y responsabilidad penal de las personas jurídicas*. Universidad de Valladolid, Grado en Derecho (Tesis de Licenciatura). La autora repasa el desarrollo histórico-normativo desde la tipificación del primer delito informático en 1995 hasta la importante reforma de 2010 que introdujo la responsabilidad penal corporativa en el Código Penal español, posteriormente modificada en 2015. Se destaca que la

protección penal frente a los ciberataques ha llegado al punto de incluir a las personas jurídicas como posibles sujetos activos de dichos delitos. Para comprender este cambio, Millán analiza la "esencia" de la responsabilidad penal de entes no naturales, concibiendo a las empresas como *"subsistemas autopoiéticos"* dentro del ordenamiento, capaces de delinquir independientemente de las personas físicas que las integran. El estudio profundiza en los bienes jurídicos tutelados por los tipos penales informáticos, debatiendo si conceptos como la "ciberseguridad" en sí misma deberían considerarse nuevos bienes jurídicos protegidos. Asimismo, examina el artículo 31 bis del CP español y su aplicación a delitos informáticos, ilustrando cómo los deberes de organización (por ejemplo, implementar sistemas de prevención y seguridad) juegan un rol en la atribución de responsabilidad a la empresa. El trabajo concluye con propuestas de mejora legal y recomendaciones para la implementación de programas de *compliance* específicos en ciberseguridad, como medio de atenuar o eximir la responsabilidad penal de la empresa. En conjunto, esta tesis sirve de antecedente académico nacional que complementa la visión internacional, mostrando cómo un país (España) ha adaptado su sistema penal para enfrentar los retos de la criminalidad informática corporativa.

7. Bautista Landaeta, L., & Perche Fuenmayor, Y. (2021). *Responsabilidad penal de la persona jurídica por delitos informáticos en Venezuela*. Los autores explican que Venezuela prevé desde 2001 la responsabilidad penal de las personas jurídicas por delitos informáticos, según un modelo de atribución ecléctico. Este modelo combina elementos de la autorresponsabilidad (*hecho propio*) con la concurrencia de personas naturales, es decir, se exige la actuación de individuos en representación de la empresa, pero la imputación legal recae directamente en la persona jurídica como

sujeto del delito.

En la práctica, la Ley Especial Contra los Delitos Informáticos (2001) y la reforma del Código Penal de 2005 establecieron que, si una empresa es condenada por un ciberdelito, enfrentará sanciones no corporales (principalmente multas cuyo monto puede duplicar el previsto para el delito cometido). Paralelamente, la persona natural involucrada puede recibir penas de prisión y multa, sin excluir la responsabilidad individual. El trabajo subraya el aumento de la ciberdelincuencia en Venezuela y cómo las personas jurídicas pueden figurar tanto como víctimas como perpetradoras en estos delitos emergentes. Esto plantea desafíos criminológicos y la necesidad de actualizar tanto la dogmática penal como las políticas públicas para abordar eficazmente la criminalidad informática empresarial. Los autores abogan por adecuar la legislación procesal y sustantiva, sugiriendo reforzar los mecanismos de cumplimiento preventivo en las organizaciones y clarificar la atribución penal en casos complejos (por ejemplo, ataques perpetrados a través de estructuras corporativas). Este artículo aporta una perspectiva latinoamericana concreta sobre la materia, ilustrando una experiencia legislativa temprana en la región (Venezuela fue pionera al legislar estos aspectos) y ofreciendo reflexiones sobre la efectividad y posibles reformas del modelo vigente para enfrentar los desafíos actuales de ciberseguridad.

Los antecedentes internacionales anteriores proporcionan una base sólida de antecedentes internacionales sobre responsabilidad penal corporativa en ciberseguridad. Incluyen desde análisis teóricos de modelos de imputación (vicarial vs. autorresponsabilidad), hasta estudios comparados de legislación en la Unión Europea, Estados Unidos y diversos países latinoamericanos, así como propuestas de evolución

normativa. Estos trabajos académicos serán útiles para fundamentar y contrastar el marco jurídico nacional en una tesis sobre la materia, aportando ejemplos de reformas legales, enfoques de *compliance* y debates doctrinales relevantes a nivel global. Cada fuente citada combina el rigor jurídico con la actualidad del tema, lo que en conjunto permite una comprensión amplia y crítica de cómo se está abordando la responsabilidad penal de las personas jurídicas por incidentes de ciberseguridad en distintas jurisdicciones del mundo.

Estos antecedentes internacionales reflejan un consenso en torno a la necesidad de extender la responsabilidad penal a las personas jurídicas frente a incidentes de ciberseguridad, aunque con variaciones significativas según la jurisdicción. Mientras en Europa se consolida un modelo mixto que combina imputación por actos de individuos y deberes de organización (Březinová, 2017; Moreno-Piedrahíta Hernández, 2019), en Latinoamérica se exploran soluciones legislativas incipientes pero prometedoras (Bautista Landaeta & Perche Fuenmayor, 2021; Riffo, 2023). Asimismo, propuestas más innovadoras sugieren adaptar los conceptos de culpabilidad a la era digital mediante nociones como el "mens rea organizacional" (Rote et al., 2025).

Estos aportes constituyen un marco de referencia indispensable para la investigación cuyo valor radica en trasladar estas experiencias al caso costarricense y formular una propuesta normativa que cierre el vacío actual en materia de responsabilidad penal corporativa por incidentes de ciberseguridad.

En síntesis, los antecedentes internacionales muestran que la tendencia comparada se orienta hacia modelos que reconocen la responsabilidad penal de las personas jurídicas en materia de ciberseguridad, ya sea bajo esquemas vicariales, de autorresponsabilidad o mixtos. La Unión Europea y España han avanzado en consolidar un marco que combina la imputación de actos individuales con la exigencia de deberes de organización (Březinová,

2017; Moreno-Piedrahíta Hernández, 2019; Millán López, 2023), mientras que Chile y Venezuela representan experiencias latinoamericanas relevantes que, con distintos alcances, han abierto la puerta a la responsabilidad corporativa en delitos informáticos (Riffo, 2023; Bautista Landaeta & Perche Fuenmayor, 2021).

Incluso en contextos donde prevalece la respuesta administrativa, como Estados Unidos o Reino Unido, surgen propuestas innovadoras para adaptar la imputación penal a los retos de la inteligencia artificial y la cultura organizacional (Rote, Bhardwaj & Sebastian, 2025). Frente a este panorama, resulta evidente que Costa Rica mantiene un rezago normativo, pues carece de un régimen penal corporativo aplicable a incidentes de ciberseguridad. Precisamente, ahí se ubica la originalidad y pertinencia de la investigación: formular una propuesta normativa que cierre este vacío, armonizando el ordenamiento costarricense con el artículo 12 del Convenio de Budapest y con las tendencias internacionales más avanzadas.

1.5 Alcances y limitaciones

El presente trabajo se plantea dentro de un marco dogmático y propositivo, orientado a analizar la responsabilidad penal de las personas jurídicas por incidentes de ciberseguridad en Costa Rica y a formular una propuesta normativa que permita superar el vacío identificado en la legislación vigente. El análisis se fundamenta en el artículo 12 del Convenio de Budapest y en experiencias comparadas de derecho europeo y latinoamericano, de modo que el estudio no se limita a un diagnóstico, sino que persigue un aporte concreto al debate jurídico nacional.

En cuanto a sus alcances, la investigación aborda los incidentes de ciberseguridad que comprometen bienes jurídicos como la confidencialidad, integridad y disponibilidad de datos y sistemas. El trabajo se centra en definir un modelo de imputación corporativa compatible

con los principios constitucionales de legalidad, culpabilidad y proporcionalidad, así como en diseñar un catálogo sancionatorio aplicable a las personas jurídicas. Asimismo, se consideran los programas de cumplimiento en ciberseguridad como posibles atenuantes o eximentes de responsabilidad, en línea con las tendencias internacionales. Temporalmente, el análisis comprende el período que inicia con la adhesión de Costa Rica al Convenio de Budapest en 2017 hasta la actualidad, mientras que metodológicamente se circunscribe al estudio de fuentes normativas, doctrinales y comparadas, sin recurrir a instrumentos empíricos como encuestas o entrevistas.

No obstante, el trabajo enfrenta ciertas limitaciones que conviene reconocer. En primer lugar, se restringe al ámbito costarricense, recurriendo al derecho comparado únicamente como marco de referencia. En segundo lugar, el análisis se concentra en la responsabilidad penal, dejando fuera un examen exhaustivo de las dimensiones civil y administrativa, aunque se mencionen de manera complementaria. En tercer lugar, la investigación se desarrolla en un contexto en el que no existe jurisprudencia nacional específica sobre la materia, lo que obliga a formular propuestas de lege ferenda apoyadas principalmente en doctrina y normativa comparada. Además, el estudio no aborda en detalle los aspectos técnicos propios de la ingeniería informática, sino que adopta nociones funcionales suficientes para comprender el impacto jurídico de los incidentes de ciberseguridad. Finalmente, se reconoce la posible obsolescencia de algunos supuestos, dado que la tecnología y las amenazas digitales evolucionan con rapidez; en consecuencia, la propuesta normativa aquí planteada debe entenderse como un punto de partida flexible y susceptible de actualización.

1.5.1 Alcances

Este trabajo se centra en el análisis dogmático y propositivo de la responsabilidad penal de las personas jurídicas frente a incidentes de ciberseguridad en Costa Rica. El alcance principal es formular una propuesta normativa que permita cerrar el vacío identificado en el ordenamiento costarricense, tomando como parámetro el artículo 12 del Convenio de Budapest y las experiencias comparadas más relevantes.

En términos materiales, el estudio aborda los incidentes de ciberseguridad que comprometen la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos, que potencialmente pueden configurar delitos tipificados en el Código Penal o que requieran nuevas figuras. El énfasis estará en el diseño de un modelo de imputación corporativa compatible con los principios de legalidad, culpabilidad y proporcionalidad, así como en el establecimiento de un catálogo sancionatorio razonable y en la función de los programas de cumplimiento (*compliance*) como atenuantes o eximentes.

En cuanto al plano temporal, el trabajo considera la evolución normativa desde la adhesión de Costa Rica al Convenio de Budapest en 2017 hasta la actualidad, con inclusión de debates doctrinales y legislativos más recientes. En lo metodológico, el alcance se limita al uso de fuentes normativas, doctrinales y comparadas, sin recurrir a técnicas de investigación empírica como encuestas o entrevistas, dado que la naturaleza del problema es fundamentalmente dogmática y de política legislativa.

1.5.2 Limitaciones

El estudio presenta varias limitaciones que deben ser reconocidas:

1. Ámbito geográfico: la investigación se circunscribe al ordenamiento costarricense. Si bien se pueden revisar modelos comparados, estos cumplen una función ilustrativa y no un análisis exhaustivo de derecho comparado.

2. Cobertura temática: el foco se ubica en la responsabilidad penal de las personas jurídicas por incidentes de ciberseguridad, dejando fuera el análisis profundo de la responsabilidad civil o administrativa, aunque se las mencione como marcos complementarios.
3. Limitación jurisprudencial: en caso de que en Costa Rica no existiera aún jurisprudencia específica sobre la materia, el trabajo se apoyaría principalmente en doctrina y derecho comparado. Esto implica que las propuestas normativas deben considerarse sujetas a validación futura en la práctica judicial.
4. Alcance técnico: la tesis no pretende entrar en detalle en aspectos de ingeniería informática o técnicas avanzadas de ciberseguridad, sino que adopta estas nociones en un nivel funcional para comprender su impacto jurídico.
5. Posible obsolescencia: dada la velocidad con que evolucionan las tecnologías y las amenazas digitales, es posible que los incidentes de ciberseguridad adquieran nuevas formas que rebasen los supuestos analizados. En ese sentido, el trabajo debe entenderse como un punto de partida dinámico más que como una solución definitiva.

En conclusión, los alcances y limitaciones de la investigación buscan delimitar con claridad el objeto de estudio y las expectativas de resultado. El trabajo no pretende ofrecer una solución definitiva a todos los problemas que plantea la responsabilidad penal corporativa en el entorno digital, sino aportar un marco conceptual y normativo sólido, pertinente y viable, que sirva como base para la discusión legislativa y doctrinal en Costa Rica.

CAPÍTULO II: MARCO TEÓRICO

2.1 Delimitaciones conceptuales clave en materia de ciberdelitos

Para comprender la responsabilidad penal por ciberdelitos es preciso delimitar conceptualmente qué se entiende por *ciberdelito* (o *delito informático*) y otros términos afines. A continuación se abordan definiciones fundamentales, las diferencias entre ciberseguridad, privacidad y protección de datos en el ámbito penal, la noción de *sistemas informáticos* y *datos informáticos* como objetos materiales del delito y la tríada de seguridad de la información (confidencialidad, integridad, disponibilidad) como bienes jurídicos funcionales en el análisis típico de estas conductas.

Definición y alcances del término "ciberdelito" o "delito informático"

En la literatura jurídica, *ciberdelito* y *delito informático* suelen usarse indistintamente para referirse a conductas ilícitas vinculadas con tecnologías digitales. En ocasiones se emplean también los términos "delitos electrónicos" o "delitos computacionales" como sinónimos (Bolaños, s.f). En síntesis, un ciberdelito puede definirse como una acción ilícita cometida mediante el uso de sistemas o tecnologías de la información, ya sea como medio para perpetrar el hecho o teniendo a dichos sistemas/datos como fin u objetivo del ataque.

Ahora bien, la expresión "delito informático" no es unívoca, pues abarca realidades heterogéneas (Mayer, 2017). La doctrina distingue dos acepciones principales: una amplia, que abarca delitos tradicionales cometidos *mediante* computadoras o redes (v.gr. estafas, extorsiones o difusión de pornografía infantil a través de Internet), y otra estricta, referente a delitos cometidos *contra* sistemas informáticos o datos (v.gr. *hacking* o sabotaje

informático) (Mayer, 2017) . En términos similares, se suele reservar el término "cibercrimen" para referir a la criminalidad informática (en sentido amplio o estricto) ejecutada a través de redes como Internet (Mayer, 2017). Este matiz subraya que no toda conducta ilícita relacionada con computadoras encaja en la categoría de ciberdelito estricto: por ejemplo, un ataque que solo daña el hardware (la componente física de un equipo) típicamente se encuadra en delitos comunes contra la propiedad (p.ej., daño simple), mientras que las conductas que inciden en el software o los datos sí ameritan un tratamiento diferenciado como delitos informáticos específicos. En definitiva, el factor distintivo del ciberdelito es la implicación esencial de la tecnología digital en la comisión del ilícito, ya sea como instrumento o como objetivo principal del ataque (Bolaños, s.f).

Por su parte, organismos internacionales han propuesto definiciones abarcadoras. La UNODC describe la *ciberdelincuencia* como un término que engloba una amplia gama de delitos, incluyendo ataques contra sistemas y datos informáticos (piratería o *hacking*, sabotaje de datos), estafas y fraudes computacionales (phishing, fraude financiero en línea), delitos relacionados con contenidos ilícitos (p. ej. distribución de pornografía infantil) y violaciones a la propiedad intelectual en entornos digitales. El Convenio de Budapest sobre Ciberdelincuencia (2001) –principal instrumento internacional en la materia, ratificado por Costa Rica en 2017– sigue un criterio similar al agrupar los delitos informáticos en cuatro categorías: (1) delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos (acceso ilícito, interceptación ilícita de datos, interferencia en sistemas o datos) (Amato, 2024); (2) delitos relacionados con contenidos ilícitos (por ej., pornografía infantil, discursos de odio); (3) delitos informáticos en sentido amplio, como la falsificación y el fraude cometidos mediante sistemas informáticos; (4) infracciones a la propiedad

intelectual en entornos digitales (Amato, 2024). Esta clasificación evidencia que los *ciberdelitos* pueden lesionar muy diversos bienes jurídicos, tradicionales y nuevos, lo cual plantea el desafío de delimitar con claridad su objeto de protección.

En el caso de Costa Rica, la incorporación progresiva de tipos penales informáticos refleja estos alcances. A partir de la Ley 8148 de 2001, se adicionaron al Código Penal figuras como la *Violación de comunicaciones electrónicas* (art. 196 bis), *Fraude informático* (217 bis) y *Alteración de datos y sabotaje informático* (229 bis) (Bonilla, 2019). Posteriormente, la Ley 9048 de 2012 reformó y amplió el catálogo, introduciendo delitos como *suplantación de identidad digital*, *espionaje informático*, *propagación de programas maliciosos*, *phishing* o suplantación de páginas web, entre otros (Bonilla, 2019). Estas reformas ubicaron inicialmente los delitos informáticos dentro del título de delitos contra la propiedad, debido en parte a su impacto patrimonial. No obstante, la doctrina local advirtió que los bienes jurídicos tutelados trascienden lo meramente patrimonial (Bonilla, 2019), sugiriendo que hubiera sido más sistemático crear un título específico de "Delitos Informáticos y conexos".

2.1.1 Ciberseguridad, privacidad y protección de datos: diferencias desde la perspectiva penal

Existen tres nociones relacionadas con los delitos informáticos que conviene diferenciar: la ciberseguridad, la privacidad (o intimidad) y la protección de datos personales. Si bien están interconectadas, cada una tiene un enfoque y tutela jurídica particular, en especial, en el ámbito penal:

Ciberseguridad: Se refiere al conjunto de medidas técnicas, organizativas y legales destinadas a proteger sistemas informáticos, redes y datos frente a accesos no autorizados, ataques o daños deliberados. En otras palabras, busca garantizar la seguridad de la información y de las infraestructuras digitales. Desde la perspectiva penal, la ciberseguridad conecta con la tipificación de conductas que vulneran esa seguridad, como el *hacking* (acceso ilícito a sistemas), la instalación de malware, el sabotaje de sistemas o la interceptación de comunicaciones. Son figuras delictivas orientadas a sancionar a quienes quiebran la confidencialidad, integridad o disponibilidad de sistemas y datos, es decir, quienes comprometen la ciberseguridad de personas, empresas o entidades estatales (Amato, 2024). La importancia penal de la ciberseguridad radica en proteger la confianza en las tecnologías digitales y prevenir que su aprovechamiento por la sociedad se vea frustrado por actividades ilícitas.

Privacidad/Intimidad: Consiste en el derecho de las personas a mantener reservada su vida privada y sus comunicaciones, controlando la divulgación de información personal. Es un bien jurídico de raigambre constitucional (derecho a la intimidad, inviolabilidad de las comunicaciones privadas) que el derecho penal tutela frente a intromisiones ilegítimas. En el contexto informático, la privacidad se ve amenazada por conductas como el espionaje electrónico, la difusión no autorizada de datos personales o la intrusión en cuentas de comunicación (correo electrónico, mensajería) sin consentimiento. Un ejemplo típico es el delito de *violación de comunicaciones*(acceso o interceptación de correos, mensajes u otras comunicaciones electrónicas ajenas), cuya penalización busca resguardar la confidencialidad de las comunicaciones y, por ende, la privacidad de los individuos (Bonilla, 2019). También los delitos de *descubrimiento y revelación de secretos* se han adaptado al entorno digital para

sancionar la obtención y difusión indebida de información privada almacenada en sistemas informáticos. En suma, desde el plano penal la privacidad se protege castigando aquellas conductas que vulneran el ámbito de intimidad personal mediante el uso de tecnologías.

Protección de datos personales: Es un concepto jurídico relacionado con la privacidad pero diferenciado: alude al marco normativo (generalmente de naturaleza administrativa y constitucional) que regula el tratamiento legítimo de los datos personales (información relacionada con una persona identificada o identificable). Implica principios y obligaciones para quienes recopilan, almacenan o utilizan datos de personas (consentimiento, finalidad, seguridad, etc.), y reconoce a los individuos derechos sobre sus datos (acceso, rectificación, cancelación, etc.). En Costa Rica, por ejemplo, existe la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (Ley N.° 8968), inspirada en estándares internacionales. Si bien la mayoría de sanciones en esta materia son administrativas o civiles, la protección de datos *también tiene aristas penales*. En contextos donde el manejo indebido de datos personales lesiona gravemente la intimidad o causa perjuicios (p. ej., comercialización ilícita de bases de datos sensibles, filtraciones masivas dolosas, violación de medidas de seguridad de datos personales), el derecho penal puede intervenir. De hecho, muchas conductas de *ciberdelito* implican simultáneamente violaciones a la seguridad de la información y a la protección de datos personales. La diferencia conceptual es que la privacidad se enfoca en el *derecho sustantivo* de la persona a su intimidad, mientras que la protección de datos se centra en las *reglas procesales y garantías* sobre el manejo de información personal. Penalmente, ambas convergen cuando, por ejemplo, un ataque informático expone datos personales de terceros: allí se lesiona tanto la seguridad del sistema como la privacidad de las personas.

En resumen, ciberseguridad, privacidad e intimidad y protección de datos son conceptos interrelacionados que apuntan a distintos aspectos del fenómeno digital. La ciberseguridad provee el *medio seguro* para la información (evitando intrusiones y daños); la privacidad/intimidad salvaguarda el *contenido personal* de esa información y las comunicaciones y la protección de datos personales establece el *marco legal* para el uso legítimo de información personal. Esta distinción analítica ayuda a comprender qué persigue cada tipo penal: unos protegen la seguridad de los sistemas en sí mismos, otros la intimidad y autodeterminación informativa de las personas, aunque en la práctica muchos ciberdelitos terminan afectando, a la vez, la seguridad informática y derechos individuales, lo cual genera solapamientos y retos interpretativos.

"Sistemas informáticos" y "datos informáticos" como objetos materiales del delito

Dos nociones técnicas resultan centrales en la dogmática de los ciberdelitos: la de sistema informático y la de dato informático. Ambos constituyen los objetos materiales sobre los que recaen muchas conductas delictivas en el entorno digital, por lo que su definición y comprensión son cruciales para delimitar el alcance de los tipos penales.

Sistema informático – Según el Convenio de Budapest y la doctrina comparada, se define como *"todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa"* (Real Academia Española & Consejo General del Poder Judicial (2001). En otras palabras, abarca desde una sola computadora hasta redes complejas de equipos, servidores y otros dispositivos digitales, incluyendo sus

componentes de hardware y software, siempre que en conjunto realicen procesamiento de información. Esta definición amplia es relevante penalmente porque clarifica que las conductas de acceso ilegítimo, daños o sabotajes pueden recaer no solo en *computadoras personales*, sino en cualquier arreglo de dispositivos con procesamiento automatizado (ej.: sistemas bancarios en red, infraestructuras críticas SCADA, servicios en la nube, etc.).

El Código Penal costarricense, tras las reformas introducidas por la Ley 9048/2012, tipifica expresamente ataques a "sistemas informáticos" utilizando esta noción inclusiva (por ejemplo, en el delito de sabotaje informático o en el de acceso no autorizado a sistemas) (Bonilla, 2019). Es importante destacar que el sistema informático, en sí, puede ser considerado el "objetivo" del delito informático: por ejemplo, en un *ataque de denegación de servicio* el objeto material es el sistema víctima cuyos recursos se inutilizan, y en un *hacking* es el sistema cuya barrera de acceso se vulnera. La jurisprudencia y doctrina han debido interpretar estos términos técnicos para aplicarlos a casos concretos, enfrentando a veces desafíos probatorios (p.ej., demostrar que un conjunto de dispositivos interconectados constituye un "sistema" específico o que un servicio en la nube equivale a un sistema informático ajeno).

