C.E.T.I.D.

Centro de Estudios Tecnológico en Informática y Derecho

CIBERSEGURIDAD

Marco Jurídico, Técnico y Estratégico

Guía de Formación Académica Especializada

CAPÍTULO 1

De la seguridad informática a la ciberseguridad estratégica

Autor

Dr. Juan José Páez Rivadeneira

Abogado experto en Derecho Digital

Director del Centro de Estudios Tecnológico en Informática y Derecho

Volumen complementario de

Consultor Protección de Datos (Páez Rivadeneira, 2026)

Quito - Ecuador

Mayo de 2026

CAPÍTULO 1

DE LA SEGURIDAD INFORMÁTICA A LA CIBERSEGURIDAD ESTRATÉGICA

Objetivos de aprendizaje

Al finalizar el estudio del presente capítulo, el lector estará en capacidad de:

- Comprender los hitos históricos que explican la transición de la seguridad informática hacia la ciberseguridad y, posteriormente, hacia la ciberresiliencia como paradigma vigente.
- Identificar los acontecimientos técnicos y jurídicos fundacionales que delimitan cada etapa evolutiva de la disciplina.
- Analizar la relación dialéctica entre el avance tecnológico, la aparición de nuevas amenazas y la respuesta normativa de los Estados.
- Aplicar este marco histórico-conceptual a la lectura crítica de las normas y políticas públicas ecuatorianas en materia de ciberseguridad.
- Valorar el papel del derecho como instrumento de regulación de un fenómeno técnico en mutación permanente.

Sumario

1.7. Evolución conceptual: de la seguridad informática a la ciberseguridad y a la ciberresiliencia.

Introducción al capítulo

La ciberseguridad no constituye una disciplina espontánea ni un campo nacido de la coyuntura digital contemporánea. Su genealogía hunde sus raíces en una tradición milenaria de protección de la información, sistematizada por la criptografía clásica, militarizada durante las dos guerras mundiales del siglo XX, formalizada como ciencia técnica con el advenimiento de la computación electrónica, y elevada al rango de política de Estado tras la consolidación del ciberespacio como quinto dominio operacional —junto a tierra, mar, aire y espacio—. El derecho ha acompañado este recorrido, primero con cierta timidez y luego con creciente intensidad, hasta configurar en la actualidad un corpus normativo sofisticado y autónomo que merece, por sí mismo, una sistematización académica rigurosa.

El presente capítulo propone una reconstrucción histórico-conceptual de la disciplina, organizada en seis grandes etapas que culminan en el examen del concepto vigente de ciberresiliencia. La premisa metodológica que orienta la exposición es que cada hito tecnológico relevante ha generado una correlativa reacción jurídica e institucional, y que entender ese vínculo dialéctico resulta indispensable para interpretar correctamente el estado actual del derecho de la ciberseguridad y prever sus desarrollos futuros. Como advirtiera Solove (2008), no es posible comprender el régimen contemporáneo de protección de la información sin examinar las transformaciones tecnológicas y sociales que lo han precedido. Esta intuición, formulada originalmente para el derecho a la privacidad, vale con idéntica fuerza para el derecho de la ciberseguridad y constituye, además, una de las premisas epistemológicas que el autor ha desarrollado en obra anterior dedicada a la inteligencia artificial jurídica (Páez Rivadeneira, 2025).

1.1. Orígenes: Enigma, Bletchley Park y la criptografía militar

La protección sistemática de la información mediante técnicas de ocultamiento del mensaje constituye una práctica documentada desde la Antigüedad. La escítala lacedemonia, los cifrados de César, los métodos polialfabéticos de Alberti y Vigenère, y el sofisticado tratado Polygraphia del abad Tritemio (1518) jalonan una tradición criptográfica continua que precede en muchos

siglos a la aparición del computador electrónico (Singh, 1999, pp. 23-87). Sin embargo, es en el período comprendido entre las dos guerras mundiales del siglo XX cuando la criptografía pasa de ser un arte erudito a una disciplina industrializada, mecanizada y, finalmente, automatizada; y es en ese tránsito donde puede situarse, con propiedad histórica, el origen remoto de la ciberseguridad moderna.

El artefacto paradigmático de esta transformación fue la máquina Enigma, desarrollada inicialmente con fines comerciales por el ingeniero alemán Arthur Scherbius en 1918 y adoptada por la Wehrmacht, la Kriegsmarine y la Luftwaffe como dispositivo estándar de cifrado militar durante el régimen nacionalsocialista. La máquina implementaba un sistema de sustitución polialfabética mediante rotores móviles, un Steckerbrett o tablero de conexiones, y un mecanismo reflector que multiplicaba exponencialmente el espacio de claves posibles. Para una configuración estándar de tres rotores, el número teórico de combinaciones superaba los 158 trillones, lo que llevó al alto mando alemán a considerar el sistema matemáticamente inviolable (Hodges, 1983, pp. 161-178; Welchman, 1982, pp. 95-132).

