

# Delincuencia digital organizada y responsabilidad penal empresarial:

transformaciones criminológicas,  
modelos de atribución y desafíos  
regulatorios

## AUTORES



Nayrud Suarez Sanchez



Teódulo Jenaro Santos Cruz



Jorge Luis Cueva Zavaleta



Diógenes Arquímedes  
Jiménez Domínguez



Jorge David Ríos Gonzales

*“Tecnología, derecho  
y ética para un entorno  
digital más seguro”*



## ***Autores***

---

### ***Nayrud Suarez Sanchez***

Doctora en Derecho y Ciencias Políticas  
Docente de la Facultad de Derecho y Ciencias  
Políticas  
Universidad Nacional de Trujillo

 [nsuarezs@unitru.edu.pe](mailto:nsuarezs@unitru.edu.pe)  
 <https://orcid.org/0000-0002-4189-3496>

### ***Teódulo Jenaro Santos Cruz***

Doctor en Derecho. Doctor en Planificación y  
Gestión  
Docente de la Facultad de Derecho y  
Ciencias Políticas  
Universidad Nacional de Trujillo

 [tsantos@unitru.edu.pe](mailto:tsantos@unitru.edu.pe)  
 <https://orcid.org/0000-0002-7679-2273>

---

### ***Jorge Luis Cueva Zavaleta***

Doctor en Derecho y en Gestión Pública  
Docente de la Facultad de Derecho y Ciencias  
Políticas  
Universidad Nacional de Trujillo

 [jcueva@unitru.edu.pe](mailto:jcueva@unitru.edu.pe)  
 <https://orcid.org/0000-0001-9175-856X>

### ***Diógenes Arquímedes Jiménez Domínguez***

Doctor en Derecho  
Docente en la Escuela de Posgrado  
Universidad Nacional de Trujillo

 [djimenezd@unitru.edu.pe](mailto:djimenezd@unitru.edu.pe)  
 <https://orcid.org/0000-0002-5298-4078>

---

### ***Jorge David Ríos Gonzales***

Magister en Educación  
Docente  
Universidad Nacional de Trujillo

 [jriosg@unitru.edu.pe](mailto:jriosg@unitru.edu.pe)  
 <https://orcid.org/0000-0001-6073-0804>

---

**Editor:** Alain Fitzgerald Castro Alfaro

**Título:**

Delincuencia digital organizada y responsabilidad penal empresarial: transformaciones criminológicas, modelos de atribución y desafíos regulatorios

**Autores:** Nayrud Suarez Sanchez, Teódulo Jenaro Santos Cruz, Jorge Luis Cueva Zavaleta, Diógenes Arquímedes Jiménez Domínguez, Jorge David Ríos Gonzales

**ISBN Versión Digital:** 978-628-97866-1-3

**Sello Editorial:**

Editorial Centro de Investigaciones y Capacitaciones Interdisciplinares SAS – CICI

**Coordinadora:** Nora González Pérez –Cartagena –Colombia

**Portada:** Linda Castro González

**Diagramación:** Alain Castro González

Prohibida la reproducción total o parcial por cualquier medio sin la autorización escrita del titular de los derechos patrimoniales

Esta obra está bajo una licencia Creative Commons – Atribución – No comercial – Sin Derivar 4.0 internacional

[https://co.creativecommons.org/?page\\_id=13](https://co.creativecommons.org/?page_id=13)



Cartagena –Colombia, Septiembre 2026

**DELINCUENCIA DIGITAL ORGANIZADA Y  
RESPONSABILIDAD PENAL EMPRESARIAL:  
TRANSFORMACIONES CRIMINOLÓGICAS, MODELOS DE  
ATRIBUCIÓN Y DESAFÍOS REGULATORIOS**

*Nayrud Suarez Sanchez*

*Teódulo Jenaro Santos Cruz*

*Jorge Luis Cueva Zavaleta*

*Jiménez Domínguez Diógenes Arquímedes*

*Jorge David Ríos Gonzales*

**Colombia  
Latinoamérica**

**2026**

# Contenido

|                                                                                |    |
|--------------------------------------------------------------------------------|----|
| RESUMEN .....                                                                  | 6  |
| CAPÍTULO I: INTRODUCCIÓN.....                                                  | 9  |
| CAPÍTULO II: METODOLOGÍA .....                                                 | 16 |
| CAPÍTULO III: RESULTADOS.....                                                  | 21 |
| 3.1. Caracterización del corpus documental .....                               | 21 |
| 3.2. Estructura temática de la producción científica .....                     | 22 |
| 3.3. Reconfiguración de la delincuencia organizada en el entorno digital ..... | 24 |
| 3.4. Manifestaciones de la delincuencia digital organizada .....               | 27 |
| 3.5. Fundamentos y modelos de responsabilidad penal empresarial .....          | 29 |
| 3.6. Tecnología, riesgo penal y cumplimiento corporativo .....                 | 33 |
| 3.7. Desafíos regulatorios, consensos y vacíos de conocimiento .....           | 35 |
| CAPÍTULO IV: DISCUSIÓN .....                                                   | 39 |
| CAPITULO V CONCLUSIONES Y RECOMENDACIONES .....                                | 46 |
| 5.1. CONCLUSIONES.....                                                         | 46 |
| 5.2. RECOMENDACIONES .....                                                     | 48 |

## RESUMEN

La delincuencia digital organizada ha transformado las estructuras, operaciones y mecanismos de coordinación de las redes criminales, planteando nuevas dificultades para atribuir responsabilidad penal a las empresas. Esta revisión narrativa tuvo como objetivo analizar la producción científica publicada entre 2022 y abril de 2026 sobre las transformaciones criminológicas, los modelos de atribución empresarial y los desafíos regulatorios asociados. Se consultaron Scopus, Web of Science y SciELO; de 558 registros identificados, 51 publicaciones integraron el corpus final, tras el cribado y la eliminación de duplicados. Los resultados evidenciaron el tránsito hacia redes flexibles, transnacionales, especializadas y tecnológicamente mediadas, vinculadas con ransomware, fraude empresarial, mercados clandestinos, criptomonedas y lavado de activos. Asimismo, los modelos tradicionales de responsabilidad vicaria e identificación mostraron limitaciones frente a decisiones fragmentadas y sistemas automatizados, mientras que el defecto de organización y la cultura corporativa ofrecieron criterios más adecuados para valorar riesgos previsibles, capacidad de control y medidas preventivas. Se concluye que la responsabilidad empresarial requiere articular la estructura funcional del delito con los deberes corporativos de prevención, evitando imputaciones automáticas. El estudio se relaciona con el ODS 16, al promover instituciones eficaces, cooperación internacional, acceso a la justicia y respuestas jurídicas frente a la criminalidad digital transnacional.

**Palabras clave:** delincuencia; derecho penal; empresa; tecnología de la información; cooperación internacional.

## ABSTRACT

Digital organized crime has transformed the structures, operations, and coordination mechanisms of criminal networks, creating new difficulties for attributing criminal liability to corporations. This narrative review aimed to analyze literature published between 2022 and April 2026 concerning criminological transformations, models of corporate attribution, and regulatory challenges. Scopus, Web of Science, and SciELO were searched; of 558 records identified, 51 publications formed the final corpus after screening and duplicate removal. The findings revealed a shift toward flexible, transnational, specialized, and technologically mediated networks associated with ransomware, corporate fraud, illicit markets, cryptocurrencies, and money laundering. Traditional models based on vicarious liability and identification also showed limitations when applied to fragmented decision-making and automated systems, whereas organizational failure and corporate culture provided more suitable criteria for assessing foreseeable risks, capacity for control, and preventive measures. The review concludes that corporate criminal liability requires linking the functional structure of criminal activity with corporate duties of prevention while avoiding automatic attribution. The study contributes to Sustainable Development Goal 16 by promoting effective institutions, international cooperation, access to justice, and legally sound responses to transnational digital crime. It highlights the need for harmonized evidentiary standards and risk-based compliance mechanisms adapted to contemporary technological and organizational complexity.

**Keywords:** crime; criminal law; enterprises; information technology; international cooperation.

# Capítulo I

## INTRODUCCION

## CAPÍTULO I: INTRODUCCIÓN

La expansión de las tecnologías digitales ha modificado profundamente las condiciones en que se planifican, coordinan y ejecutan las actividades delictivas organizadas. El ciberespacio no constituye únicamente un nuevo escenario para reproducir conductas criminales tradicionales, sino un entorno que facilita la aparición de estructuras flexibles, transnacionales y tecnológicamente especializadas, capaces de operar simultáneamente en espacios físicos y virtuales. Esta convergencia ha debilitado las fronteras conceptuales entre delincuencia organizada, ciberdelincuencia y criminalidad empresarial, debido a que los grupos delictivos pueden emplear plataformas digitales, sistemas automatizados, criptomonedas y redes descentralizadas para distribuir funciones, ocultar identidades y movilizar recursos ilícitos. En ese sentido, Di Nicola (2022) sostiene que la sociedad digital exige reconsiderar las categorías criminológicas utilizadas para interpretar la organización criminal, mientras que Lavorgna y Antonopoulos (2022) señalan que el ciberespacio ha favorecido la formación de mercados y redes criminales cuyas dinámicas superan los modelos territoriales convencionales. Por consiguiente, comprender la delincuencia digital organizada requiere una perspectiva panorámica que integre sus transformaciones estructurales, sus manifestaciones operativas y las respuestas jurídicas dirigidas a las organizaciones empresariales.

A diferencia de las organizaciones criminales tradicionales, comúnmente asociadas con jerarquías estables, control territorial, violencia y relaciones personales de confianza, las agrupaciones que operan en entornos digitales suelen estructurarse mediante redes horizontales, temporales y especializadas. Sus integrantes pueden encontrarse en diferentes países, utilizar identidades anónimas o seudónimas y asumir funciones específicas sin conocerse personalmente, lo que favorece la adaptabilidad y dificulta la identificación de sus niveles de dirección y pertenencia. Whelan et al. (2023) advierten que la aplicación rígida de las definiciones clásicas de delincuencia organizada puede excluir indebidamente a grupos dedicados al ransomware, pese a que presentan continuidad, coordinación, finalidad lucrativa y mecanismos propios de gobernanza. De manera complementaria, Di Nicola et al. (2025) identifican la colaboración, la permanencia, la orientación económica y la organización en red

como elementos recurrentes de estas agrupaciones, aunque la violencia, la corrupción y las pretensiones monopólicas aparezcan con menor frecuencia. Estas particularidades justifican una comprensión más flexible de la criminalidad organizada, basada en un continuo físico-digital y no exclusivamente en los rasgos históricos de las organizaciones mafiosas.

La delincuencia digital organizada se manifiesta mediante actividades diversas que combinan conocimientos técnicos, distribución especializada de funciones y mecanismos destinados a ocultar los beneficios ilícitos. Entre sus expresiones más relevantes se encuentran el ransomware, el fraude por compromiso del correo electrónico empresarial, la comercialización de bienes y servicios ilegales en mercados clandestinos, el robo de información, la extorsión digital y el lavado de activos mediante criptomonedas. Botchkovar et al. (2025) evidencian que los grupos de ransomware desarrollan actividades coordinadas y redes funcionales que les permiten distribuir tareas, mantener operaciones continuas y ampliar el alcance de sus ataques. Asimismo, Lazarus (2024) identifica que las redes dedicadas al fraude por correo electrónico empresarial operan mediante estructuras horizontales y adaptativas, caracterizadas por la colaboración, la especialización y las conexiones transnacionales. A ello se suma el empleo de criptoactivos, que facilita la transferencia y el encubrimiento de fondos ilícitos en distintas jurisdicciones, generando nuevas oportunidades para la criminalidad financiera (Trozze et al., 2022). Estas modalidades revelan que la tecnología no solo sirve como instrumento del delito, sino que transforma su organización, rentabilidad y capacidad de permanencia.