Dato informático – En términos generales, puede definirse como *toda representación de hechos, información o conceptos en una forma susceptible de ser procesada por un sistema informático*. El Diccionario Panhispánico Jurídico lo describe sencillamente como un dato registrado en un sistema o componente informático Real Academia Española & Consejo General del Poder Judicial. (s. f.). Esto comprende cualquier contenido digital: archivos de texto, imágenes, bases de datos, credenciales electrónicas,

registros de transacciones, etc. Los datos informáticos son intangibles, pero el derecho penal los reconoce como *entidades susceptibles de tutela jurídica*.

De hecho, varios ciberdelitos tienen por objeto específico proteger la integridad, disponibilidad o confidencialidad de los datos en cuanto tales – por ejemplo, el tipo penal de *alteración o daño informático* sanciona al que destruya, deteriore o altere datos informáticos ajenos, protegiendo así la integridad de la información. Del mismo modo, se castiga el acceso no autorizado a datos (protegiendo su confidencialidad) y la obstaculización deliberada del acceso a ellos (protegiendo su disponibilidad). Un aspecto a subrayar es que el *dato informático* como objeto material del delito rompe con la noción tradicional de "bien corporal": aquí el objeto jurídico relevante es un bien intangible (la información) que, sin embargo, puede poseer valor económico, estratégico o personal equiparable a un bien material. Esta naturaleza inmaterial de los datos ha suscitado debates doctrinarios sobre si ciertas conductas constituyen verdaderos "apoderamientos" (¿robar datos es equiparable a robar cosas?) o "daños" (¿borrar datos equivale a destruir un objeto?) (Acurio Del Pino, 2005). La tendencia ha sido reconocer que los datos, al ser soporte de derechos y bienes jurídicos (patrimonio, intimidad, información, etc.), merecen protección penal autónoma. Así, los sistemas informáticos y los datos informáticos se erigen como los "nuevos objetos" sobre los cuales pueden recaer acciones delictivas, forzando a la dogmática jurídico-penal a adaptar categorías clásicas (como el concepto de *cosa mueble* o *documento*) a la realidad tecnológica.

En la legislación comparada se han formulado definiciones legales explícitas para estos términos. Por ejemplo, la legislación española –armonizada con el Convenio de Budapest– incorpora definiciones de *sistema informático* y *dato informático* en su Código

Penal (Real Academia Española & Consejo General del Poder Judicial (2001), las cuales han servido de referencia para otros países iberoamericanos. Costa Rica, si bien no enuncia las definiciones en el texto del código, los aplica en la práctica judicial conforme al entendimiento técnico usual y la guía de instrumentos internacionales. De esta manera, al analizar tipos penales informáticos en Costa Rica (acceso indebido, sabotaje, espionaje informático, etc.), se parte de la premisa de qué constituye un "sistema" y qué se considera "dato" objeto de protección. Los tribunales costarricenses, en casos de ciberdelitos, han debido determinar, por ejemplo, si una plataforma web califica como sistema informático o si ciertos conjuntos de información digital califican como datos cuya alteración configura delito, lo que muestra la importancia de estas delimitaciones conceptuales.

2.1.2 La tríada de la seguridad de la información: Confidencialidad, Integridad, Disponibilidad (CIA)

En el campo de la seguridad informática, se reconoce universalmente la tríada CIA (por sus siglas en inglés): Confidencialidad, Integridad y Disponibilidad de la información. Estos tres conceptos describen los atributos esenciales que deben salvaguardarse en cualquier sistema o dato y han sido adoptados también en el análisis jurídico-penal para entender la naturaleza del bien jurídico protegido en muchos ciberdelitos (Amato, 2024). A continuación, se explica cada elemento de la tríada y su relevancia típica:

- Confidencialidad: Implica que la información solo sea accesible por las personas autorizadas y se mantenga secreta frente a accesos no consentidos. Garantizar la confidencialidad supone proteger la información contra espionaje, divulgación indebida o robo de datos. Penalmente, este atributo está en juego en delitos como el acceso ilícito a sistemas (cuando alguien vulnera medidas de

seguridad para obtener datos privados) o la interceptación de comunicaciones – conductas que lesionan el derecho al secreto de la información. Por ejemplo, si un atacante se introduce en una base de datos confidencial o intercepta un email ajeno, está quebrantando la confidencialidad de esos datos. La confidencialidad suele asociarse al bien jurídico de la intimidad o privacidad cuando se trata de datos personales, y al secreto empresarial o seguridad nacional cuando involucra información sensible de empresas o del Estado (Acurio del Pino, 2005).

- Integridad: Se refiere a la exactitud, fiabilidad y estado inalterado de la información y los sistemas. Un dato íntegro es aquel que no ha sido modificado o dañado sin autorización; un sistema íntegro es aquel que funciona sin alteraciones maliciosas. Las infracciones a la integridad incluyen la alteración, manipulación o destrucción no autorizada de datos o programas. Un ejemplo típico es el *ataque de modificación de datos*, donde un agente cambia registros (p. ej., manipular saldos bancarios, adulterar archivos) afectando la veracidad de la información. También la propagación de *malware* que corrompe archivos o al sabotaje de sistemas que inutiliza programas quebatentan contra la integridad. La tutela penal de la integridad se aprecia en figuras como el daño informático (destrucción o deterioro de datos ajenos) o el saboteo informático y guarda relación con proteger tanto el patrimonio (cuando la integridad comprometida produce pérdidas económicas) como la fiabilidad de la información en ámbitos como el tráfico jurídico y la prueba electrónica (Acurio del Pino, 2005).

- Disponibilidad: Significa que la información y los servicios del sistema estén accesibles y utilizables en forma oportuna por quienes están

autorizados. En otras palabras, que los sistemas funcionen continuamente y los datos puedan ser accedidos cuando se requieren. Una violación de la disponibilidad ocurre, por ejemplo, en un ataque de denegación de servicio (DoS) que tumba un servidor impidiendo el acceso de usuarios legítimos o cuando un *ransomware* bloquea la información hasta hacerla inaccesible. Penalmente, la disponibilidad se protege sancionando conductas que obstaculizan o impiden el funcionamiento de sistemas ajenos o el acceso a sus datos. La reciente tipificación de la "obstrucción o interferencia informática" en varios ordenamientos es reflejo de ello. Este aspecto de la tríada se vincula con intereses colectivos y económicos: la indisponibilidad de sistemas críticos (ej.: redes financieras, plataformas de salud, servicios gubernamentales) puede generar caos y daños masivos, afectando la funcionalidad confiable de la sociedad digital (Amato, 2024).

Estos tres ejes –confidencialidad, integridad y disponibilidad– suelen considerarse "bienes jurídicos funcionales" en los delitos informáticos, en el sentido de que describen las funciones esenciales cuya afectación lesiona intereses jurídicos concretos (Amato, 2024). De hecho, gran parte de los tipos penales informáticos pueden mapearse según cuál de estos bienes (o cuál combinación) resultan lesionados. Por ejemplo, el espionaje informático (acceso y sustracción de información secreta) lesiona la confidencialidad; el sabotaje informático (borrar o dañar datos/sistemas) ataca la integridad y disponibilidad; el phishing o la suplantación de identidad digital comprometen confidencialidad (al obtener datos privados) y también pueden lesionar patrimonio (si derivan en fraude). Entender la tríada CIA permite apreciar que los ciberdelitos no siempre encajan perfectamente en las categorías jurídicas tradicionales, pero sí afectan valores

esenciales para el normal desenvolvimiento de la vida digital. Algunos autores sostienen que estos valores –considerados en conjunto– conforman un nuevo bien jurídico informático: la *seguridad de la información* en sí misma (Acurio del Pino, 2005). Otros, en cambio, opinan que realmente continúan protegiendo bienes clásicos (intimidad, propiedad, orden público) pero en su dimensión tecnológica (Mayer, 2017). En cualquier caso, la tríada sirve como marco analítico para evaluar la gravedad y naturaleza de cada conducta: un delito que vulnere los tres aspectos (p. ej. un ataque que roba datos confidenciales, los modifica y deja inutilizable el sistema) será particularmente lesivo y, por ende, penalmente reprochable en mayor medida que otro que quizá afecte solo uno de ellos de forma limitada.

En suma, las delimitaciones conceptuales anteriores proporcionan las bases para el análisis jurídico de los ciberdelitos. Contar con definiciones claras de qué constituye un ciberdelito, qué diferencias existen con nociones afines, cuáles son los objetos técnicos protegidos (sistemas y datos) y cuáles son las dimensiones fundamentales de la seguridad informática (CIA) resulta indispensable para abordar, en el siguiente apartado, los bienes jurídicos específicos que justifican la intervención del derecho penal en este campo, especialmente, de cara a la responsabilidad de las personas jurídicas en entornos digitales.

2.1.3 Bienes jurídicos protegidos en el entorno digital

La identificación del bien jurídico tutelado en los delitos informáticos reviste una importancia cardinal, pues de ello depende la legitimación del castigo penal y la correcta interpretación de los tipos delictivos. En el entorno digital se despliega una pluralidad de intereses jurídicos dignos de protección, algunos tradicionales (como la propiedad o la intimidad) y otros emergentes o funcionales (como la seguridad de los sistemas informáticos en sí misma). La doctrina no es unánime sobre si existe un bien jurídico novedoso y

específico subyacente a todos los ciberdelitos. Una primera tesis sostiene que sí, proponiendo la tutela autónoma de un bien jurídico *informático* diferente de los clásicos (Mayer, 2017). Según esta posición, delitos como el *hacking* o el *malware* protegerían ante todo la *seguridad de la información* (entendida como la integridad de sistemas y datos en un ciberespacio interconectado) más allá de los bienes tradicionales afectados. La segunda tesis, por el contrario, afirma que los ciberdelitos no tienen un bien jurídico propio, sino que "lo informático" es solo el medio comisivo o el contexto, mientras que los intereses protegidos siguen siendo los de siempre (intimidad, patrimonio, orden público, etc.) (Mayer, 2017). En esta línea, acceder sin autorización a una computadora ajena vulneraría la intimidad igual que abrir una carta, o sabotear una base de datos ajena lesionaría el patrimonio igual que dañar una propiedad física. Existe incluso una posición intermedia que considera muchos delitos informáticos como pluriofensivos, es decir, que afectan simultáneamente a varios bienes jurídicos, por ejemplo, el *espionaje informático* lesionaría al mismo tiempo la seguridad informática *y* la privacidad; una falsificación de datos informáticos atentaría contra la fe pública *y* la integridad de sistemas (Mayer, 2017).

En la práctica legislativa costarricense y latinoamericana, la tendencia ha sido reconocer diversos bienes jurídicos en juego, tipificando conductas específicas para su protección. A continuación, se analizan los principales bienes jurídicos que se ven comprometidos en el entorno digital –y que justifican su relevancia penal–, a saber: (1) la confidencialidad de las comunicaciones, (2) la integridad y correcto funcionamiento de sistemas y datos, (3) la intimidad, privacidad y protección de datos personales y (4) el patrimonio y la confianza en los entornos digitales. Se explica la naturaleza de cada uno, por

qué merecen tutela penal y cómo se manifiestan en los delitos informáticos, con referencias a la realidad costarricense y comparada.

2.1.4 Confidencialidad de las comunicaciones

La confidencialidad de las comunicaciones es un bien jurídico tradicional adaptado al mundo digital. Se trata del derecho de cualquier persona a que sus comunicaciones privadas (conversaciones, correspondencia, mensajes electrónicos) no sean interceptadas ni divulgadas indebidamente. En términos constitucionales, suele ampararse bajo la inviolabilidad de las comunicaciones (por ejemplo, el artículo 24 de la Constitución Política de Costa Rica garantiza el secreto de las comunicaciones privadas). En el ámbito digital, este bien jurídico cobra una nueva dimensión debido al volumen de comunicaciones electrónicas (emails, chats, videollamadas, etc.) y a la facilidad con que terceros pueden intentar acceder a ellas mediante técnicas de *hacking* o vigilancia electrónica.

Penalmente, la confidencialidad de las comunicaciones se tutela mediante figuras delictivas que castigan la interceptación, acceso o revelación no autorizada de comunicaciones ajenas. Un ejemplo claro en Costa Rica es el delito de Violación de comunicaciones electrónicas introducido en el Código Penal en 2001 (Bonilla, 2019) que sanciona al que indebidamente intercepte, abra, sustraiga o desvíe comunicaciones electrónicas que no le estén dirigidas.

La relevancia penal de este bien jurídico radica en que la libre comunicación confidencial es pilar de la autonomía personal y de varias relaciones sociales (v.gr. comunicaciones abogado-cliente, fuentes periodísticas, vida familiar, etc.). Su violación no solo daña la privacidad individual, sino que socava la confianza general en el uso de medios

de comunicación. Si los ciudadanos temen que sus correos electrónicos o mensajes puedan ser interceptados impunemente, se resienten derechos fundamentales y actividades legítimas en la era digital (negocios, diálogo político, interacción social en línea). Por ello, los ordenamientos contemporáneos penalizan con rigor conductas como el *espionaje de comunicaciones*, la *interceptación telemática* o incluso la mera curiosidad informática (acceder sin autorización a buzones electrónicos ajenos, aunque sea solo por husmear).

Cabe destacar que la protección de la confidencialidad incluye no solo el contenido de la comunicación sino también, en cierta medida, los datos asociados (metadatos) cuyo acceso puede revelar aspectos igualmente privados (p.ej., los registros de comunicaciones, destinatarios, horarios, ubicación). La jurisprudencia constitucional costarricense ha aportado un matiz interesante al respecto: en una sentencia de 2010, la Sala IV indicó que en materia de delitos informáticos vinculados a Internet, *"el bien jurídico tutelado no es la red como tal, sino el derecho a la comunicación y el derecho a la información"* (Bonilla, 2019). Es decir, lo protegido es la libertad y privacidad comunicativa que Internet facilita, más que la infraestructura en abstracto. De esa afirmación, se desprende que la confidencialidad de las comunicaciones digitales se conecta también con el derecho a la información (en cuanto garantiza canales seguros de intercambio informativo) y hasta con el derecho al conocimiento de la sociedad (pues sin comunicaciones confidenciales no hay confianza en compartir conocimiento).

En suma, la confidencialidad de las comunicaciones en entornos digitales constituye un bien jurídico de primer orden, cuya violación se persigue penalmente para preservar la privacidad individual y la confianza de la sociedad en que sus comunicaciones —sean

personales o profesionales— permanecen a salvo de injerencias arbitrarias. Este bien jurídico es especialmente sensible en contextos empresariales (secretos industriales), gubernamentales (seguridad del Estado) y profesionales (secreto médico, confidencialidad abogado-cliente), lo que ha llevado a agravar penas cuando la interceptación afecta ciertas comunicaciones calificadas. Asimismo, en el ámbito internacional, tratados como el Convenio de Budapest obligan a penalizar la interceptación ilícita de datos informáticos en transmisiones no públicas (Amato, 2024) reforzando la idea de que la confidencialidad comunicativa trasciende fronteras y requiere cooperación global para su protección.

2.1.5 Integridad y funcionamiento de sistemas y datos

El correcto funcionamiento de los sistemas informáticos y la integridad de los datos que contienen es otro bien jurídico fundamental en la era digital. Aquí se refiere a garantizar que los sistemas operen sin interferencias maliciosas y que los datos digitales permanezcan completos, fiables y no corrompidos. Este bien jurídico puede describirse como la *"seguridad informática"* en sentido estricto, es decir, la situación en que los sistemas y la información gozan de integridad y disponibilidad. Su relevancia penal es evidente: en una sociedad altamente digitalizada, la alteración o sabotaje de sistemas puede paralizar servicios esenciales y la manipulación de datos puede tener consecuencias devastadoras (imaginemos la adulteración de historiales clínicos, registros contables, padrones electorales, etc.).

Bajo esta categoría se agrupan varios bienes jurídicos específicos pero interrelacionados: la integridad de los sistemas informáticos (que estos no sean dañados ni funcional ni lógicamente), la integridad de los datos (que la información no sea borrada, alterada o contaminada indebidamente) y la disponibilidad/funcionamiento de ambos (que sistemas y datos permanezcan accesibles para su uso legítimo). En el derecho comparado,

suele hablarse de la protección de la *"confidencialidad, integridad y disponibilidad"* de sistemas y datos informáticos, que en conjunto conforman la base de este bien jurídico. De hecho, esa es la primera categoría de delitos en el Convenio de Budapest, indicando su centralidad (Amato, 2024).

En Costa Rica, la tutela penal de la integridad de sistemas y datos se manifiesta en tipos penales como daño o sabotaje informático (art. 229 bis y ter CP tras la reforma de 2012), que castiga al que destruya, deteriore, altere o inutilice sistemas, redes o datos informáticos ajenos; la propagación de programas malignos (introducir virus, malware – art. 232 CP); la interferencia informática no autorizada; y, en general, cualquier perturbación del normal funcionamiento de sistemas de terceros. Todos ellos protegen el interés de que los sistemas operen correctamente y la información en ellos contenida se mantenga íntegra (Acurio Del Pino, 2005). Por ejemplo, un ataque de *ransomware* que cifra datos y los vuelve inaccesibles atenta tanto contra la integridad (los datos son alterados mediante cifrado no autorizado) como contra la disponibilidad (los legítimos dueños no pueden acceder a ellos). Del mismo modo, un ataque DoS que colapsa un servidor afecta la disponibilidad del sistema para los usuarios autorizados. Esas conductas son penalmente relevantes porque implican "sacar de la esfera de disponibilidad del dueño" sus propios sistemas o datos, asimilándose en efecto a un daño o usurpación de algo de su pertenencia, aunque ese "algo" sea intangible.

La justificación penal de este bien jurídico estriba en que la sociedad actual depende profundamente de la continuidad y confiabilidad de sus sistemas informáticos. Desde servicios básicos (electricidad, agua, transporte) hasta sectores financieros, sanitarios y de seguridad pública, todos operan sobre sistemas digitales. Un ataque exitoso a la integridad o funcionamiento de estas infraestructuras puede comprometer bienes superiores como la vida,

la salud, el orden público o la economía nacional. En términos de bien jurídico, se puede decir que se protege la "funcionalidad informática" al servicio de la colectividad (Mayer, 2017). Autores como Acurio del Pino (2005) argumentan que la información en sí misma –y por extensión los sistemas que la procesan– constituye el bien jurídico primigenio de los delitos cibernéticos, por ser un insumo vital para el desarrollo social y económico. Desde esta óptica, cualquier ataque a la integridad/funcionamiento informático es un ataque a la "columna vertebral" de la sociedad digital.

No obstante, también puede analizarse que detrás de la integridad de sistemas/datos subyacen bienes jurídicos tradicionales, por ejemplo, si un hacker borra la base de datos de una empresa, puede verse como un ataque a su patrimonio; si sabotea el software de un hospital, pone en riesgo la vida y salud de pacientes; si manipula datos electorales, vulnera la seguridad pública y el orden democrático. Esta polivalencia hace que los delitos contra sistemas y datos sean a menudo pluriofensivos, tocando varias esferas jurídicas a la vez (Acurio Del Pino, 2005). Por ello, algunos códigos penales (como el colombiano o el chileno) han optado por tipificar estas conductas en títulos de delitos contra la seguridad pública o contra la fe pública, reconociendo su impacto más amplio. En Costa Rica, como se mencionó, inicialmente se incluyeron bajo delitos contra la propiedad, pero la doctrina local enfatiza que un sabotaje informático grave trasciende lo patrimonial y puede afectar intereses colectivos de primer orden (Bonilla, 2019).

Un desafío práctico en la tutela de este bien jurídico es medir el daño causado. A diferencia de un daño material evidente (quemar un auto, romper una ventana), en lo digital a veces la afectación es silenciosa pero crítica (p.ej., alterar dígitos en una base de datos puede pasar inadvertido pero causar enormes pérdidas económicas o de confianza). Esto ha llevado

a discutir cómo graduar las penas según la gravedad del resultado: por ejemplo, muchos países agravan las sanciones si la interferencia en sistemas pone en peligro la seguridad del Estado, la integridad de un mercado financiero o la vida de personas (v.gr., hackear un semáforo o un aparato médico). Costa Rica, en su reforma de 2012, introdujo el *"daño agravado"* informático como figura que considera la especial trascendencia de ciertos ataques (Bonilla, 2019).

En conclusión, la integridad y funcionamiento de sistemas y datos informáticos es un bien jurídico cuya tutela penal asegura que la infraestructura digital –de la cual dependen derechos y servicios esenciales– no sea vulnerada impunemente. Es un interés de naturaleza tanto individual (el titular de un sistema tiene derecho a que no lo saboteen) como colectiva (la sociedad requiere confianza en la estabilidad de los sistemas críticos). Su protección penal refuerza la resiliencia del entorno digital frente a quienes intenten usar la informática como "arma" para causar perjuicios.

2.1.6 Intimidad, privacidad y protección de datos personales

La intimidad o privacidad personal y la protección de los datos personales constituyen otro conjunto de bienes jurídicos particularmente afectados en la era digital y estrechamente vinculados entre sí. Se refieren al derecho de las personas a controlar la información relativa a su esfera personal y a no ver divulgados ni utilizados sus datos sin consentimiento. Este bien jurídico ha cobrado renovada relevancia con la masificación de tecnologías que recopilan, almacenan y transmiten datos personales (redes sociales, bases de datos gubernamentales, comercio electrónico, cámaras de vigilancia, etc.), generando riesgos de violación masiva de la intimidad.

En el ámbito penal, la tutela de la intimidad y datos personales se refleja en diversas conductas típicas, muchas de las cuales se traslapan con delitos informáticos. Por ejemplo, el mencionado delito de revelación de secretos (art. 196 CP CR) protege la intimidad sancionando al que obtenga y divulgue contenidos privados (ahora extensible a entornos informáticos). También la usurpación de identidad digital (art. 230 CP CR) lesiona la privacidad al hacer uso de datos personales ajenos para suplantar a alguien, con el consiguiente menoscabo a la reputación e identidad de la víctima (Bonilla, 2019). En legislaciones comparadas, se encuentran delitos específicos como el "phishing" de datos personales sensibles, la venta ilegal de bases de datos personales o el chantaje con información íntima obtenida por medios informáticos (por ejemplo, el delito de *sextorsión* o extorsión sexual digital). Todos comparten el objeto de proteger la intimidad y los datos personales frente a injerencias indebidas.

Un caso particular de bien jurídico digital en esta categoría es el derecho a la autodeterminación informativa, concepto originado en la jurisprudencia alemana y extendido por Europa a través de las leyes de protección de datos. Implica que las personas tienen derecho a decidir sobre el uso de sus datos personales. Aunque la mayoría de normas al respecto son de naturaleza administrativa (como la obligación de empresas de no ceder datos sin consentimiento o medidas de seguridad), varias jurisdicciones prevén sanciones penales para violaciones graves, reconociendo así la dimensión penal de este bien jurídico. Por ejemplo, España introdujo en su código penal un delito de "difusión no autorizado de datos personales de carácter reservado" y otro de "suplantación de identidad", para abordar justamente la afectación a la privacidad en redes (como publicar fotos íntimas de otra persona sin permiso o usar datos de otro para abrir cuentas fraudulentas). En Costa Rica, la Ley 8968

contempla sanciones administrativas, pero podrían concurrir tipos penales generales (coacción, difusión de secretos) si la violación de datos personales lesiona gravemente la intimidad o causa daños concretos.