La complacencia germana, sin embargo, subestimó tres factores que la criptología contemporánea ha sistematizado como axiomas fundamentales. El primero es el llamado principio de Kerckhoffs, formulado en 1883 por el lingüista flamenco Auguste Kerckhoffs, según el cual la seguridad de un sistema criptográfico no debe depender del secreto del algoritmo sino exclusivamente del secreto de la clave. El segundo es la inevitable existencia de vulnerabilidades operacionales: el uso humano del sistema introduce patrones predecibles —repetición de saludos, frases protocolares, reutilización indebida de configuraciones— que erosionan la robustez teórica del cifrado. El tercero es la capacidad de la fuerza computacional bruta de transformar el cálculo numérico en herramienta de ataque sistemático, principio que anticipa, casi un siglo antes de su formulación cuántica, la lógica que hoy subyace al concepto de harvest now, decrypt later (Anderson, 2020, pp. 73-89).

La explotación conjunta de estas tres debilidades hizo posible la mayor operación criptanalítica de la historia: el descifrado sistemático de Enigma en Bletchley Park, la mansión victoriana situada en Buckinghamshire que albergó la Government Code and Cypher School británica entre 1939 y 1945. El trabajo, iniciado conceptualmente por los matemáticos polacos Marian Rejewski, Jerzy Różycki y Henryk Zygalski, fue continuado y ampliado por el equipo

británico encabezado por Alan Turing, Gordon Welchman, Dilly Knox y Hugh Alexander, con el respaldo de un personal de cerca de diez mil personas, en su gran mayoría mujeres operadoras y analistas (Copeland, 2006, pp. 51-79).

El logro de Bletchley Park no se redujo al descifrado tácticamente decisivo de mensajes militares —aporte que, según los cálculos del historiador oficial Sir Harry Hinsley, abrevió el conflicto al menos dos años y salvó cientos de miles de vidas—. Su trascendencia para la ciberseguridad contemporánea radica en tres aportaciones estructurales. En primer término, la construcción de las bombas criptográficas y, posteriormente, del computador Colossus, dispositivo programable que opera sobre datos digitales para resolver un problema concreto: el origen funcional de la informática moderna se encuentra, así, indisolublemente vinculado a una operación de inteligencia de señales. En segundo lugar, la institucionalización de los principios de compartimentación de la información, necesidad de saber (need-to-know) y clasificación por niveles, principios que la práctica de seguridad civil heredaría y que constituyen el núcleo dogmático del concepto contemporáneo de control de acceso (West-Brown et al., 2003, pp. 17-22). En tercer término, la consagración del secreto técnico operacional como bien jurídico protegido por el Estado, anticipo de las modernas categorías de inteligencia estratégica y seguridad nacional digital.

El paralelo estadounidense merece igual atención. En 1942, el Ejército y la Marina de los Estados Unidos crearon, respectivamente, el Signal Security Service y OP-20-G, organizaciones encargadas de la criptografía y el criptoanálisis que en 1952 confluirían en la actual National Security Agency (NSA). El éxito norteamericano frente al sistema japonés Purple —reverso técnico de Enigma— consolidó la doctrina de que la guerra moderna se decide tanto en el campo de batalla como en el dominio invisible de las comunicaciones cifradas (Bamford, 2008, pp. 65-92). De este modo, ya en la posguerra, las superpotencias habían internalizado tres convicciones que, transcurridos ochenta años, siguen estructurando el derecho internacional de la ciberseguridad: que la información es un activo estratégico de primer orden; que su protección y su captura constituyen funciones esenciales del Estado; y que la innovación criptográfica y criptanalítica forma parte indisociable del poder soberano.

El ordenamiento jurídico positivo tardaría décadas en asimilar estas premisas. Las primeras normas explícitas sobre uso, exportación y restricción de la criptografía datan, en los Estados

Unidos, de la Arms Export Control Act de 1976 y de las International Traffic in Arms Regulations (ITAR), que durante la década de 1990 mantuvieron a la criptografía civil sometida al régimen de los armamentos. En el plano internacional, el Acuerdo de Wassenaar de 1996 estableció controles multilaterales sobre la exportación de tecnologías de cifrado, régimen que continúa vigente con sucesivas actualizaciones. Estos antecedentes regulatorios, ajenos al ciudadano común durante mucho tiempo, demuestran que la ciberseguridad nació en el seno del derecho militar y del derecho del comercio exterior antes que en el derecho administrativo, civil o penal —circunstancia que explica, en gran medida, las tensiones entre soberanía estatal y derechos individuales que el derecho de la ciberseguridad sigue resolviendo en la actualidad (Diffie & Landau, 2007, pp. 119-156)—.

1.2. Primeros virus informáticos: de Creeper al gusano de Morris (1971-1988)

Si la criptografía militar puede considerarse el ancestro teórico de la ciberseguridad, los virus informáticos representan su detonante práctico. Fue solo cuando los sistemas informáticos pasaron del control institucional cerrado al uso distribuido y, sobre todo, en red, que emergieron amenazas que exigieron una respuesta organizada y eventualmente regulada por el derecho.