El carácter transnacional de la delincuencia digital organizada constituye uno de los principales obstáculos para su investigación y persecución, pues los autores, las víctimas, las infraestructuras tecnológicas y los recursos económicos pueden encontrarse distribuidos en diferentes jurisdicciones. El anonimato o seudonimato, la comunicación cifrada y la descentralización de las operaciones reducen la necesidad de contacto presencial y permiten que los integrantes de una red criminal colaboren a distancia, reorganicen rápidamente sus funciones y sustituyan a sus participantes cuando alguno es identificado. Lusthaus et al. (2023) sostienen que las redes cibercriminales se articulan mediante relaciones de cooperación que trascienden las fronteras nacionales y mantienen conexiones con actores externos

indispensables para ejecutar o monetizar los delitos. En concordancia, Lutovac y Lutovac (2022) señalan que las tecnologías digitales favorecen el ocultamiento de la identidad y dificultan la actuación aislada de las autoridades nacionales. Además, la confianza interpersonal puede ser reemplazada parcialmente por protocolos criptográficos y mecanismos tecnológicos de verificación, incrementando la resiliencia de estas estructuras frente a las acciones estatales (Hartmann, 2025). Estas condiciones evidencian la necesidad de fortalecer la cooperación internacional y armonizar las respuestas jurídicas frente a operaciones criminales que no respetan límites territoriales.

Las empresas ocupan una posición ambivalente frente a la delincuencia digital organizada, debido a que pueden convertirse en víctimas de ataques, facilitar involuntariamente su ejecución o constituir espacios desde los cuales se desarrollan y encubren actividades ilícitas. La dependencia de infraestructuras digitales, servicios en la nube, sistemas automatizados, inteligencia artificial y redes de terceros amplía la superficie de exposición y genera riesgos vinculados con accesos no autorizados, filtraciones de información, fraudes financieros y paralización de operaciones. Aslan et al. (2023) advierten que la diversidad de vulnerabilidades y amenazas cibernéticas exige adoptar medidas integrales de protección, puesto que las deficiencias técnicas pueden comprometer tanto los activos empresariales como los datos de clientes y usuarios. Estas vulnerabilidades adquieren relevancia penal cuando los daños se relacionan con decisiones corporativas, controles insuficientes o incumplimientos graves de los deberes de seguridad y supervisión. Al respecto, Rote et al. (2025) analizan la posibilidad de atribuir responsabilidad penal a las empresas por fallas de ciberseguridad inducidas por sistemas de inteligencia artificial, especialmente cuando afectan sectores sensibles. En consecuencia, la respuesta jurídica debe diferenciar entre la empresa afectada por una organización criminal y aquella cuya estructura, cultura o deficiente control contribuye a la producción del delito.

La responsabilidad penal empresarial surge de la necesidad de responder jurídicamente a los delitos cometidos dentro de estructuras organizacionales complejas, en las cuales la fragmentación de decisiones y funciones dificulta identificar a una única persona como responsable de la conducta. La actuación empresarial puede generar riesgos colectivos y

facilitar la comisión de delitos cuando existen políticas deficientes, controles ineficaces o prácticas corporativas orientadas a tolerar, ocultar o aprovechar comportamientos ilícitos. Vuletić (2023) señala que los sistemas contemporáneos de responsabilidad penal corporativa buscan superar las limitaciones de un derecho penal centrado exclusivamente en la persona natural, aunque su aplicación continúa planteando dificultades relacionadas con los criterios de imputación y la conexión entre el individuo y la organización. En este debate, la atribución basada en los actos de empleados o agentes permite responsabilizar a la empresa por conductas realizadas en el ejercicio de funciones corporativas y en beneficio de la entidad, pero exige determinar bajo qué condiciones resulta legítima dicha transferencia (Silver, 2023). Por ello, la responsabilidad empresarial no debería fundamentarse únicamente en la pertenencia del autor a la organización, sino en la existencia de una relación verificable entre el delito, el funcionamiento corporativo y el incumplimiento de los deberes de prevención y control.

Los ordenamientos jurídicos han desarrollado diferentes modelos para atribuir responsabilidad penal a las personas jurídicas, entre los que destacan la responsabilidad vicaria, la identificación de los órganos directivos, el defecto de organización y la cultura corporativa. La responsabilidad vicaria traslada a la empresa las consecuencias derivadas de los delitos cometidos por sus representantes o trabajadores en el ejercicio de sus funciones y con la finalidad de beneficiarla, aunque puede resultar insuficiente cuando la conducta surge de decisiones fragmentadas o actuaciones descentralizadas. Kurniawan y Hapsari (2022) explican que este modelo permite vincular la actuación individual con la responsabilidad corporativa, pero requiere delimitar la relación funcional entre el autor y la persona jurídica. Por su parte, Ali et al. (2023) destacan que la cultura corporativa puede emplearse para demostrar el componente subjetivo de la responsabilidad cuando las políticas, prácticas o tolerancias institucionales favorecen el incumplimiento de la ley. Estas aproximaciones se complementan con el modelo de defecto de organización, que centra la imputación en la ausencia o ineficacia de controles preventivos. Sin embargo, la coexistencia de distintos criterios entre jurisdicciones continúa dificultando una respuesta uniforme frente a delitos digitales transnacionales (Zazzaro, 2025).

La atribución de responsabilidad penal empresarial frente a la delincuencia digital organizada enfrenta importantes limitaciones regulatorias y probatorias. La dispersión territorial de los participantes, la utilización de identidades ficticias, el cifrado de las comunicaciones y la circulación de activos por múltiples plataformas dificultan reconstruir la secuencia delictiva y establecer la intervención de cada persona u organización. Estas dificultades se intensifican cuando las transacciones se realizan mediante criptomonedas o servicios digitales administrados desde jurisdicciones con regulaciones divergentes. Anggriawan y Susila (2024) señalan que la vinculación de los criptoactivos con el lavado de dinero y el financiamiento ilícito exige fortalecer los mecanismos de identificación, trazabilidad y supervisión conforme a estándares internacionales. Del mismo modo, Subbagari (2023) advierte que las transformaciones tecnológicas demandan actualizar las medidas destinadas a combatir el lavado de activos en el entorno digital. En el ámbito empresarial, no basta con demostrar que un sistema, empleado o directivo participó en el hecho; también debe acreditarse el beneficio corporativo, el incumplimiento de deberes de control o la existencia de una política organizacional favorecedora del delito. Por tanto, la ausencia de criterios armonizados puede producir vacíos de imputación y respuestas jurídicas fragmentadas ante operaciones de alcance transnacional.

La literatura reciente evidencia avances importantes en la conceptualización de la delincuencia digital organizada y en el análisis de los sistemas de responsabilidad penal empresarial; sin embargo, ambos campos suelen desarrollarse de manera paralela. Por una parte, las investigaciones criminológicas se concentran en explicar la estructura, continuidad y capacidad adaptativa de las redes cibercriminales, así como la necesidad de superar definiciones sustentadas exclusivamente en jerarquía, violencia y control territorial (Di Nicola, 2022; Whelan et al., 2023). Por otra, los estudios jurídicos examinan los modelos utilizados para responsabilizar a las personas jurídicas, las diferencias entre ordenamientos nacionales y la progresiva incorporación de reglas supranacionales sobre responsabilidad corporativa (Vuletić, 2023; Zazzaro, 2025). Aunque algunas publicaciones comienzan a vincular la responsabilidad empresarial con fallas de ciberseguridad y sistemas de inteligencia artificial, esta articulación todavía es limitada (Rote et al., 2025). En consecuencia, persiste una brecha respecto de cómo

atribuir responsabilidad penal a una empresa cuando el delito digital se ejecuta mediante redes descentralizadas, servicios tercerizados, decisiones automatizadas o deficiencias organizacionales distribuidas, sin que resulte claramente identificable una única persona natural que concentre el dominio de la conducta.

Frente a esta brecha, resulta necesario integrar los aportes criminológicos y jurídicos para comprender de qué manera las transformaciones de la criminalidad organizada afectan los fundamentos y criterios de imputación aplicables a las empresas. El reconocimiento de un continuo físico-digital permite analizar organizaciones que combinan redes humanas, infraestructuras tecnológicas y mecanismos automatizados, sin exigir que reproduzcan las características de las estructuras criminales tradicionales (Di Nicola et al., 2025). Paralelamente, el fortalecimiento de la responsabilidad empresarial requiere examinar la cultura corporativa, los defectos de organización y la eficacia de los programas de cumplimiento como elementos relevantes para prevenir y atribuir conductas delictivas (Aguilera Gordillo, 2024; Zazzaro, 2025). En este contexto, la presente revisión narrativa tiene como objetivo analizar la producción científica publicada entre 2022 y 2026 sobre la delincuencia digital organizada y la responsabilidad penal empresarial, identificando sus transformaciones criminológicas, principales manifestaciones, modelos de atribución y desafíos regulatorios. Para ello, la literatura se organiza en ejes conceptuales y jurídicos que permiten reconocer consensos, divergencias y vacíos, con la finalidad de construir una visión articulada del problema y aportar fundamentos para el desarrollo de respuestas penales compatibles con la complejidad de la criminalidad digital contemporánea.

# Capítulo II

## METODOLOGÍA

## CAPÍTULO II: METODOLOGÍA

El estudio se desarrolló mediante una revisión narrativa de la literatura, con enfoque cualitativo y diseño documental, orientada a integrar y analizar críticamente el conocimiento científico relacionado con la delincuencia digital organizada y la responsabilidad penal empresarial. Este tipo de revisión se consideró pertinente porque permitió examinar aportes procedentes de la criminología, el derecho penal, los estudios sobre ciberdelincuencia y la regulación corporativa, cuyos fundamentos conceptuales y metodológicos presentan una marcada heterogeneidad. A diferencia de una revisión centrada únicamente en la cuantificación de resultados, el enfoque narrativo facilitó la comparación de perspectivas teóricas, modelos jurídicos y hallazgos empíricos, así como la identificación de consensos, divergencias, tendencias emergentes y vacíos de conocimiento. El proceso comprendió la búsqueda, selección, evaluación crítica, extracción y síntesis temática de las publicaciones, procurando mantener criterios explícitos y reproducibles durante cada etapa. La revisión se delimitó a estudios publicados entre enero de 2022 y abril de 2026, en concordancia con el propósito de examinar las transformaciones recientes de la delincuencia organizada en entornos digitales y sus implicancias para la atribución de responsabilidad penal a las personas jurídicas.

La búsqueda bibliográfica se realizó durante abril de 2026 en las bases de datos Scopus, Web of Science y SciELO, seleccionadas por su cobertura multidisciplinaria y por la inclusión de publicaciones vinculadas con las ciencias jurídicas, la criminología, la ciberdelincuencia y los estudios organizacionales. Scopus y Web of Science permitieron recuperar literatura internacional publicada en revistas científicas indexadas, mientras que SciELO favoreció la identificación de investigaciones desarrolladas en contextos iberoamericanos. La búsqueda comprendió artículos publicados en inglés y español, debido a que ambos idiomas concentraban la producción científica más pertinente para los propósitos de la revisión. Los registros recuperados fueron organizados inicialmente en tres bases temáticas: delincuencia digital organizada, responsabilidad penal empresarial y estudios que articulaban ambos

campos. Posteriormente, la información bibliográfica fue consolidada en una matriz maestra de extracción y evaluación, en la que se registraron el título, autoría, año, revista, DOI, resumen, principales aportes y relación con el objetivo de la revisión. Esta organización permitió comparar los documentos recuperados, detectar coincidencias entre las bases consultadas y mantener la trazabilidad del proceso de selección y análisis.

La estrategia de búsqueda se construyó mediante términos controlados y palabras clave en español e inglés relacionadas con los dos núcleos temáticos de la revisión. Para la delincuencia digital organizada se utilizaron expresiones como “delincuencia digital organizada”, “ciberdelincuencia organizada”, “crimen organizado digital”, “organized cybercrime”, “digital organized crime” y “cybercriminal networks”. Para la responsabilidad penal empresarial se emplearon los términos “responsabilidad penal empresarial”, “responsabilidad penal corporativa”, “responsabilidad penal de las personas jurídicas”, “corporate criminal liability” y “criminal liability of legal persons”. Los descriptores se combinaron mediante los operadores booleanos AND y OR, incluyendo búsquedas integradas como (“organized cybercrime” OR “digital organized crime”) AND (“corporate criminal liability” OR “criminal liability of legal persons”). La sintaxis fue adaptada a las características de Scopus, Web of Science y SciELO, aplicándose filtros por periodo de publicación, idioma y tipo documental. Además, se realizaron búsquedas temáticas complementarias sobre ransomware, redes cibercriminales, criptomonedas, lavado de activos, inteligencia artificial, cultura corporativa, defecto de organización y cumplimiento normativo, cuando estos conceptos se relacionaban directamente con la atribución de responsabilidad penal empresarial. Finalmente, los resultados obtenidos mediante las diferentes combinaciones fueron reunidos en una única base para su posterior depuración.

