OBS Business School

La Ciberseguridad desde un enfoque normativo

Ramón Miralles
Profesor de OBS Business School

Septiembre, 2025

Partners Académicos:

Universitat de Barcelona

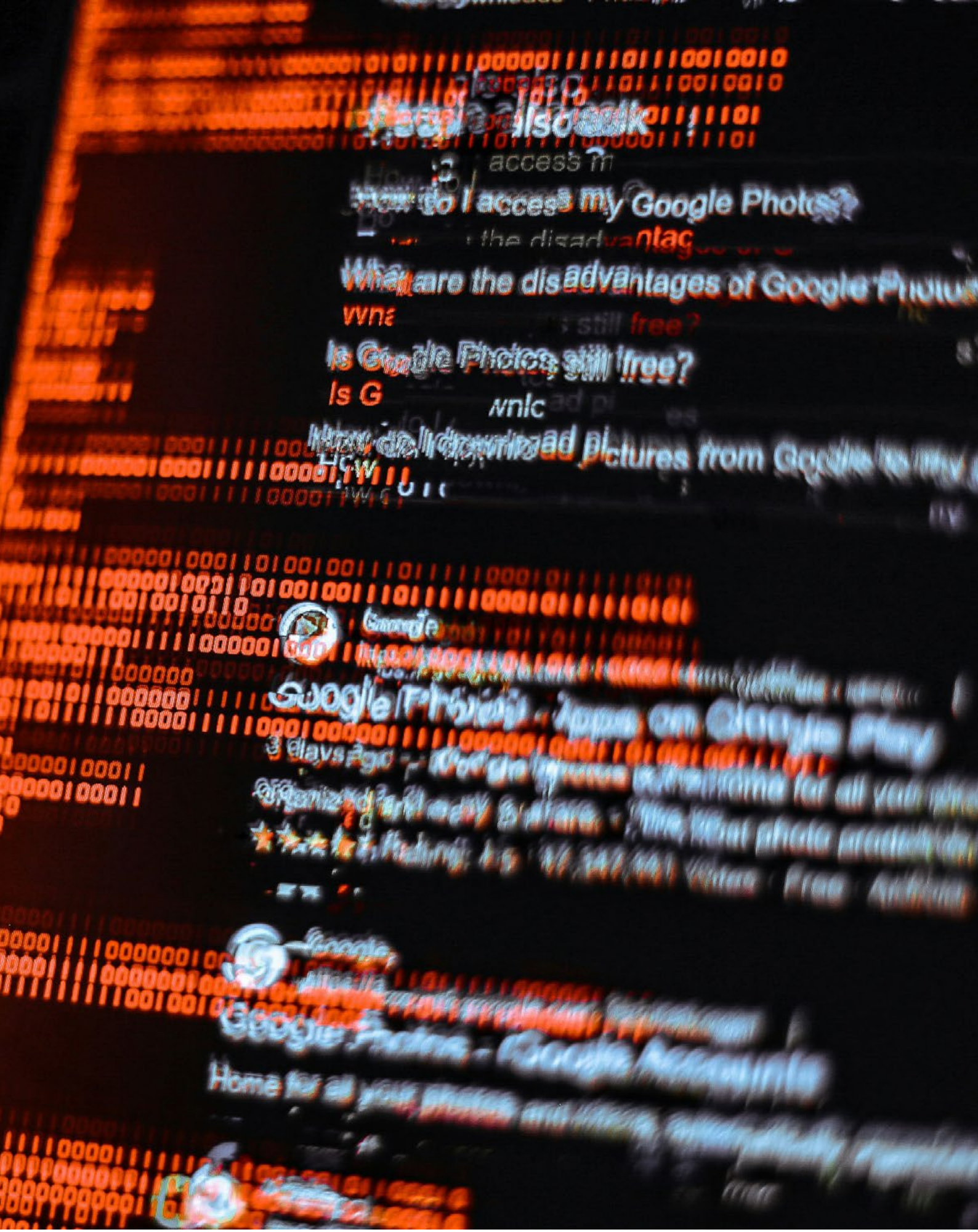
unie Universidad

OBSbusiness.school

Autor

Ramón Miralles
*Profesor de **OBS Business School.***

Ramón Miralles es licenciado en Derecho por la Universidad de Barcelona, colegiado como ejerciente en el Ilustre Colegio de Abogados de Barcelona, con una experiencia profesional de más de 38 años en el sector de las TIC, dedicados fundamentalmente a dirigir proyectos de modernización digital en las administraciones públicas, primero en oficinas judiciales y después en la administración de la Generalitat de Catalunya y en el Ayuntamiento de Barcelona, asimismo destaca por su actividad en el ámbito empresarial, siendo actualmente Socio Director del Departamento de Privacidad, Compliance y Ciberseguridad en ECIJA Abogados, en Barcelona. Experto en sistemas de gestión de la seguridad de la información, y gestión de riesgos legales y tecnológicos, ha ocupado posiciones de CISO (seguridad de la información), CIO (tecnologías de la información) y CAE (auditoria), certificado profesionalmente en ámbitos de seguridad de la información y privacidad, y miembro de las juntas directivas de diferentes asociaciones profesionales. Profesor en diversos masters de formación permanente en OBS Business School: Ciberseguridad, Dirección de Sistemas y Tecnologías de la Información, Global Data Management, Machine Learning e Inteligencia Artificial y Tech MBA, así como en diversas Universidades y centros de estudios, en los que imparte materias relacionadas con los aspectos éticos y legales en el uso de las TIC. Ha participado activamente en proyectos relacionados con las tecnologías y la acción social, entre otros, en la consultoría TIC para el desarrollo del eje tecnológico del plan estratégico de la Defensa Pública de Costa Rica, en el contexto del programa Eurosocial II de la Comisión Europea, y en el grupo impulsado por la Red Iberoamericana de protección de datos, dedicado a la adecuación al derecho a la protección de datos de carácter personal en la acción humanitaria internacional. Ha recibido diferentes reconocimientos y premios: por el directorio internacional Best Lawyers, en sus ediciones 2022 y 2023, en el área de “Privacy & Data Protection Law”, y adicionalmente en la edición 2023 premiado como "Lawyer of the Year" por su trabajo en el área de Privacy & Data Protection Law en Barcelona; premio colectivo de la Agencia Vasca de Protección de Datos 2018 al “Observatorio Iberoamericano de Protección de Datos”; y premio 2018 al profesor mejor valorado por los alumnos del plan de formación de la Asociación Profesional Española de Privacidad (APEP).


Google Photos

Índice

Capítulo 1

Introducción y contexto

La frase, *"la libertad permite a gente como usted hacer lo que le dé la gana y los derechos nos protegen a los demás de gente como usted",* pronunciada por Robert De Niro en el papel de George Mullen en la serie "Zero Day"[1], resume a la perfección la **necesidad de que existan normas que regulen el uso de las tecnologías**.

La historia de la humanidad está repleta de avances tecnológicos en base a descubrimientos e invenciones, que tienen como denominador común el hecho de aportar evidentes **ventajas y beneficios** para el propio desarrollo de la humanidad, pero que a la vez han generado **nuevos riesgos o potenciados los ya existentes**, o bien han provocado la necesidad de abordar retos de adaptación a las nuevas circunstancias derivadas de esos avances tecnológicos.

Hay multitud de ejemplos contemporáneos al respecto: la energía, la industria automovilística, la industria farmacéutica y de la salud, la aviación comercial, etc., simplemente por citar algunos entornos en los cuales esa paradoja de "beneficio" versus riesgos resulta evidente.

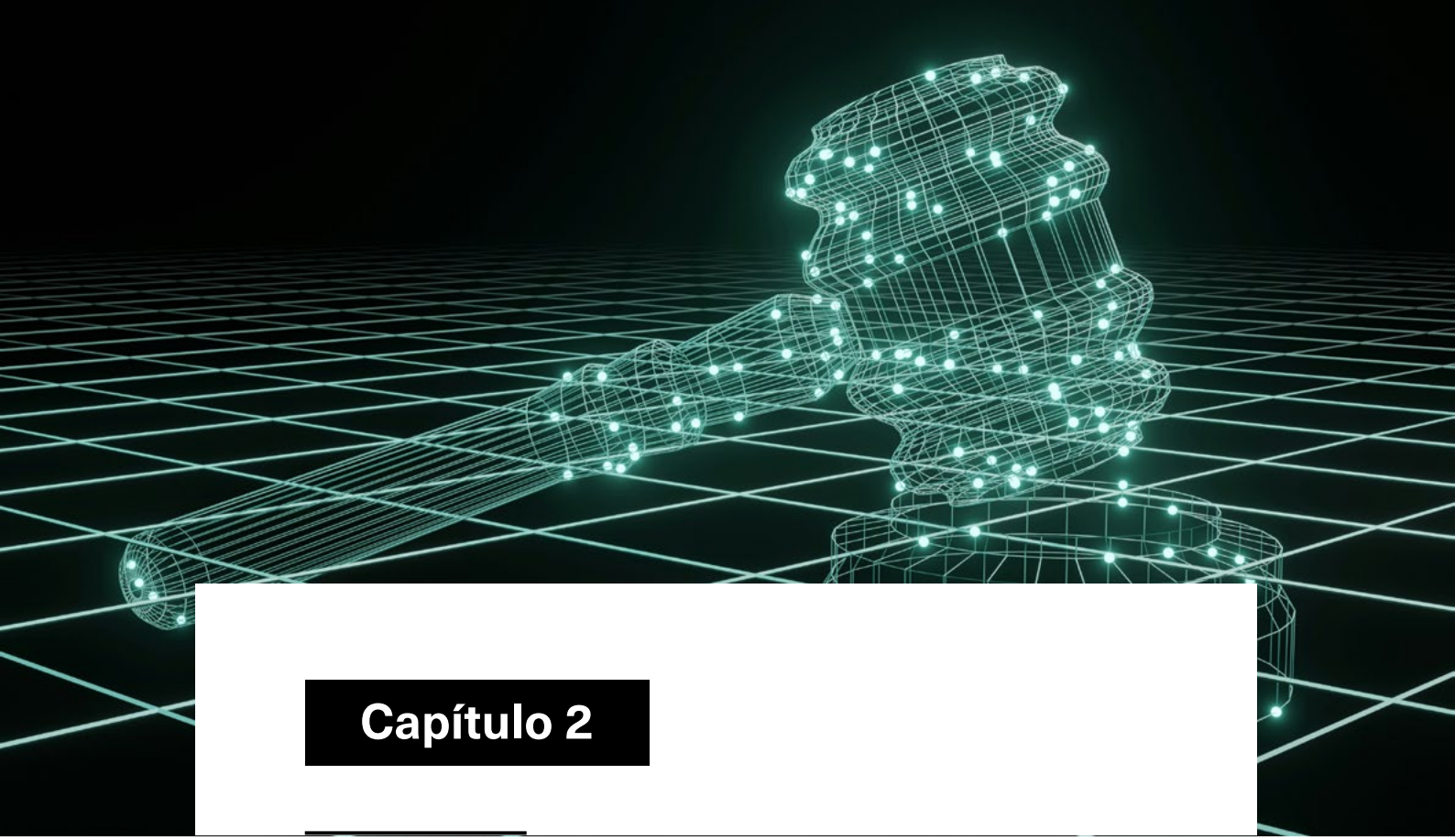
En esos supuestos, el papel de la regulación no ha sido otro que intentar mitigar esos riesgos mediante la incorporación de principios, derechos y obligaciones, de contenido jurídico, es decir, cumpliendo con la función social que debe asumir la regulación, que no es otra que crear unas condiciones de protección y convivencia aceptables, y de equilibrio, entre los intereses que pueden entrar en conflicto en determinadas situaciones.

Las tecnologías de la información y la comunicación entrañan **riesgos inherentes por su mero uso**, en buena parte el origen de esos riesgos se encuentra en amenazas como los ciberataques, cada vez más numerosos, más sofisticados y más eficaces para los intereses de los ciberdelincuentes, de ahí la necesidad de que, desde diferentes perspectivas, se regule **la ciberseguridad como una obligación jurídica**.