El primer programa autorreplicante de la historia, Creeper, fue desarrollado en 1971 por Bob Thomas, ingeniero de la firma estadounidense BBN Technologies, sobre la red ARPANET y específicamente para el sistema operativo TENEX. Creeper no era propiamente un virus en sentido moderno: se trataba de un programa experimental que se propagaba entre computadoras PDP-10 conectadas a la red, mostrando en cada nueva máquina el mensaje «I'm the Creeper, catch me if you can!». No causaba daño ni se ocultaba; constituía, más bien, una prueba conceptual del fenómeno de la autorreplicación digital. Como respuesta natural surgió Reaper, programa creado por Ray Tomlinson —el mismo inventor del correo electrónico— con la misión de localizar y eliminar las instancias de Creeper. Reaper es, en consecuencia, históricamente el primer antivirus (Cohen, 1987, pp. 22-35).

El siguiente hito relevante es el virus Elk Cloner, escrito en 1982 por Rich Skrenta, un estudiante de quince años de Pittsburgh, para el sistema operativo del Apple II. Elk Cloner se propagaba mediante disquetes infectados y, tras cincuenta ejecuciones del disco, desplegaba un poema en pantalla. Pese a su carácter inocuo, este programa demuestra dos fenómenos

sociológicamente significativos: la salida del fenómeno vírico del entorno académico-corporativo hacia el ámbito doméstico, y la aparición del hacker adolescente como figura sociotécnica que poblaría, a partir de entonces, el imaginario cultural contemporáneo.

El término virus aplicado a programas informáticos fue acuñado en 1983 por Fred Cohen, doctorando en la Universidad del Sur de California, en su tesis dirigida por Leonard Adleman —el «A» de RSA—. Cohen definió el virus informático como «un programa que puede infectar a otros programas modificándolos para incluir una copia, posiblemente evolucionada, de sí mismo» (Cohen, 1985, p. 12). Esta definición, formulada en términos de teoría de la computación, demostró matemáticamente que la detección perfecta de virus es un problema indecidible: no existe, ni puede existir, un algoritmo que distinga con certeza absoluta un programa benigno de uno malicioso. Esta proposición, conocida como teorema de Cohen, constituye el fundamento epistemológico de toda la industria antivirus contemporánea y explica por qué la detección de malware sigue siendo, esencialmente, un ejercicio probabilístico (Spafford, 1989, pp. 5-7).

En 1986 surgió Brain, considerado el primer virus diseñado para el sistema operativo MS-DOS de IBM PC y, en consecuencia, el primer virus masivo del ecosistema doméstico. Fue desarrollado en Lahore (Pakistán) por los hermanos Basit y Amjad Farooq Alvi con el propósito declarado de proteger una aplicación médica de su autoría frente a la piratería. El virus modificaba el sector de arranque del disquete e incluía los datos de contacto —nombre, dirección y números telefónicos— de sus autores, particularidad que hoy parece pintoresca pero que entonces revelaba la inexistencia del concepto de anonimato hostil como característica del ciberdelincuente moderno. Brain inauguró, asimismo, la tradición de los virus de sector de arranque que dominarían el panorama hasta la consolidación de Microsoft Windows en la década de 1990 (Brunnstein, 1990, pp. 41-63).

El acontecimiento que marca, sin discusión, el fin de la inocencia digital y el inicio de la ciberseguridad como disciplina autónoma es el gusano de Morris, liberado en la noche del 2 de noviembre de 1988 desde el Massachusetts Institute of Technology por Robert Tappan Morris, entonces estudiante de doctorado en la Universidad de Cornell. El programa explotaba simultáneamente cuatro vulnerabilidades —un buffer overflow en el servicio fingerd, una falla en la configuración de sendmail, debilidades en las contraseñas remotas y un error de implementación en el comando rsh— y se propagaba autónomamente a través de la entonces incipiente Internet,

infectando cerca de seis mil computadoras de un total estimado de sesenta mil, es decir, aproximadamente el diez por ciento de la red mundial (Spafford, 1989, pp. 12-28; Eichin & Rochlis, 1989, pp. 326-343).

El daño económico atribuido al incidente, calculado en varios millones de dólares de la época, no derivó de la finalidad destructiva del programa —que carecía de carga maliciosa explícita— sino de un error de programación que provocaba reinfecciones múltiples, saturando los recursos de las máquinas afectadas. Morris fue procesado bajo la Computer Fraud and Abuse Act de 1986, recientemente promulgada, y se convirtió en la primera persona condenada por dicha ley en los Estados Unidos. La sentencia, dictada en 1990, impuso tres años de libertad condicional, cuatrocientas horas de servicio comunitario y una multa de diez mil cincuenta dólares.