Se incluyeron publicaciones científicas difundidas entre enero de 2022 y abril de 2026, redactadas en español o inglés y relacionadas directamente con la delincuencia digital organizada, la responsabilidad penal empresarial o la articulación entre ambos fenómenos. Se consideraron estudios empíricos, revisiones de literatura, investigaciones doctrinales, análisis comparados y trabajos teórico-conceptuales que aportaran información sobre las estructuras criminales digitales, las modalidades delictivas emergentes, los modelos de imputación a las

personas jurídicas, la cultura corporativa, los defectos de organización, el cumplimiento normativo o los desafíos regulatorios y probatorios. Asimismo, se exigió que los documentos presentaran información suficiente para identificar su objetivo, enfoque analítico y principales aportes. Se excluyeron los registros duplicados, las publicaciones anteriores a 2022, los documentos redactados en idiomas distintos de los establecidos y los trabajos que abordaban la ciberseguridad desde una perspectiva exclusivamente técnica, sin vinculación con la criminalidad organizada o la responsabilidad penal. También se descartaron textos de opinión, notas informativas, documentos sin respaldo académico y publicaciones cuyo contenido se limitaba a describir delitos digitales sin aportar elementos relevantes para los objetivos de la revisión. La aplicación de estos criterios permitió conservar un corpus temáticamente coherente y adecuado para la síntesis narrativa.

La búsqueda en Scopus, Web of Science y SciELO permitió identificar inicialmente 558 registros bibliográficos. En la primera etapa se revisaron los títulos y resúmenes para determinar su correspondencia con el periodo, los idiomas y los núcleos temáticos establecidos. Como resultado de este cribado, se excluyeron 498 registros por no abordar directamente la delincuencia digital organizada, la responsabilidad penal empresarial o la relación entre ambas categorías, por desarrollar contenidos exclusivamente técnicos o por incumplir alguno de los criterios de elegibilidad. De este modo, 60 publicaciones fueron preseleccionadas para una revisión más detallada. Posteriormente, los registros procedentes de las tres estrategias temáticas de búsqueda se consolidaron en una matriz única y se compararon mediante el título y el identificador digital de objeto. Este procedimiento permitió detectar nueve registros duplicados, los cuales fueron retirados para evitar la valoración reiterada de una misma publicación. Finalmente, el corpus quedó conformado por 51 estudios únicos, cuyos resúmenes, aportes conceptuales y hallazgos fueron examinados para determinar su contribución a los objetivos de la revisión. El proceso de selección se documentó en una matriz maestra con la finalidad de garantizar la trazabilidad de las decisiones adoptadas.

La información de los 51 estudios seleccionados se organizó en la matriz FAEB, estructurada para registrar los datos bibliográficos, características metodológicas, problemas

abordados, objetivos, tecnologías implicadas, actores involucrados, hallazgos principales, conclusiones, limitaciones e implicancias jurídicas y empresariales de cada publicación. La calidad de los documentos se valoró considerando cinco criterios: actualidad, calidad de la fuente, claridad metodológica, pertinencia para la revisión y aporte teórico. Posteriormente, los contenidos fueron examinados mediante un proceso de codificación temática, identificándose conceptos recurrentes, relaciones entre estudios, coincidencias interpretativas, divergencias y vacíos de conocimiento. La síntesis se organizó en cinco categorías: reconfiguración de la delincuencia organizada en el entorno digital; manifestaciones de la delincuencia digital organizada; fundamentos y modelos de responsabilidad penal empresarial; tecnología y riesgo penal corporativo; y prevención, cumplimiento y desafíos regulatorios. Debido a la heterogeneidad de los diseños, contextos y enfoques jurídicos de las publicaciones, no se efectuó una integración estadística de los resultados. En su lugar, se desarrolló una síntesis narrativa comparativa, orientada a relacionar los aportes criminológicos y jurídicos y a explicar sus implicancias para la atribución de responsabilidad penal a las empresas.

El procesamiento y análisis de la información se apoyó en herramientas digitales especializadas. ASReview se utilizó para facilitar la priorización de los 558 registros recuperados y apoyar el cribado por títulos y resúmenes mediante aprendizaje activo, sin sustituir la evaluación realizada por los investigadores. VOSviewer se empleó para explorar las relaciones entre palabras clave, la coocurrencia de términos y la formación de agrupaciones temáticas dentro del corpus seleccionado. Asimismo, ChatGPT se utilizó como herramienta complementaria para apoyar la organización inicial de la información, la revisión lingüística y la sistematización preliminar de categorías. Las sugerencias generadas mediante inteligencia artificial fueron contrastadas con los registros originales y sometidas a revisión crítica por los autores. Las decisiones relativas a la inclusión o exclusión de publicaciones, la valoración de su calidad, la interpretación de los hallazgos y la formulación de las conclusiones permanecieron bajo responsabilidad exclusiva de los investigadores. De esta manera, las herramientas tecnológicas cumplieron una función auxiliar, manteniéndose la supervisión humana durante todas las etapas de la revisión.

# Capítulo III

## RESULTADOS

## CAPÍTULO III: RESULTADOS

### 3.1. Caracterización del corpus documental

El corpus documental quedó conformado por 51 publicaciones difundidas entre enero de 2022 y abril de 2026. La distribución temporal mostró ocho estudios publicados en 2022 (15,7 %), 13 en 2023 (25,5 %), 12 en 2024 (23,5 %), 17 en 2025 (33,3 %) y uno durante los primeros meses de 2026 (2,0 %). En conjunto, 30 publicaciones (58,8 %) correspondieron al periodo 2024-2025, lo que evidencia una concentración reciente de la producción científica relacionada con la delincuencia digital organizada y la responsabilidad penal empresarial. El incremento alcanzado en 2025 estuvo asociado con un mayor interés por la reconceptualización de las organizaciones criminales en el continuo físico-digital, el funcionamiento de las redes dedicadas al ransomware y la actualización de los modelos de responsabilidad penal corporativa (Botchkovar et al., 2025; Di Nicola et al., 2025; Zazzaro, 2025). La presencia de un solo documento de 2026 debe interpretarse considerando que la búsqueda concluyó en abril de ese año y, por tanto, no comprendió la producción científica anual completa. Estos resultados muestran que el campo se encuentra en expansión y responde a transformaciones tecnológicas y regulatorias todavía en desarrollo.

La información bibliográfica disponible mostró que 21 publicaciones (41,2 %) contaban con cuartil SJR consignado: 14 pertenecían al cuartil Q1 (27,5 % del corpus), dos al Q2 (3,9 %), cuatro al Q3 (7,8 %) y una al Q4 (2,0 %). En las 30 publicaciones restantes (58,8 %) no se registró este indicador, situación que representa ausencia de información en las bases analizadas y no necesariamente falta de indexación o calidad editorial. En cuanto a su composición metodológica, el corpus fue heterogéneo e incluyó estudios teórico-conceptuales dirigidos a redefinir la delincuencia organizada digital (Di Nicola, 2022), investigaciones empíricas sobre redes cibercriminales y dinámicas operativas (Lazarus, 2024), revisiones de literatura sobre criminalidad financiera tecnológica (Ghose et al., 2025) y análisis doctrinales o comparados de los modelos de responsabilidad penal corporativa (Vuletić, 2023). No obstante, únicamente seis registros presentaron una clasificación explícita del tipo de estudio, por lo que no resultó metodológicamente adecuado cuantificar su distribución sin efectuar una codificación

adicional. Esta diversidad confirmó el carácter interdisciplinario del campo, pero también evidenció la necesidad de interpretar los resultados considerando las diferencias entre evidencia empírica, elaboración criminológica y argumentación jurídico-doctrinal.

**Tabla 1**

*Características temporales y editoriales de las publicaciones incluidas*

| Característica         | Categoría                  | n         | %            |
|------------------------|----------------------------|-----------|--------------|
| Año de publicación     | 2022                       | 8         | 15,7         |
|                        | 2023                       | 13        | 25,5         |
|                        | 2024                       | 12        | 23,5         |
|                        | 2025                       | 17        | 33,3         |
|                        | 2026 <sup>1</sup>          | 1         | 2,0          |
|                        | <b>Total</b>               | <b>51</b> | <b>100,0</b> |
| Cuartil SJR registrado | Q1                         | 14        | 27,5         |
|                        | Q2                         | 2         | 3,9          |
|                        | Q3                         | 4         | 7,8          |
|                        | Q4                         | 1         | 2,0          |
|                        | Sin información registrada | 30        | 58,8         |
|                        | <b>Total</b>               | <b>51</b> | <b>100,0</b> |

### 3.2. Estructura temática de la producción científica

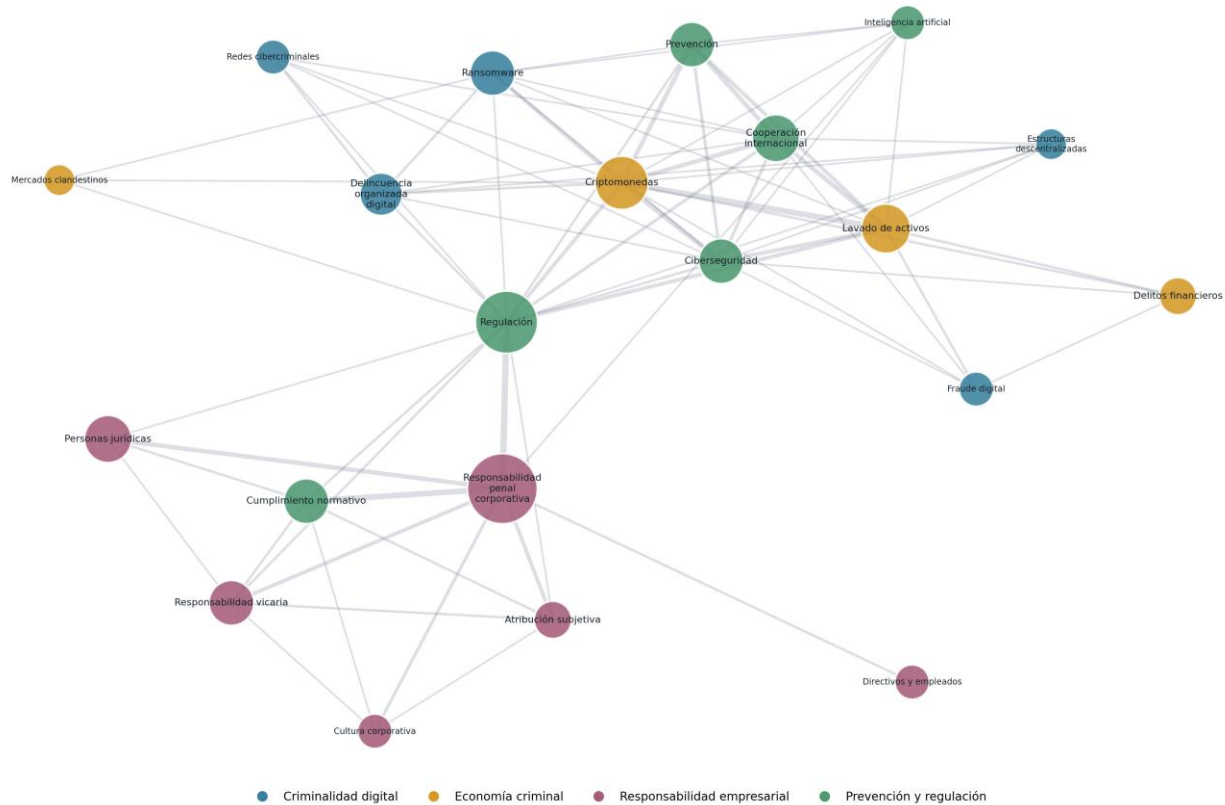
El análisis de los títulos, resúmenes y hallazgos consignados en la matriz permitió identificar como conceptos predominantes la delincuencia organizada digital, las redes cibercriminales, el ransomware, las criptomonedas, el lavado de activos, la responsabilidad penal corporativa, la cultura empresarial y el cumplimiento normativo. En el componente criminológico, los términos se concentraron alrededor de la organización en red, la descentralización, la cooperación criminal, el anonimato y la transnacionalidad, lo que reflejó el interés por explicar estructuras delictivas que no responden necesariamente a jerarquías estables o al control de territorios físicos (Di Nicola et al., 2025; Lusthaus et al., 2023). En el componente jurídico, predominaron los conceptos de responsabilidad de las personas jurídicas, responsabilidad vicaria, atribución del elemento subjetivo, defecto de organización y responsabilidad derivada de las actuaciones de empleados o directivos (Ali et al., 2023; Silver, 2023). Entre ambos campos aparecieron como categorías articuladoras la ciberseguridad, la inteligencia artificial, los activos digitales y el riesgo corporativo. Esta configuración evidenció que la producción científica no se organiza alrededor de un único problema, sino de varios

núcleos relacionados que conectan las transformaciones tecnológicas del delito con las dificultades contemporáneas de imputación empresarial.