La toma de decisiones en materia de ciberseguridad ya no depende exclusivamente de la voluntad de proteger los activos de información usados por empresas o por el sector público, es un requisito jurídico para la protección de un **nuevo bien jurídico: la seguridad de la información**.

En la era digital la información ha adquirido un valor estratégico sin precedentes, ya que es un recurso vital para el desarrollo de las actividades empresariales y de servicio público, y además se han convertido en una extensión digital de lo que son, piensan y hacen las personas individualmente y las sociedades, en definitiva, las tecnologías están irremediablemente vinculadas a la evolución de la humanidad.

[1] Thriller de conspiración política, que se desarrolla alrededor de un ciberataque de alcance global con consecuencias devastadoras; se estrenó el 20 de febrero de 2025 en la plataforma Netflix. La frase se la dirige George Mullen a la multimillonaria de las tecnologías Monica Kidder (Gaby Hoffmann), que estuvo involucrada en el ciberataque, al ser responsable de difundir malware a través de actualizaciones de su aplicación, que se había descargado en un «80% de los teléfonos en Estados Unidos».



Capítulo 2

La ciberseguridad como derecho y bien jurídico

En el contexto descrito, la seguridad de la información ha dejado de ser una cuestión exclusivamente técnica, para convertirse en un nuevo bien jurídico, cuya protección se ha convertido en una prioridad en los actuales ordenamientos jurídicos, pero la legislación sobre ciberseguridad aún va más allá, **atribuyendo a la ciberseguridad la categoría de derecho**.

Se trata de un bien jurídico que no solo está vinculado a la proteccion de intereses individuales, es *"el Derecho que todos tienen para el desenvolvimiento normal de sus vidas en paz, sosiego, bienestar y tranquilidad"*, **también en relación al uso de las tecnologías y del ciberespacio**[2].

La ciberseguridad a la práctica cumple con los requisitos formales que permiten considerarla un bien jurídico, en primer lugar porque tiene **valor social**, ya que su afectación puede comprometer la confianza en las instituciones, las empresas, los mercados y las relaciones personales; además, es **susceptible de lesión**, a causa de los ciberataques; y, como analizaremos en este estudio, es **objeto de protección por parte del ordenamiento jurídico** mediante leyes y otras normas, que regulan tanto la protección de los activos de información, como la persecución y enjuiciamiento de quienes la lesionan.

[2] La Sentencia del Tribunal Supremo de 9 de octubre de 1984, en relación a los delitos calificados como delitos de peligro abstracto, definió el derecho a la seguridad colectiva como *"el Derecho que todos tienen para el desenvolvimiento normal de sus vidas en paz, sosiego, bienestar y tranquilidad"*.

La ciberseguridad ya es un derecho que, como el resto de los derechos reconocidos por las leyes, su ejercicio efectivo no está exento de dificultades tecnológicas, jurídicas y culturales.

En 1979 el jurista checo Karel Vasak, del Instituto Internacional de Derechos Humanos en Estrasburgo[3], empezó a plantear la existencia de 3 generaciones de derechos humanos[4].

Los derechos humanos de primera generación se situarían en el ámbito de los derechos civiles y políticos, tienen su origen en los movimientos revolucionarios de finales del siglo XVIII, el estado no debía interferir en el ejercicio de esos derechos y debía favorecer las condiciones para su ejercicio, algunos de esos derechos son la libertad de expresión, libertad de asociación, derecho a un debido proceso judicial o la libertad religiosa.

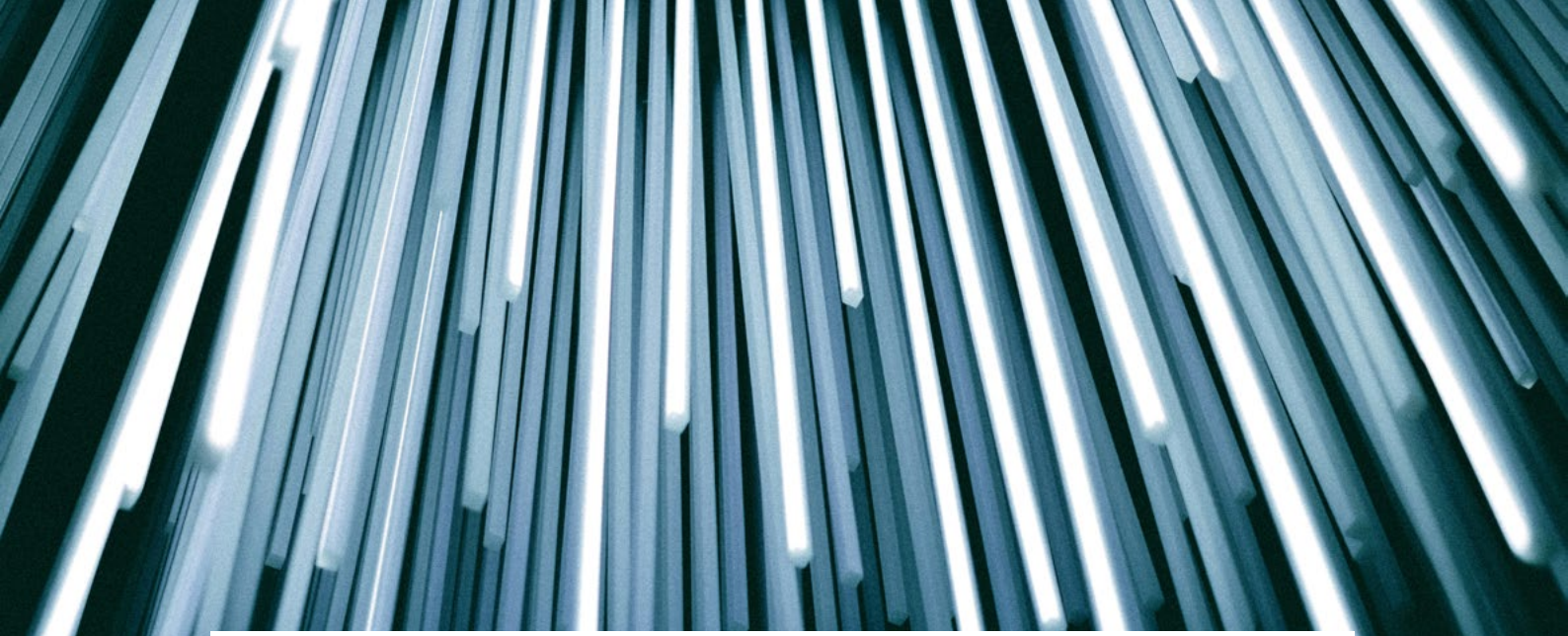
Los derechos de segunda generación son los derechos sociales, de tipo económico, social y cultural, en esencia son los que recoge la Declaración de 1948 de la Organización de Naciones Unidas[5], en este sentido el Estado de Derecho evoluciona hacía un Estado Social de Derecho.

Los derechos de tercera generación se plantean a partir de los años 80 y están estrechamente vinculados a la solidaridad, tienen en común el hecho de afectar a la vida de todos, tienen vocación de ser universales porque precisan de la colaboración de todos, por ejemplo, el derecho a la paz, a la protección del medioambiente o incluso acoge las garantías frente a la manipulación genética.

Y, finalmente, podemos añadir los derechos de cuarta generación[6], que tienen en común asegurar a todos los individuos el acceso libre y seguro a las tecnologías de la información y la comunicación, considerando que el paradigma de la sociedad de la información y del conocimiento obliga a ello.

En esa teórica cuarta generación de derechos se incluirían, entre otros: el derecho de acceso a la informática, el derecho al acceso a la información en condiciones de igualdad, al uso de las infraestructuras de telecomunicaciones, a la formación en las nuevas tecnologías, a la autodeterminación informativa[7], al "Habeas Data"[8] y la cuestión que nos ocupa en este informe: **el derecho a la seguridad digital o a la ciberseguridad**.

[3] https://www.iidh.org/
[4] Se trata de una teoría muy influenciada por la evolución de la legislación europea en materia de derechos humanos.
[5] https://www.un.org/es/about-us/universal-declaration-of-human-rights
[6] Como ejemplo tenemos la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales BOE-A-2018-16673 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
[7] https://www.cepc.gob.es/sites/default/files/2021-12/17224repne104037.pdf
[8] https://www.sic.gov.co/manejo-de-informacion-personal



Capítulo 3

Las estrategias nacionales de ciberseguridad

Las estrategias nacionales de ciberseguridad son documentos que definen la visión, los objetivos y las líneas de acción que un país adopta para proteger su ciberespacio, por tanto, determinan un **marco a partir del cual se van a desarrollar leyes y otras normas** que regularán principios, derechos y obligaciones en materia de ciberseguridad.

Estas estrategias elaboradas por los gobiernos se actualizan periódicamente para adaptarse a nuevas amenazas y tecnologías emergentes, y sirven de punto de partida del proceso legislativo, identificando los principales riesgos y vulnerabilidades del país en el ámbito digital y estableciendo las áreas en que debe enfocarse la regulación, como por ejemplo, la protección de infraestructuras críticas, la gestión de incidentes de ciberseguridad, la protección de datos personales, los ciberdelitos o la ciberdefensa.

La regulación de la ciberseguridad, con carácter general, aborda los requisitos de seguridad que deben tener en cuenta las entidades obligadas, partiendo siempre de un **enfoque a riesgos**, a lo que se añaden obligaciones relacionadas con la **notificación de incidentes de seguridad**, así como el establecimiento de un **régimen sancionador** para el caso de incumplimientos.

Como ejemplos de estrategias de ciberseguridad que han impulsado la creación de marcos jurídicos en materia de ciberseguridad, podemos aludir a la "Estrategia de Ciberseguridad de la UE para la Década Digital"[9] (Unión Europea)[10], de la cual se deriva la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión[11], que derogó la primera Directiva europea sobre ciberseguridad del 2016[12]. Este mismo planteamiento de contar con una estrategia de ciberseguridad, para después desarrollar un cuerpo normativo, se ha replicado en la mayoría de los países.

Por lo que respecta a Latinoamérica, en la presente década se ha avanzado significativamente en las definición de estrategias nacionales de ciberseguridad[13], sin perjuicio de que el grado de madurez entre los países de la región pueda ser diverso; las citadas estrategias han servido de base para la aprobación marcos jurídicos que, directa o indirectamente, han regulado cuestiones relacionadas con la ciberseguridad, también a partir de áreas como la protección de datos, los ciberdelitos, el comercio electrónico y la seguridad de las infraestructuras críticas.

[9] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOC_2022_067_R_0009 En el 2013 ya se aprobó una primer "Estrategia de ciberseguridad de la Unión Europea: «Un ciberespacio abierto, protegido y seguro»" https://www.europarl.europa.eu/doceo/document/TA-7-2013-0376_ES.html

[10] https://ec.europa.eu/commission/presscorner/detail/es/ip_20_2391

[11] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022L2555

[12] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32016L1148

[13] https://www.segurilatam.com/ciberilatam/estas-son-las-estrategias-nacionales-de-ciberseguridad-de-los-paises-latinoamericanos_20240514.html

Capítulo 4

La regulación de la ciberseguridad a nivel global

La ciber-inseguridad es un fenómeno global, como todas las cuestiones relacionadas con las tecnológicas de la información y la comunicación, y con internet.

El contexto de los ataques redes y sistemas, y el modus operandi de los ciber-atacantes[14], implica que desde cualquier lugar se pueda diseñar un ataque contra un objetivo ubicado a miles de kilómetros del centro de operaciones en el que se origina el ataque, sin que las fronteras físicas sean una barrera que pueda evitarlo, lo que conlleva que tampoco las leyes van ser un impedimento, ya que en su inmensa mayoría tienen un alcance de aplicación territorial[15], por tanto, la táctica[16] que siguen la leyes que regulan la ciberseguridad es la de **obligar a que se adopten las medidas de seguridad más adecuadas para mitigar los ciber-riesgos**, fomentando además la cooperación entre instituciones y países para reforzar la capacidad de esas leyes de minimizar los riesgos para la seguridad de los sistemas de información y las redes.