La protección penal de la intimidad y los datos personales se justifica porque, en la sociedad de la información, las bases de datos y plataformas digitales contienen aspectos sumamente sensibles de nuestra vida: historiales médicos, financieros, preferencias, comunicaciones privadas, imágenes personales, etc. La exposición o uso indebido de esa información puede lesionar desde la dignidad humana (imaginemos la filtración de información médica confidencial) hasta el patrimonio (fraudes a partir de datos robados) o la seguridad personal (acoso y amenazas basados en datos obtenidos ilícitamente). Además, en términos colectivos, si no se protege este bien jurídico, se erosiona la confianza de las personas en participar de la vida digital, contrayendo el ejercicio de derechos (libertad de expresión, asociación, comercio electrónico, etc.) por temor a la vigilancia o la difusión no autorizada de sus datos.

Es importante notar que este bien jurídico puede colisionar con otros, generando *tensiones e interpretaciones difíciles*. Por ejemplo, la persecución del delito puede requerir medidas intrusivas (como investigar comunicaciones de sospechosos), lo que, a su vez, roza la confidencialidad de comunicaciones – de ahí la necesidad de un equilibrio y controles judiciales estrictos. Otra tensión típica es entre la privacidad y la seguridad colectiva: se debate hasta qué punto es legítimo que el Estado vigile comunicaciones digitales para prevenir ciberdelitos sin menoscabar la intimidad de ciudadanos inocentes. Este debate ha surgido en Costa Rica y otros países al discutir leyes de retención de datos o de *hacking* gubernamental para investigación criminal.

En el plano dogmático, también existe discusión sobre si la "información" misma es el bien jurídico protegido. Algunos autores afirman que en última instancia los delitos informáticos tutelan la información como nuevo bien jurídico autónomo (Acurio Del Pino, 2005), y dentro de ese paraguas estaría la información personal como subcategoría. Otros replican que la información no tiene sentido sino referida a derechos tradicionales: así, la *información personal* remite a la intimidad, la *información patrimonial* al patrimonio, etc. Sea cual sea la perspectiva, la protección de la intimidad y datos personales en ciberdelitos suele articularse combinando normas tradicionales con nuevas, para cubrir lagunas. Un claro ejemplo es el fenómeno del *doxing* (publicar masivamente datos personales de alguien para dañarlo): no encajaba perfectamente en tipos clásicos, lo que ha llevado a estudiar su inclusión expresa como delito dada la gravedad con la que puede afectar la vida privada y seguridad de la persona en el mundo digital.

En conclusión, la intimidad, privacidad y protección de datos personales conforman un bien jurídico esencial que el derecho penal defiende en el ciberespacio, adaptando figuras delictivas y creando otras nuevas. La responsabilidad penal de personas jurídicas en este ámbito es particularmente relevante, pues muchas compañías manejan volúmenes enormes de datos personales (bancos, telecomunicaciones, redes sociales) y podrían incurrir en delitos si no protegen esos datos o si los explotan ilícitamente. Precisamente, el régimen de responsabilidad penal corporativa –recientemente introducido en Costa Rica en 2019– obliga a las empresas a implementar medidas de cumplimiento (*compliance*) en protección de datos, bajo riesgo de sanciones si por dolo o negligencia grave permiten violaciones a la privacidad de usuarios. De ese modo, la tutela penal de este bien jurídico se extiende tanto a individuos como a entes colectivos, reconociendo su papel central en la confianza digital.

2.1.7 Patrimonio y confianza en entornos digitales

El patrimonio (entendido como el conjunto de derechos económicos y bienes de una persona) ha sido clásicamente protegido por el derecho penal mediante delitos contra la propiedad (hurto, estafa, daños, etc.). En el entorno digital, el patrimonio sigue siendo un bien jurídico medular, pero adopta nuevas formas y plantea retos específicos. Junto al patrimonio, emerge el concepto de "confianza digital" o *seguridad en las transacciones electrónicas*, aunque no es un bien jurídico autónomo en sentido estricto, sí describe un valor colectivo indispensable para el funcionamiento del mercado y las relaciones jurídicas en línea. Por ello, aquí abordaremos ambos: cómo se protege penalmente el patrimonio en contextos informáticos y cómo ciertas figuras buscan salvaguardar la confianza de usuarios y consumidores en las tecnologías digitales.

Delitos patrimoniales informáticos: Muchos ciberdelitos tienen por finalidad última un lucro o ventaja económica indebida, afectando el patrimonio de las víctimas. Estos incluyen, por ejemplo, el fraude informático (art. 217 bis CP CR) donde alguien, alterando o interfiriendo un sistema, obtiene un beneficio patrimonial en perjuicio ajeno (Bonilla, 2019). Modalidades concretas son el *phishing* (engaño masivo para obtener credenciales bancarias y robar fondos), el *carding*(uso fraudulento de tarjetas de crédito robadas online), el *ransomware* (exigir rescate económico a cambio de liberar un sistema secuestrado), la *estafa por medios informáticos* (p.ej., tiendas en línea ficticias que no entregan productos) o la *apropiación de criptomonedas* mediante hacking. Todas estas conductas lesionan el patrimonio de las personas, empresas o incluso del Estado, por medios electrónicos. El bien jurídico protegido es el mismo que en las estafas o robos tradicionales – la propiedad o el patrimonio – pero el modus operandi digital exige ajustes típicos. Por ejemplo, el Código

Penal español en su art. 248 ya define estafa incluyendo las realizadas "mediante manipulación informática o artificio semejante" para abarcar el hacking con fines de lucro. En Latinoamérica, varios códigos (Argentina, Chile, Perú) tipifican el *"fraude informático"* como figura autónoma, describiéndolo como la manipulación de datos o sistemas para producir un perjuicio patrimonial (Amato, 2024). Costa Rica, con la reforma de 2012, fortaleció su tipo de fraude informático y añadió figuras como la suplantación de sitios web (art. 233 CP) que típicamente se usa para cometer fraudes (*phishing*) y la suplantación de identidad digital (art. 230 CP) que a menudo es medio para defraudar o para dañar la reputación y así obtener ventajas (Bonilla, 2019).

La confianza en entornos digitales, por su parte, es un intangible pero crucial factor que subyace a las transacciones electrónicas y a la economía digital en general. Se refiere a la expectativa de los usuarios de que los sistemas son seguros, que las identidades digitales son genuinas, que la información que ven en línea es veraz (al menos en contextos oficiales), y que podrán realizar interacciones económicas o sociales sin ser engañados maliciosamente. Cuando esta confianza se quiebra, el daño excede al perjuicio patrimonial individual: si prolifera, por ejemplo, el phishing y miles de personas pierden dinero en banca electrónica, el público puede perder confianza en ese servicio, afectando la estabilidad del sistema financiero digital. Por ello, muchos delitos informáticos que protegen patrimonio también protegen la confianza colectiva en ciertas plataformas o mecanismos.

Un ejemplo claro es el delito de falsedad informática o falsificación de documentos electrónicos. Si un criminal logra falsificar certificados digitales, documentos electrónicos oficiales o firmas digitales, no solo está lesionando un patrimonio o un derecho individual, sino minando la fe pública en la validez de esos documentos. Varios ordenamientos han

actualizado sus delitos de falsificación para abarcar soportes informáticos, reconociendo que la fe pública digital es tan importante como la analógica. De forma similar, la creación y difusión de noticias falsas (*fake news*) mediante sistemas informáticos, cuando alcanzan cierto nivel (por ejemplo, para manipular mercados o procesos electorales), atenta contra la confianza pública y ha abierto el debate sobre su penalización. Costa Rica incorporó en 2012 el delito de difusión de información falsa (art. 236 CP) para sancionar a quien difunda, por medios informáticos, noticias falsas que pongan en peligro algún interés público o económico (Bonilla, 2019). Detrás de esta figura subyace la protección de la confianza del público en la veracidad mínima de la información crítica que circula en las redes.

Desde el ángulo estrictamente económico, la confianza digital también implica proteger la seguridad de las transacciones en línea. Delitos como la estafa informática o el *phishing* lesionan esta confianza al introducir incertidumbre sobre si una página web es auténtica o un fraude. La tipificación de la *suplantación de sitios web* en Costa Rica (art. 233 CP) fue justificada precisamente para resguardar la confianza de los usuarios en que el sitio al que acceden es el legítimo y no una copia engañosa (Bonilla, 2019). Igual propósito tiene la criminalización de la ingeniería social maliciosa, es decir, engañar a personas para obtener datos o accesos (lo que en ciertos casos se persigue como estafa o como acceso ilegítimo según el resultado).

En términos de bien jurídico, el patrimonio y la confianza digital pueden verse por separado o conjuntamente. Algunos autores hablan de la *"seguridad del tráfico jurídico informático"* (Acurio Del Pino, 2005), que abarcaría la protección de la fiabilidad de las transacciones y documentos electrónicos – lo cual incluye tanto un componente patrimonial (que no haya perjuicios económicos por fraude) como un componente de fe pública (que la

comunidad confíe en el sistema electrónico). La doctrina chilena, por ejemplo, ha calificado a los delitos informáticos patrimoniales como pluriofensivos, protegiendo, a la vez, el patrimonio individual y la seguridad colectiva de las redes económicas (Acurio Del Pino, 2005). En esa línea, un fraude masivo tipo *phishing* afecta a cada víctima en su dinero, pero también a la sociedad al sembrar desconfianza en el comercio electrónico; un ataque a un exchange de criptomonedas lesiona los activos de los usuarios y simultáneamente merma la credibilidad de ese mercado.

La intervención penal en protección del patrimonio en entornos digitales está sobradamente justificada no solo por la magnitud de los daños posibles (algunos ataques informáticos han causado pérdidas multimillonarias), sino también por el carácter transnacional y anónimo de estas conductas, que dificulta su persecución mediante herramientas civiles. Además, el involucramiento potencial de personas jurídicas como autores o partícipes (por ejemplo, empresas que mediante empleados realizan espionaje industrial o robo de secretos comerciales a competidores, usando hacking) ha llevado a prever su responsabilidad penal en muchos sistemas jurídicos. Costa Rica, con la Ley 9699/2019, introdujo la responsabilidad penal de las personas jurídicas precisamente contemplando dentro de los delitos imputables a las empresas algunos de carácter informático (como la violación de datos personales por negligencia grave de una compañía, o el fraude informático cometido en beneficio corporativo) (Freire Altamirano et al., 2024). Esto demuestra que el Estado considera al patrimonio digital y la confianza en las transacciones electrónicas bienes jurídicos de tal relevancia que incluso las personas morales deben responder penalmente si contribuyen a su lesión.

En resumen, el patrimonio en el ciberespacio se manifiesta en nuevas formas de bienes (dinero electrónico, datos valiosos, criptomonedas) y nuevas modalidades de ataque, pero sigue siendo un pilar cuya protección penal es indispensable. Junto a él, la confianza en las tecnologías digitales actúa como presupuesto para el ejercicio seguro de derechos y negocios en línea; sin esa confianza, el progreso digital se ve comprometido. La ley penal, a través de tipos que castigan el fraude, la sabotaje, la falsificación y otras estafas informáticas, busca mantener un entorno donde tanto el individuo como la colectividad puedan interactuar digitalmente sin un riesgo desproporcionado de ser engañados o despojados de sus bienes. En última instancia, la protección de este bien jurídico dual (patrimonio-confianza) sostiene la credibilidad de la economía digital y, por ende, el normal funcionamiento del Estado de Derecho en la era de la información.

2.2 El marco normativo costarricense

En Costa Rica, la respuesta penal frente a conductas cometidas por medios tecnológicos combina tipos tradicionales adaptados al entorno digital (por ejemplo, la estafa cometida mediante TIC) con tipos específicamente informáticos (acceso, alteración o sabotaje de datos y sistemas). Este desarrollo ha sido el resultado de reformas sucesivas al Código Penal para cubrir nuevas formas de lesividad asociadas a sistemas y redes. El primer hito es la Ley N.° 8148 (24 de octubre de 2001), que adicionó al Código Penal los artículos 196 bis, 217 bis y 229 bis, introduciendo por primera vez un núcleo tipificado para los llamados “delitos informáticos”.

Una década después, la Ley N.° 9048 (10 de julio de 2012; publicada el 6 de noviembre de 2012) llevó a cabo una reforma integral de la Sección VIII, “Delitos informáticos y conexos”, actualizando y ampliando el catálogo delictivo, ajustando escalas

penales e incorporando cláusulas de neutralidad tecnológica que permiten abarcar conductas cometidas “por cualquier sistema o contenedor”.

El ciclo reformador se complementó con la Ley N.° 9135 (24 de abril de 2013), que reformó, entre otros, los artículos 196 y 196 bis (protección penal de datos personales), 230, 293 y 295, afinando redacciones y coherencia interna. En paralelo, la Ley N.° 9177 (1.º de noviembre de 2013) actualizó el tratamiento de la pornografía infantil (arts. 173 a 174 bis), incluyendo supuestos como la pseudopornografía y la pornografía virtual, para responder a prácticas de producción y circulación de contenidos ilícitos en entornos digitales.

Estas reformas permiten perseguir desde intrusiones y sabotaje de sistemas hasta fraudes, extorsiones y difusión/tenencia de material ilícito mediados por TIC, y dan cobertura a fenómenos contemporáneos como propagación de software malicioso, suplantación de sitios o identidades, exfiltración/espionaje digital y manipulaciones tecnológicas; todo ello, sin atarse a listados cerrados de tecnologías, gracias a la mencionada neutralidad tecnológica.

2.2.1 Suplantación de páginas web

La suplantación de páginas web describe la sustitución fraudulenta de sitios legítimos de Internet con el fin de engañar a las personas usuarias. En la práctica, esta conducta opera como un mecanismo de fraude por imitación de interfaces, dominios o recursos visuales de un servicio auténtico, a menudo combinada con técnicas de ingeniería social, para inducir a la víctima a revelar credenciales, realizar pagos o descargar archivos maliciosos.

El Código Penal costarricense prevé un tipo específico para esta conducta. El artículo 233 sanciona con prisión de uno a tres años a quien, en perjuicio de un tercero, suplante sitios legítimos en la red de Internet. Asimismo, contempla un supuesto agravado con pena de tres a seis años cuando, como consecuencia de la suplantación y mediante engaño

o error, se captura información confidencial de una persona física o jurídica para beneficio propio o de un tercero. Este diseño normativo incorpora una cláusula de neutralidad tecnológica, al no restringir la conducta a medios o formatos específicos, lo que permite su aplicación frente a modalidades contemporáneas de phishing, spoofing de dominios/subdominios y clonación de portales en servicios de nube y redes sociales.

2.2.2 Suplantación de identidad

En la falsificación de identidad, la actividad ocurre cuando una persona se presenta como otra, apropiándose así de sus redes sociales, sitios web, correos electrónicos, entre otros; esto también puede suceder con entidades jurídicas. Consideramos fundamental comprender las repercusiones del término identidad, el cual se define como "conjunto de características distintivas de un individuo o de un grupo que los diferencian de los demás".

Entendido lo anterior, se puede definir la suplantación de identidad como la apropiación ilícita de los datos personales de una persona con la finalidad de obtener un beneficio ulterior según González Rivera

El delito de suplantación de identidad se refiere a lo siguiente:

"Artículo 230.- Suplantación de identidad. Será sancionado con pena de prisión de uno a tres años quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información".

2.2.3 Difusión de información falsa (art. 236 C.P.) y grooming (art. 167 bis C.P.)

La difusión de información falsa fue incorporada al Código Penal mediante la Ley N.° 9048 (2012), que adicionó el artículo 236. Esta norma sanciona con tres a seis años de prisión a quien, por medios electrónicos, informáticos o de telecomunicaciones, propague o difunda noticias o hechos falsos capaces de distorsionar o perjudicar la seguridad y

estabilidad del sistema financiero o de sus usuarios. La regulación responde a riesgos propios del ecosistema digital, donde la amplificación de contenidos falsos, a menudo combinada con ingeniería social, puede producir efectos sistémicos; de ahí su foco en el sector financiero y en los usuarios como bienes jurídicos protegidos (García Chaves, 2022).

En paralelo, el ordenamiento prevé figuras para la protección de personas menores de edad frente a riesgos en línea. El grooming se tipifica en el artículo 167 bis como "seducción o encuentros con persona menor de edad o incapaz por medios electrónicos". Tras su introducción (2013), la Ley N.° 10020 (2021) endureció las penas: pasó de uno a tres a dos a cuatro años para los supuestos de comunicaciones sexuales, y de dos a cuatro a tres a cinco años cuando se procura un encuentro físico (Salas, 2023). De acuerdo con datos públicos divulgados en el marco de campañas interinstitucionales, entre 2017 y setiembre de 2023 el OIJ registró 426 denuncias por grooming (PANI, 2023), lo que evidencia su relevancia criminológica actual.

Como se ve, el artículo 236 aborda la propagación de falsedades dañinas con potencial sistémico, especialmente en el ámbito financiero, mientras que el artículo 167 bis protege a personas menores de edad frente a acercamientos sexuales en línea, reforzado por la Ley N.° 10020. Ambos tipos reflejan el giro del legislador hacia la neutralidad tecnológica y la adaptación del derecho penal a dinámicas de comunicación y contacto mediadas por TIC.

2.2.4 Facilitación de delito informático

El artículo 234 del Código Penal tipifica la facilitación del delito informático y sanciona con prisión de uno a cuatro años a quien provea medios para la comisión de un delito realizado mediante sistemas o redes informáticas o telemáticas, o por medio de contenedores electrónicos, ópticos o magnéticos. La figura cumple una función accesoria: no requiere que la persona ejecute el hecho principal, sino que aporta instrumentos, canales o

soportes que lo hacen posible, por ejemplo, infraestructura tecnológica, credenciales de acceso, herramientas de anonimización o cuentas de recepción/transferencia de fondos.

En la práctica costarricense, un escenario recurrente es el de las llamadas "mulas" o prestanombres bancarios: personas que ceden sus cuentas para recibir y mover dineros de origen ilícito, a menudo derivados de estafas en línea, phishing o fraudes con ingeniería social, a cambio de una comisión. Esa conducta, al habilitar el circuito financiero del fraude, se adecua al tipo de facilitación previsto por el legislador.

2.2.5 Espionaje informático

En sentido general, el espionaje remite a obtener de forma encubierta información secreta de personas, empresas o Estados; la voz deriva de espiar —acechar u observar disimuladamente, o procurar informaciones reservadas— (Real Academia Española [RAE], s. f.). Trasladado al entorno digital, el espionaje informático comprende la apropiación o injerencia no autorizada en información con valor económico mediante tecnologías de la información (p. ej., intrusiones, copias o desvíos de datos en sistemas informáticos).

El Código Penal costarricense tipifica esta conducta en el artículo 231, que sanciona con tres a seis años de prisión a quien, sin autorización del titular o responsable y valiéndose de manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle información con valor para el tráfico económico de la industria y el comercio. Este precepto fue adicionado por la Ley N.° 9048 (2012), en el marco de la reforma de la Sección VIII: Delitos informáticos y conexos, que actualizó el régimen penal para cubrir técnicas contemporáneas de acceso y exfiltración de datos.

2.2.6 El sabotaje informático (art. 229 ter C.P.)

En el ordenamiento costarricense, el sabotaje informático abarca las acciones dirigidas a dañar, obstaculizar o interrumpir datos, programas o el funcionamiento de un

sistema de tratamiento de información (hardware o software), siempre que exista un perjuicio verificable para la víctima y la conducta se ejecute en provecho propio o de un tercero. A diferencia de otros tipos donde la mera injerencia configura el ilícito, aquí el núcleo de antijuridicidad reside en el resultado lesivo sobre la información o el sistema.

El artículo 229 ter sanciona con prisión de tres a seis años a quien destruya, altere, entorpezca o inutilice información contenida en una base de datos, o impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema informático, sus partes o componentes físicos o lógicos. La pena se agrava a cuatro a ocho años cuando concurre alguna de estas circunstancias:

a) La conducta ocasiona peligro colectivo o daño social.

b) La realiza un empleado con funciones de administración o soporte —o con acceso funcional— a sistemas, redes o contenedores electrónicos, ópticos o magnéticos.

c) El sistema es de carácter público o la información reposa en bases de datos públicas.

d) Se emplean medios tecnológicos para impedir el acceso lícito de personas autorizadas a sistemas o redes de telecomunicaciones.

Este tipo penal fue incorporado por la Ley N.° 9048 (2012), dentro de la reforma integral de la Sección VIII, “Delitos informáticos y conexos”, con el objetivo de cubrir escenarios contemporáneos de interferencia maliciosa (p. ej., denegación de servicio, borrado o cifrado destructivo, manipulación de control industrial), bajo un diseño de neutralidad tecnológica.

2.2.7 Violación de correspondencia o comunicaciones (art. 196 C.P.)

El artículo 196 del Código Penal tutela la intimidad y la privacidad frente a injerencias no autorizadas en documentos y comunicaciones. Castiga con prisión de uno a

tres años a quien, sin autorización del titular y con peligro o daño para su intimidad o privacidad, se apodere, acceda, modifique, altere, suprima, intervenga, intercepte, abra, entregue, venda, remita o desvíe de su destino comunicaciones o documentación dirigida a otra persona. La misma pena rige para quien use o difunda el contenido de comunicaciones o documentos privados sin interés público, así como para quien promueva, incite, instigue, prometa o pague un beneficio para que un tercero ejecute dichas conductas.

El precepto contempla un supuesto agravado (pena de dos a cuatro años) cuando la conducta del primer párrafo la ejecutan:

a) Encargados de recolección, entrega o salvaguarda de documentos o comunicaciones; o

b) Administradores/soporte de sistemas o redes informáticas o telemáticas, o quienes, por sus funciones, tienen acceso a esos sistemas o a contenedores electrónicos, ópticos o magnéticos.

Estas agravantes fueron afinadas por la Ley N.° 9135 (24 de abril de 2013), que actualizó el tipo a la realidad tecnológica actual.

En términos de política criminal, el artículo 196 opera como cláusula de neutralidad tecnológica: protege comunicaciones y documentos con independencia del soporte (físico o digital) y cierra espacios de impunidad en entornos informáticos y telemáticos, manteniendo el equilibrio con la libertad de información mediante la exigencia de ausencia de interés público para sancionar la divulgación de contenidos privados.

2.2.8 Estafa informática

En el fraude informático se clasifican diversas acciones ilegales; estas incluyen la manipulación, acceso, procesamiento, programación, entre otras, de los sistemas informáticos, sin el consentimiento de su propietario, con la intención ilícita de obtener

ganancias, ya sea en beneficio propio o en detrimento de un tercero, siendo estos los componentes característicos de este delito. “Los componentes característicos que conforman el delito de fraude informático son: la manipulación informática y artificios similares, transferencia "patrimonio no autorizado por el titular, del mismo, ánimo de lucro, y daño a terceros. La estafa cibernética ha sido otro de los delitos digitales con mayor incidencia delictiva en nuestro país, Este tipo de estafa en nuestro país fue clasificada inicialmente como fraude cibernético. En el año 2013, con la reforma realizada por la ley N.º 9048, se amplió la tipificación penal, quedando como hoy lo conocemos en el artículo 217bis:" según Adalid Medrano.

El delito de estafa informática se refiere a lo siguiente:

"Artículo 217 bis. - Estafa informática se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.

La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos." (Reforma de

la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal Ley N° 9048).