El análisis relacional de los términos permitió distinguir cuatro núcleos temáticos interconectados. El primero reunió conceptos relacionados con delincuencia organizada digital, redes cibercriminales, ransomware, fraude electrónico y estructuras descentralizadas, destacando la transformación de las formas tradicionales de organización criminal (Whelan et al., 2023; Di Nicola et al., 2025). El segundo agrupó criptomonedas, lavado de activos, delitos financieros y financiamiento ilícito, evidenciando la importancia de las tecnologías de transferencia y ocultamiento de recursos dentro de la economía criminal digital (Trozze et al., 2022; Anggriawan & Susila, 2024). El tercer núcleo comprendió responsabilidad penal corporativa, personas jurídicas, responsabilidad vicaria, cultura empresarial y atribución subjetiva, concentrando los debates acerca de los fundamentos utilizados para imputar delitos a las organizaciones (Ali et al., 2023; Silver, 2023). Finalmente, el cuarto integró ciberseguridad, inteligencia artificial, cumplimiento normativo, prevención y regulación, funcionando como punto de conexión entre el riesgo tecnológico y los deberes empresariales de control (Aguilera Gordillo, 2024; Rote et al., 2025). En conjunto, estas agrupaciones mostraron una proximidad conceptual creciente entre criminología digital y responsabilidad empresarial, aunque la articulación directa entre ambos campos continuó siendo limitada.

**Figura 1**

*Red de coocurrencia de términos sobre delincuencia digital organizada y responsabilidad penal empresarial*



### 3.3. Reconfiguración de la delincuencia organizada en el entorno digital

Los estudios analizados evidenciaron que la digitalización ha favorecido el tránsito desde organizaciones criminales predominantemente jerárquicas y territorializadas hacia redes más flexibles, horizontales y tecnológicamente mediadas. Di Nicola (2022) identificó la coexistencia de organizaciones tradicionales, grupos dedicados exclusivamente a la ciberdelincuencia y estructuras híbridas que combinan operaciones físicas y virtuales. En estas configuraciones, las tecnologías digitales no se limitaron a facilitar la comunicación entre los participantes, sino que intervinieron en la distribución de funciones, la selección de objetivos, la ejecución de ataques y la circulación de los beneficios ilícitos. Lazarus (2024) encontró que los participantes en esquemas de fraude mediante correo electrónico empresarial operaban sin una jerarquía rígida que determinara permanentemente sus posiciones y remuneraciones; por el contrario,

predominaban la colaboración horizontal, la especialización y la adaptación de los roles. De manera similar, Hartmann (2025) señaló que las formaciones criminales mediadas por tecnologías funcionan como sistemas adaptativos en los que los protocolos criptográficos pueden sustituir parcialmente las relaciones personales de confianza. En conjunto, los estudios mostraron que la capacidad organizativa de estas redes no depende necesariamente de una dirección centralizada, sino de la coordinación funcional entre actores especializados.

A pesar de su menor estabilidad jerárquica, las organizaciones criminales digitales conservaron elementos que permiten reconocerlas como formas de delincuencia organizada. El análisis de 71 casos judiciales realizado por Di Nicola et al. (2025) mostró que estas agrupaciones presentan reiteradamente colaboración entre participantes, continuidad de las operaciones, orientación lucrativa, distribución empresarial de actividades y organización en red. Asimismo, Lusthaus et al. (2023) identificaron que las redes cibercriminales articulan relaciones de cooperación interna y conexiones con actores externos que proporcionan conocimientos técnicos, infraestructura, acceso a víctimas o mecanismos para movilizar los beneficios obtenidos. El estudio del grupo Gozi también evidenció una estructura comparable con una empresa criminal, caracterizada por la división del trabajo y la participación coordinada de desarrolladores, administradores y operadores especializados (Lusthaus et al., 2022). En consecuencia, la especialización funcional apareció como un rasgo central del corpus: los participantes no necesitaban intervenir en todas las etapas del delito, sino aportar capacidades específicas dentro de una cadena operativa. Esta distribución permitió mantener las actividades ilícitas, sustituir integrantes y diversificar modalidades delictivas sin comprometer necesariamente la continuidad del conjunto, mientras que la obtención de beneficios económicos permaneció como su principal elemento articulador.

Los hallazgos también mostraron que la distinción entre delincuencia organizada física y digital resulta cada vez menos precisa. Las organizaciones examinadas podían utilizar infraestructuras tecnológicas para ejecutar delitos completamente virtuales, apoyar actividades desarrolladas fuera de línea o articular operaciones híbridas en las que participaban actores ubicados en ambos espacios. Lavorgna y Antonopoulos (2022) identificaron que los mercados y redes criminales del ciberespacio mantienen relaciones funcionales con estructuras

delictivas tradicionales, especialmente para obtener recursos, blanquear ganancias y convertir activos digitales en beneficios utilizables en la economía convencional. En el caso del ransomware, Whelan et al. (2023) encontraron que las actividades criminales, las estructuras sociales de los ofensores y sus mecanismos de gobernanza presentan suficientes elementos organizativos para ser analizados desde la criminología del crimen organizado, aunque no reproduzcan características clásicas como la violencia territorial o el control monopolico. En concordancia, Di Nicola et al. (2025) propusieron comprender el crimen organizado mediante un continuo físico-digital, en el cual la dimensión tecnológica actúa como un atributo transversal. La evidencia revisada mostró, por tanto, un desplazamiento desde definiciones basadas en modelos mafiosos hacia criterios centrados en colaboración, continuidad, finalidad económica, especialización y capacidad de coordinación.

**Tabla 2**

*Transformación de las organizaciones criminales en el continuo físico-digital*

| Dimensión                           | Organización criminal tradicional                                     | Organización criminal digital                                                | Organización criminal híbrida                                      |
|-------------------------------------|-----------------------------------------------------------------------|------------------------------------------------------------------------------|--------------------------------------------------------------------|
| <b>Estructura</b>                   | Jerárquica y relativamente estable                                    | Horizontal, flexible y descentralizada                                       | Combina jerarquías con redes flexibles                             |
| <b>Ámbito de actuación</b>          | Territorial y predominantemente físico                                | Transnacional y principalmente virtual                                       | Articula espacios físicos y digitales                              |
| <b>Relaciones entre integrantes</b> | Basadas en contacto personal, lealtad y confianza                     | Mediadas por anonimato, seudónimos y protocolos tecnológicos                 | Combinan vínculos personales y coordinación digital                |
| <b>Distribución de funciones</b>    | Roles relativamente permanentes                                       | Funciones especializadas y sustituibles                                      | Roles estables en el núcleo y flexibles en la periferia            |
| <b>Mecanismos de coordinación</b>   | Dirección centralizada y control directo                              | Plataformas digitales, comunicación cifrada y automatización                 | Dirección humana apoyada por infraestructura tecnológica           |
| <b>Modalidades delictivas</b>       | Extorsión, tráfico ilícito, corrupción y control territorial          | Ransomware, fraude digital, robo de datos y mercados clandestinos            | Lavado de activos, fraude, tráfico ilícito y operaciones digitales |
| <b>Uso de la violencia</b>          | Frecuente como medio de control y gobernanza                          | Menos visible; predominan coerción digital y extorsión                       | Puede combinar violencia física y amenazas digitales               |
| <b>Alcance geográfico</b>           | Local, regional o nacional                                            | Global y transfronterizo                                                     | Transnacional, con operaciones territoriales específicas           |
| <b>Ocultamiento de beneficios</b>   | Empresas de fachada, testaferros y efectivo                           | Criptomonedas, billeteras digitales y servicios de anonimización             | Integra activos digitales y mecanismos financieros convencionales  |
| <b>Rasgos organizativos comunes</b> | Continuidad, colaboración, finalidad lucrativa y división del trabajo | Continuidad, colaboración, finalidad lucrativa y especialización tecnológica | Integra características tradicionales y digitales                  |

### **3.4. Manifestaciones de la delincuencia digital organizada**

El ransomware se presentó como una de las manifestaciones más representativas de la delincuencia digital organizada, debido a que su ejecución exige coordinación técnica, distribución de funciones y mecanismos para obtener y movilizar los pagos exigidos. Los estudios revisados mostraron que estas operaciones pueden involucrar desarrolladores de programas maliciosos, proveedores de acceso, operadores encargados de penetrar los sistemas, negociadores, administradores de infraestructura y actores responsables de lavar los activos obtenidos. Botchkovar et al. (2025) identificaron que las actividades de los grupos de ransomware se organizan mediante redes sociales y funcionales que permiten compartir recursos, asignar tareas y mantener la continuidad de las operaciones. Por su parte, Whelan et al. (2023) determinaron que estas agrupaciones reúnen características propias del crimen organizado, entre ellas estabilidad relativa, cooperación, finalidad lucrativa y mecanismos de gobernanza aplicados a sus actividades y relaciones internas. La evidencia indicó que no todos los participantes mantienen el mismo nivel de pertenencia ni intervienen en cada fase del ataque; sin embargo, sus aportes se integran dentro de una cadena delictiva común. Esta división funcional incrementa la capacidad operativa de las redes y dificulta individualizar la responsabilidad de quienes dirigen, facilitan o se benefician de los ataques.

El fraude por compromiso del correo electrónico empresarial y los mercados clandestinos digitales constituyeron otras manifestaciones relevantes dentro del corpus. En los esquemas de fraude empresarial, los actores utilizaron técnicas de ingeniería social, suplantación de identidad y manipulación de comunicaciones para inducir transferencias de dinero o acceder a información corporativa. Lazarus (2024) encontró que las redes vinculadas con estas operaciones presentaban estructuras horizontales, roles adaptables y conexiones transfronterizas, sin que existiera necesariamente una jerarquía rígida para determinar la participación o remuneración de sus integrantes. De manera complementaria, Lusthaus et al. (2023) evidenciaron que las redes cibercriminales mantienen relaciones de cooperación con intermediarios externos que facilitan conocimientos, infraestructura, contactos y mecanismos de monetización. Los mercados clandestinos, por su parte, funcionaron como espacios de intercambio donde podían adquirirse datos robados, credenciales, programas maliciosos y servicios especializados, favoreciendo la interacción entre participantes que no se conocían

directamente (Lavorgna & Antonopoulos, 2022). En conjunto, estos hallazgos mostraron la consolidación de un ecosistema criminal basado en la tercerización de funciones y el acceso a recursos ilícitos como servicios, lo que disminuye las barreras de ingreso, amplía el número de participantes y dificulta delimitar los vínculos entre autores, colaboradores e intermediarios.

Las criptomonedas ocuparon una posición transversal en las manifestaciones de delincuencia digital organizada, principalmente como mecanismo de pago, transferencia y ocultamiento de los beneficios ilícitos. Su alcance transnacional, la rapidez de las operaciones y la posibilidad de utilizar múltiples billeteras o servicios de intercambio favorecieron su incorporación en esquemas de ransomware, mercados clandestinos, fraude digital y financiamiento ilícito. Trozze et al. (2022) identificaron una relación creciente entre los criptoactivos y diversas formas de criminalidad financiera, aunque advirtieron que su utilización no es intrínsecamente delictiva y depende de las condiciones de la operación. Nazzari (2023) encontró que los ciberdelincuentes emplean estrategias diversificadas para lavar sus ganancias, combinando transacciones digitales, intermediarios y mecanismos financieros convencionales con la finalidad de dificultar la trazabilidad de los fondos. Asimismo, Anggriawan y Susila (2024) destacaron que la supervisión de los criptoactivos requiere aplicar medidas de identificación, monitoreo y cooperación acordes con los estándares internacionales contra el lavado de dinero y el financiamiento del terrorismo. En síntesis, la evidencia mostró que las criptomonedas no sustituyen completamente los mecanismos tradicionales de blanqueo, sino que se integran en cadenas financieras híbridas que conectan activos digitales, instituciones financieras, empresas y economías convencionales.