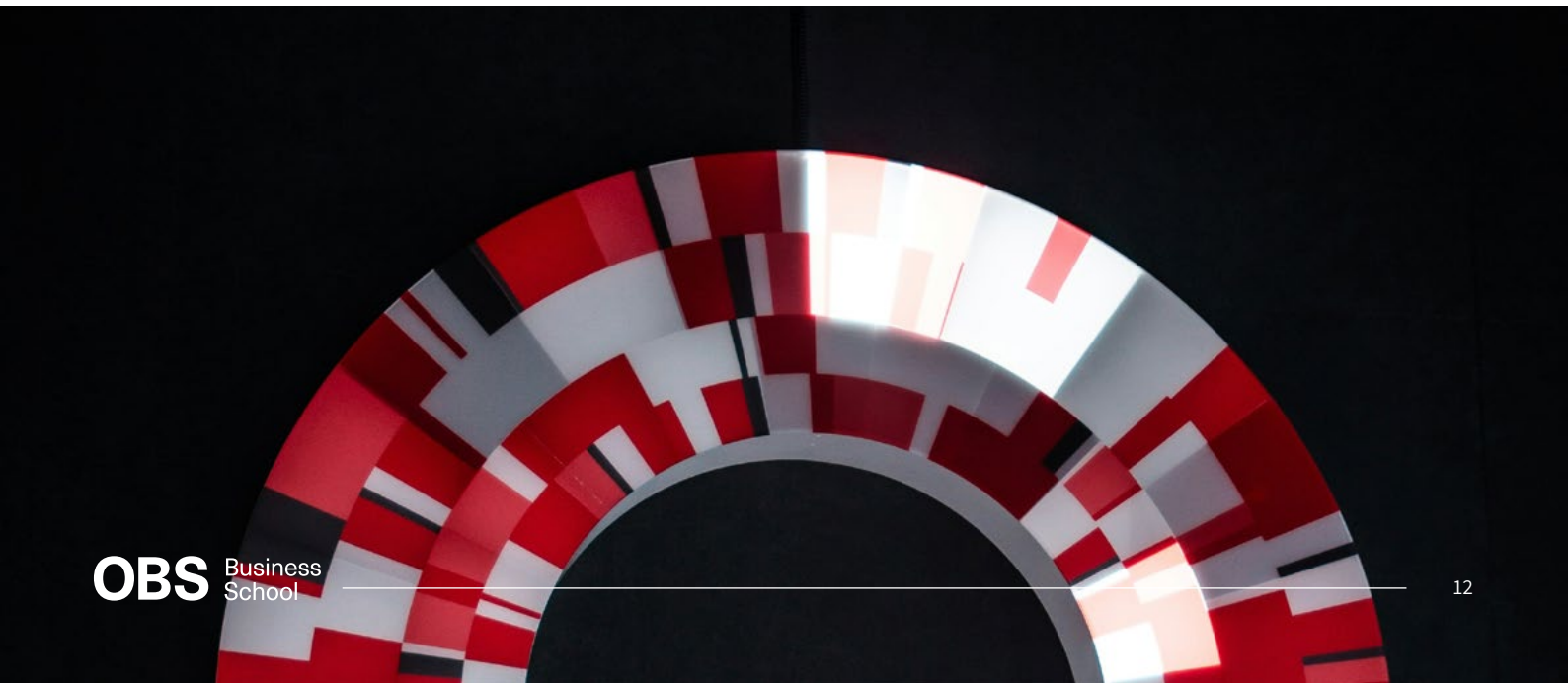
[14] En este concepto agrupamos cualquier motivación que conlleve afectar a la seguridad de los sistemas y redes, ya sea de tipo delictivo, político, por activismo, o derivada de conflicto entre países (ciberguerra o ciberespionaje).
[15] Sin perjuicio de la potencial aplicación de mecanismos e instrumentos jurídicos relacionados con el derecho internacional.
[16] Se trata de conseguir un alto nivel de seguridad de los sistemas y redes obligando, a todas las entidades públicas y privadas que participan en su gestión, a implementar medidas de seguridad que sean adecuadas para mitigar los riesgos a los que, de manera específica, pueden estar expuestos sus activos de información.

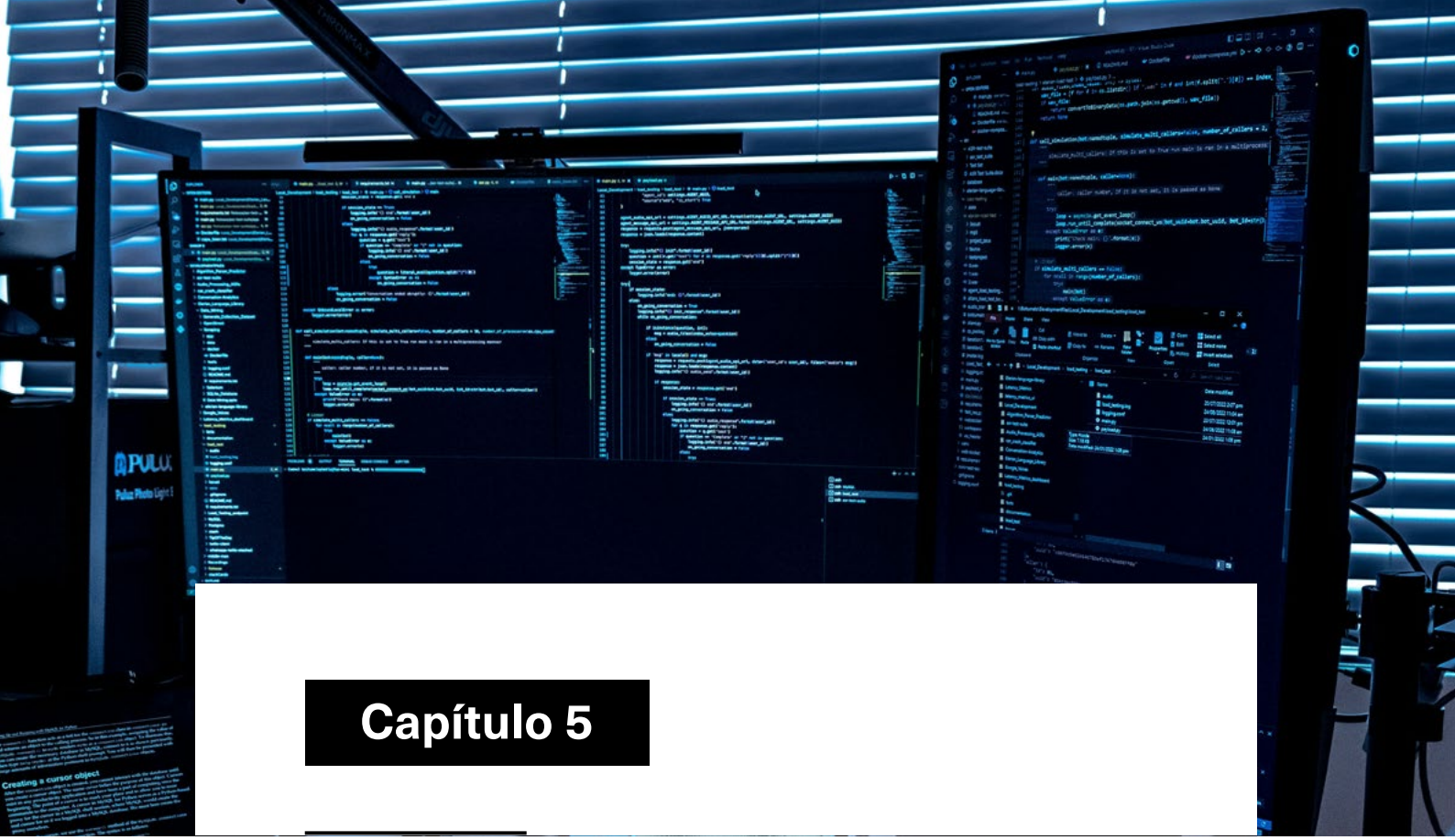
Los ciber-riesgos se resumen en la posibilidad de afectar negativamente a los servicios que se apoyan en el uso de tecnologías de la información y la comunicación, y en la posibilidad de afectar a la información que usan esos servicios, en ambos casos los ciberataques irán dirigidos a **lesionar la confidencialidad integridad y disponibilidad de los sistemas y/o de la información**. Las consecuencias de los ciberataques, en forma de daños y perjuicios, también se pueden resumir en: daños económicos, reputacionales, sociales y para las personas.

Los procesos legislativos para regular la ciberseguridad se puede considerar que son equivalentes en el contexto de los estados de derecho, pero existen **diferencias entre los países en cuanto al nivel de despliegue de leyes que regulan las cuestiones relativas a la ciberseguridad**, la diferencia no reside solo en la cultura jurídica y los mecanismos de regulación, también influye la capacidad de regular y de aplicar este tipo de leyes en cada país, lo cual a su vez está relacionado con su nivel de desarrollo económico y las prioridades en cuanto a qué dedicar los recursos del Estado y de las empresas.

En los que respecta a las leyes relativas a ciberseguridad, estas se pueden agrupar en dos tipos, aquellas que de manera específica se dedican a regular obligaciones relacionadas con la seguridad de la información y que tienen por objeto la **protección de lo que se consideran servicios esenciales** que se apoyan en el uso tecnologías de la información y la comunicación, orientándose a alcanzar un nivel homogéneo y alto en los que respecta a la protección de los sistemas y de redes, en particular los usados en las consideradas infraestructuras críticas; y aquellas **otras que regulan ámbitos en los que la ciberseguridad tiene un peso significativo**, como pueden ser el ámbito de las telecomunicaciones, el comercio electrónico, la protección de datos personales o los ciberdelitos, materias todas ellas en las que la componente seguridad de la información tienen un peso importante en relación al objeto principal que regulan.

A continuación, se analizan varios escenarios, a fin de comparar la situación de la regulación de la ciberseguridad en diferentes regiones geopolíticas, concretamente en la Unión Europea, haciendo foco en España, Latinoamérica y los Estados Unidos de América.





Capítulo 5

Análisis comparativo de las medidas legales en materia de ciberseguridad

La Unión Internacional de Telecomunicaciones (UIT)[17] es el organismo especializado de la Organización de Naciones Unidas para las tecnologías digitales, y entre las diversas actividades que lleva a cabo[18], elabora el denominado **"Global Cybersecurity Index"**(CGI)[19].

En la quinta edición del CGI[20] (2024) se evalúa compromiso de los países con la ciberseguridad, teniendo en cuenta las acciones que han llevado a cabo en los cinco pilares en que se fundamenta el cálculo del índice de ciberseguridad: **legal, técnico, organizativo, desarrollo de capacidades y cooperación**.