2.2.9 Daño Informático (arts. 229 bis, 229 ter y 232 C.P.)

Daño informático (art. 229 bis). En el ordenamiento costarricense, el daño informático protege la integridad de la información alojada en sistemas o redes. Comete el delito quien, sin autorización del titular o excediendo la concedida, y en perjuicio de un tercero, suprime, modifica o destruye datos almacenados en un sistema o red informática/telemática, o en contenedores electrónicos, ópticos o magnéticos. La agravación procede cuando la información afectada resulta insustituible o irrecuperable, caso en el cual la pena se eleva. Relación con el sabotaje informático (art. 229 ter). Aunque en la práctica a veces se solapan, ambos tipos protegen bienes jurídicos distintos:

El 229 bis se centra en el dato (integridad, existencia o disponibilidad de la información). El 229 ter se orienta al sistema de tratamiento de información en sí (funcionamiento de *hardware* o *software*) y castiga impedir, alterar, obstaculizar o modificar su operación, además de destruir/entorpecer información. De allí que las agravantes también difieran: en el 229 bis el énfasis está en la irrecuperabilidad del dato; en el 229 ter se contemplan, entre otras, la condición del autor con acceso funcional, el carácter público del sistema o base de datos y la generación de peligro colectivo.En la aplicación práctica, la distinción ayuda a resolver concursos aparentes, privilegiando el tipo cuyo bien jurídico resulte primariamente lesionado.

Instalación o propagación de programas informáticos maliciosos (art. 232). Aparte del daño a datos o sistemas, el Código Penal tipifica la introducción y difusión de malware. Incurre en el delito quien, sin autorización, instale programas maliciosos por cualquier medio en un sistema/red o en contenedores electrónicos; la misma pena alcanza a quien: (i) induce

a error a otra persona para lograr dicha instalación; (ii) inserta aplicaciones dañinas en sitios legítimos para convertirlos en vectores de propagación ("sitios atacantes"); (iii) invita a descargar archivos o visitar páginas que facilitan la instalación; (iv) distribuye programas diseñados para crear malware; o (v) ofrece/contrata servicios como denegación de servicio, spam masivo o propagación de malware (Costa Rica, s. f., art. 232). La norma agrava la pena cuando, entre otros supuestos, el programa malicioso afecta entidades financieras o estatales, servicios públicos, sistemas de salud (con riesgo a la vida o la salud), permite control remoto (botnets), busca beneficio patrimonial o se replica autónomamente (art. 232).

En términos de política criminal, el art. 232 recoge tanto la acción directa (instalar) como las formas mediatas de diseminación (ingeniería social, comprometer sitios legítimos), lo que refuerza la neutralidad tecnológica y cierra rutas típicas de infección contemporánea. Los arts. 229 bis y 229 ter completan el cuadro sancionando, respectivamente, el daño al dato y la afectación al sistema. Estas figuras fueron introducidas/actualizadas por la Ley N.° 9048 (2012), que reformó integralmente la Sección VIII "Delitos informáticos y conexos".

2.3 Delitos informáticos que incluye el Código Penal costarricense

2.3.1 Tenencia de material pornográfico (art. 173 bis C.P.)

En continuidad con los tipos orientados a la protección penal de la niñez en entornos digitales, el artículo 173 bis del Código Penal tipifica la tenencia de material pornográfico infantil. El texto vigente sanciona con pena de prisión de dos a cinco años a quien posea material pornográfico en el que aparezca una persona menor de edad o incapaz, ya sea utilizando su imagen y/o su voz; prevé igual pena para supuestos funcionalmente asimilables que comportan almacenamiento digital. Esta norma, introducida originalmente por la Ley N.° 8590 (2007) y posteriormente reformada —incluida la Ley N.° 9177 (2013)—, se

inscribe en una política de actualización de la respuesta penal frente a las dinámicas tecnológicas de circulación y acopio de contenidos ilícitos.

La razón de política criminal que sostiene este tipo penal es clara: la disponibilidad y el intercambio de pornografía infantil se han intensificado con Internet y los medios digitales, lo que exige abarcar no solo la producción o difusión, sino también la mera posesión como eslabón que alimenta la demanda y perpetúa el daño a las víctimas. La doctrina y los análisis institucionales recientes en Costa Rica coinciden en ese diagnóstico y en la necesidad de reforzar prevención, persecución y prueba digital.

2.3.2 Difusión de pornografía (art. 174 C.P.)

En la línea de protección penal frente a daños sexuales contra personas menores de edad o incapaces, el artículo 174 del Código Penal tipifica las conductas de entrega, comercio, difusión, distribución o exhibición de material pornográfico dirigidas a ese grupo protegido. La previsión alcanza cualquier modalidad de comunicación o puesta a disposición, sin importar el medio utilizado (incluidas plataformas digitales, redes y servicios telemáticos).

Asimismo, el precepto agrava la respuesta penal cuando el contenido difundido incluye la imagen, voz o presencia de personas menores de edad, o cuando la tenencia del material tiene como finalidad su divulgación, distribución o comercialización. Con ello, el tipo no solo reprime la circulación inmediata del material, sino también eslabones previos que alimentan su disponibilidad en ecosistemas digitales.

Desde una perspectiva de política criminal, el alcance “por cualquier medio y cualquier título” asegura la neutralidad tecnológica del tipo penal y permite su aplicación a esquemas contemporáneos de compartición en línea, *streaming*, mensajería cifrada o

almacenamiento en la nube, donde la prueba digital y la trazabilidad de la distribución resultan determinantes.

2.3.3 Pornografía virtual y pseudo pornografía (art. 174 bis C.P.)

Bajo la lógica de neutralidad tecnológica del derecho penal, la pornografía virtual describe contenidos sexuales generados sin utilizar personas menores de edad reales: por ejemplo, adultos caracterizados para aparentar minoría de edad o representaciones gráficas/animadas (ilustraciones, animación, CGI, *deepfakes)* que simulan a una persona menor en actividades sexuales. El debate jurídico ha girado en torno a su penalización, justamente porque el daño no proviene del uso de un cuerpo infantil real sino de creaciones que aparentan tal condición.

Por su parte, la pseudopornografía remite a montajes o composiciones en los que se introduce la imagen (total o parcial) de una persona menor de edad real, por ejemplo, su rostro, en escenas sexuales en las que nunca participó. Aquí, la afectación al bien jurídico es directa: se lesionan la dignidad, el derecho a la imagen y el honor de una persona identificable, aun cuando el acto representado sea ficticio.

El artículo 174 bis del Código Penal, incorporado por la Ley N.° 9177 (2013), tipifica estas conductas y sanciona con pena de prisión de seis meses a dos años a quien posea, produzca, venda, distribuya, exhiba o facilite, por cualquier medio, material pornográfico en el que, sin haber intervenido personas menores de edad reales:
a) Se emplee a una persona adulta que simule ser menor de edad realizando actividades sexuales; o
b) Se emplee una imagen, caricatura, dibujo o representación de cualquier clase que aparente o simule a una persona menor de edad realizando actividades sexuales.

Este diseño normativo cubre tanto la simulación por caracterización como las representaciones sintéticas o manipuladas, y permite aplicar el tipo a prácticas contemporáneas de edición digital y generación algorítmica de imágenes (p. ej., *deepfakes*), así como a su almacenamiento y circulación en línea.

2.3.4 Violación de datos personales (art. 196 bis C.P.)

La tutela penal de los datos personales en Costa Rica se consolidó a partir de dos hitos normativos complementarios. En el plano administrativo-constitucional, la Ley N.° 8968, Ley de protección de la persona frente al tratamiento de sus datos personales (2011), fijó principios, derechos y deberes para el tratamiento de información personal. En el plano penal, la Ley N.° 9048 (2012) reformó el Título VII del Código Penal e introdujo el artículo 196 bis "Violación de datos personales", incorporando por primera vez un tipo penal específico para conductas de apoderamiento, acceso, modificación, transmisión, publicación, tratamiento no autorizado u otras formas de injerencia sobre datos o imágenes de personas, sin autorización del titular y con peligro o daño para la intimidad o la privacidad.

De manera sintética, el artículo 196 bis sanciona con pena de prisión de tres a seis años a quien, en beneficio propio o de un tercero, y sin autorización del titular, realice acciones como apoderarse, acceder, copiar, modificar, transmitir, publicar, difundir, recopilar, interceptar, retener, vender, comprar, desviar del fin para el que fueron recolectados o dar tratamiento no autorizado a datos o imágenes de personas físicas o jurídicas, cuando estén almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos.

El precepto prevé agravantes que elevan la pena a cuatro a ocho años cuando:

a) Las conductas las realiza personal técnico o de soporte, administradores o quienes, por sus funciones, tienen acceso al sistema, la red o a los contenedores;

b) Los datos son de carácter público o están contenidos en bases de datos públicas;

c) La información vulnerada corresponde a una persona menor de edad o incapaz;

d) Se afectan datos especialmente sensibles, como los que revelan ideología, religión, creencias, salud, origen racial, preferencia u orientación sexual de una persona.

Este diseño normativo articula el régimen penal con el marco de protección de datos: por un lado, desincentiva el acceso y tratamiento ilícito de información personal en entornos digitales; por otro, refuerza los incentivos de cumplimiento para quienes operan sistemas y bases de datos (públicos o privados), atendiendo al principio de seguridad y al deber de confidencialidad que emanan de la Ley N.° 8968.

2.3.5 Lo relativo a la pornografía

El primer ilícito a considerar, por su centralidad en la protección penal de la niñez frente a daños en entornos digitales, es el previsto en el artículo 173 del Código Penal bajo la rúbrica "Fabricación, producción o reproducción de pornografía". Esa disposición sanciona con pena de prisión a quien, "por cualquier medio", fabrique, produzca o reproduzca material pornográfico infantil, y también reprime las conductas de transporte o ingreso al país de dicho material; su texto vigente es producto de la reforma introducida por la Ley N.° 9177 (1.º de noviembre de 2013), que actualizó escalas y supuestos típicos para adecuarlos a dinámicas tecnológicas actuales.

Para la correcta interpretación del tipo, el propio Código define material pornográfico infantil como toda representación escrita, visual o auditiva —obtenida por cualquier medio— de una persona menor de edad, su imagen o su voz (incluso si han sido alteradas), dedicada a actividades sexuales explícitas reales o simuladas, o la representación de las partes genitales de una persona menor de edad con fines sexuales. Esta precisión

normativa delimita el objeto material del delito y orienta la valoración probatoria en contextos digitales.

Además, existe un estándar internacional convergente: el Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía define la pornografía infantil como toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas (reales o simuladas) o de sus genitales con fines primordialmente sexuales. Costa Rica aprobó este instrumento por la Ley N.° 8172, por lo que su contenido integra el parámetro interpretativo aplicable a la materia.

Como se ve, la coordinación entre el artículo 173 del Código Penal (según reforma de la Ley N.° 9177) y el Protocolo Facultativo ofrece un marco claro y suficiente para abordar las conductas de fabricación, producción o reproducción de pornografía infantil también cuando se ejecutan mediante medios informáticos o telemáticos, cerrando el paso a intentos de eludir responsabilidad por la sola mediación tecnológica.

2.3.6 Extorsión (art. 214 C.P.)

El artículo 214 del Código Penal tipifica la extorsión como la conducta de quien, con intimidación o amenazas graves y con fin de lucro, obliga a otra persona a adoptar una disposición patrimonial perjudicial para sí o para un tercero. El precepto prevé una pena base de cuatro a ocho años de prisión. Asimismo, el legislador incorporó un supuesto agravado cuando la conducta se ejecuta valiéndose de manipulación informática, telemática, electrónica o tecnológica, caso en el cual la sanción se eleva a cinco a diez años de prisión. Esta cláusula de neutralidad tecnológica permite abarcar formas contemporáneas de extorsión mediadas por TIC —como esquemas de “sextorsión”, amenazas mediante

mensajería digital o exigencias patrimoniales tras la intrusión y cifrado de sistemas—, sin necesidad de enumerar de manera taxativa los medios técnicos empleados.

2.3.7 Espionaje (art. 295 C.P.)

El bien jurídico protegido es el secreto de Estado —formalmente decretado— vinculado a la seguridad interna o externa, la defensa de la soberanía y las relaciones exteriores de Costa Rica. El artículo 295 del Código Penal sanciona con prisión de uno a seis años a quien procure u obtenga indebidamente tales secretos de Estado.

El tipo incorpora, además, un supuesto agravado de carácter tecnológico: la pena se eleva a dos a ocho años cuando la conducta se ejecuta mediante manipulación informática, programas informáticos maliciosos o mediante el uso de tecnologías de la información y la comunicación. Esta fórmula de neutralidad tecnológica permite abarcar intrusiones, exfiltración o interceptación digital de información clasificada, sin necesidad de enumerar medios específicos.

Históricamente, el precepto fue actualizado en el marco de la reforma integral de los delitos informáticos y conexos introducida por la Ley N.° 9048 (10 de julio de 2012) y ajustes posteriores (v.gr., Ley N.° 9135, 24 de abril de 2013), que reordenaron y modernizaron la sección correspondiente del Código Penal.

2.3.8 Narcotráfico y crimen organizado

establece una agravante específica: la pena se duplica cuando cualquiera de los delitos cometidos “por medio de un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos” afecta la lucha contra el narcotráfico o el crimen organizado.

Esta previsión responde a la necesidad de proteger la integridad de las políticas públicas contra estructuras criminales que se apoyan en tecnologías de la información para

facilitar o encubrir sus operaciones (p. ej., comunicaciones cifradas, plataformas de intercambio, almacenamiento digital), de allí la neutralidad tecnológica del enunciado (“por cualquier sistema o contenedor”).

El precepto fue adicionado por la Ley N.° 9048 (10 de julio de 2012), que reformó integralmente la Sección VIII del Código Penal para actualizar el tratamiento penal de la ciberdelincuencia y sus vínculos con la criminalidad organizada.

2.3.9 Robo de datos personales por medio de código QR

En Costa Rica, el apoderamiento o uso indebido de información personal constituye el delito de violación de datos personales, tipificado en el artículo 196 bis del Código Penal. La conducta punible comprende actos como acceder, apropiarse, modificar, transmitir o divulgar datos sin autorización del titular, con sanciones que oscilan entre uno y tres años de prisión. En este contexto, han proliferado fraudes vinculados al uso de códigos QR en espacios públicos.

La modalidad replica, en el entorno digital, el conocido “skimming”: personas delincuentes colocan una calcomanía con un QR falso sobre el código legítimo. Al escanearlo, la víctima es redirigida a un sitio web que instala de forma automática un programa malicioso (spyware) en el dispositivo. Al creer que se ingresa a una página confiable —por ejemplo, para consultar un menú o acceder a una promoción—, el malware se ejecuta y puede capturar credenciales sensibles, como contraseñas de correo electrónico, claves de banca en línea y documentos almacenados en el teléfono o la tableta (Siles, 2023).

2.3.10 Bloque constitucional y leyes conexas

Como hilo conductor entre la tipificación de los ciberdelitos y el régimen de responsabilidad penal de las personas jurídicas analizado en este trabajo, este apartado parte del bloque constitucional: la garantía de intimidad y secreto de las comunicaciones del

artículo 24 de la Constitución, aplicable a entornos digitales, sirve tanto de pilar para definir los límites de acceso, interceptación y divulgación de datos como de parámetro de control de las medidas investigativas tecnológicas. En el plano legal, las piezas conexas de la vida digital (Ley N.° 8454 sobre documentos y firma digital y Ley N.° 8968 de protección de datos personales) complementan ese sustento constitucional y orientan la lectura de los tipos penales y de las exigencias probatorias en sede informática.

A su vez, la dimensión convencional impone un estándar específico: el Convenio de Budapest y, en particular, su artículo 12, requieren habilitar la imputación a entes colectivos cuando el delito informático se comete en su beneficio o media un defecto de organización, lo que conecta este bloque con los deberes de prevención y cumplimiento corporativo que la tesis propone desarrollar para cerrar la actual brecha costarricense en materia de responsabilidad penal de personas jurídicas por incidentes de ciberseguridad.

Si bien la Constitución Política de Costa Rica no menciona de manera explícita la responsabilidad penal de las personas jurídicas, el punto de partida del marco costarricense es el bloque constitucional. El artículo 24 de la Constitución Política garantiza la intimidad y el secreto de las comunicaciones incluidas las escritas, orales y “de cualquier otro tipo”, y solo admite excepciones bajo ley especial y control judicial. Esta cláusula opera como pilar del tratamiento penal de conductas de acceso, interceptación y divulgación en entornos digitales, y como límite a las medidas de investigación tecnológica (Constitución Política de Costa Rica, art. 24). En esa línea, la jurisprudencia y la doctrina han reconocido que la inviolabilidad de comunicaciones del art. 24 aplica plenamente a actividades en línea, de modo que tanto la interceptación de mensajes electrónicos como el secuestro de dispositivos deben someterse a legalidad estricta, necesidad y proporcionalidad (Constitución Política de Costa Rica, art. 24).

Como se verá más adelante, en el plano convencional, Costa Rica accedió al Convenio sobre Ciberdelincuencia (Budapest) el 22 de septiembre de 2017; la entrada en vigor para el país rige desde el 1 de enero de 2018. Este instrumento sirve como parámetro hermenéutico para armonizar tipos penales y medidas procesales con estándares comparados, en especial respecto de acceso ilícito (art. 2), interceptación ilícita (art. 3), interferencia en datos y sistemas (arts. 4–5), abuso de dispositivos (art. 6), fraude/falsificación informáticos (arts. 7–8) y responsabilidad de las personas jurídicas (art. 12). (Council of Europe, 2017)

A nivel legal, el ordenamiento cuenta con dos leyes claves para la vida digital: (i) la Ley N.º 8454, de Certificados, Firmas Digitales y Documentos Electrónicos, que equipara el valor probatorio de la firma digital a la manuscrita (art. 9) y estructura el ecosistema de documentos electrónicos en el sector público y privado, con su respectivo reglamento; y (ii) la Ley N.º 8968, de Protección de la Persona frente al Tratamiento de sus Datos Personales, que consagra principios, derechos y un régimen sancionatorio administrativo a cargo de PRODHAB (Ley N.º 8454; Reglamento de la Ley N.º 8454; Ley N.º 8968).

Además, la cuestión que se aborda en esta tesis la incorpora la Ley N° 9699 del 2019, que establece que las personas jurídicas pueden ser consideradas penalmente responsables por delitos cometidos en su nombre, cuenta y beneficio, ya sea por sus representantes o por aquellos que actúen con un grave incumplimiento de sus deberes de supervisión:

> Artículo 4- Atribución de responsabilidad penal de las personas jurídicas Las personas jurídicas descritas tienen el deber legal de supervisión, vigilancia y control de su actividad, para evitar la comisión de los delitos descritos en el artículo 1 de esta ley.
>
> Serán penalmente responsables las personas jurídicas:

a) De los delitos cometidos en nombre o por cuenta de estas y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que, actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades generales de organización y control dentro de esta.

b) De los delitos cometidos, en el ejercicio de actividades de las personas jurídicas y por cuenta y en beneficio directo o indirecto de estas, por quien, estando sometido a la autoridad de las personas físicas mencionadas en el inciso anterior, han podido realizar los hechos por haberse incumplido por parte de aquellos indicados en el inciso anterior, los deberes de supervisión, vigilancia y control de su actividad, atendidas las concretas circunstancias del caso.

c) De los delitos cometidos en nombre o por cuenta de estas, y en su beneficio directo o indirecto, por medio de intermediarios ajenos a la persona jurídica, pero contratados o instados por sus representantes legales o por aquellos que, actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para tomar decisiones en nombre de la persona jurídica, por haberse incumplido por las personas indicadas en el inciso a) sus deberes de supervisión, vigilancia y control de su actividad, atendidas las concretas circunstancias del caso.

Las personas jurídicas no serán responsables penalmente en los casos en que las personas físicas indicadas en los incisos b) y c) anteriores hubieran cometido el delito en ventaja propia o a favor de un tercero, o si la representación invocada por el agente fuera falsa, o si lo hubieren cometido eludiendo fraudulentamente el modelo de organización, prevención de delitos, gestión y control, sin perjuicio de la responsabilidad civil o administrativa en que pudieran incurrir.

La responsabilidad de las personas jurídicas no excluye la responsabilidad individual de la persona física, sean estos directores o empleados o de cualquier otra persona que participe de la comisión de las conductas citadas en este artículo y que se determinará por lo dispuesto en otras leyes

La responsabilidad penal de las personas jurídicas se extiende, pues, a la capacidad de una empresa de enfrentar sanciones por los delitos cometidos por sus representantes, administradores o empleados. Estos actos deben estar en nombre de la compañía, buscando su beneficio directo o indirecto, e implicar el incumplimiento de los deberes de supervisión. Las sanciones, no incluyen la prisión; solo multas, prohibiciones de contratar con el Estado, así como pérdida de beneficios y, hasta en casos muy serios, la disolución de la empresa.

Cuando las personas físicas señaladas en los incisos b) y c) actúan buscando su propio beneficio —o el de un tercero—, cuando se amparan en una representación falsa, o cuando cometen el hecho eludiendo de forma fraudulenta el modelo de organización, prevención, gestión y control, la persona jurídica no asume responsabilidad penal. Eso sí: podrían quedar vigentes las responsabilidades civil o administrativa que correspondan.

Que exista responsabilidad de la persona jurídica no borra la responsabilidad individual. Directores, empleados o cualquier otra persona que participe en las conductas descritas también responden personalmente, según lo establezcan las demás leyes aplicables.

En síntesis, la responsabilidad penal de la empresa surge cuando sus representantes, administradores o trabajadores cometen delitos en su nombre, buscando un beneficio para ella —directo o indirecto— y fallando en los deberes de supervisión. Las sanciones para la persona jurídica no incluyen cárcel: se traducen en multas, inhabilitaciones para contratar con el Estado, pérdida de beneficios y, en supuestos muy graves, hasta la disolución de la compañía.

2.4 Convenio de Europa sobre Ciberdelincuencia (Convenio de Budapest)

Aprobación y adhesión en el año 2001 y rige a partir de los veintiséis días del mes de mayo del año dos mil diecisiete. Su Artículo 12. "Responsabilidad de las personas jurídicas" indica que:

> 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos de conformidad con el presente Convenio, cuando sean cometidos por cuenta de las mismas, por cualquier persona física, tanto en calidad individual como en su condición de miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en la misma, en virtud de:
>
> a. un poder de representación de la persona jurídica;
>
> b. una autorización para tomar decisiones en nombre de la persona jurídica;
>
> c. una autorización para ejercer funciones de control en la persona jurídica
>
> 2. Además de los casos ya previstos en el apartado 1 del presente artículo, cada Parte adoptará las medidas necesarias para asegurar que pueda exigirse responsabilidad a una persona jurídica cuando la falta de vigilancia o de control por parte de una persona física mencionada en el apartado 1 haya hecho posible la comisión de un delito previsto de conformidad con el presente convenio en beneficio de dicha persona jurídica por una persona física que actúe bajo su autoridad.
>
> 3. Con sujeción a los principios jurídicos de cada Parte, la responsabilidad de la persona jurídica podrá ser penal, civil o administrativa.
>
> 4. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito.

Costa Rica se enfrentó a su brecha legal sobre la responsabilidad penal de las empresas, también la de ciberseguridad, con la Ley N. 9699 de 2019, esta ley introdujo esa responsabilidad, y también alineo la ley nacional con los preceptos del Convenio de Budapest, principalmente el Artículo 12 el cual pide responsabilidad penal para empresas por crímenes definidos en el convenio.

Artículo 13. Sanciones y medidas

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos en los artículos 2 al 11 puedan dar lugar a la aplicación de sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.

2. Cada Parte garantizará la imposición de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas las sanciones pecuniarias, a las personas jurídicas consideradas responsables de conformidad con el artículo 12.

Así, en Costa Rica, el Convenio de Budapest ha sido el catalizador para ajustar la legislación nacional. Esto ocurrió con el artículo 106 del Código Penal que habla de las responsabilidades de las entidades legales.