**Tabla 3**

Principales manifestaciones de la delincuencia digital organizada identificadas en la literatura

| <b>Manifestación</b>                            | <b>Organización y participantes</b>                                                                | <b>Tecnologías o recursos utilizados</b>                                                         | <b>Finalidad principal</b>                                                     | <b>Implicancias empresariales</b>                                                             |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <b>Ransomware</b>                               | Desarrolladores, proveedores de acceso, operadores, negociadores y actores encargados del lavado   | Programas maliciosos, cifrado, accesos remotos, redes anónimas y criptomonedas                   | Extorsionar mediante el cifrado o sustracción de información                   | Paralización operativa, pérdida de datos, pagos ilícitos y afectación reputacional            |
| <b>Fraude por correo empresarial</b>            | Redes horizontales, suplantadores, reclutadores, intermediarios financieros y receptores de fondos | Correo electrónico, ingeniería social, credenciales robadas y cuentas bancarias                  | Inducir transferencias fraudulentas o acceder a información corporativa        | Pérdidas económicas, vulneración de controles internos y posible intervención de empleados    |
| <b>Mercados clandestinos digitales</b>          | Administradores, vendedores, compradores, intermediarios y proveedores de servicios ilícitos       | Darknet, comunicación cifrada, sistemas de reputación y criptoactivos                            | Comercializar datos, credenciales, programas maliciosos y servicios delictivos | Circulación de información empresarial robada y adquisición de recursos para ataques          |
| <b>Lavado de activos con criptomonedas</b>      | Operadores financieros, intermediarios, titulares de billeteras y proveedores de intercambio       | Billeteras digitales, múltiples transferencias, servicios de mezcla y plataformas de intercambio | Ocultar el origen, movimiento o destino de los beneficios ilícitos             | Riesgo de utilización de plataformas, cuentas o servicios empresariales para movilizar fondos |
| <b>Redes de criminalidad financiera digital</b> | Especialistas técnicos, defraudadores, intermediarios y organizaciones transnacionales             | Criptomonedas, plataformas financieras, identidades digitales y sistemas automatizados           | Ejecutar fraudes, movilizar capitales y financiar actividades ilícitas         | Exigencia de debida diligencia, trazabilidad financiera y fortalecimiento del cumplimiento    |

### 3.5. Fundamentos y modelos de responsabilidad penal empresarial

La literatura examinada mostró que la responsabilidad penal empresarial se fundamenta en la necesidad de responder a delitos producidos dentro de estructuras organizacionales complejas, en las cuales las decisiones, los conocimientos y las funciones se encuentran distribuidos entre diferentes niveles. Vuletić (2023) identificó que los sistemas contemporáneos han incorporado mecanismos para sancionar directamente a las personas jurídicas cuando la actividad delictiva se relaciona con sus operaciones, beneficios o deficiencias de control. De manera concordante, Saipudin et al. (2025) señalaron que la responsabilidad corporativa ha

evolucionado desde una imputación dependiente exclusivamente de la conducta individual hacia modelos que reconocen a la organización como un centro autónomo de decisiones, riesgos y deberes. Sin embargo, la revisión también encontró posiciones críticas que cuestionan la legitimidad y eficacia de castigar penalmente a una entidad carente de voluntad en sentido humano, especialmente cuando las sanciones pueden afectar a trabajadores, accionistas o terceros ajenos al delito (Smith, 2022). Pese a esta divergencia, predominó la consideración de que la complejidad empresarial exige mecanismos de atribución capaces de superar la identificación de un único responsable individual. En este marco, la conexión entre el hecho delictivo y la empresa se construyó principalmente mediante el beneficio obtenido, la actuación funcional de sus miembros o la existencia de defectos organizacionales relevantes.

La responsabilidad vicaria y el modelo de identificación aparecieron como mecanismos tradicionales para vincular la conducta de las personas naturales con la responsabilidad penal de la empresa. En el primero, la imputación se produce cuando un empleado, representante o agente comete un delito dentro del ámbito de sus funciones y con la intención de beneficiar a la organización. Kurniawan y Hapsari (2022) sostuvieron que este modelo permite trasladar a la persona jurídica las consecuencias derivadas de actuaciones funcionalmente relacionadas con su actividad, aunque exige delimitar el vínculo entre el autor individual, las facultades asignadas y el interés corporativo. Silver (2023) destacó que la aplicación del principio respondeat superior plantea interrogantes sobre el grado de supervisión, autorización o conocimiento necesario para justificar la responsabilidad penal de la entidad. Por su parte, el modelo de identificación atribuye a la empresa las decisiones de sus órganos superiores, al considerar que los directivos representan su voluntad; sin embargo, Horder y Watts (2023) advirtieron dificultades para responsabilizar a los altos administradores por delitos ejecutados por empleados o agentes cuando el conocimiento y el control se encuentran fragmentados. En conjunto, estos modelos mostraron mayores limitaciones frente a empresas descentralizadas, donde ninguna persona concentra toda la información o dirección del hecho delictivo.

Frente a las limitaciones de los modelos dependientes de la actuación individual, la literatura identificó una tendencia hacia la responsabilidad autónoma de la empresa basada en el defecto de organización. Este modelo centra la imputación en la ausencia, insuficiencia o

ineficacia de los mecanismos internos destinados a prevenir, detectar y responder a las conductas delictivas. Aguilera Gordillo (2024) vinculó la responsabilidad de las personas jurídicas con la capacidad de la organización para establecer sistemas de cumplimiento adecuados a sus riesgos, de modo que la omisión de controles relevantes puede constituir un fundamento propio de responsabilidad. Asimismo, Zazzaro (2025) observó que las directivas europeas han fortalecido progresivamente las obligaciones corporativas de prevención, supervisión y cooperación, aunque mantienen diferencias en la forma en que los Estados concretan la responsabilidad empresarial. Desde esta perspectiva, la imputación no requiere demostrar que una única persona dirigió o conoció íntegramente el delito, sino comprobar que la estructura corporativa generó, toleró o no controló adecuadamente el riesgo que facilitó su comisión. Este enfoque resultó especialmente pertinente frente a la delincuencia digital, debido a que las decisiones sobre ciberseguridad, contratación de terceros, automatización y administración de datos suelen distribuirse entre diferentes unidades y niveles organizacionales.

La cultura corporativa constituyó otro criterio relevante para explicar cómo las prácticas, valores y tolerancias institucionales pueden favorecer o impedir la comisión de delitos. Ali et al. (2023) sostuvieron que la cultura organizacional puede utilizarse para acreditar el componente subjetivo de la responsabilidad empresarial cuando las políticas formales o informales evidencian aceptación, incentivo o indiferencia frente a conductas ilícitas. Este modelo amplía el análisis más allá de los actos aislados de empleados y directivos, pues examina patrones de funcionamiento, sistemas de incentivos, comunicaciones internas y respuestas previas ante incumplimientos. No obstante, la revisión mostró diferencias importantes entre los ordenamientos jurídicos. Mientras algunos sistemas recurren principalmente a la responsabilidad derivada de las personas naturales, otros reconocen una responsabilidad autónoma sustentada en defectos estructurales o incumplimientos de deberes corporativos (Díaz, 2024; Ismaïdar et al., 2025). Zazzaro (2025) también identificó variaciones en la regulación europea respecto de los presupuestos de imputación y las sanciones aplicables. En consecuencia, no se encontró un modelo universalmente uniforme, sino combinaciones de

criterios que vinculan la actuación individual, el beneficio empresarial, la cultura organizacional y la eficacia de los sistemas de prevención.

**Tabla 4**

*Modelos de atribución de responsabilidad penal empresarial identificados en la literatura*

| <b>Modelo de atribución</b>     | <b>Fundamento de la responsabilidad</b>                                                                       | <b>Criterio de vinculación con la empresa</b>                                                            | <b>Principal aporte</b>                                                                                      | <b>Limitaciones frente a la delincuencia digital</b>                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Responsabilidad vicaria</b>  | La empresa responde por el delito cometido por empleados, representantes o agentes                            | Actuación dentro de las funciones asignadas y orientada a beneficiar a la organización                   | Permite vincular directamente la conducta individual con la persona jurídica                                 | Puede ampliar excesivamente la imputación y no explica adecuadamente los delitos ejecutados mediante redes externas o funciones fragmentadas |
| <b>Modelo de identificación</b> | Los órganos superiores expresan la voluntad y actuación de la empresa                                         | Participación, conocimiento, autorización o tolerancia de directivos con capacidad decisoria             | Delimita la responsabilidad a quienes representan el centro de dirección empresarial                         | Resulta insuficiente en empresas descentralizadas, donde ninguna persona concentra el conocimiento o control de la operación                 |
| <b>Defecto de organización</b>  | La empresa responde por no establecer medidas adecuadas de prevención, supervisión y control                  | Ausencia o ineficacia de controles frente a riesgos previsibles vinculados con su actividad              | Reconoce una responsabilidad autónoma basada en el funcionamiento de la organización                         | Exige determinar qué controles eran razonables según el riesgo tecnológico, tamaño y capacidad de la empresa                                 |
| <b>Cultura corporativa</b>      | Las políticas, prácticas, incentivos o tolerancias institucionales favorecen el delito                        | Existencia de valores, patrones o decisiones organizacionales que promueven o permiten el incumplimiento | Permite valorar conductas colectivas y prácticas informales, aunque no exista una orden individual explícita | La cultura empresarial es difícil de acreditar y requiere analizar múltiples evidencias internas                                             |
| <b>Modelo combinado</b>         | Integra la actuación individual, el beneficio empresarial, el defecto organizacional y la cultura corporativa | Concurrencia de distintos criterios según el ordenamiento y las características del caso                 | Ofrece una respuesta más adecuada ante estructuras corporativas complejas                                    | Puede generar incertidumbre si los criterios de atribución no se encuentran claramente delimitados                                           |

### **3.6. Tecnología, riesgo penal y cumplimiento corporativo**

La ciberseguridad apareció en la literatura como un componente relevante del deber empresarial de organización y prevención, especialmente cuando las actividades corporativas implican el tratamiento masivo de datos, la administración de infraestructuras críticas o la prestación de servicios digitales. Aslan et al. (2023) identificaron que las vulnerabilidades técnicas, los errores de configuración, las deficiencias de actualización y la ausencia de controles de acceso incrementan la exposición de las organizaciones frente a ataques y usos ilícitos de sus sistemas. Sin embargo, la existencia de una vulnerabilidad no generó automáticamente responsabilidad penal empresarial; para ello, debía demostrarse su relación con un riesgo previsible, la omisión de medidas razonables y la producción o facilitación de un resultado jurídicamente relevante. Rote et al. (2025) señalaron que esta valoración adquiere especial importancia en sectores sensibles, donde las fallas de ciberseguridad pueden comprometer servicios esenciales, datos personales o la integridad de los usuarios. Desde la perspectiva del defecto de organización, los hallazgos mostraron que los deberes corporativos comprenden la evaluación periódica de riesgos, la actualización de sistemas, la supervisión de accesos, la capacitación del personal y la respuesta oportuna ante incidentes. Su incumplimiento sistemático puede constituir un indicador de tolerancia organizacional frente al riesgo digital.

La incorporación de inteligencia artificial y sistemas automatizados amplió las dificultades para atribuir responsabilidad cuando una decisión tecnológica contribuye a producir, facilitar o intensificar un resultado delictivo. Rote et al. (2025) analizaron esta problemática en sistemas sanitarios y señalaron que las fallas de ciberseguridad vinculadas con inteligencia artificial pueden comprometer la responsabilidad corporativa cuando derivan de decisiones empresariales relacionadas con el diseño, implementación, supervisión o mantenimiento de la tecnología. La revisión evidenció que la automatización distribuye la intervención entre desarrolladores, proveedores, administradores, usuarios y directivos, lo que dificulta identificar a una sola persona como autora o controladora del riesgo. Aguilera Gordillo (2024) sostuvo que la atribución debe considerar la estructura organizacional y los mecanismos de cumplimiento implementados para prevenir conductas ilícitas, en lugar de limitarse a buscar una voluntad individual equivalente a la decisión del sistema. En este contexto, adquirieron relevancia la

previsibilidad del riesgo, la calidad de los datos, la supervisión humana, la trazabilidad de las decisiones y la capacidad de intervenir ante resultados anómalos. Por tanto, los estudios no atribuyeron responsabilidad penal a la inteligencia artificial como entidad autónoma, sino que orientaron el análisis hacia las personas y organizaciones encargadas de gestionar los riesgos derivados de su utilización.