[17] https://www.itu.int/es/Pages/default.aspx#/es

[18] Tal y como describe en su página la actividad de la UIT se centra en las siguientes actividades: *"Facilitamos la conectividad internacional en las redes de comunicación. Atribuimos espectro radioeléctrico y órbitas de satélite de todo el mundo, elaboramos las normas técnicas que garantizan una conexión fluida de redes y tecnologías, y trabajamos para mejorar el acceso a las tecnologías digitales en comunidades insuficientemente atendidas de todo el mundo. La UIT trabaja para llevar la conectividad digital a todo el mundo, proporcionando una plataforma multilateral fiable para negociar acuerdos y normas internacionales, compartir conocimientos, crear capacidades y trabajar con miembros y asociados para extender el acceso a la tecnología en todo el mundo".*

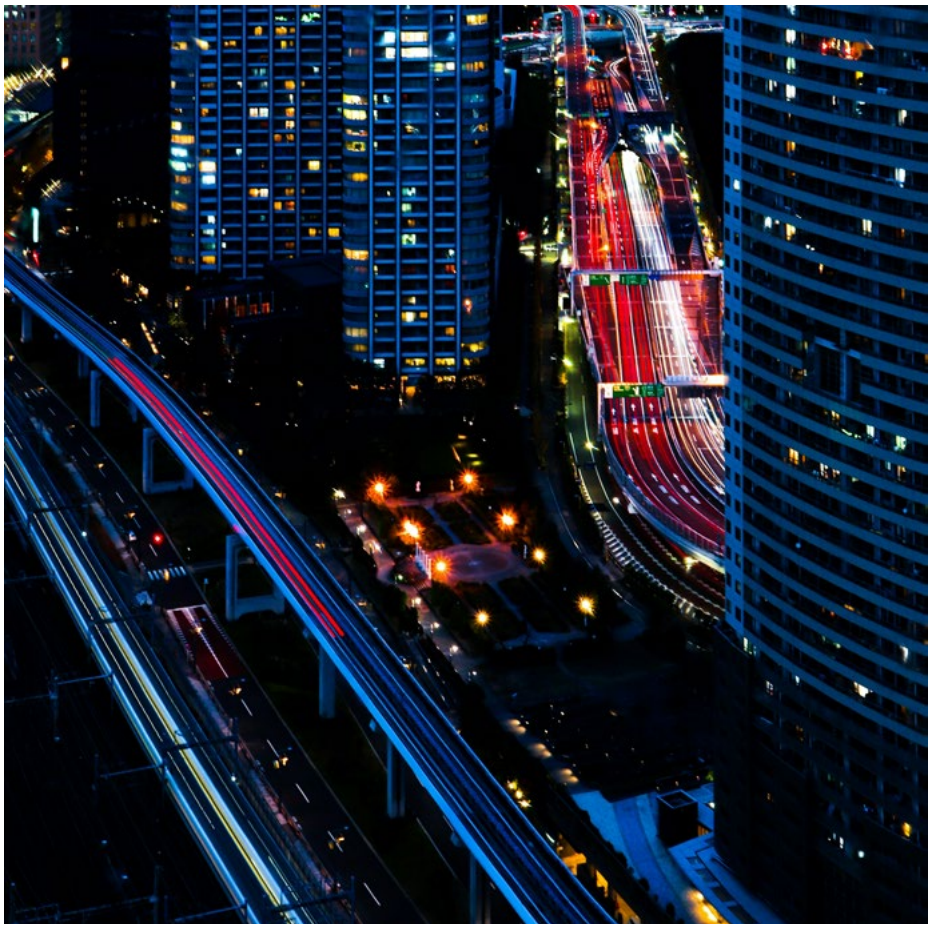
[19] https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf El último "Índice Global de Ciberseguridad" es el del año 2024 (5ª edición, publicada en septiembre de 2024), la primera edición se publicó en el 2015.

[20] Metodología utilizada para el cálculo de GCI https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/513560_2S.pdf

En relación a esos cinco pilares del GCI, la mayoría de los países analizados (194 países), donde muestran **mayores fortalezas es en el pilar de medidas legales**.

En el citado informe sobre el GCI 2024, se recogen algunas cifras significativas respecto de los desarrollos legislativos, por ejemplo: que 177 países (de 194) tenían en vigor o en desarrollo, al menos una regulación sobre protección de datos personales[21], protección de la privacidad o notificación de incidentes (brechas de seguridad), que 151 países tienen en vigor una normativa de protección de datos, o que en 104 disponen de regulaciones relacionadas con la protección de sus infraestructuras críticas.

Algunas de las conclusiones que recoge el GCI sobre las medidas legales se refieren a que buena parte de ellas están alineadas con el GDPR[22] o tratados internacionales sobre ciberdelincuencia[23], y se afirma que **las leyes y regulaciones de privacidad están aumentando y son cada vez más necesarias**.



[21] Complementariamente es útil el mapa interactivo de la CNIL "Data protection around the world", que permite consultar la legislación y otras cuestiones relativas a la regulación de la protección de datos personales en el mundo https://www.cnil.fr/en/data-protection-around-the-world

[22] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

[23] En este ámbito el Convenio de Budapest es muy relevante, ya que como tratado internacional ha impulsado desde su aprobación que determinadas conductas sean consideradas como delitos y por tanto, sancionables penalmente, en este informe se hace referencia más detallada al mismo

Capítulo 6

Regulación de la ciberseguridad en Europa y en España

La Unión Europea tiene desarrollado un **marco normativo con un alto grado de madurez**, y ello sin perjuicio de que muchas de sus normas sean de reciente aprobación o revisión; ese marco tiene por objeto, a través de diferentes medidas legislativas, proteger la infraestructura digital de la UE, garantizar la privacidad de los ciudadanos y fomentar la resiliencia frente a las ciberamenazas.

Por lo que respecta a la normativa específica en materia de Ciberseguridad, la principal normal de carácter general sería la denominada Directiva NIS2[24], que derogó la Directiva NIS del año 2016[25], es decir, se trata de una regulación que ya ha sido revisada y actualizada, en lo que podemos considerar un corto espacio de tiempo, al menos desde la perspectiva del ciclo de vida de los procesos legislativos.

[24] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022L2555

[25] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016L1148

Se trata de una regulación que aplica a los sectores esenciales[26] y servicios digitales, que principalmente obliga a las entidades sujetas a la norma[27] a **implementar políticas de seguridad y gestionar los riesgos de ciberseguridad, y los incidentes de seguridad** (ciber-incidentes), incluyendo obligaciones de notificación de las brechas de seguridad a las autoridades competentes, la formación de los empleados o las responsabilidades de los directivos.

Como derivadas de la Directiva NIS2 deben mencionarse dos leyes especiales, conocidas como Reglamento DORA y Reglamento MiCA.

El Reglamento DORA (Digital Operational Resilience Act)[28] tienen por objeto **garantizar la resiliencia operativa digital del sector financiero** frente a interrupciones graves causadas por fallos tecnológicos o ciberataques, por tanto, se aplica a: bancos, aseguradoras, fondos de inversión fintechs y proveedores críticos para el sector financiero.

Se trata de una ley especial respecto de la NIS2, adaptando obligaciones ya previstas en la Directiva, como la gestión de riesgos TIC y la obligación de notificación de incidentes, pero añadiendo otras obligaciones, como las relativas a la realización de pruebas de resiliencia operativa y a la supervisión de terceros proveedores de TIC.

Por su parte, el Reglamento MiCA (Markets in Crypto-Assets)[29] tiene por objeto regular los criptoactivos no cubiertos por la legislación financiera tradicional; este Reglamento aplica a proveedores de servicios de criptoactivos y a emisores de tokens y plataformas de intercambio.

MiCA no es una norma cuyo objeto principal sea la ciberseguridad, pero **exige medidas de seguridad para plataformas de criptoactivos**, y se completa con la NIS2 en aquellos casos en que las entidades reguladas por MiCA pueden estar también obligadas a cumplir con la Directiva, en el caso de que operen como proveedores digitales críticos.

[26] Servicios esenciales que se apoyan en infraestructuras críticas de sectores como la energía, salud, transporte o servicios digitales, entre otros.

[27] Las entidades esenciales, que operan en sectores de alta criticidad y las entidades importantes, que operan en sectores relevantes, pero con menor impacto directo.

[28] Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.o 1060/2009, (UE) n.o 648/2012, (UE) n.o 600/2014, (UE) n.o 909/2014 y (UE) 2016/1011 https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32022R2554

[29] Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n.o 1093/2010 y (UE) n.o 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937 https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32023R1114

En materia de regulación de la ciberseguridad en Europa también debe tenerse en cuenta el Reglamento de Ciberresiliencia[30], que aplica a *"los productos con elementos digitales comercializados cuya finalidad prevista o uso razonablemente previsible incluya una conexión de datos directa o indirecta, lógica o física, a un dispositivo o red"*[31].

En relación a los ciber-incidentes, cuya gestión como obligación hemos visto que se reitera en toda la normativa de ciberseguridad, también se regula desde un punto de vista de la gobernanza de la ciberseguridad, haciendo foco en la necesaria cooperación para hacer frente eficazmente a las ciberamenazas, de ello se ocupa el denominado "Reglamento de Cibersolidaridad"[32] (diciembre de 2024), que tienen por objeto *"reforzar las capacidades de la Unión a fin de detectar amenazas e incidentes de ciberseguridad, prepararse para ellos y responder a ellos"*[33].

Finalmente, también desde el punto de vista de la gobernanza de la ciberseguridad, el Reglamento de Ciberseguridad[34] tiene por objeto reforzar el papel de ENISA (Agencia de la Unión Europea para la Ciberseguridad)[35] y establecer un marco de certificación para productos y servicios TIC[36], que plantea como objetivo proporcionar **sistemas de certificación a escala de la Unión Europea**, mediante un conjunto completo de normas, requisitos técnicos y procedimientos, que permita evaluar las características de seguridad de un producto o servicio específico basado en las tecnologías de la información y la comunicación.

El marco regulatorio general de la ciberseguridad en Europa se completa con una serie de normas que se centran en regular determinados ámbitos o actividades en los que las tecnologías de la información y la comunicación son relevantes y que, por tanto, están expuestas a los riesgos relacionados con la seguridad de la información.

Así, el Reglamento General de Protección de Datos (RGPD)[37] se considera una norma que indirectamente ha impulsado la ciberseguridad en Europa, ya que **la seguridad en el tratamiento de los datos personales en un requisito consustancial a la protección de los datos personales y de la privacidad**.

---

[30] Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) n.° 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia) https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R2847

[31] Art. 2.1 del Reglamento de Ciberresiliencia, y art. 1que regula su objeto: *"El presente Reglamento establece: normas para la comercialización de productos con elementos digitales a fin de garantizar la ciberseguridad de dichos productos; requisitos esenciales de ciberseguridad para el diseño, el desarrollo y la fabricación de productos con elementos digitales, así como obligaciones de los operadores económicos en relación con dichos productos en lo que respecta a la ciberseguridad; requisitos esenciales de ciberseguridad para los procesos de gestión de las vulnerabilidades establecidos por los fabricantes a fin de garantizar la ciberseguridad de los productos con elementos digitales durante el tiempo en que se prevea que los productos vayan a utilizarse, así como obligaciones de los operadores económicos en relación con dichos procesos; normas relativas a la vigilancia del mercado, incluida la supervisión, y a la aplicación de los requisitos y las normas a que se refiere el presente artículo."*

[32] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32025R0038

[33] Art. 1 del Reglamento (UE) 2025/38

[34] Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.o 526/2013 («Reglamento sobre la Ciberseguridad») https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv%3AOJ.L_.2019.151.01.0015.01.SPA&toc=OJ%3AL%3A2019%3A151%3ATOC

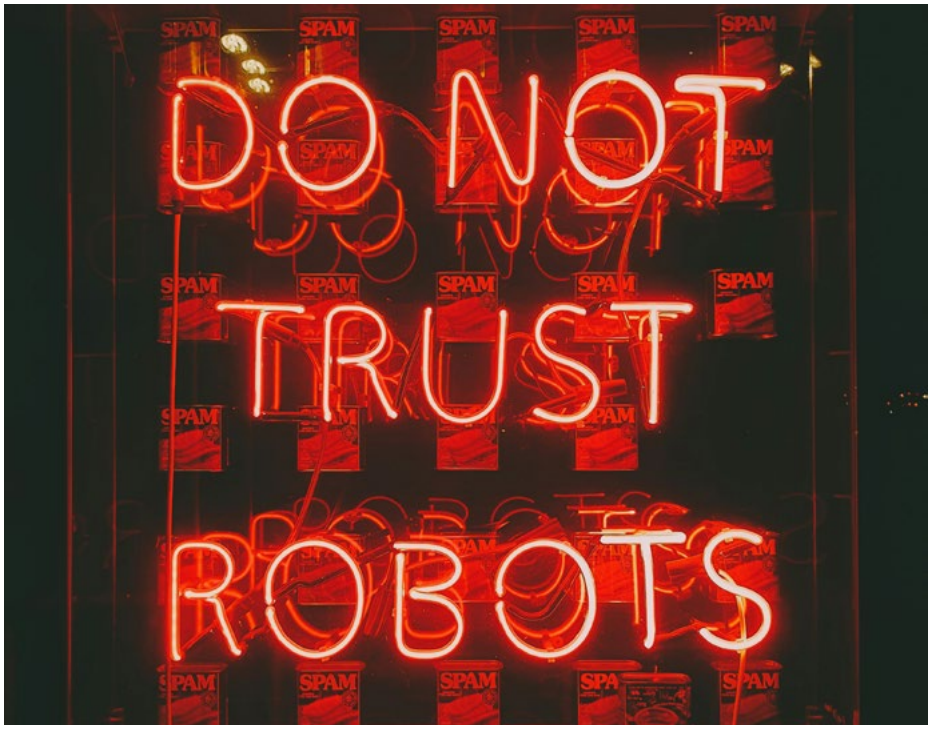
[35] https://www.enisa.europa.eu/

[36] https://digital-strategy.ec.europa.eu/es/policies/cybersecurity-certification-framework

[37] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

En consecuencia, el RGPD exige medidas técnicas y organizativas para proteger los datos personales, introduce la obligación de notificar las brechas de seguridad a la autoridad de protección de datos competente y todo ello en base a un enfoque a riesgos y a la responsabilidad proactiva de las empresas.