El gusano de Morris tuvo cuatro consecuencias estructurales que delimitan el inicio del derecho de la ciberseguridad propiamente dicho. En primer lugar, demostró empíricamente la interdependencia sistémica de la red, hasta entonces percibida como un experimento técnico de baja criticidad. En segundo término, acreditó la insuficiencia de la respuesta puramente técnica frente a incidentes que afectaban a múltiples organizaciones simultáneamente, evidenciando la necesidad de coordinación supraorganizacional. En tercer lugar, motivó el primer uso significativo de una norma penal específica contra delitos informáticos, sentando jurisprudencia sobre la tipicidad del acceso no autorizado a sistemas informáticos. En cuarto término, y por encima de los anteriores, condujo a la creación del primer equipo de respuesta a incidentes informáticos de la historia, el CERT/CC de Carnegie Mellon, cuyo análisis ocupa el apartado siguiente.

1.3. El nacimiento del primer CERT (CMU/SEI, 1988)

A los diez días de la liberación del gusano de Morris, el 17 de noviembre de 1988, la Defense Advanced Research Projects Agency (DARPA) suscribió un acuerdo con el Software Engineering Institute (SEI) de la Universidad Carnegie Mellon (Pittsburgh) para establecer el Computer Emergency Response Team Coordination Center (CERT/CC), primer equipo institucional dedicado a la respuesta coordinada frente a incidentes de seguridad informática en redes interconectadas. La rapidez con que se adoptó la decisión revela el grado de alarma generado por el incidente y constituye, en sí misma, una declaración política sobre el carácter prioritario que la administración estadounidense atribuía al problema (West-Brown et al., 2003, pp. 1-15).

El modelo CERT/CC se inspiró parcialmente en los esquemas militares de respuesta a emergencias y en los equipos hospitalarios de respuesta rápida, pero incorporó tres innovaciones organizacionales que terminarían por convertirse en estándares de la industria. La primera fue la centralización de la inteligencia sobre vulnerabilidades, sistematizada en boletines técnicos —los célebres CERT Advisories— de distribución pública. La segunda fue el establecimiento de canales de comunicación confidencial con desarrolladores, administradores y agencias gubernamentales, lo que permitió la divulgación coordinada y responsable de fallos de seguridad antes de su publicación general. La tercera fue la articulación de una función pedagógica dirigida a la comunidad técnica, que incluyó la elaboración de guías metodológicas, plantillas operativas y programas de formación reconocidos internacionalmente.

La proliferación de equipos similares fue rápida. En Australia se creó AUSCERT en 1993; en Alemania, DFN-CERT en 1992; en los Países Bajos, CERT-NL; y en el Reino Unido, JANET-CERT. En 1990 se constituyó el Forum of Incident Response and Security Teams (FIRST) con sede en Estados Unidos, que reúne en la actualidad a más de seiscientos equipos de respuesta de noventa países y constituye la organización paraguas que articula la cooperación internacional especializada en la materia. El modelo se replicó en América Latina con la creación de CERT.br (Brasil, 1997), CERT-AR (Argentina, 1999), ColCERT (Colombia, 2009), y, en el caso ecuatoriano, EcuCERT, adscrito a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) y constituido formalmente como Centro de Respuesta a Incidentes Informáticos del Ecuador en virtud de la Resolución ARCOTEL-2014-0457 (MINTEL, 2021).

La institucionalización del modelo CERT-CSIRT a escala global tiene una consecuencia jurídica que conviene subrayar. La aparición de equipos especializados con funciones técnicas reconocidas, capacidad de coordinación supranacional y reputación profesional acreditada generó la necesidad de definir su estatuto jurídico, su régimen de responsabilidades y los límites de su potestad operativa. ¿Puede un CERT acceder sin autorización judicial a un sistema comprometido para contener un incidente en curso? ¿Está protegido por secreto profesional? ¿Qué grado de inmunidad le asiste cuando comparte información sobre vulnerabilidades con terceros? ¿Cuál es su régimen de responsabilidad civil por error u omisión? Estas cuestiones, ya complejas en el plano nacional, alcanzan vertiginosa dificultad cuando se proyectan al ámbito transfronterizo. La respuesta normativa, aún incipiente en muchos países de la región —entre ellos el Ecuador—,

constituye uno de los principales déficits regulatorios contemporáneos y será objeto de análisis detallado en los Libros Cuarto y Quinto del presente volumen.

Conviene cerrar esta sección señalando que el modelo CERT consagró, también, un cambio cultural decisivo: la transición desde una concepción reactiva e individualizada de la seguridad informática —cada organización gestiona sus propios incidentes con sus propios medios— hacia una concepción cooperativa y sistémica, en la que la información sobre amenazas circula, las defensas se coordinan y la respuesta se concibe como un bien público compartido. Esta transformación, hoy traducida en marcos jurídicos como la Directiva NIS 2 europea o el modelo CISA estadounidense, encuentra su origen conceptual en la decisión adoptada en Pittsburgh durante aquel otoño de 1988.

1.4. La era de la masificación de Internet (1990-2000)

La década de 1990 constituye, en la historia de la ciberseguridad, el período de la democratización del riesgo. La invención de la World Wide Web por Tim Berners-Lee en el CERN en 1989, la liberación de su código fuente en 1993 y la aparición de los primeros navegadores comerciales —Mosaic en 1993, Netscape Navigator en 1994, Internet Explorer en 1995— marcaron la transición de la red desde su uso estrictamente académico y gubernamental hacia su masificación civil. En diez años, el número estimado de usuarios pasó de aproximadamente dos millones a más de trescientos sesenta millones, configurando un fenómeno sin precedentes en la historia de la tecnología (Castells, 2001, pp. 33-58).