Los programas de cumplimiento se identificaron como mecanismos esenciales para reducir los riesgos penales derivados del uso empresarial de tecnologías digitales. Aguilera Gordillo (2024) sostuvo que su eficacia depende de la capacidad para reconocer los riesgos específicos de la organización y establecer controles verificables, en lugar de limitarse a la aprobación formal de códigos o protocolos. Entre las medidas señaladas en la literatura se encontraron la evaluación periódica de amenazas, la asignación de responsabilidades, la debida diligencia respecto de trabajadores y terceros, la capacitación del personal, los canales de denuncia, la supervisión de sistemas automatizados y los procedimientos de respuesta ante incidentes. Asimismo, Ali et al. (2023) destacaron que la cultura corporativa permite valorar si la empresa promueve efectivamente el cumplimiento o si tolera prácticas orientadas a eludir controles y obligaciones legales. Zazzaro (2025) identificó una tendencia regulatoria hacia el fortalecimiento de los deberes preventivos empresariales, aunque con diferencias respecto del valor atribuido a los programas de cumplimiento. En conjunto, los estudios mostraron que la mera existencia documental de un programa no excluye automáticamente la responsabilidad penal; su relevancia depende de que haya sido implementado, actualizado, dotado de recursos y aplicado antes de la comisión del delito. La eficacia preventiva, por tanto, se convirtió en el criterio central para valorar el comportamiento organizacional.

**Tabla 5**

*Riesgos tecnológicos, deberes empresariales y mecanismos de prevención penal*

| <b>Riesgo tecnológico</b>                          | <b>Deber empresarial comprometido</b>                                    | <b>Medidas preventivas y de control</b>                                                                             | <b>Relevancia para la responsabilidad penal</b>                                                                   |
|----------------------------------------------------|--------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Vulnerabilidades de ciberseguridad</b>          | Proteger sistemas, datos e infraestructuras frente a riesgos previsibles | Actualización de sistemas, controles de acceso, pruebas de seguridad, monitoreo continuo y copias de respaldo       | La omisión reiterada de controles razonables puede evidenciar un defecto de organización                          |
| <b>Uso ilícito de sistemas por trabajadores</b>    | Supervisar las actividades realizadas mediante recursos corporativos     | Segregación de funciones, registro de accesos, límites de privilegios, capacitación y auditorías internas           | Permite valorar si la empresa previno, toleró o facilitó la conducta del empleado                                 |
| <b>Riesgos derivados de proveedores y terceros</b> | Aplicar debida diligencia y controlar servicios externalizados           | Evaluación previa, cláusulas de cumplimiento, monitoreo contractual y procedimientos de desvinculación              | La ausencia de supervisión puede vincular a la empresa con delitos ejecutados mediante terceros                   |
| <b>Operaciones con criptomonedas</b>               | Prevenir el lavado de activos y asegurar la trazabilidad financiera      | Identificación de clientes, monitoreo de transacciones, alertas de riesgo y comunicación de operaciones sospechosas | Los controles insuficientes pueden facilitar el ocultamiento o movilización de fondos ilícitos                    |
| <b>Inteligencia artificial y automatización</b>    | Diseñar, implementar y supervisar sistemas tecnológicos de manera segura | Validación de datos, evaluación de impactos, trazabilidad, supervisión humana y mecanismos de interrupción          | La falta de control sobre riesgos previsibles puede sustentar responsabilidad por defecto organizacional          |
| <b>Ataques de ransomware</b>                       | Prevenir incidentes y garantizar continuidad operativa                   | Segmentación de redes, autenticación multifactor, capacitación, respaldo de datos y plan de respuesta               | La preparación y reacción empresarial permiten valorar la diligencia desplegada ante el ataque                    |
| <b>Detección y comunicación de incidentes</b>      | Investigar, contener y reportar oportunamente hechos relevantes          | Canales de denuncia, equipos de respuesta, conservación de evidencia y protocolos de notificación                   | El encubrimiento o la respuesta tardía pueden revelar tolerancia, incumplimiento o cultura corporativa deficiente |
| <b>Programa de cumplimiento meramente formal</b>   | Implementar controles efectivos y adaptados a los riesgos reales         | Recursos suficientes, independencia del responsable, revisiones periódicas y medidas disciplinarias                 | La existencia documental del programa no excluye responsabilidad si carece de aplicación efectiva                 |

### 3.7. Desafíos regulatorios, consensos y vacíos de conocimiento

La literatura revisada identificó que el carácter transnacional, descentralizado y anónimo de la delincuencia digital organizada limita la eficacia de las respuestas jurídicas construidas desde marcos territoriales. Lutovac y Lutovac (2022) señalaron que los grupos cibercriminales pueden distribuir a sus integrantes, víctimas, servidores y recursos financieros entre diferentes

países, dificultando la determinación de la jurisdicción competente y la cooperación oportuna entre autoridades. En el ámbito probatorio, la volatilidad de los datos, el cifrado de las comunicaciones, la utilización de identidades ficticias y la intervención de múltiples intermediarios complican la reconstrucción de las operaciones y la identificación de sus responsables. Anggriawan y Susila (2024) destacaron que las transacciones con criptomonedas exigen fortalecer los procedimientos de trazabilidad, identificación y conservación de evidencia, particularmente cuando los fondos atraviesan plataformas sometidas a regulaciones distintas. Asimismo, Subbagari (2023) encontró que las medidas contra el lavado de activos requieren adaptarse a las nuevas tecnologías financieras y reforzar la cooperación internacional. En el ámbito empresarial, estas dificultades se trasladaron a la necesidad de demostrar la relación entre el delito, el beneficio corporativo, las decisiones organizacionales y los controles omitidos. La diversidad normativa entre jurisdicciones incrementó el riesgo de respuestas fragmentadas y vacíos de imputación.

La síntesis del corpus permitió identificar como principal consenso que las organizaciones criminales digitales pueden constituir formas de delincuencia organizada aun cuando carezcan de jerarquías rígidas, control territorial o uso sistemático de violencia, siempre que presenten continuidad, colaboración, especialización y finalidad lucrativa (Di Nicola et al., 2025; Whelan et al., 2023). También existió acuerdo respecto de la necesidad de superar los modelos de responsabilidad empresarial dependientes exclusivamente de la identificación de una persona natural, especialmente cuando las decisiones y los conocimientos se encuentran distribuidos en estructuras corporativas complejas (Aguilera Gordillo, 2024; Zazzaro, 2025). Las principales divergencias se concentraron en el fundamento y alcance de la responsabilidad penal de las personas jurídicas, el grado de conexión exigible entre la conducta individual y la empresa, y la eficacia eximente o atenuante de los programas de cumplimiento. En cuanto a los vacíos, fueron escasos los estudios que articularon directamente la organización de las redes cibercriminales con los criterios de imputación penal empresarial. Asimismo, se identificó limitada evidencia empírica sobre la aplicación judicial de estos modelos frente a ransomware, inteligencia artificial, servicios tercerizados y operaciones con criptoactivos. En consecuencia, la literatura ofrece avances conceptuales importantes, pero todavía no presenta un marco

integrado que relacione estructuras delictivas digitales, riesgos corporativos, deberes de prevención y atribución de responsabilidad penal.

**Tabla 6**

*Consensos, divergencias y vacíos identificados en la literatura revisada*

| <b>Eje de análisis</b>                                         | <b>Consensos</b>                                                                                                                  | <b>Divergencias</b>                                                                                                  | <b>Vacíos de conocimiento</b>                                                                                              |
|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Conceptualización de la delincuencia digital organizada</b> | La continuidad, colaboración, especialización y finalidad lucrativa permiten reconocer formas organizadas de criminalidad digital | Persiste desacuerdo sobre la necesidad de violencia, jerarquía, gobernanza extralegal o control territorial          | Faltan criterios universalmente aceptados para delimitar organizaciones, redes temporales y proveedores independientes     |
| <b>Estructura de las redes cibercriminales</b>                 | Predominan configuraciones flexibles, transnacionales y funcionalmente especializadas                                             | No existe consenso sobre el grado de estabilidad necesario para considerar organizada una red                        | Son limitados los estudios empíricos sobre liderazgo, permanencia, sustitución de integrantes y distribución de beneficios |
| <b>Responsabilidad penal empresarial</b>                       | La complejidad corporativa exige superar la imputación centrada exclusivamente en una persona natural                             | Los sistemas difieren entre responsabilidad vicaria, identificación, defecto de organización y cultura corporativa   | Faltan modelos integrados aplicables a decisiones fragmentadas, tercerización y sistemas automatizados                     |
| <b>Ciberseguridad e inteligencia artificial</b>                | Las empresas deben identificar y controlar riesgos tecnológicos previsibles                                                       | No existe uniformidad respecto del nivel de diligencia exigible ni de las consecuencias penales de su incumplimiento | Se requiere evidencia sobre aplicación judicial, trazabilidad algorítmica y estándares de supervisión humana               |
| <b>Criptomonedas y lavado de activos</b>                       | Los activos digitales pueden facilitar la transferencia y ocultamiento de beneficios ilícitos                                     | Se discute el equilibrio entre regulación, innovación financiera y prevención penal                                  | Faltan criterios armonizados sobre trazabilidad, debida diligencia y responsabilidad de intermediarios digitales           |
| <b>Programas de cumplimiento</b>                               | Su valor depende de la implementación efectiva y adaptación a los riesgos de la empresa                                           | Los ordenamientos difieren sobre su efecto eximente, atenuante o probatorio                                          | Son escasos los estudios que evalúan empíricamente la eficacia de programas frente a delitos digitales                     |
| <b>Cooperación y regulación internacional</b>                  | La naturaleza transnacional del fenómeno exige cooperación entre Estados y empresas                                               | Existen diferencias jurisdiccionales sobre obtención de evidencia, sanciones y atribución corporativa                | Falta armonización normativa y procedimental para investigaciones digitales transfronterizas                               |

# Capítulo IV

## DISCUSIÓN

## CAPÍTULO IV: DISCUSIÓN

El principal hallazgo de la revisión evidencia que la transformación digital de la delincuencia organizada y la evolución de la responsabilidad penal empresarial constituyen procesos estrechamente relacionados, aunque todavía son abordados de manera fragmentada por la literatura. Las redes criminales digitales han sustituido parcialmente la jerarquía, el control territorial y la confianza interpersonal por estructuras flexibles, especialización técnica y mecanismos tecnológicos de coordinación, sin perder continuidad ni orientación lucrativa (Di Nicola et al., 2025; Hartmann, 2025). Esta transformación cuestiona los modelos de imputación empresarial que dependen de identificar a una persona natural con dominio suficiente sobre la conducta, debido a que tanto las actividades criminales como las decisiones corporativas pueden distribuirse entre numerosos actores, plataformas y sistemas automatizados. En concordancia, Aguilera Gordillo (2024) y Zazzaro (2025) muestran una tendencia hacia criterios que valoran el defecto de organización, la cultura corporativa y los deberes de prevención. Por ello, los resultados sugieren que la respuesta penal debe conectar dos dimensiones: la estructura funcional de las redes criminales y la forma en que las empresas crean, administran o toleran riesgos tecnológicos. La responsabilidad no debería derivarse automáticamente del daño producido, sino de una relación demostrable entre riesgo previsible, capacidad de control, beneficio organizacional y omisión de medidas razonables.

Los resultados respaldan la necesidad de revisar las definiciones clásicas de delincuencia organizada, pues la exigencia acumulativa de jerarquía, violencia, corrupción y control territorial puede impedir el reconocimiento de redes digitales que presentan capacidad organizativa y permanencia delictiva. Whelan et al. (2023) sostienen que determinados grupos de ransomware deben considerarse organizaciones criminales cuando existe coordinación, continuidad y gobernanza funcional, aunque sus integrantes no reproduzcan una estructura mafiosa. Esta posición coincide con Di Nicola et al. (2025), quienes proponen un continuo físico-digital sustentado en elementos como colaboración, orientación económica, especialización y organización en red. Sin embargo, ampliar excesivamente el concepto podría ocasionar que cualquier cooperación temporal entre ciberdelincuentes sea calificada como crimen

organizado. En ese sentido, los hallazgos de Lazarus (2024) y Lavorgna y Antonopoulos (2022) permiten distinguir entre una asociación ocasional y una estructura organizada mediante la existencia de roles complementarios, acceso estable a recursos, conexiones con intermediarios y capacidad para mantener o reproducir operaciones. Por consiguiente, la digitalización no debería eliminar los umbrales conceptuales, sino modificar sus indicadores: la estabilidad puede observarse en la continuidad de funciones y servicios, mientras que la cohesión puede manifestarse mediante protocolos, reputación digital y dependencia operativa, incluso cuando los participantes cambian o no se conocen personalmente.