También las normas que regulan el comercio electrónico, los servicios digitales o las telecomunicaciones imponen obligaciones de seguridad a los sujetos obligados; y desde otra perspectiva la regulación de los ciberdelitos permite perseguir y enjuiciar las conductas relacionadas con los ciberataques, así el objeto de la Directiva 2013/40/UE[38] es *"establecer normas mínimas relativas a la definición de las infracciones penales y a las sanciones aplicables en el ámbito de los ataques contra los sistemas de información. También tiene por objeto facilitar la prevención de dichas infracciones y la mejora de la cooperación entre las autoridades judiciales y otras autoridades competentes"*.



No es suficiente que existan normas que establezcan obligaciones en lo que respecta a la implementación de medidas de ciberseguridad, necesariamente deben existir **mecanismos que permitan actuar contra los responsables de tales conductas**, sin perjuicio de las dificultades que ello puede suponer en el contexto del ciberespacio, en cuanto a la identificación de los autores y su efectiva persecución, y puesta a disposición de las autoridades judiciales, pero en todo caso, un primer paso imprescindible es identificar esas conductas y tipificarlas como delitos, para que puedan tener una respuesta contundente por parte del ordenamiento jurídico en forma de sanción penal.

[38] Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo https://eur-lex.europa.eu/eli/dir/2013/40/oj?locale=es

La Directiva 2013/40/UE establece que los Estados miembros deben adoptar las medidas necesarias para que ciertas **conductas relacionadas con ataques a sistemas de información sean sancionables como infracción penal**, concretamente se refiere a: el acceso ilegal a sistemas de información, interferencia ilegal en sistemas, interferencia ilegal en datos, interceptación ilegal de comunicaciones electrónicas y a la producción intencional, venta, adquisición para el uso, importación, distribución u otra forma de puesta a disposición de herramientas[39] para cometer los delitos citados anteriormente.

El estado de la regulación sobre ciberseguridad en España, como estado miembro de la Unión Europea, sigue la hoja de ruta trazada por las instituciones europeas, siendo los principales instrumentos regulatorios los reglamentos y las directivas europeas[40].

El reglamento como instrumento de regulación en el contexto de la Unión Europea, implica que este tipo de norma sea de aplicación directa a los estados miembros, por tanto, una vez aprobado el reglamento y teniendo en cuenta los plazos para su entrada en vigor, este ya será exigible en los estados miembros, se trata de actos legislativos vinculantes que deben aplicarse en su integridad en toda la Unión Europea.

El caso de las directivas es diferente, ya que una vez aprobadas para su efectiva aplicación en cada estado miembro requieren que estas sea objeto de transposición al ordenamiento jurídico de cada estado miembro, lo cual se lleva a cabo mediante una ley nacional de cada país, por tanto, las directivas son actos legislativos que establecen objetivos que todos los países de la Unión Europea deben asumir, pero corresponde a cada estado miembro elaborar sus propias leyes sobre cómo alcanzar esos objetivos.

En consecuencia, **el estado de la regulación sobre ciberseguridad en España está absolutamente vinculada a lo establecido por la Unión Europea**, pero sin perjuicio de lo anterior, hay ciertas regulaciones que resultan relevantes como la Ley de Seguridad Nacional[41], en la que se apoya la protección de infraestructuras críticas, o la Estrategia Nacional de Ciberseguridad[42] (del 2019, actualmente en proceso de revisión[43]) y el Plan Nacional de Ciberseguridad[44].

En el caso de las directivas, como requieren de transposición al ordenamiento jurídico de cada estado miembro, mediante una ley nacional, sí que hay un mayor margen de decisión respecto a cómo y cuándo incorporar en cada país las directrices regulatorias de la directiva, aunque por supuesto debe hacerse dentro de los límites establecidos en esta.

[39] Concretamente: programas informáticos, contraseñas de ordenador, códigos de acceso o datos similares que permitan acceder de manera no autorizada a la totalidad o a una parte de un sistema de información.
[40] También existen otros actos legislativos: decisiones, recomendaciones y dictámenes.
[41] Ley 36/2015, de 28 de septiembre, de Seguridad Nacional https://www.boe.es/eli/es/l/2015/09/28/36/con
[42] Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional https://www.boe.es/eli/es/o/2019/04/26/pci487/con
[43] Orden PJC/522/2025, de 23 de mayo, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de 24 de abril de 2025, por el que se aprueba el procedimiento para la elaboración de una nueva Estrategia Nacional de Ciberseguridad https://www.boe.es/eli/es/o/2025/05/23/pjc522
[44] https://www.lamoncloa.gob.es/consejodeministros/referencias/Paginas/2022/refc20220329_corregidav02.aspx#ciberseguridad

En el caso de la Directiva NIS 2, España está en proceso de transposición[45], mediante el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, aprobado en enero de 2025[46] y todavía en proceso de tramitación legislativa[47].

Algunas de las cuestiones que regula el citado anteproyecto de ley es la creación del Centro Nacional de Ciberseguridad, la responsabilidad directa en materia de ciberseguridad de la Alta Dirección en aquellas entidades que sea esenciales, la gestión de los riesgos y la adopción de las medidas adecuadas para garantizar la seguridad de sus redes y sistemas de información, lo que incluye evaluar también los servicios externos con acceso a datos críticos, la obligación de notificar incidentes significativos, así como la designación de responsables de seguridad de la información y la supervisión. del cumplimiento de la norma por parte de autoridades sectoriales como Interior, Defensa y Transformación Digital.

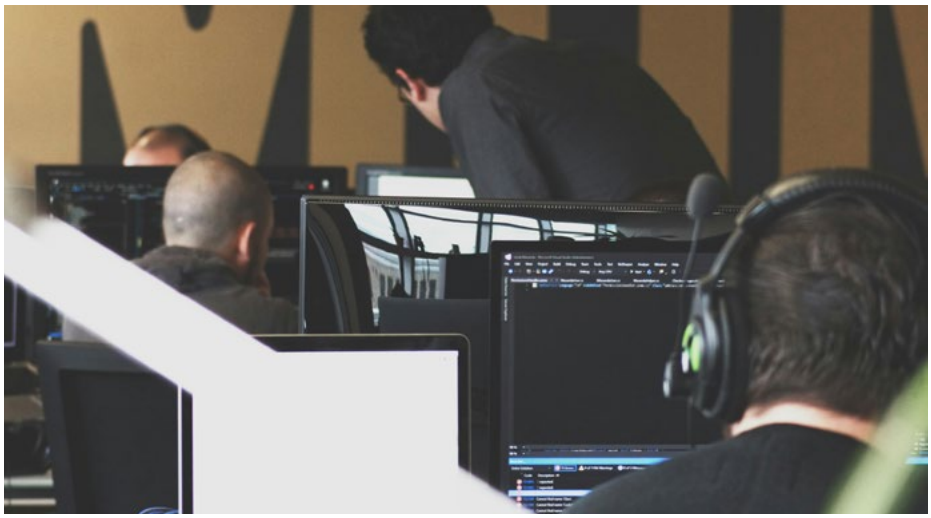
Una de las normas españolas que abordan la ciberseguridad, sin que se derive directamente de actos legislativos de la Unión Europea, es el denominado Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 311/2022[48], que derogó una anterior regulación del 2010; la regulación se adaptó las necesidades derivadas de nuevos retos en al ámbito de la ciberseguridad.

[45] La fecha límite de transposición era el 17 de octubre de 2024
[46] https://www.fundacionesys.com/wp-content/uploads/2025/01/01_2025_Anteproyecto_ley_coordinacion_gobernanza_ciberseguridad.pdf
[47] Está previsto que la norma se tramite por el procedimiento de urgencia
[48] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad https://www.boe.es/eli/es/rd/2022/05/03/311/con

El objeto principal del ENS es establecer la **política de seguridad en el uso de medios electrónicos por parte de las administraciones públicas y entidades que colaboran con ellas**[49], a fin de garantizar la protección de los sistemas de información, los datos, las comunicaciones y los servicios electrónicos, facilitando así el ejercicio de derechos y el cumplimiento de obligaciones por medios digitales.

En lo que respecta a instituciones públicas especializadas en ciberseguridad, y que son clave desde diferentes puntos de vista para la aplicación efectiva de las normas relacionadas con la ciberseguridad, en España existe el Centro Criptológico Nacional (CCN)[50], el Instituto Nacional de Ciberseguridad (INCIBE)[51] y en el contexto de las cuerpos y fuerzas de seguridad los grupos especializados en investigación tecnológica y delitos informáticos[52]; también cabe mencionar la existencia de la fiscalía de delitos informáticos[53] que lleva a cabo la unificación de criterios relativos a los ciberdelitos y vela por una adecuada coordinación en las investigaciones relativas a este tipo de delitos.

En definitiva, **el nivel de normas y gobernanza de España en materia de ciberseguridad se puede considerar maduro**, lo cual resulta necesario, por el elevado nivel de ciberataques de que es objeto España, indicador de ello son las preguntas en sede de control parlamentario dirigidas al Gobierno en materia de ciberseguridad, que se refieren al refuerzo de la ciberseguridad, que tras el aumento de ciberataques recibidos hace que España sea uno de los países "más afectado del mundo", incluso superando a los Estados Unidos de América e Israel[54].



[49] Art. 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público: *"El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada."* https://www.boe.es/eli/es/l/2015/10/01/40/con

[50] https://www.ccn.cni.es/index.php/es/

[51] https://www.incibe.es/

[52] https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit# y https://web.guardiacivil.es/es/institucional/conocenos/especialidades/gdt/

[53] https://www.fiscal.es/-/criminalidad-informatica

[54] Pregunta al Gobierno con respuesta escrita (01/07/2025): *"Medidas adoptadas por el Gobierno para reforzar la ciberseguridad, tras la reciente oleada de ataques que ha convertido al país en el más afectado del mundo, superando a Estados Unidos de América e Israel. (184/026041)" https://www.congreso.es/es/busqueda-de-iniciativas?p_p_id=iniciativas&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&_iniciativas_mode=mostrarDetalle&_iniciativas_legislatura=XV&_iniciativas_id=184/026041*

Capítulo 7

Regulación de la ciberseguridad en los Estados Unidos de América

- El nivel de madurez de la regulación de la ciberseguridad en los Estados Unidos de América (USA), **es equivalente al de la Unión Europea**, sin perjuicio de que tenga sus propias características, derivadas del **papel que este país ejerce en el contexto mundial, y de sus capacidades de liderazgo en la evolución de las tecnología de la información y la comunicación**, tanto en productos como en servicios, por tanto, si bien esa equivalencia se puede propugnar respecto del marco jurídico, no debe considerarse así desde la perspectiva tecnológica, que es donde podemos encontrar diferencias significativas entre ambas zonas geo-políticas.