Solidaridad de los partícipes.

Artículo 106.-Es solidaria la acción de los partícipes de un hecho punible, en cuanto a la reparación civil.

Están igualmente obligados solidariamente con los autores del hecho punible, al pago de los daños y perjuicios:

1) Las personas naturales o jurídicas dueñas de empresas de transporte terrestre, marítimo o aéreo de personas o de cosas;

2) Las personas jurídicas cuyos gerentes, administradores o personeros legales, resulten responsables de los hechos punibles;

3) Las personas naturales o jurídicas dueñas de establecimientos de cualquier naturaleza, en que se cometiere un hecho punible por parte de sus administradores, dependientes y demás trabajadores a su servicio;

4) Los que por título lucrativo participaren de los efectos del hecho punible, en el monto en que se hubieren beneficiado; y

5) Los que señalen leyes especiales.

El Estado, las Instituciones Públicas, autónomas o semi-autónomas y las municipalidades, responderán subsidiariamente del pago de los daños y perjuicios derivados de los hechos punibles cometidos por sus funcionarios con motivo del desempeño de sus cargos.

2.5 Código Penal: catálogo vigente de tipos informáticos y afines

2.5.1 Acceso e interceptación ilícita / violación de comunicaciones

a) Bien jurídico y ubicación sistemática

Estas figuras protegen, en núcleo, la confidencialidad de la comunicación y de los datos asociados (dimensión “C” de la tríada CIA que se explica en el Capítulo 2). En Costa Rica, el art. 196 tipifica la violación de correspondencia o comunicaciones, contemplando apoderamiento, acceso, modificación, supresión, intercepción o desvío de comunicaciones sin autorización y con peligro o daño para la intimidad de la víctima.

Las reformas informáticas también introdujeron tipos específicos de daño e interferencia que, si bien se enfocan en integridad/disponibilidad, dialogan con el acceso no autorizado cuando el ingreso al sistema es presupuesto del daño (arts. 229 bis y 229 ter). (Código Penal de Costa Rica, arts. 196, 229 bis y 229 ter).

b) Elementos objetivos y subjetivos

Conducta: acceder, apoderarse, interceptar o desviar comunicaciones dirigidas a otra persona; o bien suprimir/alterar información o el funcionamiento del sistema (cuando se conecta con 229 bis/ter).

Objeto: "documentos o comunicaciones" y sus equivalentes electrónicos; sistemas/redes cuando el acceso es medio para la interceptación o el daño.

Ilicitud: sin autorización del titular o excediendo la autorización concedida — criterio reiterado en los tipos informáticos costarricenses.

Resultado: en 196, "peligro o daño" a la intimidad; en 229 bis/ter, daño o afectación funcional de datos/sistemas.

Dolo: conocimiento de la ajenidad y ausencia/exceso de autorización; eventual dolo de aprovechamiento cuando se vincula con otras conductas (p. ej., fraude). (Código Penal de Costa Rica, arts. 196, 229 bis, 229 ter).

c) Límites constitucionales y probatorios

Toda obtención de evidencia por interceptación o acceso forzoso exige habilitación legal y control judicial en clave de necesidad y proporcionalidad, en armonía con el art. 24 constitucional y con la doctrina sobre inviolabilidad de comunicaciones en entornos digitales (Constitución Política de Costa Rica, art. 24).

d) Proporcionalidad y concursos

La escala de penas de 196 se agrava en supuestos calificados; 229 bis/ter escalan cuando la información es irrecuperable, hay peligro colectivo o se inutiliza un sistema crítico. Es frecuente el concurso con delitos patrimoniales (p. ej., fraude informático), o con facilitación del delito informático del art. 234 cuando un tercero provee medios tecnológicos. (Código Penal de Costa Rica, arts. 229 bis, 229 ter, 234).

e) Adecuación a Budapest (micro-mapeo)

Art. 2 (acceso ilícito): Costa Rica cubre parcialmente el acceso no autorizado a sistemas cuando se integra con 229 bis/ter (daño/sabotaje) y con 196 si el acceso tiene por fin interceptar/apoderarse de comunicaciones. Falta un tipo autónomo y general de "acceso ilícito" desprovisto de exigencias adicionales de daño o peligro a la intimidad. (Budapest ETS 185; Código Penal de Costa Rica, arts. 196, 229 bis/ter).

Art. 3 (interceptación ilícita): el art. 196 resulta alineado en lo esencial al sancionar la interceptación sin autorización, con matices sobre el elemento "peligro/daño" a la intimidad. (Código Penal de Costa Rica, art. 196; Budapest ETS 185). En el caso de Costa Rica, será necesario en futuras investigaciones además documentar casos y peritajes donde el "peligro o daño" del 196 genere umbrales probatorios más altos que los exigidos por Budapest para la simple interceptación ilícita (art. 3).

A continuación se presenta una matriz comparativa inicial entre Budapest y el marco normativo costarricense que será ampliada con análisis sobre observaciones de cumplimiento o no en materia de personas jurídicas en el capítulo 4:

Tabla 1 Matriz inicial de adecuación a Budapest

Estándar Budapest	***Norma CR (art./ley)***
Art. 2 Acceso ilícito	CP arts. 196 (cuando el acceso es medio), 229 bis/ter (cuando hay daño/sabotaje)
Art. 3 Interceptación ilícita	CP art. 196
Arts. 4–5 Interferencia en datos y sistemas	CP arts. 229 bis (daño a datos), 229 ter (sabotaje a sistemas)
Art. 6 Abuso de dispositivos	(Remisiones parciales: 234 facilitación; figuras de suplantación 233)

Nota: elaboración propia

2.5.2 Fraude/estafa informáticos y falsedad informática

a) Bien jurídico y ubicación sistemática

El eje aquí es doble: patrimonio (protección frente a desplazamientos patrimoniales provocados por artificios informáticos) y fe pública/tráfico jurídico electrónico (confianza en la autenticidad e integridad de datos y documentos digitales). En Costa Rica, el tratamiento típico combina:

- figuras tradicionales de estafa y falsedades documentales,
- con tipos o agravantes vinculados al uso de medios informáticos/electrónicos (según la reforma que tengas recogida en la tesis).

Esta "doble vía" es útil, pero genera riesgos de solapamiento y lagunas cuando la maniobra no encaja bien en el molde clásico de "engaño a persona" (p. ej., manipulación de datos o interfaz que automatiza la transferencia sin contacto humano directo).

b) Elementos objetivos y subjetivos (lectura funcional)

- Fraude/estafa informáticos

- Conducta: manipular un sistema, dato o proceso electrónico para provocar una disposición patrimonial en perjuicio de otro (pago, transferencia, cargo, emisión de valor, etc.).
- Medio: artificio informático (script, inyección, alteración de parámetros, uso no autorizado de credenciales, ingeniería social apoyada por automatismos).
- Resultado: perjuicio económico; el desplazamiento puede ser mediado por el sistema sin víctima humana "engañada" en sentido clásico.
- Dolo: intención de obtener un beneficio ilícito (propio o de tercero).

2.5.3 Falsedad informática

Conducta: crear, alterar o suprimir datos o documentos electrónicos de modo idóneo para producir efectos jurídicos o patrimoniales; o usar tales datos/documentos con conocimiento de su falsedad.

Objeto: datos, firmas, documentos electrónicos y registros que gocen de valor probatorio según la legislación de firma/documento digital.

Finalidad/aptitud: que la alteración sea idónea para engañar en el tráfico jurídico (no se exige siempre daño consumado).

c) Problemas recurrentes de aplicación

Engaño vs. automatismo: cuando el "engaño" recae sobre el sistema y no sobre una persona, el tipo clásico de estafa puede quedar corto; por eso se requieren tipos que reconozcan la manipulación informática como medio idóneo autónomo.

Prueba de la manipulación: exige forensia digital, cadena de custodia y pericia sobre logs, metadatos y hash para demostrar autoría y trazabilidad.

Concursos: es frecuente el concurso con acceso ilícito/interceptación (para obtener credenciales) y con abuso de dispositivos (tenencia/producción de herramientas).

Proporcionalidad: las escalas penales deben graduarse por monto, número de afectados, sistemas críticos y habitualidad; y contemplar agravantes cuando hay afectación masiva (p. ej., phishing a gran escala).

2.5.4 Daño, alteración e interferencia en datos y sistemas (sabotaje informático)

a) Bien jurídico y ubicación sistemática

Este bloque protege, de forma directa, la integridad y la disponibilidad de la información y de los sistemas (dimensiones "I" y "D" de la tríada CIA que se explicó en el capítulo 2). Se tutela tanto el contenido (datos) como la funcionalidad (sistemas, redes, servicios). Por eso, en la práctica, conviene distinguir entre:

- Interferencia en datos: destruir, deteriorar, suprimir, alterar o hacer inaccesibles datos.
- Interferencia en sistemas: obstaculizar o impedir el funcionamiento de un sistema, red o servicio (p. ej., ataques DoS/ DDoS, cripto-bloqueos, sabotaje lógico).

Esta separación dialoga uno a uno con los arts. 4 y 5 del Convenio de Budapest y ayuda a ordenar la prueba y la calificación jurídica.

b) Núcleo típico y elementos (lectura funcional)

- Conducta
    - En datos: borrar, cifrar, corromper, modificar, insertar o suprimir datos sin autorización o excediendo la autorizada, y con aptitud para afectar la veracidad, integridad o disponibilidad del contenido.

    - En sistemas: introducir, transmitir o ejecutar instrucciones capaces de interrumpir, degradar o inutilizarparcial o totalmente el sistema o el servicio.
- Objeto material: bases de datos, archivos, respaldos, metadatos y, del lado de sistemas, servidores, endpoints, ICS/SCADA, aplicaciones o servicios críticos (salud, finanzas, educación, energía, telecomunicaciones, sector público).
- Ilicitud: ausencia de autorización o exceso de la autorización concedida (p. ej., insider que rompe la política de accesos).
- Resultado/aptitud: según la redacción vigente, puede requerirse resultado (daño, inutilización, pérdida, indisponibilidad) o bastar la aptitud concreta para producirlo (modelo de peligro).
- Dolo: voluntad de producir el daño o la indisponibilidad; también vale el dolo eventual cuando el riesgo es alto y el agente lo asume (p. ej., pruebas "imprudentes" con scripts en producción).

c) Problemas recurrentes de aplicación

1. Delimitación "datos" vs. "sistemas": en ataques modernos, lo que parece daño a datos (p. ej., cifrado con ransomware) produce inmediatamente indisponibilidad sistémica. Usá bien la acumulación homogénea: podés calificar por datos y por sistemas si la ley lo permite, cuidando el non bis in idem.
2. "Sin autorización" vs. abuso de privilegios: el insider con permisos administrativos que actúa fuera de la finalidad otorgada cae en exceso de autorización (es clave anclarlo a políticas internas y contratos de confidencialidad/uso).
3. Umbral probatorio: debés acreditar integridad técnica de la evidencia (hash, cadena de custodia, logs, imágenes forenses), trazabilidad de la ejecución (p. ej., Job IDs,

registros SIEM/EDR) y, cuando se alegue indisponibilidad, métricas (SLA, tiempos de caída, reportes de monitoreo).

4. Concursos: es muy común el concurso con acceso ilícito (ingreso inicial), abuso de dispositivos(tenencia/producción de malware) y extorsión (pago para recuperar claves/descifrado).
5. Culpa vs. dolo: incidentes por negligencia grave (p. ej., borrar producción por error) suelen quedar fuera del ámbito penal salvo que exista tipo culposo expreso; esto se traslada a la responsabilidad civil o administrativa.

d) Política criminal y proporcionalidad

La proporcionalidad debe graduarse por: criticidad del servicio, magnitud del impacto, duración de la caída, irrecuperabilidad de datos, costo de recuperación y número de afectados. Cuando el hecho es instrumental a otra finalidad (p. ej., extorsión con ransomware), corresponde agravar o concurrir con la figura principal.

e) Implicaciones para personas jurídicas (PJ) y *compliance*

Aunque el régimen vigente de PJ sea acotado, estos hechos suelen beneficiar directa o indirectamente a organizaciones (p. ej., reducción de competencia, presión extorsiva, lucro por fraude).

2.5.5 Suplantación de identidad digital y abuso de dispositivos

a) Bien jurídico y ubicación sistemática

Acá confluyen dos núcleos:

1. la identidad y la intimidad (confianza en la atribución de actos y mensajes en entornos digitales), y
2. la seguridad de los sistemas (prevención de la fabricación, tenencia y provisión de herramientas destinadas a cometer ciberdelitos).

En el ordenamiento costarricense, la suplantación suele abordarse mediante figuras que sancionan el uso no autorizado de credenciales (p. ej., obtención/uso de contraseñas, tokens, llaves), la apropiación de cuentas o perfiles y ciertas formas de falsedad en medios electrónicos; mientras que el "abuso de dispositivos" se relaciona con tipos de facilitación o provisión de medios para delinquir (malware, keyloggers, skimmers, tarjetas/clonación, "herramientas" de intrusión), incluso cuando no se ha consumado el delito principal.

b) Conductas típicas (lectura funcional)

- Suplantación de identidad digital
    - Uso de credenciales ajenas o apropiación de cuentas (correo, banca, redes, firma/identidad electrónica) para realizar actos como si fueran del titular.
    - Creación de perfiles falsos o alteración de identificadores con potencial dañino (daño reputacional, engaño, fraude).
    - Ingeniería social y SIM-swap como medios de apoderamiento; cuando median automatismos o APIs, se vuelve clave probar el rastro técnico (IP, user-agent, logs, OTP).
- Abuso de dispositivos / facilitación
    - Producir, vender, adquirir, importar, distribuir o poner a disposición programas, dispositivos o datos de acceso (p. ej., diccionarios de contraseñas, listas de credenciales, capturadores de pulsaciones, troyanos, exploits, dongles de bypass) con la finalidad de cometer delitos contra datos/sistemas o comunicaciones.
    - Tenencia con finalidad delictiva: exige anclar el elemento subjetivo especial de tendencia (propósito de cometer un delito informático), evitando

criminalizar herramientas de uso dual (pentesting, forense, administración de sistemas).

c) Elementos y notas probatorias

- Ilicitud: "sin autorización" o exceso del permiso otorgado (insider que usa credenciales para fines ajenos a su función).
- Finalidad (en dispositivos): el corazón del tipo es probar la intención (p. ej., empaquetado con manuales de uso, foros de venta, precio, configuración, pruebas en víctimas, vínculos con otros hechos).
- Rastreo técnico: logs de autenticación, registros de cambio de contraseña, MFA/OTP, evidencias de SIM-swap (bitácoras de operador), metadatos de apps y hash/firma de binarios cuando se trata de malware.

d) Problemas frecuentes

1. Herramientas de uso dual: muchos programas de administración/seguridad (p. ej., escáneres de puertos, sniffers) pueden usarse con fines legítimos; el derecho penal debe delimitar por la finalidad y el contexto de uso, no por la mera posesión.
2. Tipificación dispersa: cuando el "abuso de dispositivos" no es un tipo autónomo, la cobertura suele descansar en "facilitación" o "complicidad" y puede quedar corta para castigar la producción/tenencia con propósito delictivo antes del ataque.
3. Suplantación vs. falsedad: si solo existe falsedad documental clásica, ciertos supuestos de suplantación de cuentas (sin documento en sentido estricto) podrían quedar en zona gris.
4. Prueba del ánimo de lucro (en fraudes) vs. finalidad (en abuso de dispositivos): no confundir; el art. 6 de Budapest no exige lucro, exige propósito de cometer los delitos informáticos.

e) Proporcionalidad y concursos

- Atenuar o eximir cuando se acredite investigación legítima (p. ej., auditorías autorizadas, pentesting con contrato) y sancionar más gravemente cuando:
    - hay afectación masiva (campañas de phishing, botnets),
    - se dirigen a servicios críticos,
    - se combina con extorsión o fraude.
- Concursos: usual con acceso ilícito, interceptación, interferencia en datos/sistemas, falsedad y fraude.

2.6 Leyes especiales y normativa complementaria

Este apartado identifica y ordena la normativa no penal que enmarca la prevención, la investigación y la respuesta a los incidentes y delitos informáticos en Costa Rica:

2.6.1 Protección de datos personales (Ley N.° 8968 y reglamentación)

Esta ley tiene como foco la tutela de la intimidad y del tratamiento lícito de datos personales, con un régimen sancionatorio administrativo y potestades de la autoridad de control (PRODHAB). La ley se puede resumir de la siguiente manera:

- Principios y bases de licitud: consentimiento, finalidad, proporcionalidad, calidad y seguridad. En clave penal, estos principios fijan el "estándar de diligencia" mínimo que se espera de responsables y encargados.
- Derechos de las personas: acceso, rectificación, cancelación, oposición; notificación de tratamientos y, cada vez más relevante, gestión de **incidentes** que puedan afectar la confidencialidad o integridad de datos.
- Seguridad y deber de resguardo: obligación de medidas técnicas y organizativas. Cuando el incumplimiento es grave y deliberado (p. ej., obtención o divulgación

ilícita**),** puede abrir la puerta a responsabilidad penal por otras figuras (revelación de secretos, daños a datos, etc.).

- Interacción con lo penal**:** el eje administrativo no excluye la respuesta penal cuando hay dolo/beneficio o cuando la conducta trasciende la mera infracción regulatoria. Para tesis: dejar claros los criterios de intervención (reserva penal) y los supuestos de concurso aparente**.**

2.6.2 Documentos y firma digital (Ley N.° 8454 y reglamentación)

Su foto está en la equiparación jurídica de la firma digital a la manuscrita y reconocimiento del documento electrónico con valor probatorio. Su contenido se resume de la siguiente manera:

- Valor probatorio: la firma digital avanzada habilita presunciones de autenticidad e integridad, clave para la falsedad informática y para la valoración de evidencia en soporte electrónico.
- Infraestructura: jerarquía de certificación, certificados, revocación y sellos de tiempo. Todo ello conecta con la cadena de custodia digital (hash, metadatos, logs).
- Tensiones prácticas: si el sistema probatorio privilegia soportes físicos o exige formalidades ajenas a lo digital, pueden aparecer brechas que afectan la persecución de la falsificación y el fraude informático.

2.6.3 Otras normas y estándares complementarios (soft law y sectoriales)

Además del derecho penal y de las leyes especiales ya revisadas, existe un conjunto de normas y lineamientos que, sin crear delitos, condicionan la diligencia debida y, por esa vía, influyen en cómo se prueba y valora un incidente informático. En la contratación pública y en la gestión del sector público, es cada vez más habitual que las instituciones exijan políticas explícitas de seguridad de la información, prácticas de gestión de TI, y esquemas de

continuidad del negocio y respaldo. Estas exigencias aterrizan en los pliegos y contratos mediante cláusulas de seguridad, acuerdos de nivel de servicio (SLA) y facultades de auditoría. En la práctica, si un proveedor incumple esas obligaciones—por ejemplo, no mantiene respaldos verificados o administra mal los accesos—esa omisión no solo agrava el impacto del incidente, sino que también debilita su posición probatoria ante una investigación administrativa, civil o penal.

Algo similar ocurre en el sector financiero y de pagos, donde las normas prudenciales y operativas imponen controles de ciberseguridad y gestión de riesgos operacionales más estrictos. Estos marcos funcionan como un estándar de diligencia: cuando un incidente revela que la entidad no aplicó controles mínimos (segmentación de red, doble factor, monitoreo continuo, pruebas de restauración), esa brecha pesa al valorar responsabilidad e, incluso, la proporcionalidadde una sanción.

Por último, los estándares internacionales—como ISO/IEC 27001/27002, el NIST Cybersecurity Framework o las guías OWASP—no tipifican conductas ni sustituyen la ley, pero sí operan como referente técnico para medir la debida organización corporativa. En peritajes y dictámenes, sirven para explicar qué controles eran razonables, qué evidencias debieron preservarse (hash, logs, bitácoras EDR/SIEM) y cómo se debió responder al incidente. En otras palabras: aportan el "metrónomo" con el cual se evalúa la diligencia antes, durante y después del ataque.

2.7 A modo de cierre

En conjunto, este bloque muestra que Costa Rica dispone de una arquitectura mixta: la protección de datos (Ley 8968), el soporte probatorio y de firma/documento electrónico (Ley 8454) y una base de reformas penales y procesales que permiten investigar y sancionar.

Sin embargo, persisten tres nudos que condicionan la adecuación al Convenio de Budapest y la eficacia práctica del sistema:

A) un régimen de responsabilidad penal de personas jurídicas todavía estrecho para los ciberdelitos nucleares;

B) medidas procesales con umbrales o lagunas (p. ej., conservación rápida, obtención en tiempo real, datos de tráfico/abonado y plazos de respuesta transfronteriza); y

C) desalineaciones técnicas entre la lógica de la prueba digital y ciertos formalismos probatorios tradicionales.

CAPÍTULO III: MARCO METODOLÓGICO

3.1 Enfoque de la investigación

La investigación adopta un enfoque cualitativo de naturaleza jurídico-dogmática y propositiva, complementado con un componente de derecho comparado. El propósito central es analizar la adecuación, suficiencia y sistematicidad del marco penal costarricense frente a la ciberdelincuencia conforme al Convenio de Budapest y derivar pautas de técnica legislativa aplicables al contexto nacional.

Este enfoque es coherente con los objetivos del estudio y con el carácter normativo del problema planteado.

3.2 Método de la investigación

Para esta tesis, se sigue un diseño no experimental y documental. En coherencia con el enfoque descrito, se sigue un diseño no experimental y documental. No se aplican técnicas empíricas como encuestas, entrevistas u observación participante, pues la naturaleza del problema es fundamentalmente normativa y dogmática. El método combina:

1. Análisis dogmático de normas penales: se estudian los tipos penales informáticos y afines contenidos en el Código Penal y en leyes especiales, atendiendo a elementos como el bien jurídico protegido, la descripción de la conducta, los sujetos activo y pasivo, la antijuridicidad, la culpabilidad y la punibilidad.

2. Hermenéutica jurídica: se realiza una interpretación sistemática, teleológica y conforme a estándares internacionales de las normas nacionales, de modo que puedan ser

leídas a la luz del bloque de constitucionalidad y de los compromisos asumidos por Costa Rica en el Convenio de Budapest.

4. Análisis de política criminal: con base en los hallazgos anteriores, se valora la coherencia interna del catálogo de delitos informáticos, la proporcionalidad de las sanciones y el lugar que ocupa la responsabilidad penal corporativa en la arquitectura general del sistema.

Desde el punto de vista de su alcance, el estudio es descriptivo-analítico porque identifica y caracteriza vacíos, solapamientos y ambigüedades del marco vigente, y evaluativo al contrastar dicho marco con los estándares del Convenio de Budapest y propositivo, al plantear ajustes normativos concretos y redacciones tipo para eventuales reformas legislativas.

3.3 Delimitación temporal y espacial

Esta tesis se circunscribe al ordenamiento costarricense y al período 2017–2025, es decir, desde la adhesión a Budapest a la actualidad.

3.4 Fuentes

El corpus de información de la tesis está integrado por fuentes jurídicas y doctrinales seleccionadas a partir de criterios de pertinencia temática y actualidad. Se privilegian aquellas que guardan relación directa con: i) los delitos informáticos y la ciberdelincuencia, ii) los bienes jurídicos en entornos digitales, iii) la responsabilidad penal de las personas jurídicas y iv) los estándares del Convenio de Budapest, en particular su artículo 12.