La presencia conjunta de ransomware, fraude empresarial, mercados clandestinos, criptomonedas y lavado de activos evidencia que la delincuencia digital organizada funciona como un ecosistema de servicios interdependientes y no únicamente como una suma de delitos aislados. Botchkovar et al. (2025) muestran que los grupos de ransomware distribuyen funciones entre participantes especializados, mientras que Lazarus (2024) identifica una lógica semejante en las redes dedicadas al fraude por correo electrónico empresarial. Esta organización facilita que un actor adquiera accesos, programas maliciosos, credenciales o mecanismos de monetización sin controlar toda la cadena delictiva. Las criptomonedas fortalecen dichas conexiones al facilitar pagos y transferencias transnacionales; sin embargo, su presencia no constituye por sí misma evidencia de criminalidad, porque también poseen usos legítimos. Trozze et al. (2022) advierten que la relación entre criptoactivos y delito debe analizarse atendiendo al contexto, los patrones transaccionales y los mecanismos de ocultamiento utilizados. De manera similar, Nazzari (2023) demuestra que el lavado de ganancias cibercriminales combina recursos digitales con intermediarios y sistemas financieros convencionales. Por ello, las respuestas centradas únicamente en prohibir tecnologías específicas resultarían insuficientes. La intervención debería orientarse hacia las relaciones funcionales que sostienen el ecosistema, especialmente los proveedores de acceso, intermediarios financieros, plataformas de intercambio y mecanismos de conversión de activos ilícitos.

Los modelos de responsabilidad vicaria e identificación ofrecen una vía inicial para vincular la conducta de empleados, agentes o directivos con la empresa, pero presentan limitaciones ante organizaciones descentralizadas y operaciones tecnológicamente complejas. La responsabilidad vicaria permite imputar a la persona jurídica los delitos cometidos dentro del ámbito funcional y en su beneficio; sin embargo, puede generar una atribución excesivamente automática si no se examinan la capacidad de control y la relación real entre el hecho y la estructura empresarial (Kurniawan & Hapsari, 2022; Silver, 2023). El modelo de identificación, por su parte, exige localizar la voluntad corporativa en los órganos superiores, supuesto difícil de acreditar cuando las decisiones sobre datos, ciberseguridad, contratación tecnológica y operaciones financieras se encuentran fragmentadas. Horder y Watts (2023) muestran que la atribución a altos directivos por delitos de empleados o agentes plantea problemas cuando aquellos no poseen conocimiento directo ni control inmediato sobre la conducta. En consecuencia, estos modelos pueden producir dos efectos contrapuestos: dejar impunes deficiencias organizacionales graves por no identificarse a una persona que concentre la decisión o responsabilizar a la empresa únicamente por la relación laboral con el autor. Por ello, su aplicación requiere complementarse con criterios que examinen el beneficio corporativo, la previsibilidad del riesgo, la distribución efectiva de competencias y la calidad de los mecanismos internos de supervisión.

Los modelos basados en el defecto de organización y la cultura corporativa ofrecen una respuesta más adecuada frente a delitos producidos mediante decisiones colectivas, omisiones acumuladas o controles distribuidos. Aguilera Gordillo (2024) plantea que la responsabilidad de la persona jurídica puede sustentarse en la ausencia o ineficacia de mecanismos destinados a prevenir riesgos propios de su actividad, lo que permite analizar el funcionamiento empresarial sin depender exclusivamente de la identificación de un autor individual. A su vez, Ali et al. (2023) destacan que la cultura corporativa puede revelar tolerancia, incentivo o indiferencia frente al incumplimiento, incluso cuando no existe una orden explícita de cometer el delito. No obstante, estos enfoques también presentan riesgos: si todo incidente tecnológico se interpreta como prueba de una organización defectuosa, la responsabilidad penal podría transformarse en una forma de responsabilidad objetiva. Por ello, resulta indispensable valorar

la previsibilidad del riesgo, la capacidad real de intervención y la adecuación de los controles antes del hecho. Asimismo, un programa de cumplimiento meramente formal no debería excluir la responsabilidad cuando carece de recursos, supervisión o aplicación efectiva. La tendencia regulatoria identificada por Zazzaro (2025) refuerza esta orientación preventiva, pero la diversidad entre jurisdicciones demuestra que todavía no existe uniformidad sobre los efectos eximentes o atenuantes del cumplimiento. En consecuencia, la eficacia material, y no la simple existencia documental, debe constituir el criterio principal de valoración.

La ciberseguridad y la inteligencia artificial amplían el contenido de los deberes empresariales de prevención, pero también obligan a distinguir cuidadosamente entre la empresa víctima de un ataque y aquella que crea, facilita o tolera riesgos penalmente relevantes. Aslan et al. (2023) muestran que las vulnerabilidades pueden originarse en fallas técnicas, configuraciones inadecuadas, errores humanos o ausencia de actualizaciones; sin embargo, la materialización de una amenaza no demuestra por sí sola la existencia de responsabilidad corporativa. La imputación requiere valorar si el riesgo era previsible, si la organización contaba con capacidad para mitigarlo y si omitió controles razonables. Esta exigencia adquiere mayor complejidad cuando intervienen sistemas de inteligencia artificial, debido a la distribución de funciones entre desarrolladores, proveedores, administradores y usuarios. Rote et al. (2025) relacionan las fallas inducidas por inteligencia artificial con decisiones corporativas sobre diseño, implementación y supervisión, desplazando el análisis desde la supuesta autonomía del sistema hacia la gestión humana del riesgo. En consecuencia, los programas de cumplimiento deben incorporar evaluación de impactos, trazabilidad, supervisión humana y protocolos de respuesta. No obstante, estas obligaciones deben aplicarse proporcionalmente al tamaño, actividad y capacidad tecnológica de la empresa, pues exigir medidas idénticas a todas las organizaciones podría convertir el deber preventivo en una carga imposible y debilitar la legitimidad de la responsabilidad penal.

La naturaleza transnacional de la delincuencia digital organizada exige respuestas coordinadas, pues la fragmentación jurisdiccional permite que los participantes, las infraestructuras y los activos se distribuyan estratégicamente entre países con capacidades regulatorias diferentes. Lutovac y Lutovac (2022) subrayan que el anonimato y la actuación

internacional de los grupos cibercriminales dificultan su identificación y requieren cooperación entre autoridades. Esta dificultad se intensifica cuando los fondos circulan mediante criptomonedas, plataformas de intercambio o intermediarios ubicados en varias jurisdicciones. Anggriawan y Susila (2024) destacan la necesidad de fortalecer la identificación de usuarios, la trazabilidad de operaciones y la aplicación de estándares internacionales contra el lavado de activos. Asimismo, Subbagari (2023) sostiene que las medidas tradicionales de prevención financiera deben adaptarse a los mecanismos tecnológicos contemporáneos. Sin embargo, la armonización normativa no debería limitarse a incrementar obligaciones o sanciones, sino establecer criterios comunes sobre obtención, conservación, intercambio y valoración de la evidencia digital. También debe garantizarse la legalidad de las actuaciones, la protección de datos y el derecho de defensa. En materia empresarial, la cooperación internacional resulta indispensable para determinar qué organización administraba el riesgo, qué controles podía ejercer y quién obtuvo el beneficio. Sin reglas compatibles, una misma conducta puede quedar sin sanción, investigarse de forma duplicada o recibir respuestas contradictorias entre jurisdicciones.

En el plano teórico, los hallazgos permiten articular la criminología digital con la responsabilidad penal empresarial mediante una categoría común: la organización del riesgo. Desde la criminología, el continuo físico-digital propuesto por Di Nicola et al. (2025) desplaza la atención desde la forma externa de los grupos hacia su capacidad de coordinación, continuidad y especialización. Desde el derecho penal empresarial, el enfoque organizacional defendido por Aguilera Gordillo (2024) permite examinar cómo las políticas, controles y decisiones corporativas contribuyen a prevenir o facilitar conductas ilícitas. Esta convergencia resulta útil para analizar situaciones en las que empresas legítimas, intermediarios tecnológicos y redes criminales participan en una misma cadena operativa con diferentes niveles de conocimiento y control. En el ámbito práctico, los resultados justifican que las organizaciones incorporen los riesgos digitales a sus programas de cumplimiento, supervisen a proveedores, aseguren la trazabilidad de las decisiones automatizadas y conserven evidencia sobre los controles aplicados. Asimismo, las autoridades deberían emplear equipos interdisciplinarios capaces de combinar análisis jurídico, financiero y tecnológico. No obstante, como advierte Zazzaro

(2025), la diversidad de modelos regulatorios exige evitar soluciones uniformes que ignoren las particularidades nacionales. Por ello, el principal aporte de la revisión no consiste en proponer una imputación automática, sino en ofrecer criterios integrados para diferenciar entre victimización empresarial, facilitación negligente, tolerancia organizacional y participación corporativa deliberada.

Esta revisión presenta limitaciones que deben considerarse al interpretar sus aportes. La búsqueda se restringió a Scopus, Web of Science y SciELO, a publicaciones en inglés y español y al periodo comprendido entre 2022 y abril de 2026, por lo que podrían haberse omitido estudios difundidos en otros idiomas, bases especializadas o fuentes jurídicas nacionales. Asimismo, la heterogeneidad de los trabajos —empíricos, doctrinales, comparados, conceptuales y de revisión— impidió establecer una jerarquía uniforme de evidencia. En 30 publicaciones no se registró el cuartil SJR y solo seis contaban con una clasificación metodológica explícita, lo que limitó la caracterización cuantitativa del corpus. Además, el predominio de análisis teóricos redujo la posibilidad de contrastar los modelos de responsabilidad con decisiones judiciales concretas. Las futuras investigaciones deberían examinar expedientes sobre ransomware, criptoactivos, servicios tercerizados e inteligencia artificial, así como comparar la aplicación de los modelos de imputación en diferentes jurisdicciones. La propuesta físico-digital de Di Nicola et al. (2025) requiere mayor validación empírica, mientras que los riesgos empresariales asociados con inteligencia artificial identificados por Rote et al. (2025) demandan estudios sobre trazabilidad y supervisión humana. También resulta necesario analizar contextos latinoamericanos, pequeñas empresas e intermediarios tecnológicos para construir estándares de prevención proporcionales y jurídicamente aplicables.

# Capítulo V

## CONCLUSIONES Y RECOMENDACIONES

## CAPITULO V CONCLUSIONES Y RECOMENDACIONES

### 5.1. CONCLUSIONES

La revisión narrativa permitió concluir que la delincuencia digital organizada representa una transformación sustantiva de las formas tradicionales de criminalidad organizada. Las estructuras jerárquicas, territoriales y sustentadas en relaciones personales coexisten actualmente con redes flexibles, descentralizadas, transnacionales y tecnológicamente mediadas. Estas nuevas configuraciones conservan elementos esenciales de organización, como la continuidad, colaboración, especialización funcional y finalidad lucrativa, aunque no recurran necesariamente a la violencia, el control territorial o una dirección centralizada. En consecuencia, su reconocimiento criminológico requiere adoptar criterios capaces de comprender la organización criminal dentro de un continuo físico-digital.

El ransomware, el fraude mediante correo electrónico empresarial, los mercados clandestinos, las criptomonedas y el lavado de activos constituyen manifestaciones interrelacionadas de un ecosistema criminal digital. La tercerización de funciones y el acceso a servicios ilícitos especializados permiten que distintos participantes intervengan en etapas específicas sin conocer o controlar toda la operación. Esta fragmentación incrementa la capacidad de adaptación y permanencia de las redes, pero dificulta establecer los niveles de participación y responsabilidad. Las criptomonedas cumplen una función relevante en la transferencia y ocultamiento de beneficios, aunque su utilización no constituye por sí misma evidencia de una actividad delictiva y debe evaluarse según el contexto y los patrones operativos.

Los modelos tradicionales de responsabilidad vicaria e identificación resultan insuficientes cuando las decisiones y los conocimientos se encuentran distribuidos entre empleados, directivos, proveedores y sistemas automatizados. Frente a esta limitación, el defecto de organización y la cultura corporativa ofrecen fundamentos más adecuados para valorar la responsabilidad autónoma de la empresa. No obstante, su aplicación debe evitar una responsabilidad penal objetiva: la imputación requiere demostrar una relación concreta entre el

delito, el riesgo previsible, la capacidad empresarial de control, el beneficio obtenido y la omisión de medidas razonables de prevención.