  Hay que tener en cuenta que los conflictos internacionales en los que, de manera directa o indirecta, están involucrados los USA, también generan una necesidad especial en materia de ciberseguridad, dada la incidencia de cuestiones como la ciberguerra y el ciberespionaje, que se agrupan bajo el concepto de ciberseguridad nacional.

  Del mismo modo que la Unión Europea, los USA cuentan con un **conjunto diverso de leyes, regulaciones y estrategias que abordan la ciberseguridad desde diferentes perspectivas**: privacidad (protección de datos personales), infraestructuras críticas, respuesta a incidentes, ciberdelitos y otras a las que ya hemos hecho referencia en relación al análisis de la Unión Europea.

  Del mismo modo que en Europa se trazan estrategias de ciberseguridad, que después se implementan y desarrollan mediante leyes y otros instrumentos regulatorios, en USA se diseña y planifica la ciberseguridad y su regulación en base a una estrategia.

  En el año 2023 la administración Biden aprobó una Estrategia Nacional de Ciberseguridad[55], en la que se planteaban cinco pilares estratégicos: defensa de infraestructuras críticas, desmantelamiento de actores maliciosos, reformas de mercado para impulsar la seguridad, inversión en resiliencia digital y alianzas internacionales para combatir amenazas globales.

  A nivel federal algunas de las leyes más relevantes en materia de ciberseguridad son la HIPAA (Health Insurance Portability and Accountability Act[56]), que regula la protección de la información en el sector salud, en base a exigencias en materia de seguridad de la información[57] orientadas a proteger los datos relativos a la salud de las personas.

  En relación a la seguridad de la información en el sector financiero, la GLBA (Gramm-Leach-Bliley Act[58]) obliga a las instituciones financieras a proteger la información sensible de sus clientes.

  Y desde un punto de vista del sector público, es relevante mencionar la FISMA (Federal Information Security Management Act[59]), que exigía a las agencias federales la implementación de programas de seguridad de la información, esta ley fue actualizada mediate la "Strengthening American Cybersecurity Act of 2022"[60], que pone al día los requisitos de seguridad para las agencias federales.

[55] https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/
[56] https://www.hhs.gov/programs/hipaa/index.html
[57] https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/index.html
[58] https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act
[59] https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/10/M-19-02.pdf
[60] https://www.congress.gov/117/bills/s3600/BILLS-117s3600es.pdf

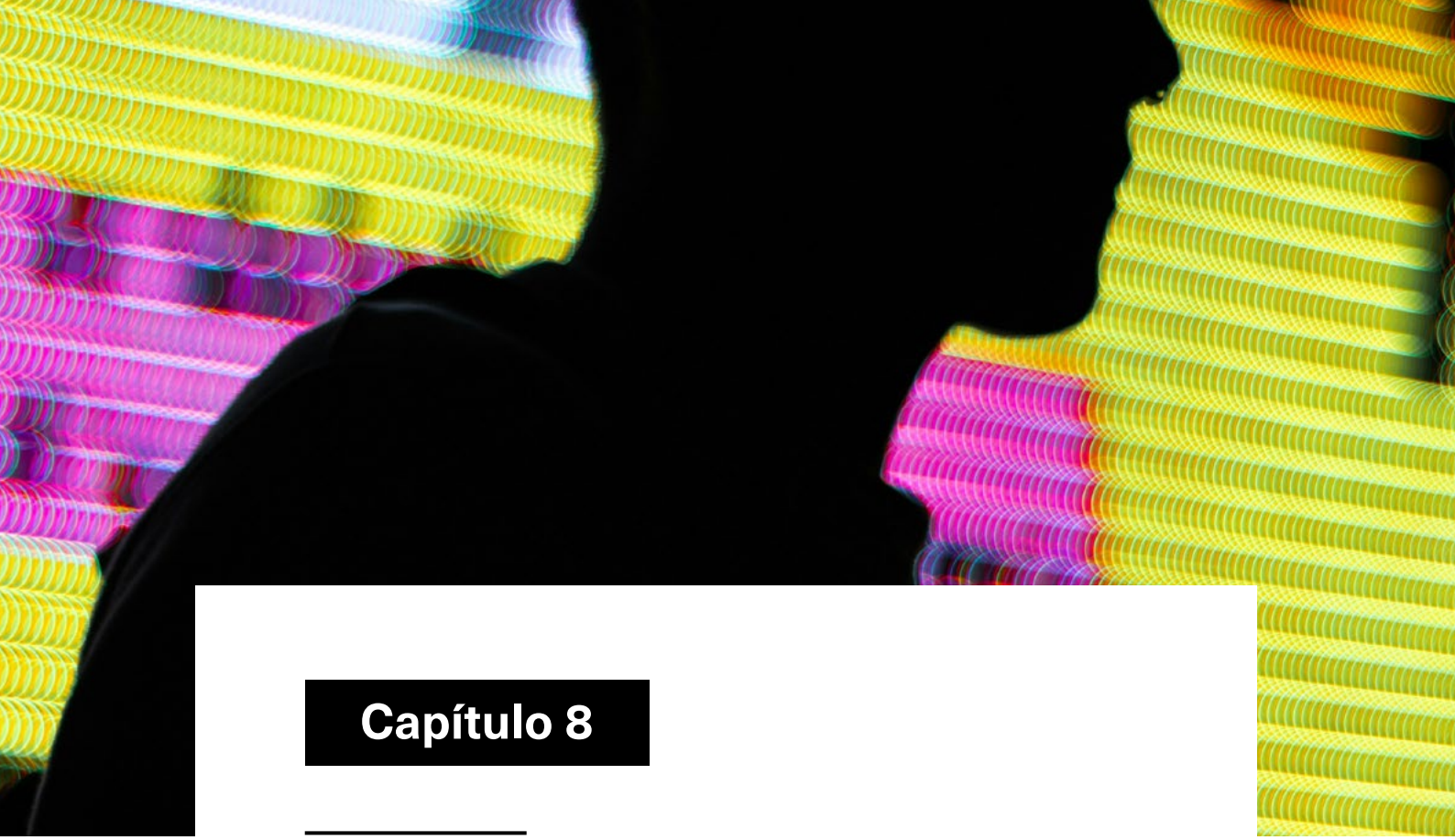
Debe mencionarse que la Strengthening American Cybersecurity Act combina tres iniciativas clave: la CIRA (Cyber Incident Reporting for Critical Infrastructure Act[61]), que obliga a reportar incidentes cibernéticos en un plazo de 72 horas; la ya citada actualización de FISMA; y la FSCIJA (Federal Secure Cloud Improvement and Jobs Act[62]), que regula aspectos relacionados con el uso seguro de tecnologías en la nube.

Además, desde el punto de vista de la colaboración y cooperación en materia de ciberseguridad, es muy relevante la CISA Act (Cybersecurity Information Sharing Act[63]), que regula el intercambio de información sobre ciberseguridad entre el gobierno de los USA y el sector privado.

En lo que respecta a entidades u organismos que son clave en la regulación de la ciberseguridad, resulta de especial relevancia el papel del NIST[64] (National Institute of Standards and Technology), que desarrolla marcos y estándares tecnológicos, siendo uno de los más conocidos en relación a la ciberseguridad el "NIST Cybersecurity Framework 2.0 (CSF)"[65], ampliamente adoptado por empresas y agencias, no solo en los Estados Unidos de América, también en otros países, ya que si hay un elemento que no debe perderse de vista, es que **los aspectos tecnológicos y de gestión de la ciberseguridad son neutrales desde el punto de vista territorial e incluso político**, así que con cierta facilidad la normas y estándares relativos a la ciberseguridad pueden ser adoptados por países con diferencias sociales, políticas y económicas significativas, que no les impiden seguir un modelo de ciberseguridad sustentado en las mismos fundamentos, sin perjuicio de que sean adaptados a las particularidades y realidad de cada país.

En resumen, desde el punto de vista regulatorio **la situación en los Estados Unidos de América tiene muchos puntos en común con la de la Unión Europea**, sin perjuicio de que desde el punto de vista tecnológico los USA puedan estar en un nivel más avanzado, aunque este aspecto de la ciberseguridad no forma parte del análisis de este informe.

[61] https://www.cisa.gov/resources-tools/resources/cyber-incident-reporting-critical-infrastructure-act-2022-fact-sheet
[62] https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/S%203099_As%20Introduced.pdf
[63] https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Information%20Sharing%20Act%20of%202015.pdf
[64] https://www.nist.gov/?hl=es
[65] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.spa.pdf



Capítulo 8

Regulación de la ciberseguridad en Latinoamérica, con una especial referencia a Colombia y Perú

La ciberseguridad en Latinoamérica ha avanzado considerablemente en la última década, el aumento de amenazas digitales y la necesidad de proteger infraestructuras críticas, datos personales y sistemas gubernamentales, han motivado la necesidad de disponer de regulación en estas materias, es decir, siguiendo los pasos tanto de la Estados Unidos de América como de la Unión Europea.

En el ámbito de los ciberdelitos los países latinoamericanos[66] se han ido adhiriendo al Convenio de Budapest (del mismo modo que países europeos y los Estados Unidos de América), se trata de un instrumento clave de cooperación internacional en la lucha contra los ciberdelitos.

[66] Entre otros, Argentina, Brasil, Chile, Colombia, Costa Rica, Panamá, Paraguay, Perú y República Dominicana lo han firmado, mientras que México, Uruguay, Ecuador y Guatemala participan como observadores o invitados

El Convenio de Budapest sobre la ciberdelincuencia fue aprobado por el Consejo de Europa el 8 de noviembre de 2001, siendo el primer y más relevante acuerdo internacional que plantea como objetivo principal combatir la ciberdelincuencia, mediante el establecimiento de una política penal común que proteja frente a este tipo de delitos, por ello el Convenio y sus protocolos adicionales[67] son **instrumentos internacionales vinculantes, en consecuencia son de obligado cumplimiento para los países adheridos al mismo**.

Asimismo, una buena parte de los países de la región han desarrollado estrategias nacionales de ciberseguridad o marcos de ciberseguridad[68], al estilo europeo o estadounidense**;** Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, México, Panamá, Paraguay y Perú han desarrollado planes nacionales de ciberseguridad que sirven de apoyo y refuerzo a las políticas públicas y a la actividad legislativa en relación a la protección de los sistemas de información, la protección de los datos personales, la protección de infraestructuras críticas y la cooperación internacional en materia de ciberdelincuencia y ciberseguridad.

El **desarrollo económico y tecnológico marca el ritmo de este tipo de reformas legislativas**, que para su efectiva aplicación no es suficiente la aprobación de las leyes, requiere en paralelo la **implantación de una cultura de ciberseguridad y de concienciación, tanto en las organizaciones, como a nivel social**.

El **nivel de desarrollo de la regulación en materia de ciberseguridad en Latinoamérica es desigual**, si volvemos a fijarnos en el GCI[69], este mide el desempeño de los países en materia de ciberseguridad, desde el tier 1 (nivel más alto de desarrollo), al tier 5 (más bajo), así los agrupa en: aquellos que son un modelo a seguir (nivel 1), los que están avanzando (nivel 2), los que han establecido las bases para avanzar (nivel 3), los que han alcanzado un compromiso básico con la ciberseguridad (nivel 4) y los que están todavía construyendo la bases mínimas (nivel 5).