Esta expansión, sin embargo, trajo consigo la generalización de amenazas previamente confinadas al entorno académico o experimental. Los virus de macro, encabezados por Concept (1995) y popularizados con Melissa (1999), explotaron la integración entre el procesador de texto Microsoft Word y el correo electrónico para propagarse a velocidades antes inconcebibles. El virus ILOVEYOU, liberado el 4 de mayo de 2000 por dos jóvenes filipinos, infectó cerca de cincuenta millones de computadoras en una semana y causó pérdidas estimadas entre cinco y diez mil millones de dólares en daños y costes de respuesta. La novedad de estos episodios no estribó tanto en su sofisticación técnica —relativamente modesta— como en la magnitud del fenómeno, la rapidez de su propagación y la imposibilidad de las autoridades de procesar a sus autores en jurisdicciones que carecían de normas penales aplicables. El caso filipino resulta particularmente

ilustrativo: el principal sospechoso debió ser liberado porque la legislación penal de su país no contemplaba, al momento del hecho, la conducta como típica (Saín, 2015, pp. 89-104).

La respuesta jurídica internacional al fenómeno se articuló a través de tres líneas convergentes. La primera fue la promulgación de leyes penales específicas sobre delitos informáticos en numerosos países. Estados Unidos amplió en sucesivas reformas la Computer Fraud and Abuse Act; el Reino Unido aprobó la Computer Misuse Act en 1990; Alemania incorporó los §§ 202a, 263a y 303a-303b a su Código Penal; Francia adoptó la Loi Godfrain en 1988; España introdujo los delitos informáticos en su Código Penal de 1995 (Téllez Valdés, 2008, pp. 187-214). En América Latina, Chile promulgó la Ley 19.223 en 1993, primer cuerpo normativo regional sobre delitos informáticos, y Venezuela aprobó la Ley Especial contra los Delitos Informáticos en 2001. Ecuador, en este capítulo, llegaría con cierto retraso: la primera tipificación sistemática de delitos informáticos en el país se incorporó mediante la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos de 2002, complementada posteriormente por el Código Orgánico Integral Penal de 2014 (Acurio del Pino, 2016, pp. 41-78).

La segunda línea fue la elaboración del primer instrumento internacional vinculante en la materia: el Convenio del Consejo de Europa sobre Ciberdelincuencia, conocido como Convenio de Budapest, abierto a la firma el 23 de noviembre de 2001 en la capital húngara. El instrumento, fruto de cuatro años de negociaciones, estableció definiciones armonizadas de los principales delitos informáticos, instituyó reglas procesales especiales para la preservación de evidencia digital y creó un mecanismo de cooperación internacional disponible las veinticuatro horas del día. Su análisis pormenorizado se desarrollará en el Capítulo 18 del presente volumen; baste señalar aquí que la apertura del Convenio coincidió, no por casualidad, con los meses inmediatamente posteriores a los atentados del 11 de septiembre de 2001 en Estados Unidos, que aceleraron decisivamente la voluntad política internacional de regular el ciberespacio (Markopoulou, Papakonstantinou & de Hert, 2019, pp. 4-9).

La tercera línea —menos visible pero igualmente decisiva— fue la consolidación de estándares técnicos internacionales elaborados por organizaciones no gubernamentales. La British Standards Institution publicó en 1995 la norma BS 7799, primer estándar moderno de gestión de seguridad de la información, que sería elevada al rango de norma internacional en 2000 con la designación ISO/IEC 17799, antecedente directo de las actuales ISO/IEC 27001 e ISO/IEC 27002.

La aparición de estos instrumentos demuestra una característica estructural del derecho de la ciberseguridad que sigue vigente: su carácter híbrido normativo-técnico, en el que las normas formales se combinan con estándares de origen privado que adquieren fuerza vinculante por vía de la incorporación contractual, regulatoria o reputacional. Esta característica ha sido analizada con detalle en el volumen complementario de esta serie editorial, dedicado a la protección de datos personales, donde se examina la misma lógica aplicada al ecosistema del Reglamento General de Protección de Datos europeo y la Ley Orgánica de Protección de Datos Personales ecuatoriana (Páez Rivadeneira, 2026).

El cierre de la década dejó, en consecuencia, un escenario radicalmente distinto al de su comienzo. Internet había dejado de ser una red académica para convertirse en infraestructura económica esencial; los virus habían pasado de curiosidad técnica a amenaza global con impacto medible en miles de millones de dólares; el cibercrimen había emergido como categoría jurídica autónoma; la cooperación internacional había producido su primer tratado vinculante; y la industria de la ciberseguridad —en 2000 estimada en aproximadamente cinco mil millones de dólares— se encontraba en franca expansión. Faltaba, sin embargo, un acontecimiento que llevara la disciplina al rango de asunto de Estado de primera magnitud. Ese acontecimiento llegaría diez años después.