3.4.1 Fuentes primarias

Dentro de las fuentes primarias se incluyen, en primer término, las normas del ordenamiento costarricense relevantes para la materia: el Código Penal, las leyes especiales en materia informática y conexa, así como la normativa constitucional vinculada con derechos fundamentales afectados por la ciberdelincuencia (intimidad, protección de datos, secreto de comunicaciones, entre otros).

También se consideran fuentes primarias los instrumentos internacionales y supranacionales, especialmente, el Convenio de Budapest sobre ciberdelincuencia y sus materiales explicativos. Finalmente, cuando existe, se incorpora jurisprudencia penal y constitucional nacional relacionada con delitos informáticos, protección de datos o responsabilidad de personas jurídicas, en tanto aporta criterios interpretativos indispensables para comprender el alcance de las normas vigentes.

3.4.2 Fuentes secundarias

Las fuentes secundarias están integradas por doctrina nacional e internacional especializada, artículos académicos, tesis de grado y posgrado, informes técnicos de organismos internacionales y guías o marcos de referencia en materia de ciberseguridad y responsabilidad penal corporativa.

Estas fuentes permiten reconstruir el debate teórico sobre la imputación penal de las personas jurídicas, los modelos de regulación de la ciberdelincuencia y la función de los programas de cumplimiento (*compliance*) en la prevención y mitigación de incidentes de ciberseguridad. Asimismo, sirven para contrastar la situación costarricense con tendencias

comparadas y para respaldar las propuestas de lege ferenda que se formulan en los capítulos finales.

3.5 Variables o unidades de análisis

Dado el carácter cualitativo y jurídico-dogmático de la investigación, no se trabaja con variables cuantificables en sentido estadístico. En su lugar, se definieron unidades de análisis o categorías temáticas que permiten ordenar el estudio y vincularlo directamente con los objetivos planteados. Las principales unidades de análisis son las siguientes:

1. Conceptualización de la ciberdelincuencia y de los bienes jurídicos protegidos en el entorno digital. Incluye la delimitación de las conductas informáticas relevantes, su clasificación y la identificación de los intereses individuales y supraindividuales que el Derecho Penal busca resguardar.

2. Catálogo de delitos informáticos y afines en el ordenamiento costarricense. Se analiza la configuración actual de los tipos penales vinculados al uso indebido de tecnologías de la información y la comunicación (acceso ilícito, daño o sabotaje informático, estafa informática, violación de datos personales, entre otros).

3. Adecuación del marco normativo costarricense a los estándares del Convenio de Budapest. Esta unidad de análisis se centra en la correspondencia entre las exigencias del Convenio y las figuras penales, procesales y de cooperación internacional previstas en el derecho interno.

4. Responsabilidad penal de las personas jurídicas por incidentes de ciberseguridad. Se examinan los supuestos en que la estructura organizativa de una empresa facilita, tolera o

encubre conductas delictivas y se valora la existencia o ausencia de un régimen de imputación adecuado.

5. Criterios de política criminal y proporcionalidad sancionatoria. Esta categoría permite evaluar si el sistema costarricense ofrece respuestas claras, coherentes y proporcionadas frente a la complejidad de la ciberdelincuencia y a los riesgos que genera para personas, organizaciones e infraestructuras críticas.

3.6 Instrumentos

Para ordenar y sistematizar el material recopilado se diseñaron varios instrumentos de trabajo, de naturaleza principalmente documental:

a) Matriz de adecuación al Convenio de Budapest. Se construyen diferentes matrices en las que se cruzan los artículos del Convenio (en particular los relativos a delitos informáticos nucleares, medidas procesales y responsabilidad de personas jurídicas) con las normas costarricenses vigentes. En cada casilla, se determina si la exigencia internacional se cumple, se cumple parcialmente o no se cumple, incorporando notas técnicas que explican la valoración.

Estos instrumentos no generan datos numéricos, pero sí permiten una lectura ordenada y comparativa del material jurídico, facilitando la identificación de vacíos, solapamientos y posibles líneas de reforma.

3.7 Proceso para la recolección y análisis de datos

El proceso metodológico seguido para la recolección y el análisis de los datos entendidos aquí como información normativa, jurisprudencial y doctrinal se desarrolló en varias etapas sucesivas pero interrelacionadas:

1. Identificación del problema y de los criterios de búsqueda. A partir de la pregunta de investigación y de los objetivos específicos, se definieron las palabras clave y los criterios de inclusión y exclusión ya mencionados (delitos informáticos, bienes jurídicos en entornos digitales, responsabilidad penal de personas jurídicas y estándares del Convenio de Budapest).

2. Recolección de fuentes primarias. Se compiló la normativa nacional relevante (Constitución, Código Penal, leyes especiales), los instrumentos internacionales aplicables y, cuando existía, la jurisprudencia vinculada. Esta recolección se realizó mediante la consulta de bases de datos oficiales, repositorios legislativos y portales institucionales.

3. Recolección de fuentes secundarias. Paralelamente, se localizaron y seleccionaron estudios doctrinales, tesis y artículos académicos que abordaran la ciberdelincuencia, la responsabilidad penal corporativa y la política criminal en materia de ciberseguridad, tanto en el contexto costarricense como en el comparado.

4. Clasificación y delimitación del corpus. Las fuentes recopiladas se organizaron en función de las unidades de análisis señaladas (conceptualización, catálogo de delitos, adecuación a Budapest, responsabilidad de personas jurídicas y política criminal), lo que permitió depurar el corpus y concentrarse en el material más pertinente.

5. Análisis dogmático y hermenéutico. Sobre la base de la clasificación anterior, se procedió al examen detallado de las normas y de la doctrina. En esta etapa, se identificaron los elementos típicos de cada figura delictiva, los bienes jurídicos involucrados, los problemas de interpretación y las tensiones con los estándares internacionales.

6. Elaboración de matrices y esquemas comparativos. Los resultados del análisis se presentan en las matrices de adecuación a Budapest y en los esquemas de imputación penal corporativa, lo que facilitó una visión panorámica de las fortalezas y debilidades del sistema costarricense y permitió detectar con mayor claridad los vacíos y solapamientos normativos.

7. Síntesis y formulación de propuestas. Finalmente, se integraron los hallazgos en una síntesis que alimenta los capítulos de análisis y de conclusiones. A partir de esta síntesis se formularon lineamientos de reforma y propuestas de técnica legislativa orientadas a armonizar el ordenamiento costarricense con el Convenio de Budapest y con las tendencias comparadas más relevantes.

3.8 Ámbitos de la investigación

Ámbito material. El estudio se centra en la ciberdelincuencia y, en particular, en los tipos penales vinculados con el uso indebido de tecnologías de la información y la comunicación. Esto incluye conductas como la violación de datos personales, la estafa informática, el daño y sabotaje informático, la interceptación ilícita de comunicaciones, la extorsión tecnológica, el espionaje y el abuso de dispositivos, entre otras. El análisis considera tanto las figuras actualmente previstas en el Código Penal y en leyes especiales como aquellas que podrían requerir ajustes o nuevas formulaciones a la luz del Convenio de Budapest.

Ámbito subjetivo. La investigación se orienta al estudio del marco jurídico aplicable a personas físicas que cometen delitos informáticos, así como a la eventual extensión de la responsabilidad penal a personas jurídicas cuando su estructura organizativa facilite, encubra o tolere estas conductas. También se contempla el papel de entes estatales y privados en la

prevención y persecución de la ciberdelincuencia, siempre atendiendo a las limitaciones y reservas que impone el orden constitucional costarricense.

Viabilidad. El trabajo se ajusta al marco institucional y a los criterios académicos definidos por la Universidad Central. La coherencia entre el planteamiento del problema, los objetivos y el método, así como la disponibilidad de fuentes normativas, doctrinales y comparadas, garantizan la factibilidad del proyecto. Además, el cronograma previsto y los recursos disponibles resultan adecuados para la conclusión de la investigación dentro de los plazos establecidos.

CAPÍTULO IV: ANÁLISIS DE RESULTADOS

Este capítulo examina el marco costarricense descrito en el Capítulo III a la luz del Convenio de Budapest. El objetivo es doble: i) identificar fortalezas y brechas normativas que inciden en la prevención, investigación y sanción de los hechos informáticos; y ii) extraer criterios operativos que orienten una eventual propuesta de *lege ferenda* sobre responsabilidad penal de personas jurídicas (PJ) y ajustes de tipificación y medidas procesales. La metodología combina análisis dogmático (bienes jurídicos, tipicidad, concursos y proporcionalidad), lectura procesal-probatoria (estándares de evidencia digital) y contraste funcional con casos tipo (ransomware, fraude por manipulación de sistemas, DDoS, insider).

Como se podrá observar, el balance es claro: Costa Rica cuenta con piezas funcionales (protección de datos, documento/firma digital, interferencia en datos/sistemas, interceptación con control judicial), pero convive con vacíos y solapamientos que afectan la adecuación a Budapest y la eficacia práctica: acceso ilícito autónomo, abuso de dispositivos como punición ex ante, y la zona gris entre estafa y fraude informático. A nivel procesal-probatorio, el "talón de Aquiles" podrían ser los plazos y formatos en cooperación y la necesidad de reforzar preservación y minimización.

4.1 Adecuación a Budapest

Con base en lo detallado en el capítulo anterior, queda claro que el Art. 2 de Budapest (acceso ilícito) Costa Rica cubre parcialmente el acceso no autorizado a sistemas cuando se integra con 229 bis/ter (daño/sabotaje) y con 196 si el acceso tiene por fin interceptar/apoderarse de comunicaciones. Falta un tipo autónomo y general de "acceso

ilícito" desprovisto de exigencias adicionales de daño o peligro a la intimidad (Budapest ETS 185; Código Penal de Costa Rica, arts. 196, 229 bis/ter).

En relación con el artículo 3 (interceptación ilícita), el artículo 196 resulta alineado en lo esencial al sancionar la interceptación sin autorización, con matices sobre el elemento "peligro/daño" a la intimidad. (Código Penal de Costa Rica, art. 196; Budapest ETS 185).

En relación con el artículo 7 (falsificación informática) Costa Rica suele cumplir cuando reconoce la alteración o creación de datos/documentos electrónicos con aptitud para producir efectos jurídicos y sanciona tanto la producción como el uso. Donde hay divergencias, suele ser en la definición de "documento" y en la prueba de su autenticidad electrónica.

En relación con el Art. 8 (fraude informático), hay una cobertura parcial o plena según exista un tipo autónomo que sancione la manipulación de datos/sistemas para causar un perjuicio patrimonial, sin exigir engaño directo a una persona. Cuando solo hay agravantes de la estafa clásica por uso de medios informáticos, quedan zonas grises (automatismos, APIs, bots, etc.).

Frente al artículo 6, cuando la legislación nacional solo contempla "facilitación" genérica o complicidad del delito principal, el alineamiento con el artículo 6 es parcial: se pierde la punición ex ante de la cadena de suministro delictiva (marketplaces de malware, kits de phishing, venta de "fullz", etc.):

Tabla 2 Matriz de adecuación a Budapest

Estándar Budapest	*Norma CR (art./ley)*	*¿Cumple?*	*Observaciones de técnica legislativa*	*Impacto CIA*	*Nota sobre personas jurídicas*
Art. 2 Acceso ilícito	Código Penal (violación de comunicaciones, daño/ interferencia cuando media acceso)	Parcial	Falta un tipo autónomo de acceso no autorizado sin exigir peligro/daño; dispersión entre figuras de interceptación y daño.	C (y I/D si hay daño)	Régimen de PJ no se aplica de forma general a ciberdelitos; brecha frente al art. 12.
Art. 3 Interceptación ilícita	Código Penal (violación de comunicaciones)	Sí, con matices	Exigencia de "peligro/daño" a la intimidad puede elevar el umbral probatorio frente al estándar de Budapest.	C	Igual observación general.
Art. 4 Interferencia en datos	Código Penal (daño/alteración de datos)	Sí	Tipificación expresa con agravantes por criticidad/resultado.	I	Igual observación general.
Art. 5 Interferencia en sistemas	Código Penal (sabotaje/afectación de sistemas)	Sí	Cobertura adecuada de indisponibilidad; afinar definiciones de "sistema" y "crítico".	D (y I)	Igual observación general.
Art. 6 Abuso de dispositivos	Código Penal (facilitación; tenencia/producción de medios)	Parcial	Si no hay tipo autónomo de abuso de dispositivos, la "facilitación" no cubre toda tenencia/producción con finalidad delictiva.	C/I/D	Igual observación general.
Art. 7 Falsificación informática	Código Penal (falsedades con soporte electrónico + ley de firma/documento digital)	Sí	Alinear definiciones de documento electrónico y criterios de autenticidad; sancionar uso además de creación/alteración.	C/I	Aplicable a PJ si se amplía el catálogo con conductas informáticas.

Art. 8 Fraude informático	Código Penal (estafa con medios informáticos o tipo autónomo de fraude informático)	Parcial/Sí(según configuración vigente)	Si solo hay agravante de estafa, quedan lagunas cuando el engaño recae en el sistema y no en una persona. Se recomienda tipo autónomo.	Patrimonio (con C/I/D como medios)	Clave para PJ en fraudes sistémicos (p. ej., fintech, e-commerce).
Arts. 12–13 Personas jurídicas y sanciones	Régimen costarricense de responsabilidad penal de PJ (ámbito material actual)	Parcial	Si el régimen no abarca de forma expresa los ciberdelitos o exige delitos taxativos distintos, hay brecha. Recomendable: incluir delitos informáticos y prever programas de compliance como atenuante/eximente.	—	Urge alinear con Budapest: sanciones efectivas, proporcionales y disuasorias para PJ.
Arts. 14–21 Medidas procesales	Leyes procesales y especiales (interceptación, conservación rápida, allanamientos lógicos, órdenes sobre datos)	Parcial/Sí	Verificar existencia de conservación rápida de datos, recolección en tiempo real, acceso a datos de tráfico y contenido con control judicial, y cadena de custodia digital.	—	Indirecto: la posibilidad de investigar eficazmente también disuade a PJ.

En la tabla a continuación se describe además una Matriz de adecuación a Budapest con detalle para arts. 4 y 5:

Tabla 3 Matriz con detalle artículos 4 y 5

Estándar Budapest	*Norma CR (art./ley)*	*¿Cumple?*	*Observaciones de técnica legislativa*	*Impacto CIA*	*Nota sobre personas jurídicas*
Art. 4 Interferencia en datos	Código Penal (tipo de daño/alteración/supresión/ inaccesibilidad de datos)	Sí	Incluir expresamente la inaccesibilidad por cifrado y la supresión lógica(soft delete). Recomiendo definir "dato" en clave amplia (contenido y metadatos).	I (integridad) y D(disponibilidad)	Incluir el art. 4 en el catálogo para PJ; prever atenuante por programas de back-up/DRPefectivos (compliance).
Art. 5 Interferencia en sistemas	Código Penal (tipo de sabotaje/indisponibilidad de sistemas/servicios)	Sí	Mejor si no exige daño permanente: basta interrupción u obstaculización grave. Añadí mención explícita a ataques distribuidos (DDoS) y a servicios críticos con agravantes.	D(disponibilidad) y I (integridad), según caso	Extender a PJ y contemplar sanciones por impacto en usuarios y duración ; atenuante por plan de respuesta a incidentes probado.

Por otro lado, en relación con las implicaciones para personas jurídicas *y compliance,* el análisis permite indicar que existe un riesgo corporativo: áreas de marketing, soporte o TI pueden, sin controles, albergar o distribuir herramientas riesgosas (scripts, dumps, "utilitarios") que derivan en responsabilidad si hay beneficio directo/indirecto.

Además, con respecto a los modelos de organización (compliance en ciberseguridad): políticas de gestión de credenciales**,** MFA**,** segregación de funciones**,** revisión de accesos**,** concientización anti-phishing**,** control de descargas **y** listas blancas de software; todo ello como atenuante/eximente si se incorpora un régimen claro de responsabilidad penal de personas jurídicas en materia de ciberdelitos:

Tabla 4 Matriz de adecuación a Budapest (bloque de art. 6)

Estándar Budapest	*Norma CR (art./ley)*	*¿Cumple?*	*Observaciones de técnica legislativa*	*Impacto CIA*	*Nota sobre personas jurídicas*
Art. 6 Abuso de dispositivos(programas/dispositivos/datos de acceso con finalidad de cometer ciberdelitos)	Código Penal (figuras de facilitación/provisión de medios; eventuales tipos sobre datos de acceso y herramientas informáticas)	Parcial	Si no existe un tipo autónomo que sancione producción/tenencia /venta/puesta a disposición con finalidad delictiva, la cobertura queda limitada a complicidad y pierde eficacia ex ante. Incluir excepción para usos legítimos (auditoría/pentest).	C/I/D (según el delito que habilita)	Recomendado extender el catálogo aplicable a PJ para cubrir art. 6 e introducir atenuante/eximente por compliance (controles de software, MFA, MDM, hardening, capacitación).

Nota: elaboración propia.

4.2 Vacíos, solapamientos y ambigüedades del marco costarricense

Con base en lo que se ha discutido en este capítulo, el panorama normativo muestra avances relevantes, pero también zonas ciegas que afectan la coherencia dogmática y la eficacia práctica. En síntesis, hay tres tipos de problemas:

(a) Vacíos de tipificación.

- Acceso ilícito autónomo: cuando no hay daño, peligro específico o afectación a la intimidad, el ingreso no autorizado a un sistema puede quedar sin encaje claro.
- Abuso de dispositivos: si la legislación reposa solo en "facilitación/complicidad", no se alcanza la producción/tenencia/venta/puesta a disposición con finalidad delictiva previa al ataque.
- Suplantación de identidad digital: algunos supuestos (apropiación de cuentas, SIM-swap, uso de credenciales) se tratan de forma indirecta vía falsedades o estafa, con riesgo de dejar huecos cuando no hay "engaño a persona" sino engaño al sistema.

(b) Solapamientos y concursos problemáticos.

- Interceptación vs. acceso: el artículo que protege comunicaciones puede absorber conductas de simple acceso a buzones o repositorios, creando confusión sobre el bien jurídico (¿intimidad o confidencialidad de sistemas?).
- Daño a datos vs. interferencia en sistemas: en ataques modernos (ransomware), el mismo hecho afecta datos e indisponibilidad sistémica. Sin reglas claras, hay riesgo de doble incriminación o, al revés, de atipicidad parcial.
- Estafa clásica vs. fraude informático: cuando el desplazamiento patrimonial ocurre por automatismos, el "engaño a persona" compite con la "manipulación de sistemas", generando calificaciones inestables.

(c) Ambigüedades técnicas.

- “Sin autorización” y “exceso de autorización”: hace falta anclarlo a políticas internas, contratos de uso y controles de acceso para no convertir disputas laborales o disciplinarias en penales.
- Definiciones de “sistema”, “dato”, “dispositivo” y “herramienta” de uso dual: si quedan abiertas, impactan la legalidad y la previsibilidad.
- Umbrales probatorios: exigencias como “peligro/daño a la intimidad” para interceptación podrían elevar indebidamente el estándar frente a la lógica de Budapest.

Estos nudos reducen la previsibilidad del *ius puniendi*, dificultan la prueba (porque obliga a forzar tipos) y restan disuasión en contextos corporativos donde la beneficialidad puede ser indirecta. Por eso, el cierre propositivo sugerirá tipos autónomos, definiciones técnicas mínimas y criterios de proporcionalidad (criticidad del servicio, alcance del impacto, duración, recuperabilidad de datos, habitualidad).

4.3 Otros hallazgos relevantes: análisis por figuras nucleares

4.3.1 Acceso ilícito

Hallazgo. La cobertura es parcial cuando el ingreso no autorizado al sistema no produce daño, no conlleva interceptación ni genera peligro específico a la intimidad: el *simple acceso* puede quedar en una zona gris que debilita la tutela de la confidencialidad del sistema (Budapest, art. 2).

Efecto. Se reduce la capacidad disuasoria frente a intrusiones iniciales que sirven como pivote de ataques mayores (p. ej., escalamiento lateral), y se incentiva forzar la calificación por otras figuras, con riesgo de inseguridad jurídica.

Criterio. Un tipo autónomo de acceso no autorizado, sin requisito de resultado lesivo, devolvería coherencia al sistema, que permite graduar la pena por medios, alcance, reiteración y afectación potencial (Budapes, art. 2).

Prueba. Debe acreditarse la ausencia o el exceso de autorización con evidencia técnica: logs de autenticación, correlaciones SIEM/EDR, ventanas temporales, políticas de acceso y, cuando aplique, rastro de MFA/OTP (Constitución Política de Costa Rica, 1949, art. 24).

4.3.2 Interceptación de comunicaciones

Hallazgo. La figura está alineada con matices: exigir "peligro/daño" a la intimidad eleva el umbral probatorio respecto del estándar de Budapest, que sanciona la interceptación *per se* (Budapest, art. 3; Constitución Política de Costa Rica, 1949, art. 24).

Efecto. En supuestos de *sniffing* o desvío de tráfico sin demostración de afectación a la esfera íntima, la exigencia adicional puede vaciar de eficacia el tipo.

Criterio. Mantener la centralidad de la intimidad como bien jurídico, para evitar convertirla en una condición que haga inoperante la tutela frente a interceptaciones técnicamente probadas.

Prueba. Registro técnico de la herramienta empleada, preservación con hash, trazabilidad de paquetes, minimización de datos no pertinentes y control judicial reforzado (Constitución Política de Costa Rica, 1949, art. 24).

4.3.3 Interferencia en datos y sistemas (daño/sabotaje)

Hallazgo. La cobertura es robusta en lo material, aunque el reto práctico es delimitar datos vs. sistemas en ataques híbridos (p. ej., ransomware que cifra datos y, a la vez, interrumpe servicios). La inaccesibilidad por cifrado debería considerarse afectación

de datos, y para sistemas basta una interrupción grave, sin exigir daño permanente (Budapest, arts. 4–5).

Efecto. Sin reglas claras, se corre el riesgo de doble incriminación (calificar el mismo hecho como daño a datos y a sistemas) o, en el extremo opuesto, de dejar lagunas si se pide destrucción o pérdida irreparable.

Criterio. Reconocer explícitamente la inaccesibilidad (por cifrado u otros bloqueos) como modalidad de afectación a datos y, en sistemas, centrar la gravedad en la duración y el alcance de la indisponibilidad, con agravantes por servicios críticos.

Prueba. Métricas de SLA y monitoreo, reportes de disponibilidad, evidencia de backups y pruebas de restauración, bitácoras EDR/SIEM y documentación de la arquitectura afectada.

4.3.4 Abuso de dispositivos / facilitación

Hallazgo. Cuando la legislación descansa sólo en facilitación o complicidad, el alineamiento con el artículo 6 de Budapest es parcial: no se alcanza la producción, tenencia, venta o puesta a disposición de herramientas con finalidad delictiva antes del ataque (Budapest, art. 6).

Efecto. Se debilita la punición ex ante de la cadena de suministro (kits de phishing, *malware*, listas de credenciales).

Criterio. Incorporar un tipo autónomo con elemento subjetivo de finalidad, más una cláusula de uso legítimo(pentesting autorizado, forensia, administración de sistemas) para proteger la investigación y la seguridad defensiva.

Prueba. Contexto de comercialización y uso (foros, manuales, configuración, *builds*), ensayos en víctimas, vínculos con fraudes o intrusiones y huellas de distribución.

4.3.5 Falsificación y fraude informáticos

Hallazgo. En falsedad, el sistema funciona si se reconoce el documento electrónico y su uso, apoyado por la firma digital y la infraestructura de certificación (Ley N.º 8454, 2005). En fraude, aparecen lagunas cuando el "engaño" recae en el sistema (p. ej., manipulación de parámetros o interfaces) y no en una persona, si sólo existe una agravante de la estafa clásica (Budapest, arts. 7–8).