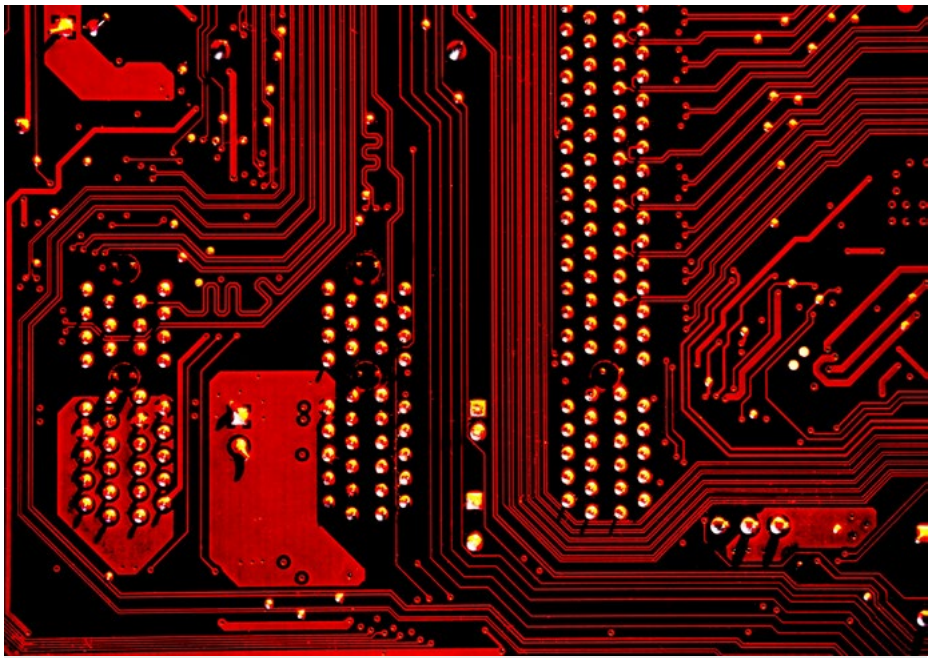
Según el CGI, los países de Latinoamérica y Caribe están agrupados del siguiente modo:

- **Nivel 1:** Brasil
- **Nivel 2:** Ecuador, México y Uruguay
- **Nivel 3:** Chile, Colombia, Costa Rica, Cuba, República Dominicana, Jamaica, Panamá, Paraguay, Perú y Trinidad y Tobago.
- **Nivel 4:** Argentina, Bahamas, Barbados, Belice, Bolivia, Dominica, El Salvador, Granada, Guatemala, Guyana, Haití, Honduras, Nicaragua, San Cristóbal y Nieves, Santa Lucía, San Vicente y las Granadinas, Surinam y Venezuela.
- **Nivel 5:** Antigua y Barbuda.

[67] El Convenio de Budapest ha sido revisado desde su aprobación, para adaptarse a la evolución de las tecnologías y de los ciberdelitos. En enero de 2003 se firmó en Estrasburgo el protocolo adicional al Convenio, que se centra los actos de índole racista y xenófoba cometidos en las redes en mayo de 2022, se firmó un segundo protocolo adicional, cuyo principal objetivo es reforzar la cooperación en materia de ciberdelitos.

[68] https://www.segurilatam.com/ciberilatam/estas-son-las-estrategias-nacionales-de-ciberseguridad-de-los-paises-latinoamericanos_20240514.html

[69] Índice Global de Ciberseguridad (2024)



Por lo datos obtenidos para la elaboración del CGI, la mayoría de países de la región se sitúan en los niveles 3 y 4, por tanto, se puede decir que existe una base suficiente como para construir sobre ella desarrollos más maduros en materia de ciberseguridad, es destacable que se han estado haciendo importantes esfuerzos legislativos, incluyendo el diseño de estrategias nacionales de ciberseguridad, en este sentido una dificultad para evaluar el impacto que puede tener a medio plazo la citada regulación en la mejora de la ciberseguridad, es que las normas son diversas y su nivel de aplicación es difícil de cuantificar, en resumen **los países de Latinoamérica y Caribe, salvo contadas excepciones, todavía tienen evidentes debilidades en materia de ciberseguridad, aunque hayan reforzado los aspectos regulatorios**.

Esta situación contrasta con la que podemos encontrar en los Estados Unidos de América (situado en el nivel 1 del CGI) y la Unión Europea para la que 15 países (de 27) se sitúan en el nivel 1, 10 países en el nivel 2 y solo 2 países están en un nivel 3[70], lo que supone a efectos prácticos una **mayor capacidad de hacer frente a las ciberamenazas, en comparación frente a las capacidades desarrolladas hasta el momento por los países de Latinoamérica**.

Colombia y Perú se sitúan en el nivel 3, que según la descripción que hace la ITU[71] de lo que, con carácter general significa estar en esa zona de su índice de ciberseguridad, representa a aquellos países que han obtenido una puntuación global de al menos 55 puntos sobre 100, al demostrar un **compromiso básico con la ciberseguridad** en las medidas impulsadas por esos países, lo que incluye la evaluación, el establecimiento o la aplicación de medidas de ciberseguridad significativas solo en alguno de los cinco pilares que se usan para calcular el CGI.

[70] Bulgaria y Letonia

[71] *" Tier 3 (T3) – Establishing represents countries that obtained an overall score of at least 55/100 by demonstrating a basic cybersecurity commitment to government-driven actions that encompass evaluating, establishing or implementing certain generally accepted cybersecurity measures across a moderate number of pillars or indicators".*

Como ya se ha descrito anteriormente en al análisis comparativo de las medidas legales en materia de ciberseguridad, uno de los pilares en los que se apoya el cálculo del CGI es el destinado a evaluar las iniciativas de regulación de la ciberseguridad de cada país (medidas legales), al respecto se pueden extraer algunas conclusiones:

- En general los países con mejor CGI (nivel 1), siempre obtienen el máximo de puntuación en este pilar (20 puntos), sería el caso de Brasil, España y los Estados Unidos de América.
- Ahora bien, no siempre una buena puntuación en relación a las iniciativas legales permite alcanzar ese nivel, por ejemplo, en el caso de Perú, si bien también tienen una puntuación de 20, se sitúa en el nivel 3, ya que las puntuaciones del resto de pilares fluctúan entre 13,51 y 18,27
- Por su parte, Colombia, que también se sitúa en el nivel 3 de desarrollo, obtiene una puntuación de 13,37 en lo que se refiere a medidas legales
- De análisis comparativo entre Perú y Colombia, se pone en evidencia que en Colombia las medidas legales es el pilar con una puntuación más baja, mientras que para Perú es la más alta, en cambio el pilar relativo a medidas técnicas[72] tiene la mayor puntuación de los cinco pilares en el caso de Colombia, mientras que para Perú es el pilar que ha recibido la menor puntuación, lo que significa que no siempre un alto nivel de regulación conlleva necesariamente un desarrollo relevante de las medidas tecnológicas.

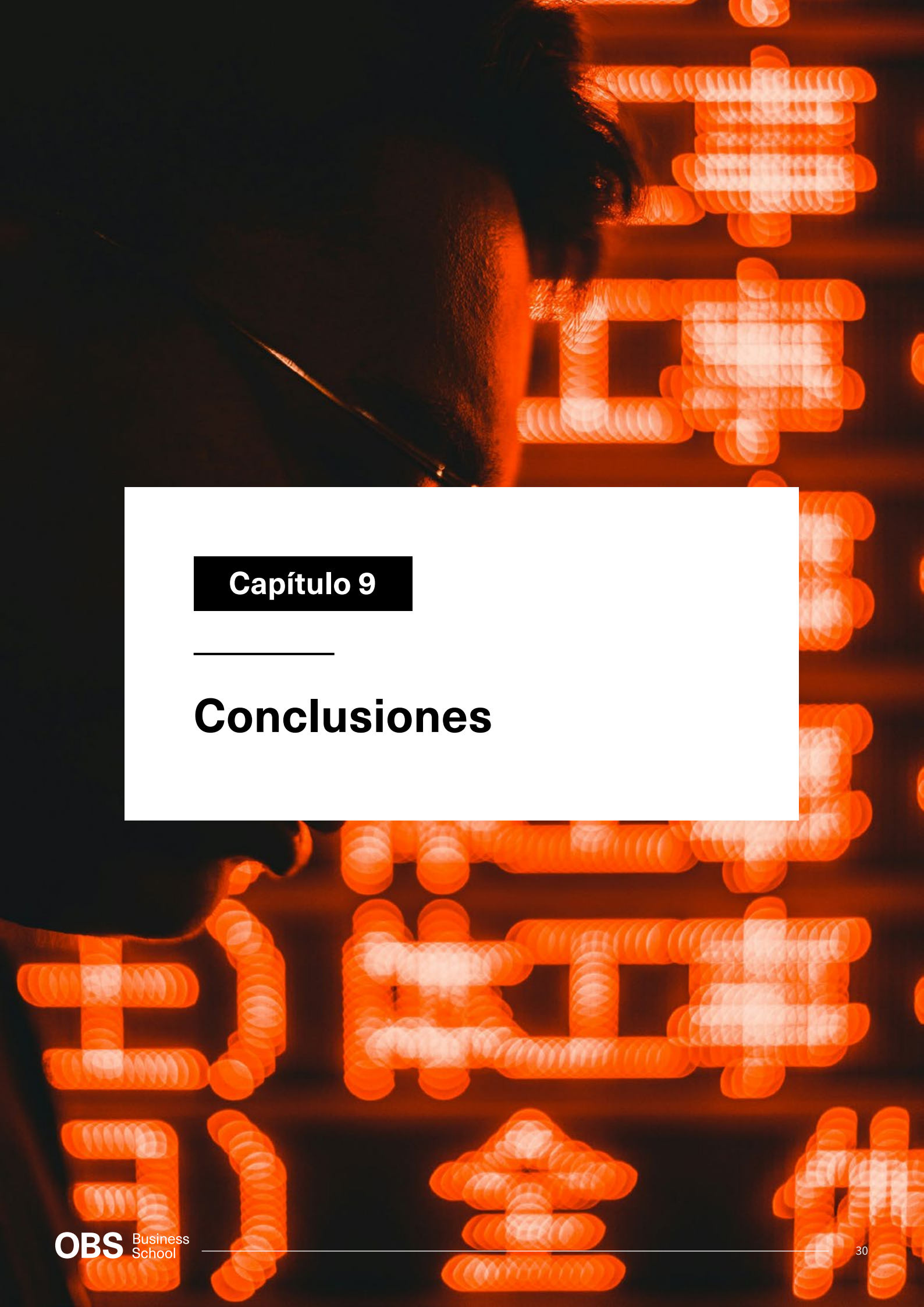
[72] Este pilar se centra en analizar y valorar la existencia de instituciones técnicas, normas y marcos que se ocupan de la ciberseguridad y la ciberdelincuencia, al respecto la UTI considera que el desarrollo y el uso eficientes de las TIC solo pueden desarrollarse y avanzar en un entorno de confianza y seguridad y que, en consecuencia, *"los países deben contar con las capacidades y los medios técnicos necesarios para identificar, detectar, proteger y responder eficazmente a los riesgos y amenazas cibernéticos, y recuperarse de los ataques, así como para promover el intercambio de información y evaluar y aplicar normas, buenas prácticas de ciberseguridad y planes para garantizar la seguridad de las TIC"* (extraído del Global Cybersecurity Index 2024, traducción no oficial del autor).