1.5. La era de la ciberguerra: Stuxnet (2010) como punto de inflexión

El 17 de junio de 2010, la firma bielorrusa de seguridad informática VirusBlokAda detectó en una computadora iraní una pieza de malware de complejidad inusual que provocaba reinicios inexplicables en el sistema operativo. El examen pormenorizado del código, asumido durante los meses siguientes por Symantec y Kaspersky Lab, reveló la existencia de lo que la literatura especializada considera el primer arma cibernética desplegada operacionalmente en la historia: Stuxnet (Falliere, Murchu & Chien, 2011, pp. 1-69; Zetter, 2014, pp. 1-19).

Stuxnet poseía características que, examinadas en conjunto, descartaban su origen criminal común y apuntaban inequívocamente hacia un actor estatal con recursos masivos. El programa explotaba cuatro vulnerabilidades de día cero simultáneamente —cifra inédita en la historia del malware—, utilizaba certificados digitales legítimos sustraídos a dos empresas taiwanesas (Realtek y JMicron), incorporaba conocimiento profundo de los controladores lógicos

programables Siemens S7-300 y S7-400 utilizados específicamente en centrifugadoras industriales, y se diseñó para activarse únicamente cuando detectara una configuración exacta de cascadas centrífugas compatible con las plantas iraníes de enriquecimiento de uranio de Natanz. La carga maliciosa modificaba sutilmente la velocidad de rotación de las centrifugadoras hasta provocar su destrucción mecánica, mientras paralelamente enviaba a los operadores lecturas falsas que simulaban un funcionamiento normal (Langner, 2013, pp. 6-23).

El impacto operacional fue significativo: las estimaciones más conservadoras sugieren que aproximadamente mil de las cinco mil centrifugadoras IR-1 de Natanz quedaron inutilizadas, retrasando el programa nuclear iraní en al menos dieciocho meses. Más allá del impacto técnico, sin embargo, lo que confiere a Stuxnet su carácter de hito histórico es su dimensión doctrinal. El incidente demostró tres proposiciones que han reconfigurado el derecho de la ciberseguridad contemporáneo.

La primera es la demostración empírica de la cibernética como medio de hostilidad estatal. Hasta 2010, la noción de ciberguerra se debatía en el plano teórico y especulativo; tras Stuxnet, dejó de ser una hipótesis para convertirse en un hecho documentado. Reportajes posteriores publicados por The New York Times y otros medios atribuyeron la operación, bajo el nombre clave Olympic Games, a una alianza entre la NSA estadounidense y la Unidad 8200 israelí. Aunque ninguno de los dos gobiernos ha confirmado oficialmente su participación, la atribución es ampliamente aceptada en la literatura especializada y en los círculos de inteligencia (Sanger, 2012, pp. 188-225).

La segunda proposición es la vulnerabilidad de las infraestructuras críticas físicas frente a ataques digitales. Stuxnet demostró que una intervención en el código informático podía causar destrucción material en el mundo físico —centrifugadoras de acero pulverizadas— sin necesidad de presencia humana en el lugar del ataque, sin sobrevuelo, sin proyectiles, sin marca de proveniencia evidente. Esta característica, denominada por la doctrina como convergencia cibernético-cinética (cyber-kinetic convergence), reordena radicalmente las categorías clásicas del derecho internacional humanitario y del derecho de la responsabilidad estatal por hecho internacionalmente ilícito (Lindsay, 2013, pp. 365-404).

La tercera proposición es la insuficiencia del derecho internacional clásico para tratar el fenómeno. ¿Constituyó Stuxnet un acto de fuerza prohibido por el artículo 2.4 de la Carta de

Naciones Unidas? ¿Un ataque armado en el sentido del artículo 51 que habilitara la legítima defensa iraní? ¿Una intervención prohibida en los asuntos internos de otro Estado? ¿Un acto de sabotaje sometido al régimen del espionaje? La doctrina sigue dividida y, lo que resulta más significativo, los principales actores estatales han evitado pronunciarse de manera definitiva. El Manual de Tallinn sobre el derecho internacional aplicable a la ciberguerra, publicado en 2013 por el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN, intenta sistematizar el régimen aplicable, pero su carácter doctrinal —no vinculante— y la persistencia de disensos profundos en cuestiones centrales evidencian que la materia se encuentra aún en formación. La segunda edición del Manual, publicada en 2017 bajo el título Manual de Tallinn 2.0 sobre el derecho internacional aplicable a las ciberoperaciones, amplía el alcance a operaciones por debajo del umbral del conflicto armado, pero confirma más que disipa las incertidumbres normativas (Schmitt, 2017, pp. 1-32).