Efecto. Inseguridad en escenarios fintech y e-commerce y sobreextensión de la estafa tradicional para supuestos que no encajan en su estructura de engaño a persona.

Criterio. Tipificar de forma autónoma el fraude informático como manipulación de datos o sistemas con perjuicio patrimonial, con graduación por monto, número de afectados y criticidad del servicio.

Prueba. Trazabilidad de transacciones y de APIs, reglas antifraude, correlaciones temporales, integridad de registros (hash, firmas, sellos de tiempo) y evidencia de autenticación/autorización.

4.3.6 Procesal-probatorio (síntesis)

La eficacia investigativa descansa en cinco pilares: preservación rápida (para evitar pérdida de datos), allanamiento lógico acotado (con límites de alcance, rutas y fechas), imágenes forenses con hash y cadena de custodia, distinción tráfico vs. contenido con control judicial reforzado y documentación exhaustiva de herramientas y parámetros para garantizar repetibilidad y verificabilidad (Constitución Política de Costa Rica, 1949, art. 24; Budapest, arts. 14–21).

Donde persisten fricciones es en plazos y formatos de cooperación internacional, especialmente, con proveedores extranjeros, lo que puede afectar la admisibilidad local (Budapest, arts. 23–35).

4.3.7 Personas jurídicas (PJ): diagnóstico y llave de política criminal

Diagnóstico. El régimen costarricense de responsabilidad penal de las personas jurídicas es aún estrecho para los ciberdelitos nucleares; la falta de inclusión expresa de conductas como acceso ilícito, interferencia, abuso de dispositivos, falsedad y fraude informáticos produce una brecha frente al artículo 12 de Budapest (Budapest, 2001, arts. 12–13).

Riesgo. Menor disuasión cuando el hecho reporta beneficio directo o indirecto para organizaciones (por ejemplo, lucro por fraude sistémico, ahorro de costos por descuido estructural en ciberseguridad).

La imputación debería descansar en el defecto de organización y en el beneficio (directo/indirecto), con compliance de ciberseguridad como atenuante o eximente verificable: controles de acceso (mínimo privilegio, MFA), gestión de vulnerabilidades, backups 3-2-1 con pruebas de restauración, monitoreo (SIEM/EDR), respuesta a incidentes, formación periódica y preservación de evidencia (ISO/IEC, 2022; NIST, 2024; OWASP, 2021).

Las sanciones deberían ser efectivas, proporcionales y disuasorias (multas por tramos según facturación, inhabilitaciones, programas de cumplimiento supervisado y publicidad de la condena).

4.3.8 Hacia un modelo costarricense de responsabilidad penal corporativa en ciberseguridad

A partir de lo anterior, se ordenan los elementos que una propuesta de *lege ferenda* debería contemplar para alinear el ordenamiento con Budapest (art. 12–13) y con buenas prácticas comparadas, cuidando la legalidad, la proporcionalidad y la seguridad jurídica.

(1) Ámbito material (¿sobre qué delitos responde la PJ?).

- Incluir expresamente los ciberdelitos nucleares: acceso ilícito, interceptación ilícita, interferencia en datos y sistemas, abuso de dispositivos, falsificación informática y fraude informático.
- Prever la posibilidad de concurso con delitos patrimoniales, de secretos, extorsión y competencia desleal cuando el hecho informático sea instrumental.

(2) Modelo de imputación (¿cuándo se atribuye a la PJ?).

- Hechos cometidos por directivos, representantes o empleados en el marco de sus funciones o con tolerancia orgánica (defecto de organización).
- Criterio de beneficio: directo o indirecto (reducción de costos por controles omitidos, ventajas competitivas indebidas, lucro por fraude sistémico).
- Debida organización: si la empresa cuenta con un modelo de gestión de ciberseguridad adecuado y eficaz, ello atenúa o exime responsabilidad (ver punto 3).

(3) *Compliance* de ciberseguridad como atenuante/eximente.

- Elementos mínimos verificables: políticas de acceso mínimo y segregación de funciones, MFA, gestión de vulnerabilidades, backups 3-2-1 con pruebas de restauración, monitoreo (SIEM/EDR), respuesta a incidentes con roles y tiempos, formación periódica (phishing y uso seguro), gestión de proveedores críticos, registro y preservación de evidencias (hash, logs, cadena de custodia).

- Eficacia ex ante y ex post: el modelo debe existir antes del hecho y demostrar funcionamiento real (auditorías, métricas, correcciones). Programas "de papel" no cuentan.

(4) Catálogo de sanciones (efectivas, proporcionales y disuasorias).

- Multas por tramos vinculadas a facturación: inhabilitaciones para contratar o licitar, publicidad de la condena, medidas de programa de cumplimiento supervisado (monitores externos por plazo).
- Proporcionalidad por criticidad del sector: número de afectados, duración de la indisponibilidad, irrecuperabilidad de datos y cooperación post-incidente (autodenuncia, preservación de evidencias, reparación).

(5) Garantías y límites.

- Respeto a la autonomía del proceso de la persona física (no se exclusiviza ni reemplaza).
- No criminalización del uso legítimo de herramientas de doble uso (*pentesting* autorizado, forensia, administración).
- Reglas claras para pymes: escalamiento proporcional (no exigir a microempresas lo propio de una entidad financiera), sin sacrificar los mínimos de diligencia.

(6) Implementación y gobernanza.

- Incentivos: atenuante por cooperación temprana y programas de reparación a víctimas.
- Coordinación interinstitucional (fiscalía, policía judicial, autoridad de datos, reguladores sectoriales) con protocolos de intercambio y plazos.
- Guías técnicas (*soft law*) que detallen el "cómo" del programa de ciberseguridad y de la preservación probatoria.

Este encuadre te permite, en el capítulo de reformas, aterrizar un texto articulado breve y claro (definiciones, catálogo, imputación, *compliance*, sanciones y disposiciones procesales básicas).

4.4 Cierre del capítulo

El capítulo mostró que el ordenamiento costarricense dispone de piezas clave (protección de datos, documento/firma digital, tipos penales de daño/interferencia y violación de comunicaciones) y de bases procesales para investigar hechos informáticos. A la vez, se identificó vacíos y solapamientos que afectan la adecuación a Budapest y, sobre todo, la efectividad frente a incidentes reales: el acceso ilícito autónomo, el abuso de dispositivos como tipo previo a la ejecución y las zonas grises entre estafa clásica y fraude informático.

De este diagnóstico emergen dos ejes para el resto de la tesis:

1. un análisis crítico (próximo capítulo) que probará, con casuística y criterios probatorios, dónde el sistema funciona y dónde falla (umbrales probatorios, concursos, definición de bienes jurídicos, proporcionalidad); y
2. una propuesta normativa (capítulo de *lege ferenda*) que ajuste el catálogo de conductas, extienda de forma clara la responsabilidad penal de personas jurídicas a los ciberdelitos nucleares y armonice medidas procesales y estándares técnicos de preservación de evidencia.

En términos operativos, estas matrices de adecuación propuestas recogen estas conclusiones en formato "Sí/Parcial/No" con notas técnicas breves por cada estándar de Budapest (arts. 2–8, 12–13, 14–21, 23–35). Ese insumo alimenta directamente lo siguiente:

- contraste de doctrina y jurisprudencia si existiera en Costa Rica;
- insumos para una sección propositiva.

Para cerrar este capítulo, se propone una síntesis ejecutiva de adecuación al Convenio de Budapest con criterio: Sí (alineado), Parcial (cobertura incompleta o con umbrales/lagunas) y No (ausencia):

Tabla 5 Matriz de adecuación al Convenio de Budapest (síntesis ejecutiva)

Estándar Budapest	***Norma CR (referencia funcional)***	***¿Cumple?***	***Observaciones de técnica legislativa / práctica***	***Impacto CIA / Patrimonio***	***Nota sobre personas jurídicas***
Art. 2 Acceso ilícito	Violación de comunicaciones + daño/interferencia cuando media acceso	Parcial	Falta un tipo autónomo de acceso no autorizado sin exigir peligro/daño resultado; dispersión entre figuras; riesgo de atipicidad de "simple acceso".	C (y I/D si hay daño)	Catálogo de PJ no cubre expresamente acceso ilícito; brecha frente a art. 12.
Art. 3 Interceptación ilícita	Violación de comunicaciones	Sí (con matices)	Exige "peligro/daño" a la intimidad: puede elevar el umbral probatorio respecto del estándar de Budapest (interceptación per se).	C	Igual brecha general de PJ.
Art. 4 Interferencia en datos	Daño/alteración/supresión/inaccesibilidad de datos	Sí	Ideal incluir inaccesibilidad por cifrado y "soft delete"; definir dato en sentido amplio (incluye metadatos).	I y D	Recomendar extensión explícita a PJ + atenuante por backups/DRP efectivos.
Art. 5 Interferencia en sistemas	Sabotaje/indisponibilidad de sistemas/servicios	Sí	Mejor sin exigir daño permanente: basta interrupción grave; mención explícita a DDoS y servicios críticos.	D (e I según caso)	Extender a PJ; sanción graduada por duración e impacto.
Art. 6 Abuso de dispositivos	Facilitación / provisión de medios (no autónomo)	Parcial	Si no hay tipo autónomo(producir, vender, distribuir, poseer con finalidad), la punición ex ante se debilita; prever excepción para usos legítimos (pentest/forense).	C/I/D (según delito habilitado)	Incluir en catálogo PJ; compliance como atenuante/eximente.

Art. 7 Falsificación informática	Falsedades en soporte electrónico + firma/documento digital	Sí	Alinear definiciones de documento electrónico y autenticidad; sancionar uso además de creación/alteración.	C/I (fe pública)	Extender a PJ para fraudes sistémicos/documentales.
Art. 8 Fraude informático	Estafa con medios informáticos o tipo autónomo	Parcial/Sí	Si solo es agravante de estafa clásica, hay lagunas cuando el "engaño" recae en el sistema; recomendable tipo autónomo de manipulación de datos/sistemas con perjuicio.	Patrimonio (con C/I/D como medios)	Clave para PJ (e-commerce/fintech).
Arts. 12–13 PJ y sanciones	Régimen actual de PJ (ámbito taxativo, sanciones no privativas)	Parcial	Catálogo no incluye de forma clara los ciberdelitos nucleares; proponer extensión, criterios de beneficio e imputación por defecto de organización, y compliance como atenuante/eximente.	—	Urge alinear con Budapest: sanciones efectivas, proporcionales y disuasorias.
Arts. 14–15 Garantías / competencia	Reglas procesales generales	Sí	Marco general suficiente si se aplica con control judicial reforzado en medidas intrusivas (art. 24).	—	Indirecto para PJ (investigabilidad).
Arts. 16–17 Preservación rápida / revelación expedita	Órdenes de preservación y de identificación de abonados	Parcial	Necesario consolidar procedimientos ágiles y plazos; formación a fiscalías sobre formatos técnicos para proveedores.	—	Relevante para incidentes corporativos con terceros.
Art. 18 Órdenes de producción	Requerimientos de datos específicos	Sí/Parcial	Funciona si hay tipificación clara de datos (abonado, tráfico, contenido) y formatos estandarizados; riesgo de demoras con proveedores extranjeros.	—	Importante para trazabilidad en casos que involucren PJ.

Art. 19 Registro y aseguramiento de datos	Allanamiento lógico / incautación y copia forense	Sí	Priorizar imágenes forenses y hash; protocolos claros de minimización y segregación de datos no pertinentes.	—	Determina calidad probatoria frente a PJ.
Art. 20 Recolección en tiempo real de tráfico	Interceptación de tráfico (no contenido)	Parcial	Reforzar distinción tráfico vs. contenido, documentación de herramientas y trazabilidad; tiempos de respuesta de ISPs.	—	Impacta investigaciones con múltiples víctimas corporativas.
Art. 21 Intercepción de contenido	Interceptación de comunicaciones	Sí (con controles)	Exige control judicial y proporcionalidad estricta; mantener bitácoras y validaciones técnicas.	—	—
Arts. 23–25 Cooperación general / redes 24/7	Asistencia mutua / punto de contacto	Parcial	Asegurar punto 24/7 operativo y protocolos de preservación transfronteriza; métricas de plazo de respuesta.	—	Esencial cuando los datos residen fuera del país.
Arts. 26–29 Órdenes y registros transfronterizos	Cooperación con proveedores globales	Parcial	Estandarizar plantillas y bases jurídicas; uso de canales directos cuando existan; cuidar admisibilidad en sede local.	—	Casos con cloud / SaaS.
Arts. 30–35 Extradición / asistencia	Regímenes generales de cooperación	Sí/Parcial	Depende de tratados vigentes y de la tipificación espejo; coordinar prioridades en incidentes de alto impacto.	—	—

Nota: elaboración propia.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

En primer lugar, la presente investigación logró definir el concepto de ciberdelincuencia y los bienes jurídicos protegidos en este ámbito, cumpliendo así el primer objetivo específico. Se determinó que la ciberdelincuencia comprende aquellas conductas ilícitas cometidas mediante tecnologías de la información y comunicación o dirigidas contra sistemas informáticos, datos y activos digitales. Son delitos de naturaleza multidimensional, pues pueden lesionar diversos bienes jurídicos tradicionales (patrimonio, intimidad, integridad física, seguridad pública, etc.) a través de medios electrónicos, al igual que bienes de nueva índole eminentemente digitales.

En efecto, el estudio corroboró que la información y la seguridad de los sistemas informáticos emergen como bienes jurídicos fundamentales en la era digital, junto con la confidencialidad, integridad y disponibilidad de los datos. Se constató la existencia de un debate doctrinal sobre si la ciberdelincuencia afecta simplemente bienes jurídicos clásicos mediante medios informáticos o si introduce bienes jurídicos inéditos; no obstante, nuestros hallazgos indican que coexisten múltiples bienes jurídicos digitales dignos de tutela penal (por ejemplo, los datos personales, el correcto funcionamiento de sistemas computacionales, la privacidad en línea y la confianza en el comercio electrónico).

En síntesis, la ciberdelincuencia se definió operativamente como toda acción u omisión dolosa realizada en o por medio del ciberespacio que lesiona intereses jurídicos protegidos, siendo el ciberespacio un entorno que exige adaptaciones del Derecho Penal para resguardar eficazmente esos nuevos valores sociales. Esta clarificación conceptual estableció la base teórica necesaria para comprender los retos jurídicos posteriores, los cuales

evidencian que el Derecho Penal costarricense debe reconocer y proteger estos bienes jurídicos digitales con el mismo rigor que protege los bienes tradicionales.

En segundo lugar, en relación con el marco normativo vigente en Costa Rica y la identificación de vacíos, solapamientos y ambigüedades, la investigación ofreció un diagnóstico detallado (objetivo específico 2). Se examinó la evolución legislativa nacional, desde las reformas pioneras al Código Penal a inicios de los 2000 (como la Ley N.° 8148 de 2001, que introdujo los artículos 196 bis, 217 bis y 229 bis, entre otros, para tipificar delitos informáticos) hasta las modificaciones más recientes orientadas a fortalecer la lucha contra la ciberdelincuencia.

Los resultados muestran que Costa Rica ha avanzado significativamente en la tipificación de delitos informáticos, incorporando figuras como el acceso ilícito a sistemas, el daño o sabotaje informático, la suplantación de identidad digital, la estafa informática, la difusión de programas maliciosos e incluso modalidades específicas como la suplantación de sitios web (*phishing*) y la pornografía virtual. Estas adiciones han contribuido a cerrar brechas importantes en la legislación penal.

Sin embargo, el análisis evidenció la persistencia de ciertos vacíos legales y problemas de solapamiento normativo. Por ejemplo, algunas conductas delictivas propias del entorno digital podrían no estar explícitamente cubiertas por las disposiciones actuales o presentan definiciones imprecisas, lo que dificulta su aplicación.

Se advirtió que figuras penales tradicionales se superponen con nuevas tipificaciones informáticas, que generan ambigüedades sobre cuál norma aplicar en casos concretos (por ejemplo, fraudes convencionales vs. fraude informático, daño patrimonial vs. daño a sistemas informáticos). Asimismo, se identificó ambigüedad en conceptos técnicos-jurídicos empleados en la legislación: nociones como acceso no autorizado, manipulación informática

o programa malicioso" carecen de una definición legal uniforme, lo que puede dar lugar a interpretaciones dispares.

Un hallazgo crítico del diagnóstico fue la ausencia o limitación de la responsabilidad penal de las personas jurídicas en el contexto de la ciberdelincuencia: el ordenamiento costarricense hasta fechas recientes seguía el principio tradicional de *societas non delinquere potest*, por lo que las empresas no podían ser penalmente responsables de la mayoría de delitos, incluidos los informáticos.

Si bien en 2019 se promulgó la Ley N.° 9699 que introduce la responsabilidad penal de personas jurídicas, su alcance inicial se restringe a delitos de corrupción y algunas áreas específicas, dejando por fuera a los ciberdelitos. Esta laguna normativa implica que empresas que faciliten o no prevengan ataques informáticos (por acción u omisión grave) difícilmente enfrenten sanciones penales, lo que resulta incongruente con estándares internacionales. En conjunto, el estudio constató que el marco penal costarricense sufre un desfase respecto a la vertiginosa evolución tecnológica, presentando vacíos y ambigüedades que podrían ser explotados por delincuentes digitales.

Tal desfase normativo es comprensible dado el ritmo acelerado de aparición de nuevas formas de ciberdelito, pero subraya la necesidad de ajustes constantes. En definitiva, el segundo objetivo confirmó que, aunque la normativa patria ha progresado en materia de ciberdelincuencia, subsisten retos importantes de técnica legislativa: es preciso depurar el entramado legal para eliminar duplicidades, aclarar conceptos y llenar lagunas, asegurando así coherencia y eficacia en la aplicación de la ley penal frente a la delincuencia informática.

En tercer lugar, se contrastó la legislación costarricense con los estándares del Convenio de Budapest (objetivo específico 3), a fin de medir el grado de adecuación de nuestro ordenamiento a dicho instrumento internacional. El Convenio de Budapest (Consejo

de Europa, 2001) es el tratado marco en materia de ciberdelincuencia y establece estándares mínimos que los Estados adherentes deben implementar en sus legislaciones penales sustantivas y procesales. Costa Rica se adhirió formalmente a este convenio en 2017 y asumió el compromiso de armonizar su normativa interna con las disposiciones allí contenidas.

La investigación determinó que Costa Rica ha incorporado la mayoría de las tipificaciones exigidas por el Convenio de Budapest, especialmente, a través de la reforma integral del Título VII del Código Penal que creó la sección de "Delitos Informáticos y Conexos".

Nuestro código penal tipifica actualmente conductas contra la confidencialidad, integridad y disponibilidad de los sistemas y datos, tales como el acceso ilícito a sistemas informáticos, la interceptación o espionaje de información electrónica, la interferencia/daños a datos (borrado, alteración o destrucción de información), la interferencia a sistemas (sabotaje o entorpecimiento de servicios), el abuso de dispositivos informáticos (creación y difusión de malware, ataques de denegación de servicios, etc.), así como los delitos informáticos tradicionales previstos en el convenio: fraude informático, falsificación informática, delitos relacionados con pornografía infantil en línea e infracciones a la propiedad intelectual en entornos digitales.

En términos generales, puede afirmarse que la legislación penal costarricense vigente cumple en gran medida con las exigencias sustantivas del Convenio de Budapest, habiendo incluso tipificado figuras delictivas adicionales no contempladas expresamente en el tratado (por ejemplo, la suplantación de identidad en redes sociales y la creación de sitios web fraudulentos, que amplían la protección frente al phishing y otros engaños en línea más allá del mínimo convencional).

No obstante, el contraste también reveló áreas de mejora para alcanzar una plena conformidad con los estándares internacionales. En particular, se advirtió que ciertos tipos penales podrían requerir refinamiento o mayor precisión para alinearse totalmente con las definiciones del Convenio. Por ejemplo, la figura de interceptación ilícita de datos en tránsito –obligatoria según el artículo 3 del Convenio– no tiene un correlato inequívoco en nuestra normativa, pues si bien el espionaje informático castiga el apoderamiento de información industrial reservada, no existe un tipo general que sancione la interceptación per se de comunicaciones o datos privados durante su transmisión (fuera de supuestos tradicionales de violación de comunicaciones).

De igual forma, se identificó la necesidad de revisar las disposiciones sobre pornografía infantil en medios informáticos para asegurarse de que abarcan todas las conductas previstas internacionalmente (producción, distribución, posesión de material ilegal, incluidas representaciones virtuales o simuladas de menores, conforme a estándares avanzados). Un aspecto crítico es la ya mencionada responsabilidad de las personas jurídicas: el Convenio de Budapest exige a los Estados adoptar medidas para declarar responsables a entes jurídicos por delitos informáticos cometidos en su beneficio, algo que Costa Rica aún no ha implementado plenamente en el ámbito de los ciberdelitos.

Asimismo, más allá de los tipos penales, el Convenio impone estándares en materia procesal (por ejemplo, mecanismos de preservación rápida de datos, órdenes de entrega de información de suscriptores, facultades para interceptación legal de tráfico de datos, cooperación internacional expedita, etc.) que en nuestra legislación requieren desarrollos adicionales.

El estudio encontró que, si bien se han dado pasos importantes (como la creación de la Fiscalía Especializada en Cibercrimen y la participación en redes internacionales de

cooperación), todavía falta incorporar en la normativa interna todas las herramientas procesales modernas sugeridas por Budapest para la investigación eficiente de estos delitos transnacionales.

En conclusión, el contraste con el Convenio de Budapest evidenció que Costa Rica ha logrado significativos avances de convergencia normativa (convirtiéndose incluso en referente regional en algunos aspectos), pero persisten brechas que urge subsanar para garantizar un cumplimiento pleno del Convenio y, por ende, una respuesta penal verdaderamente integral frente a la ciberdelincuencia conforme a los más altos estándares internacionales.

Por último, la investigación revisó experiencias de derecho comparado y propuso pautas de técnica legislativa orientadas a fortalecer la respuesta jurídico-penal costarricense contra los ciberdelitos (objetivo específico 4). Este análisis comparativo que abarcó principalmente legislaciones de países pioneros en la materia y lineamientos supranacionales permitió extraer valiosas lecciones sobre mejores prácticas legislativas.

Se observaron modelos normativos de otras jurisdicciones (tanto de naciones europeas parte del Convenio de Budapest, como de países latinoamericanos que recientemente modernizaron sus leyes penales) para identificar qué estrategias han resultado efectivas al tipificar y perseguir delitos informáticos.

Entre los hallazgos comparados más relevantes, destaca la importancia de contar con marcos legales integrales y actualizados periódicamente. En varios países, la evolución legislativa no se ha limitado a reformas aisladas, sino que se han promulgado leyes especiales de ciberdelincuencia o capítulos completos dentro de sus códigos penales dedicados a estos ilícitos, acompañados de glosarios de términos técnicos. Estas experiencias sugieren que una

sistematización legislativa agrupando los delitos informáticos bajo principios comunes mejora la claridad y aplicabilidad de la ley, evitando la dispersión normativa.

Asimismo, se identificó como buena práctica la incorporación de definiciones legales precisas (por ejemplo, definir qué debe entenderse por "sistema informático", "dato informático", "programa malicioso", "documento electrónico" y otros conceptos técnicos), lo cual reduce la incertidumbre interpretativa y facilita el trabajo judicial. Otra pauta derivada del derecho comparado es la necesidad de asegurar la neutralidad tecnológica de las descripciones típicas: las leyes más eficaces utilizan un lenguaje amplio que trasciende tecnologías específicas, de modo que la norma siga siendo aplicable ante futuras innovaciones (evitando así que los delincuentes eludan la ley por meros cambios en la técnica empleada).