Y ya para finalizar, se incluyen a continuación algunas de las medidas normativas adoptadas por Colombia y Perú en relación a la ciberseguridad, centrándonos en los 3 tipos de instrumentos jurídicos relacionados con la ciberseguridad que son habituales en la mayoría de los países:

- Ambos países disponen de una estrategia nacional de ciberseguridad, en el caso de Colombia es la "Estrategia Nacional de Seguridad Digital"[73] y en el caso de Perú la "Estrategia Nacional de Ciberseguridad" [74], ambas de reciente aprobación (posterior al CGI 2024).
- También en ambos países tienen vigentes leyes de protección de datos; en Colombia la Ley estatutaria 1581 de 2012[75], cuya actualización se está tramitando en el Congreso de la República de Colombia, mediante el Proyecto de Ley 152 de 2024 y en el caso de Perú está vigente la Ley 29733 de 2011[76], que fue actualizada mediante el Decreto Supremo 016-2024-JUS (de noviembre de 2024) que aprueba el nuevo Reglamento de la Ley 29733.
- Y finalmente, respecto de la inclusión en el ordenamiento jurídico de los ciberdelitos, para ello en Colombia se modificó el Código Penal mediante la Ley 1273 de 2009[77], y en Perú está vigente la Ley 30096 de 2013[78], que ha sufrido varias modificaciones desde su aprobación, la última mediante la Ley 32314[79] (abril de 2025).

Estos tres ejemplos de tipos de normas nos dan idea de la necesidad de actualizar la regulación en materia de ciberseguridad, ya que los ciber-riesgos son cambiantes.

[73] De marzo de 2025, para el periodo 2025-2027 https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/403023:La-Estrategia-Nacional-de-Seguridad-Digital-llega-para-enfrentar-las-crecientes-amenazas-ciberneticas
[74] De julio de 2025, para el periodo 2026-2028 https://www.gob.pe/institucion/pcm/informes-publicaciones/7046161-estrategia-nacional-de-ciberseguridad-del-peru-2026-2028-esnacib
[75] https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981
[76] https://cdn.www.gob.pe/uploads/document/file/272360/Ley%20N%C2%BA%2029733.pdf.pdf?v=1618338779
[77] *"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones" https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492*
[78] https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/239569-30096
[79] https://busquedas.elperuano.pe/dispositivo/NL/2394851-2 que incluye el uso de la inteligencia artificial en la comisión de delitos

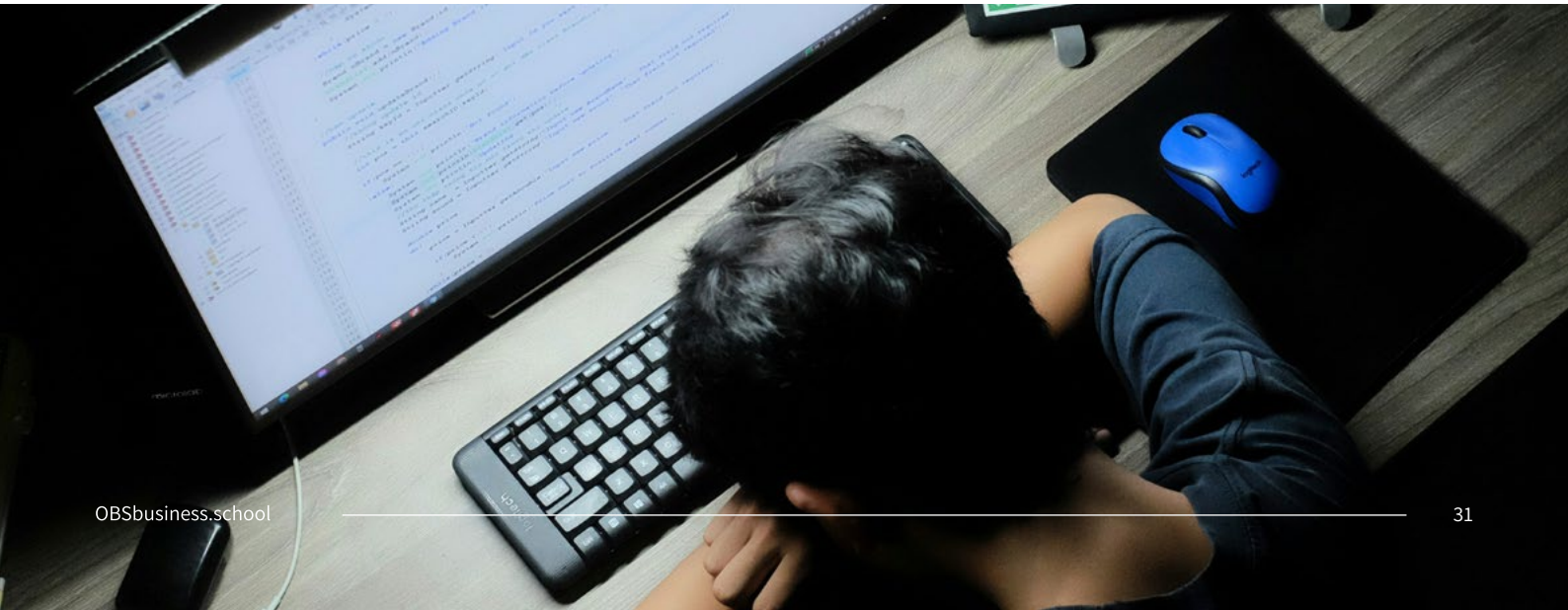


Capítulo 9

Conclusiones

Partiendo de la base de que resulta absolutamente imprescindible que la ciberseguridad se regule como una obligación jurídica, esa necesidad nace de que el uso de las tecnologías de la información y la comunicación está expuesto a riesgos, que, en caso de materializarse en forma de incidentes de ciberseguridad, acaban ocasionando a las organizaciones y a las personas, daños y perjuicios de todo tipo (físicos, materiales e inmateriales):

- La ciberseguridad es un nuevo bien jurídico, que su protección se ve reforzada por el reconocimiento del derecho a la seguridad de la información o a la ciberseguridad.
- Las estrategias nacionales de ciberseguridad son el punto de partida del desarrollo de leyes y normas relativas a la ciberseguridad.
- La regulación de la ciberseguridad se despliega en diferentes ámbitos, principalmente la protección de infraestructuras críticas, la gestión de incidentes de ciberseguridad, la protección de datos personales, los ciberdelitos y la ciberdefensa.
- El principal objetivo de las normas en materia de ciberseguridad es obligar a que se adopten las medidas de seguridad más adecuadas para mitigar los ciber-riesgos, fomentando además la cooperación entre instituciones y entre países.
- A pesar de que los ciberincidentes son un fenómeno global, existen diferencias significativas entre los países y regiones en cuanto al nivel de despliegue efectivo de las leyes que regulan las cuestiones relativas a la ciberseguridad.
- En relación a los cinco pilares del Cybersecurity Global Index, la mayoría de los países analizados (194 países), donde muestran mayores fortalezas es en el pilar de medidas legales.
- Los Estados Unidos de América y la Unión Europea tiene desarrollado un marco normativo con un alto grado de madurez, y ello sin perjuicio de que muchas de sus normas sean de reciente aprobación o revisión.
- El estado de la regulación en materia de ciberseguridad en Latinoamérica y Caribe es desigual, estando la mayoría de los países de la región diseñando o construyendo las bases para después alcanzar un mayor grado de maduración, si bien su ritmo de avance se puede considerar alto, en particular en lo que se refiere a las medidas legales.



Referencias bibliográficas

1. Biden White House Archives. (2023). *National Cybersecurity Strategy*. https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/

2. CISA. (2015). *Cybersecurity Information Sharing Act of 2015.* https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Information%20Sharing%20Act%20of%202015.pdf

3. CISA. (2022). *Cyber Incident Reporting for Critical Infrastructure Act of 2022: Fact sheet.* https://www.cisa.gov/resources-tools/resources/cyber-incident-reporting-critical-infrastructure-act-2022-fact-sheet

4. Congreso de los Diputados de España. (2025, 1 de julio). *Pregunta al Gobierno con respuesta escrita: Medidas adoptadas para reforzar la ciberseguridad (184/026041).* https://www.congreso.es/es/busqueda-de-iniciativas?p_p_id=iniciativas&p_p_mode=view&_iniciativas_id=184/026041

5. Congreso de los Estados Unidos. (2022). *Strengthening American Cybersecurity Act of 2022, S.3600.* https://www.congress.gov/117/bills/s3600/BILLS-117s3600es.pdf

6. Fundación ESYS. (2025). *Anteproyecto de ley de coordinación y gobernanza en ciberseguridad*. https://www.fundacionesys.com/wp-content/uploads/2025/01/01_2025_Anteproyecto_ley_coordinacion_gobernanza_ciberseguridad.pdf

7. Gobierno de Colombia, Ministerio TIC. (2025, marzo). *Estrategia Nacional de Seguridad Digital 2025–2027*. https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/403023:La-Estrategia-Nacional-de-Seguridad-Digital-llega-para-enfrentar-las-crecientes-amenazas-ciberneticas

8. Gobierno de España. (2015). *Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público*. Boletín Oficial del Estado. https://www.boe.es/eli/es/l/2015/10/01/40/con

9. Gobierno de España. (2022). *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad*. Boletín Oficial del Estado. https://www.boe.es/eli/es/rd/2022/05/03/311/con

10. Gobierno del Perú. (2021). *Ley N.º 29733, Ley de Protección de Datos Personales.* https://cdn.www.gob.pe/uploads/document/file/272360/Ley%20N%C2%BA%2029733.pdf.pdf

11. Gobierno del Perú. (2025, julio). *Estrategia Nacional de Ciberseguridad del Perú 2026–2028 (ESNACIB)*. https://www.gob.pe/institucion/pcm/informes-publicaciones/7046161-estrategia-nacional-de-ciberseguridad-del-peru-2026-2028-esnacib

12. Gobierno del Perú, Congreso de la República. (s. f.). *Norma legal N.º 30096, Delitos Informáticos.* https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/239569-30096

13. Gobierno del Perú, Diario Oficial El Peruano. (s. f.). *Dispositivo NL/2394851-2: Uso de inteligencia artificial en la comisión de delitos*. https://busquedas.elperuano.pe/dispositivo/NL/2394851-2

14. Guardia Civil de España. (s. f.). *Grupo de Delitos Telemáticos (GDT)*. Recuperado el 1 de septiembre de 2025, de https://web.guardiacivil.es/es/institucional/conocenos/especialidades/gdt/

15. HHS – U.S. Department of Health & Human Services. (s. f.-a). *HIPAA Program overview*. https://www.hhs.gov/programs/hipaa/index.html

16. HHS – U.S. Department of Health & Human Services. (s. f.-b). *HIPAA Security Rule: Notice of Proposed Rulemaking*. https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/index.html

17. HSGAC – U.S. Senate Committee on Homeland Security & Governmental Affairs. (2022). *S.3099, Cybersecurity legislation draft*. https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/S%203099_As%20Introduced.pdf

18. INCIBE. (s. f.). *Instituto Nacional de Ciberseguridad de España*. Recuperado el 1 de septiembre de 2025, de https://www.incibe.es/

19. Índice Global de Ciberseguridad. (2024). *Informe global sobre ciberseguridad*. [Fuente oficial no indicada en detalle].

20. NIST. (s. f.). *National Institute of Standards and Technology*. https://www.nist.gov/?hl=es

21. NIST. (2023). *Special Publication 1299 (Spanish edition)*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.spa.pdf

22. Policía Nacional de España. (s. f.). *Brigada Central de Investigación Tecnológica*. Recuperado el 1 de septiembre de 2025, de https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit

23. Segurilatam. (2024, 14 de mayo). *Estas son las estrategias nacionales de ciberseguridad de los países latinoamericanos*. https://www.segurilatam.com/ciberilatam/estas-son-las-estrategias-nacionales-de-ciberseguridad-de-los-paises-latinoamericanos_20240514.html

24. Unión Europea. (2013). *Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo. Diario Oficial de la Unión Europea, L 218*. https://www.eur-lex.europa.eu/eli/dir/2013/40/oj

25. Unión Europea. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos, RGPD). Diario Oficial de la Unión Europea, L 119*. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

26. U.S. Federal Trade Commission. (s. f.). *Gramm-Leach-Bliley Act (GLBA): Privacy and security guidance*. https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

OBS Business School

School of **Business Administration & Leadership**

School of **Innovation & Technology Management**

Planeta Formación y Universidades