Stuxnet inauguró, en consecuencia, lo que la historiografía técnica denomina la era de la ciberguerra, caracterizada por la proliferación de operaciones cibernéticas atribuibles —con grados diversos de certeza— a actores estatales o paraestatales. La lista de incidentes posteriores documenta el fenómeno: Duqu (2011), Flame (2012), Shamoon contra Saudi Aramco (2012), los ataques de APT1 chino documentados por Mandiant (2013), las operaciones rusas contra Ucrania mediante BlackEnergy (2015) y NotPetya (2017), el ataque norcoreano WannaCry (2017), la operación SolarWinds atribuida a actores rusos (2020), y los ciberataques sistemáticos contra la infraestructura ucraniana desde 2022 en el marco del conflicto con la Federación Rusa.

La respuesta jurídico-institucional a este escenario ha sido intensa pero fragmentada. Los Estados Unidos elevaron el ciberespacio al rango de quinto dominio operacional mediante la International Strategy for Cyberspace de 2011 y crearon el United States Cyber Command en 2010, ascendido a comando unificado en 2018. La OTAN reconoció el ciberespacio como dominio operacional en la Cumbre de Varsovia de 2016. La Unión Europea aprobó la Directiva NIS en 2016, primer instrumento europeo vinculante sobre ciberseguridad de redes y sistemas. China promulgó su Cybersecurity Law en 2017. Rusia adoptó su doctrina de seguridad de la información en 2016. Israel reorganizó su arquitectura institucional mediante la creación del National Cyber Directorate en 2017. Y la Asamblea General de Naciones Unidas mantiene desde 2018 un Grupo de Expertos Gubernamentales y un Grupo de Composición Abierta dedicados específicamente al comportamiento responsable de los Estados en el ciberespacio.

América Latina, y en particular Ecuador, ingresó a esta etapa con considerable retraso institucional. La Política Nacional de Ciberseguridad ecuatoriana fue formalizada únicamente en 2021 mediante el Decreto Ejecutivo 811, expedido casi una década después de los incidentes que motivaron las decisiones equivalentes en otras latitudes. Esta asimetría temporal —que se traduce en una asimetría material de capacidades, de doctrina y de talento humano— constituye uno de los desafíos estructurales más significativos para el país y será objeto de tratamiento detallado en el Capítulo 26 del presente volumen. Como se ha sostenido en obra anterior del autor, el problema de fondo es epistemológico antes que técnico: el ordenamiento ecuatoriano carece todavía de una doctrina jurídica autóctona suficientemente sedimentada para sostener una política pública de ciberseguridad con vocación de permanencia, y esta carencia se proyecta sobre el modo en que el país aborda cuestiones contiguas como la regulación de la inteligencia artificial (Páez Rivadeneira, 2025, pp. 47-68).

1.6. La era de la ciberresiliencia: NIS, NIS 2, DORA y el Cyber Resilience Act

La constatación de que ningún sistema informático puede ser absolutamente seguro y de que los incidentes graves son, en realidad, inevitables, condujo durante la década de 2010 a una transformación conceptual de alcance considerable. Si Stuxnet había demostrado la vulnerabilidad estructural de las infraestructuras críticas, los incidentes subsiguientes —desde el ataque a Sony Pictures en 2014 hasta la oleada de ransomware iniciada con WannaCry en 2017, pasando por el desastre de Equifax en 2017 y el episodio SolarWinds en 2020— mostraron que incluso las organizaciones con mayor inversión en seguridad sufrían incidentes consumados. La consecuencia regulatoria fue el desplazamiento del paradigma desde la prevención absoluta —objetivo intrínsecamente inalcanzable— hacia la resiliencia operativa, entendida como la capacidad de una organización para anticipar, soportar, recuperarse y adaptarse frente a eventos cibernéticos adversos (Anderson, 2020, pp. 991-1023).

La Unión Europea ha sido el espacio jurídico que con mayor sistematicidad ha articulado normativamente este nuevo paradigma. Cuatro instrumentos resultan especialmente representativos. El primero es la Directiva (UE) 2016/1148, conocida como Directiva NIS, adoptada el 6 de julio de 2016, que estableció por primera vez en el derecho europeo obligaciones armonizadas de gestión del riesgo y notificación de incidentes para operadores de servicios

esenciales y proveedores de servicios digitales. La Directiva NIS tuvo el mérito histórico de constituir el primer instrumento europeo vinculante en la materia, pero su implementación nacional fragmentada y su limitado alcance subjetivo motivaron la promulgación de su sucesora.

El segundo instrumento, y referencia central del derecho europeo vigente, es la Directiva (UE) 2022/2555, conocida como Directiva NIS 2, adoptada el 14 de diciembre de 2022, que sustituye y amplía sustancialmente a la Directiva NIS de 2016. NIS 2 amplía notablemente el ámbito subjetivo de aplicación, incorporando sectores como la administración pública, el sector espacial, la gestión de residuos, la fabricación de productos médicos críticos, la producción y distribución de alimentos, y los proveedores de servicios digitales en sentido amplio. Establece obligaciones reforzadas de gestión del riesgo, plazos de notificación de incidentes en tres etapas —veinticuatro horas para alerta temprana, setenta y dos horas para notificación formal, un mes para informe final—, responsabilidad personal de los órganos de dirección, y un régimen sancionador que alcanza el dos por ciento del volumen de negocios anual mundial en el caso de entidades esenciales (Schmitz-Berndt, 2023, pp. 1-15).