Igualmente, se observó en el derecho comparado una clara tendencia a prever la responsabilidad penal de las personas jurídicas en el ámbito de la delincuencia informática, ya sea mediante disposiciones generales en el código penal o a través de leyes especiales de responsabilidad corporativa que incluyen los ciberdelitos dentro de los ilícitos imputables a empresas. Esta medida, un estándar en muchos países desarrollados, busca incentivar a las corporaciones a adoptar medidas de seguridad y protocolos de prevención (*compliance*) so pena de enfrentar sanciones severas si sus sistemas son utilizados para delinquir. En cuanto a la técnica legislativa, el estudio resaltó la conveniencia de armonizar la legislación nacional con los instrumentos internacionales pertinentes.

Muchos países han tomado como base el texto del Convenio de Budapest para redactar sus tipos penales, lo que no solo asegura el cumplimiento de obligaciones convencionales sino que también facilita la cooperación jurídica internacional al hablar todos "un mismo idioma" legal en materia de ciberdelitos. Por otro lado, las experiencias

extranjeras enseñan que la redacción de nuevos delitos informáticos debe hacerse con proporcionalidad y prudencia: evitar sobrecriminalizar conductas que puedan solucionarse por vías menos drásticas (p. ej., sanciones administrativas en ciertos casos de uso indebido de datos) y respetar los derechos fundamentales en juego (libertad de expresión, derecho a la privacidad, etc.), para no comprometer garantías por combatir la ciberdelincuencia.

Los ejemplos comparados evidencian que una mala técnica legislativa puede derivar en normas inconstitucionales o inaplicables –verbigracia, leyes demasiado vagas que penalizan conductas difusas o tan estrictas que entorpecen el trabajo periodístico o la investigación académica–. Por fortuna, el análisis de casos ajenos proporcionó valiosas advertencias para no repetir errores legislativos en Costa Rica. En síntesis, este cuarto objetivo permitió delinear pautas concretas de mejora legislativa, basadas en evidencia comparada, orientadas a lograr una normativa penal coherente, moderna y eficaz frente a la ciberdelincuencia.

Estas pautas –que abarcan desde cómo redactar correctamente los tipos penales informáticos, cómo integrar la responsabilidad de personas jurídicas, hasta cómo garantizar la adaptación continua de la ley– sientan las bases de nuestras recomendaciones finales. De este modo, el capítulo de conclusiones refleja tanto el diagnóstico realizado (identificando las carencias y desafíos actuales) como las directrices para la reforma normativa, brindando una visión integradora de los hallazgos clave sobre responsabilidad penal corporativa, técnica legislativa, protección de bienes jurídicos digitales y cumplimiento del Convenio de Budapest, que son esenciales para cerrar la tesis con sólidas propuestas de mejora.

5.2 Recomendaciones

A la luz de las conclusiones expuestas, se plantean las siguientes recomendaciones para reforzar el marco jurídico-penal costarricense frente a la ciberdelincuencia, combinando soluciones normativas y de política criminal acordes con los estándares internacionales:

1. Consolidar y modernizar la legislación penal en materia de ciberdelincuencia: se recomienda emprender una reforma integral que sistematice los delitos informáticos en la legislación costarricense. Esto podría implicar la promulgación de una ley especial en delitos informáticos o, alternativamente, una reorganización del Código Penal creando un capítulo autónomo para ciberdelitos con numeración corrida (evitando el uso excesivo de artículos "bis", "ter", etc., que fragmentan la coherencia del código). Una compilación ordenada de las figuras penales informáticas facilitará su conocimiento y aplicación por jueces, fiscales y operadores jurídicos.

En este proceso de consolidación normativa, se deben eliminar solapamientos y lagunas detectadas, por ejemplo, aclarar la frontera entre delitos tradicionales y sus contrapartes informáticas para que cada conducta tenga un tipo penal único y claro, evitando duplicidades. También resulta conveniente actualizar o suprimir aquellas disposiciones obsoletas o inaplicables ante las nuevas tecnologías. Esta modernización legislativa debe realizarse con la asistencia de expertos en derecho penal y en seguridad de la información, garantizando que la norma resultante sea tecnológicamente neutra (aplicable a distintas plataformas y avances futuros) y armonizada con el Convenio de Budapest. El resultado esperado es un marco legal unificado, claro y contemporáneo, capaz de dar respuesta efectiva a las diversas manifestaciones de la ciberdelincuencia.

2. Introducir la responsabilidad penal de las personas jurídicas en los ciberdelitos: Una recomendación prioritaria es extender el régimen de responsabilidad penal corporativa para

abarcar los delitos informáticos. Dado que Costa Rica ya dio un primer paso con la Ley N.° 9699 de 2019 (enfocada en delitos de corrupción), se sugiere ampliar dicho régimen a los ciberdelitos previstos en el Código Penal, en cumplimiento de los compromisos del Convenio de Budapest. Esto implicaría reformar la legislación vigente para establecer que las empresas, sociedades y entes jurídicos puedan ser declarados penalmente responsables cuando, por falta de controles o por decisiones de sus órganos, se cometan delitos informáticos en su beneficio o mediante sus plataformas.

Junto a la atribución de responsabilidad, deberán preverse sanciones idóneas y proporcionales para las personas jurídicas, tales como multas elevadas calculadas sobre ingresos, suspensión de actividades, cancelación de licencias, inhabilitación para contratar con el Estado e incluso la disolución en casos extremos de uso deliberado de la empresa como vehículo del delito. Estas sanciones, más que punitivas en sí mismas, tienen un efecto disuasorio fundamental: motivar a las corporaciones a invertir en ciberseguridad, capacitación y cumplimiento para evitar incurrir en responsabilidad. Además, la reforma podría incentivar la adopción de programas internos de *compliance* digital, de modo que una empresa que demuestre haber implementado medidas eficaces de prevención y respuesta a incidentes informáticos pueda atenuar su eventual sanción. Incorporar la responsabilidad penal de personas jurídicas por ciberdelitos alineará a Costa Rica con la práctica internacional y cerrará la brecha actual que permite la impunidad corporativa en ataques informáticos de gran escala.

3. Perfeccionar la técnica legislativa mediante definiciones claras y tipificaciones precisas: como parte de las mejoras normativas, se aconseja incluir en la ley penal definiciones expresas de los términos técnicos más relevantes en ciberdelincuencia. Siguiendo las recomendaciones de la experiencia comparada, sería beneficioso añadir un artículo

preliminar (o una sección de definiciones) que explique conceptos como “sistema informático”, “datos informáticos”, “acceso no autorizado”, “interceptación de datos”, “programa informático malicioso (malware)”, “documento electrónico”, entre otros. Esto garantizará una interpretación uniforme de los tipos penales en todo el país y brindará seguridad jurídica tanto a operadores de justicia como a ciudadanos y empresas. Asimismo, en la redacción de las conductas delictivas, se recomienda emplear descripciones objetivas y acotadas para evitar términos ambiguos que puedan prestarse a confusión.

Cada delito debe estructurarse especificando con claridad el verbo rector (ej. “acceder”, “interceptar”, “dañar”, “suplantar”), el objeto material (sistema, datos, página web, etc.), la intención o propósito cuando sea relevante (p. ej., “con el fin de obtener un beneficio económico indebido” en el caso de fraudes informáticos) y las circunstancias agravantes o atenuantes aplicables. Una técnica legislativa depurada en este sentido ayudará a cerrar las brechas de interpretación que actualmente existen –por ejemplo, distinguiendo adecuadamente entre acceso ilegítimo e interceptación de datos, o entre daño informático simple y sabotaje informático agravado–.

Adicionalmente, se sugiere revisar las penas asignadas a cada delito informático, para asegurar que guardan proporción con la gravedad de la conducta y están en línea con los estándares internacionales. Ciertas conductas podrían ameritar un aumento de las sanciones (por ejemplo, ataques informáticos contra infraestructuras críticas o delitos que comprometen datos sensibles de muchas personas), mientras que otras quizás requieran penas diferenciadas según el daño efectivo causado. Ajustar las escalas penales contribuirá a una aplicación más justa y efectiva, evitando tanto la sobrepenalización de conductas menores como la subpenalización de ataques severos. En resumen, al perfeccionar la técnica legislativa con

definiciones claras y tipos penales bien delimitados, se fortalecerá la certeza y eficacia del Derecho Penal frente a los retos del ciberespacio.

4. Garantizar el pleno cumplimiento del Convenio de Budapest y otros instrumentos internacionales: se recomienda que el país tome las medidas necesarias para alcanzar la total conformidad con los requerimientos del Convenio de Budapest en todos sus extremos. En cuanto al Derecho Penal Sustantivo, además de los ajustes ya mencionados (nuevos delitos y responsabilidad de personas jurídicas), habría que verificar que ninguna conducta exigida por el Convenio quede sin tipificar. Si aún subsiste alguna laguna (por ejemplo, tipificar explícitamente la interceptación ilegítima de datos en comunicaciones privadas, de modo análogo a como está tipificado el acceso ilícito), debe subsanarse mediante la reforma. Por otro lado, en el ámbito procesal es imperativo actualizar el Código Procesal Penal o leyes especiales para introducir las herramientas investigativas modernas que prevé el Convenio: órdenes de preservación rápida de datos informáticos, facultades para la obtención expedita de registros de tráfico telemático, habilitar la interceptación legal de comunicaciones electrónicas con control judicial, medidas para la colaboración de los proveedores de servicios de Internet en las investigaciones, entre otras.

Si bien estas cuestiones trascienden el Derecho Penal Sustantivo, su implementación normativa resulta crucial para que las tipificaciones de ciberdelitos no sean letra muerta sino que puedan perseguirse eficazmente. Asimismo, se aconseja reforzar los mecanismos de cooperación internacional en la persecución del cibercrimen: designar formalmente (y dotar de recursos) el punto de contacto 24/7 establecido por el Convenio de Budapest, agilizar mediante acuerdos bilaterales o participación en redes como Interpol y Ameripol la asistencia judicial mutua en casos informáticos y capacitar al personal encargado de trámites de extradición o levantamiento de evidencia digital transfronteriza.

En complemento, Costa Rica debería ratificar los protocolos adicionales del Convenio (como el Segundo Protocolo Adicional relativo a la colaboración y obtención de pruebas electrónicas), tal como ya se ha avanzado en la Asamblea Legislativa para 2023, a fin de mantenerse a la vanguardia en la cooperación internacional contra la ciberdelincuencia.

El país debe entonces traducir su compromiso internacional en acciones legislativas concretas que aseguren un cumplimiento cabal del Convenio de Budapest, lo cual no solo evitará posibles responsabilidades por incumplimiento, sino que fortalecerá la capacidad nacional para prevenir, investigar y sancionar los delitos cibernéticos en un contexto globalizado.

5. Adoptar medidas de política criminal y capacitación acordes con la reforma legal: Finalmente, aunque va más allá del texto normativo, es indispensable acompañar los cambios legales con estrategias de política criminal integrales. Se recomienda establecer programas permanentes de capacitación especializada en ciberdelincuencia para fiscales, jueces, fuerzas de seguridad y peritos forenses, de manera que conozcan a profundidad las nuevas figuras penales y las herramientas técnicas para investigarlas. Solo con personal debidamente formado se logrará la aplicación efectiva de la ley y se evitarán errores en la interpretación de los novedosos tipos delictivos.

Asimismo, es pertinente fortalecer las unidades especializadas ya existentes (por ejemplo, la Fiscalía de Delitos Informáticos y el Centro de Respuesta a Incidentes de Seguridad Informática) dotándolas de mayores recursos tecnológicos y humanos, conforme aumente la complejidad y volumen de casos.

En el plano de prevención, el Estado debe impulsar campañas educativas para usuarios, empresas e instituciones sobre ciberseguridad básica y buenas prácticas, pues un componente importante de la lucha contra el cibercrimen es reducir la vulnerabilidad de

posibles víctimas y sistemas ante los ataques. De igual forma, se sugiere incentivar la colaboración público-privada, por ejemplo, marcos para que las empresas de tecnología informen prontamente de ciberataques o brechas, y para que compartan información con las autoridades sin temor a repercusiones legales injustas.

Estas medidas de política criminal, aunque extrapenales, son complementarias a la reforma legislativa y potencian sus efectos y aseguran que la normativa no opere en el vacío sino inserta en un entorno institucional capaz de aplicarla y en una sociedad consciente de su rol en la prevención.

Las recomendaciones anteriores conforman una propuesta normativa y de gestión integral para encarar los retos del derecho penal costarricense frente a la ciberdelincuencia. Se propone un equilibrio entre endurecer y clarificar el marco legal (con nuevos tipos penales, inclusión de sujetos responsables y mejoras de redacción) y fortalecer la aplicación práctica de dicho marco (mediante capacitación, cooperación y prevención).

Solo a través de este enfoque dual será posible cerrar las brechas identificadas en la tesis y dotar a Costa Rica de un sistema de justicia penal robusto, moderno y armonizado internacionalmente contra el cibercrimen. Al concluir este trabajo, queda enfatizado que el fenómeno de la ciberdelincuencia continuará evolucionando con la tecnología; por ende, el Derecho Penal Costarricense debe permanecer dinámico y vigilante, dispuesto a adaptar sus normas y estrategias conforme surjan nuevas amenazas en el ciberespacio.

Las conclusiones y recomendaciones aquí vertidas buscan servir de hoja de ruta para ese proceso continuo de mejora, de forma tal que nuestro país enfrente la ciberdelincuencia con claridad normativa, solidez argumentativa y eficacia operativa, protegiendo así los bienes jurídicos digitales y los derechos fundamentales de todas las personas en la sociedad de la información.

REFERENCIAS BIBLIOGRÁFICAS

Acurio Del Pino, S (2005). *Delitos Informáticos: generalidades.* https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf#:~:text=manipulaciones%20de%20datos%20que%20da,de%20los%20bancos%20de%20datos

Alfaro Ulate, D., & Rojas Rodríguez, M. (2022). *La imputación de la responsabilidad penal de la persona jurídica: un análisis crítico de la regulación costarricense* [Tesis de licenciatura, Universidad de Costa Rica]. Repositorio Institucional UCR.

Amato, M. I. (2024). Cibercrimen y delitos informáticos. *Revista Iberoamericana de Derecho, Cultura y Ambiente (RIDCA), (5)*, Derecho Penal y Criminología.

Asamblea Legislativa de la República de Costa Rica. (1970). *Código Penal, Ley N.º 4573*. Sistema Costarricense de Información Jurídica (SCIJ).

Asamblea Legislativa de la República de Costa Rica. (2001). *Ley N.º 8148. Adición de los artículos 196 bis, 217 bis y 229 bis al Código Penal*. SCIJ.

Asamblea Legislativa de la República de Costa Rica. (2017). *Aprobación de la Adhesión al Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest), Exp. N.º 18.484*. SCIJ.

Asamblea Legislativa de la República de Costa Rica. (2019). *Ley N.º 6999. Responsabilidad de las personas jurídicas sobre cohechos domésticos, soborno transnacional y otros delitos*

Asamblea Legislativa. (2005). Ley N.° 8454, Ley de Certificados, Firmas Digitales y Documentos Electrónicos. *La Gaceta*, Costa Rica.

Asamblea Legislativa. (2011). Ley N.° 8968, Protección de la Persona frente al Tratamiento de sus Datos Personales. *La Gaceta*, Costa Rica.

Asamblea Nacional Constituyente (1949). Constitución Política de la República de Costa Rica. San José, Costa Rica.

Bautista Landaeta, L., & Perche Fuenmayor, Y. (2021). Responsabilidad penal de la persona jurídica por delitos informáticos en Venezuela [Tesis de Maestría]. *Universidad Internacional de La Rioja (UNIR)*.

Bolaños Jaimes, M. (s. f.). *Los ciberdelitos: retos que enfrenta el Código Penal en Costa Rica* [Tesis de licenciatura, ULACIT]. Repositorio Institucional ULACIT. https://repositorio.ulacit.ac.cr/bitstream/handle/20.500.14230/7282/011428.pdf?isAllowed=y&sequence=1

Bonilla Rodríguez, P. (2019). El espectro actual de los delitos informáticos. *Revista Judicial, Poder Judicial de Costa Rica, (126)*, 220–225.

Březinová, K. (2017). *Company criminal liability for unlawful attacks against information systems within the scope of EU law* (Charles University in Prague, Faculty of Law Research Paper No. 2017/II/3). Charles University.

Consejo de Europa. (2001). *Convenio sobre la Ciberdelincuencia (Budapest)*. (Referencia a arts. 12 y 13). Enlace oficial citado por la doctrina nacional.

Council of Europe. (2001). Convention on Cybercrime (ETS No. 185). Strasbourg: Council of Europe. [Costa Rica: adhesión 22/09/2017; entrada en vigor 01/01/2018].

Elizondo Alfaro, L. A. (2021). *Implicaciones penales de la aplicación del Convenio de Budapest en el ordenamiento jurídico costarricense: un análisis de acuerdo con el derecho comparado* [Tesis de licenciatura, Universidad de Costa Rica]. Facultad de Derecho, Universidad de Costa Rica.

Esquivel Alpízar, C., & Romero Salmerón, A. (2021). *Delitos informáticos en la actualidad costarricense* [Tesis de licenciatura, Universidad de Costa Rica]. Universidad de Costa Rica.

Fernández, R. (2024). La responsabilidad penal de la persona jurídica en Costa Rica. *Revista del Poder Judicial*, 18(2), 45–70. https://pjenlinea3.poder-judicial.go.cr/biblioteca/uploads/Archivos/Articulo/RESPONSABILIDAD%20PENAL%20FERNANDEZ.pdf

Freire Altamirano, J. E., Villalobos Cisneros, M. V., Morales Herrera, J. L., Nieves Licoa, L. S., & Colon Ferruzola Gomez, E. (2024). La responsabilidad penal derivada de los delitos de apropiación ilícita a través de medios electrónicos. *Sinergia Académica, 7*(Esp. 7), 1–?.

Fundación Paniamor. (2023). *Análisis del marco legal y propuestas de reforma para una acción pública y privada contra los delitos cibernéticos*. San José.

García Chaves, A. (2022, 22 de noviembre). *Comentario al artículo 236 del Código Penal*. vLex. https://vlex.co.cr/vid/comentario-articulo-236-codigo-1025830533?utm_source=

González Rivera, M (2022). Suplantación de identidad https://diccionariousual.poderjudicial.go.cr/index.php/diccionario/suplantaci%C3%B3n-de-p%C3%A1ginas-electr%C3%B3nicas (Accedido el 25 de octubre, 2025). https://www.google.com/search?q=Suplantaci%C3%B3n+de+identidad&oq=Suplantaci%C3%B3n+de+identidad+&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIMCAEQABhDGIAEGIoFMgcIAhAAGIAEMgcIAxAAGIAEMgcIBBAAGIAEMgcIBRAAGIAEMgcIBhAAGIAEMgcIBxAAGIAEMgcICBAAGIAEMgcICRAAGIAE0gEJMTgyMGowajE1qAIIsAIB8QXdnuA7bssfiQ&sourceid=chrome&ie=UTF-8

International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection: Information security management systems — Requirements. Geneva: ISO.

Jiménez Mora, L., & Merayo Ramírez, P. (2017). *Los ciberataques en el marco de la responsabilidad internacional de los Estados en tiempos de paz* [Tesis de licenciatura, Universidad de Costa Rica]. Corte Interamericana de Derechos Humanos. https://www.corteidh.or.cr/tablas/33456.pdf

Mayer Lux, L. (2017). El bien jurídico protegido en los delitos informáticos. *Revista Chilena de Derecho, 44*(1), 31–59. https://doi.org/10.4067/S0718-34372017000100011

Millán López, E. (2023). *Delitos informáticos: situación actual, acceso ilícito y responsabilidad penal de las personas jurídicas* [Tesis de licenciatura, Universidad de Valladolid]. Repositorio de la Universidad de Valladolid.

Moreno-Piedrahíta Hernández, C. (2019). El ocaso de los modelos de responsabilidad penal de las personas jurídicas en la jurisprudencia y doctrina españolas. *Política Criminal, 14*(28), 323–354. https://doi.org/10.4067/S0718-33992019000200323

Naciones Unidas. (2000). *Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía*. Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos.

National Institute of Standards and Technology. (2024). NIST Cybersecurity Framework 2.0. Gaithersburg, MD: U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29 (si no usás DOI, podés citar la página oficial de NIST).

OWASP Foundation. (2021). OWASP Top 10: Web Application Security Risks. https://owasp.org/www-project-top-ten/

PANI – Patronato Nacional de la Infancia. (2023, 13 de noviembre). *En el Día Nacional de la lucha contra el grooming presentan campaña educativa* (incluye datos OIJ 2017–2023). https://pani.go.cr/en-el-dia-nacional-de-la-lucha-contra-el-grooming-presentan-campana-educativa/

Poder Ejecutivo de la República de Costa Rica. (2017). *Convenio sobre la Ciberdelincuencia (Budapest), Decreto N.º 40546-MP-MIDEPLAN-RREE*. SCIJ.

Poder Judicial de la República de Costa Rica. (2025) diccionario

Real Academia Española & Consejo General del Poder Judicial. (2001). *Sistema informático*. En *Diccionario panhispánico del español jurídico (DPEJ)*. https://dpej.rae.es/lema/sistema-informático

Real Academia Española & Consejo General del Poder Judicial. (s. f.). *Dato informático*. En *Diccionario panhispánico del español jurídico (DPEJ)*. https://dpej.rae.es/lema/dato-informático

Riffo, F. (2023, 14 de septiembre). Ciberseguridad: cuando la responsabilidad depende de la jurisdicción. *Idealex Press*. https://idealex.press/ciberseguridad-empresas-dependen-de-la-jurisdiccion/

Rojas Salas, M. (2023). El "Child Grooming" como conducta típica en el Código Penal: su regulación legislativa en Costa Rica ["Child Grooming" as a typical conduct in the Criminal Code: its legislative regulation in Costa Rica]. *Revista de Ciencias Jurídicas*, (162), 1–31.

Rote, N., Bhardwaj, S., & Sebastian, A. (2025). Corporate criminal liability for AI-induced cybersecurity failures in healthcare systems. *Lex Localis – Journal of Local Self-Government, 23*(S1), 95–106. https://lex-localis.org/index.php/LexLocalis/article/view/800212/1167

Ruiz, Paula (2019, 6 enero). Producir y difundir fake news podría llevarlo a la cárcel. https://www.crhoy.com/producir-y-difundir-fake-news-podria-llevarlo-a-la-carcel/

Santana Grimaldi, G. (2022, 20 de julio). Distintos modelos de imputación penal de las personas jurídicas (I). *Acento*. https://acento.com.do/opinion/los-distintos-modelos-de-imputacion-penal-de-las-personas-juridicas-i-9084359.html

Siles Andrei. (2023, 5 octubre). *Ahora pueden robarle todo su dinero al escanear un código QR engañoso en sitios públicos*. La República. https://www.larepublica.net/noticia/ahora-pueden-robarle-todo-su-dinero-al-escanear-un-codigo-qr-enganoso-en-sitios-publicos

Universidad Central (UC). (2020). *Instructivo de modalidad Trabajo Final de Graduación (TFG), Versión 3*. Departamento de Investigación. (Criterios sobre Cap. I, estructura y estilo APA).