La ciberseguridad, la inteligencia artificial y la automatización amplían los deberes empresariales de identificación, supervisión y mitigación de riesgos tecnológicos. Los programas de cumplimiento adquieren relevancia cuando se encuentran efectivamente implementados, adaptados a las características de la organización y respaldados por recursos, capacitación, monitoreo y mecanismos de respuesta. Su sola existencia documental no debería excluir o atenuar la responsabilidad. Asimismo, debe diferenciarse entre la empresa que sufre un ataque, aquella que facilita negligentemente una operación y la organización que tolera, promueve o se beneficia deliberadamente de la conducta delictiva.

Por último, persiste una limitada articulación entre los estudios criminológicos sobre redes criminales digitales y la literatura jurídica sobre responsabilidad penal empresarial. La ausencia de criterios regulatorios armonizados, las dificultades para conservar y compartir evidencia digital y las diferencias entre jurisdicciones generan vacíos de imputación frente a operaciones transnacionales. Por ello, se requiere desarrollar un marco integrado que relacione la estructura funcional del delito, la administración corporativa del riesgo y los deberes de prevención. Este marco deberá sustentarse en cooperación internacional, estándares probatorios compatibles y criterios de responsabilidad proporcionales, capaces de responder a la complejidad tecnológica sin debilitar las garantías propias del derecho penal.

## **5.2. RECOMENDACIONES**

Se recomienda que los legisladores y organismos reguladores actualicen los marcos jurídicos aplicables a la delincuencia digital organizada y la responsabilidad penal empresarial, incorporando criterios que permitan valorar las estructuras criminales descentralizadas, la fragmentación de decisiones y la intervención de sistemas automatizados. Esta actualización debe armonizar los mecanismos de atribución sin establecer responsabilidades automáticas, garantizando que la imputación se sustente en la previsibilidad del riesgo, la capacidad de control, el beneficio corporativo y la omisión de medidas razonables de prevención.

Las autoridades judiciales, fiscales y policiales deberían fortalecer la cooperación internacional para investigar operaciones que involucren participantes, plataformas, servidores y activos distribuidos en diferentes jurisdicciones. Resulta necesario establecer procedimientos compatibles para obtener, conservar, intercambiar y valorar evidencia digital, así como mejorar la trazabilidad de transacciones con criptoactivos. Estas medidas deben aplicarse respetando la legalidad, la protección de datos, la cadena de custodia y el derecho de defensa.

Se recomienda que las empresas integren los riesgos digitales en sus programas de cumplimiento penal y eviten limitarse a adoptar protocolos meramente formales. Los sistemas preventivos deben incluir evaluaciones periódicas de ciberseguridad, controles de acceso, debida diligencia sobre trabajadores y terceros, capacitación, canales de denuncia, monitoreo de operaciones financieras y planes de respuesta ante incidentes. Asimismo, deben asignarse recursos suficientes y responsabilidades claramente definidas para garantizar la aplicación efectiva de estas medidas.

Las organizaciones que emplean inteligencia artificial o procesos automatizados deberían implementar mecanismos de trazabilidad, validación de datos, supervisión humana y evaluación de impactos. También conviene documentar las decisiones relacionadas con el diseño, adquisición, implementación y actualización de los sistemas, de manera que pueda demostrarse cómo fueron identificados y gestionados los riesgos previsibles. Estas exigencias deben aplicarse proporcionalmente al tamaño, actividad y capacidad tecnológica de cada empresa.

Para finalizar, se recomienda desarrollar investigaciones empíricas y comparadas sobre la aplicación judicial de los modelos de responsabilidad penal empresarial en casos de ransomware, fraude digital, lavado de activos con criptomonedas y fallas de ciberseguridad vinculadas con inteligencia artificial. Deben priorizarse estudios realizados en contextos latinoamericanos y en pequeñas y medianas empresas, debido a la limitada evidencia disponible. Asimismo, resulta pertinente evaluar la eficacia real de los programas de cumplimiento y formular criterios que permitan diferenciar entre la empresa víctima, la facilitación negligente, la tolerancia organizacional y la participación corporativa deliberada.

## REFERENCIAS BIBLIOGRAFICAS

- Aguilera Gordillo, R. (2024). Socio-legal basis of criminal liability of legal persons and corporate compliance to prevent crimes: Anthropic approach and behavioral game theory. *Oñati Socio-Legal Series*, 14(2), 530–553. <https://doi.org/10.35295/osls.iisl.1830>
- Ali, H. M., Said, M. H. M., & Che Man, S. Z. B. (2023). Corporate culture as a means of proving *mens rea* in corporate criminal liability under Malaysian anti-corruption law. *Jurnal Undang-Undang dan Masyarakat*, 33. <https://doi.org/10.17576/juum-2023-33-10>
- Anggriawan, R., & Susila, M. (2024). Cryptocurrency and its nexus with money laundering and terrorism financing within the framework of FATF recommendations. *Novum Jus*, 18(2). <https://doi.org/10.14718/novumjus.2024.18.2.10>
- Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yılmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6), 1333. <https://doi.org/10.3390/electronics12061333>
- Botchkovar, E. V., Cui, K., Antonaccio, O., Perkins, R., & Maimon, D. (2025). The organized activities of ransomware groups: A social network approach. *Technology in Society*, 81, 102873. <https://doi.org/10.1016/j.techsoc.2025.102873>
- Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trends in Organized Crime*. <https://doi.org/10.1007/s12117-022-09457-y>
- Di Nicola, A., Baratto, G., & Vettori, B. (2025). Criminological definitions of organized crime on the digital test bench: Towards a physical–digital framework. *Trends in Organized Crime*. <https://doi.org/10.1007/s12117-025-09575-3>
- Díaz, C. (2024). Corporate criminal liability: Similarities and differences between Spain and Philippines. *Forensic Research & Criminology International Journal*, 12. <https://doi.org/10.15406/frcij.2024.12.00416>
- Ghose, P., Parvin, M., Akter, S., Rakib, S., & Bhuiyan, M. R. I. (2025). Gravitating towards technology-based emerging financial crime: A PRISMA-based systematic review. *International Journal of Innovative Research and Scientific Studies*, 8(2). <https://doi.org/10.53894/ijirss.v8i2.6014>

- Hartmann, A. (2025). From syndicates to protocols: Rethinking organized crime in the age of cybercrime. *International Journal of Criminology and Sociology*, 14. <https://doi.org/10.6000/1929-4409.2025.14.11>
- Horder, J., & Watts, G. (2023). Senior corporate managers' criminal liability for the crimes of employees or agents. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4414383>
- Ismaidar, I., AR, A., Telaumbanua, S. E., Tarigan, R. S., Maulana, A., Ndruru, R., Zalukhu, Z. E., Sinambela, L., Limbong, H. P. U., Saragih, E., Sembiring, R. Y. S. S., Mulyadi, M., Syavica, Z., Dharmawan, T. M. R. F., Hadi, M. F., Ibrahim, I., Rangkuti, E. E., Husny, T. I. A., Siahaan, N. B., . . . Pangaribuan, C. N. (2025). A comparative study of corporate criminal liability systems in Indonesia and the United States. *Mutiara: Jurnal Penelitian dan Karya Ilmiah*, 3(3). <https://doi.org/10.59059/mutiara.v3i3.2268>
- Kurniawan, K. D., & Hapsari, D. R. I. (2022). Pertanggungjawaban pidana korporasi menurut vicarious liability theory. *Jurnal Hukum Ius Quia Iustum*, 29(2). <https://doi.org/10.20885/iustum.vol29.iss2.art5>
- Lavorgna, A., & Antonopoulos, G. A. (2022). Criminal markets and networks in cyberspace. *Trends in Organized Crime*. <https://doi.org/10.1007/s12117-022-09450-5>
- Lazarus, S. (2024). Cybercriminal networks and operational dynamics of business email compromise (BEC) scammers: Insights from the "Black Axe" confraternity. *Deviant Behavior*. <https://doi.org/10.1080/01639625.2024.2352049>
- Lusthaus, J., Kleemans, E., Leukfeldt, R., Levi, M., & Holt, T. (2023). Cybercriminal networks in the UK and beyond: Network structure, criminal cooperation and external interactions. *Trends in Organized Crime*. <https://doi.org/10.1007/s12117-022-09476-9>
- Lusthaus, J., van Oss, J., & Amann, P. (2022). The Gozi group: A criminal firm in cyberspace? *European Journal of Criminology*. <https://doi.org/10.1177/14773708221077615>
- Lutovac, S., & Lutovac, N. (2022). The role of digital technologies in organized crime. *Megatrend Revija*. <https://doi.org/10.5937/megrev2202069>
- Nazzari, M. (2023). From payday to payoff: Exploring the money laundering strategies of cybercriminals. *Trends in Organized Crime*. <https://doi.org/10.1007/s12117-023-09505-1>

- Rote, N., Bhardwaj, S., & Sebastian, D. (2025). Corporate criminal liability for AI-induced cybersecurity failures in healthcare systems. *Lex Localis—Journal of Local Self-Government*. <https://doi.org/10.52152/800212>
- Saipudin, L., Hs, S., Rodliyah, R., & Wulandari, L. (2025). The concept of corporate criminal liability in the Indonesian criminal law system. *Jurnal IUS Kajian Hukum dan Keadilan*, 13(2). <https://doi.org/10.29303/ius.v13i2.1817>
- Silver, K. (2023). When should the master answer? *Respondeat superior* and the criminal law. *Criminal Law and Philosophy*. <https://doi.org/10.1007/s11572-023-09659-7>
- Smith, S. F. (2022). Corporate criminal liability: End it, don't mend it. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4031945>
- Subbagari, S. (2023). Counter measures to combat money laundering in the new digital age. *Digital Threats: Research and Practice*. <https://doi.org/10.1145/3626826>
- Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T. P., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, 11. <https://doi.org/10.1186/s40163-021-00163-8>
- Vuletić, I. (2023). Corporate criminal liability: An overview of the Croatian model after 20 years of practice. *Laws*, 12(2), 27. <https://doi.org/10.3390/laws12020027>
- Whelan, C., Bright, D., & Martin, J. (2023). Reconceptualising organised (cyber)crime: The case of ransomware. *Journal of Criminology*. <https://doi.org/10.1177/26338076231199793>
- Zazzaro, F. (2025). Corporate criminal liability in EU directives: An overview of the EU discipline. *New Journal of European Criminal Law*. <https://doi.org/10.1177/20322844251338625>

# Delincuencia digital organizada y responsabilidad penal empresarial:

transformaciones criminológicas, modelos de atribución y desafíos regulatorios

## SINOPSIS

La presente obra examina, desde una perspectiva interdisciplinaria, los principales desafíos que plantea la delincuencia digital organizada y la responsabilidad penal empresarial en un entorno global caracterizado por la transformación tecnológica, la interconexión de mercados y la creciente sofisticación de las amenazas cibernéticas.

A través del análisis de las transformaciones criminológicas, los modelos de atribución de responsabilidad penal y los desafíos regulatorios contemporáneos, los autores ofrecen un enfoque crítico y propositivo orientado a fortalecer la prevención, la detección y la sanción de conductas delictivas en el ámbito digital, así como a promover una cultura empresarial de integridad, cumplimiento normativo y responsabilidad social.

Dirigido a académicos, profesionales del derecho, del compliance, de la ciberseguridad y de la gestión empresarial, este libro constituye un aporte significativo para el debate actual sobre la gobernanza digital, la seguridad jurídica y la construcción de entornos económicos más éticos, seguros y sostenibles.

## AUTORES



Nayrud Suarez Sanchez



Teódulo Jenaro Santos Cruz



Jorge Luis Cueva Zavaleta



Diógenes Arquímedes  
Jiménez Domínguez



Jorge David Ríos Gonzales

**Editorial  
CICI**

CENTRO DE INVESTIGACIONES  
Y CAPACITACIONES INTERDISCIPLINARES

*Conocimiento que genera  
sociedades más seguras*

*“Un entorno digital  
seguro también es  
un pilar del desarrollo  
sostenible.”*



CIBERSEGURIDAD  
Y PREVENCIÓN



RESPONSABILIDAD  
EMPRESARIAL



MARCO  
REGULATORIO



DESAFÍOS  
GLOBALES

CIBERCRIMEN

RESPONSABILIDAD PENAL

GOBERNANZA DIGITAL

COMPLIANCE

ISBN:  
978-628-97866-1-3

*Derecho, tecnología  
y ética para un futuro  
más justo*