El tercer instrumento es el Reglamento (UE) 2022/2554, conocido como DORA —Digital Operational Resilience Act—, adoptado en paralelo con NIS 2 y aplicable desde el 17 de enero de 2025. DORA establece un régimen armonizado y vinculante de resiliencia operativa digital para el sector financiero europeo, sustituyendo el mosaico previo de normas sectoriales nacionales y de directrices de las autoridades europeas de supervisión. El Reglamento articula cinco pilares: gestión del riesgo de las TIC, notificación de incidentes graves relacionados con las TIC, pruebas de resiliencia operativa digital, gestión del riesgo de terceros proveedores de servicios TIC, e intercambio de información sobre amenazas y vulnerabilidades. DORA constituye, en muchos aspectos, el referente regulatorio internacional más avanzado en materia de ciberresiliencia del sector financiero, y su influencia se proyectará previsiblemente sobre las jurisdicciones latinoamericanas en los próximos años.

El cuarto instrumento es el Cyber Resilience Act (CRA), formalmente el Reglamento (UE) 2024/2847, adoptado el 23 de octubre de 2024, que introduce requisitos obligatorios de ciberseguridad para todos los productos con elementos digitales comercializados en el mercado europeo, desde dispositivos del internet de las cosas hasta software de consumo. El CRA constituye una innovación regulatoria significativa por dos motivos. En primer lugar, traslada el

deber de seguridad desde el usuario final —que clásicamente debía configurar y proteger sus dispositivos— hacia el fabricante, instaurando un régimen de responsabilidad por defecto del producto en el dominio digital. En segundo lugar, establece la obligación de proporcionar actualizaciones de seguridad durante todo el ciclo de vida útil esperado del producto, ruptura sin precedentes con la práctica industrial dominante.

La articulación de NIS 2, DORA y CRA con instrumentos complementarios —el Cybersecurity Act de 2019, el Cyber Solidarity Act de 2024, el Critical Entities Resilience Directive, la AI Act y el Data Governance Act— configura el ecosistema regulatorio más sofisticado del mundo en materia de ciberseguridad. Esta densidad normativa no es casual: refleja la apuesta estratégica europea por consolidar un modelo regulatorio propio, distinto del modelo estadounidense de regulación sectorial y desregulación general, y del modelo chino de control estatal centralizado del ciberespacio. La doctrina especializada coincide en señalar que esta convergencia de modelos hacia tres paradigmas globales —europeo, estadounidense y chino— constituye la principal característica geopolítica del derecho de la ciberseguridad contemporáneo, y que las jurisdicciones intermedias —entre ellas la ecuatoriana— deberán definir progresivamente su posicionamiento respecto de cada uno de ellos (Bygrave, 2022, pp. 47-72).

Conviene destacar, finalmente, que la era de la ciberresiliencia ha consolidado una herramienta conceptual que dominará el análisis del derecho de la ciberseguridad en los capítulos siguientes: la gestión del riesgo basada en escenarios y proporcionalidad. A diferencia del paradigma anterior, que tendía a exigir el cumplimiento de listas estandarizadas de controles, el paradigma actual requiere a las organizaciones identificar sus riesgos específicos, calibrar la respuesta a su contexto operacional y demostrar la racionalidad de las decisiones adoptadas. Este enfoque, profundamente influenciado por la filosofía del Reglamento General de Protección de Datos —analizada con detalle en el volumen complementario de esta serie editorial (Páez Rivadeneira, 2026)—, traslada al destinatario de la norma una carga argumentativa significativa y, correlativamente, una responsabilidad reforzada por las decisiones tomadas.

1.7. Evolución conceptual: de la seguridad informática a la ciberseguridad y a la ciberresiliencia

El recorrido histórico que hemos trazado permite ahora una sistematización conceptual de las tres nociones que articulan el campo: seguridad informática, ciberseguridad y ciberresiliencia. Aunque la práctica profesional y la literatura periodística suelen emplear los términos como sinónimos, su análisis riguroso revela tres etapas distintas de un mismo proceso evolutivo, cada una con su propio paradigma técnico, jurídico e institucional.

La seguridad informática designa el conjunto de medidas técnicas, físicas y administrativas orientadas a proteger los recursos informáticos —equipos, redes, datos, programas— de una organización determinada. Su ámbito de aplicación es organizacional, estático y predominantemente reactivo. Asume como referente al sistema cerrado o de conectividad limitada, presupone un perímetro defendible, y articula sus controles en torno a la triada clásica de confidencialidad, integridad y disponibilidad. Este paradigma fue dominante hasta mediados de la década de 1990 y sigue presente, residualmente, en la cultura técnica de muchas organizaciones, especialmente en aquellas que no han adaptado plenamente sus marcos a la realidad de la nube, la movilidad y los servicios distribuidos.

La ciberseguridad, por contraste, designa el conjunto de medidas orientadas a proteger no solo los recursos informáticos sino el ciberespacio en su integralidad, entendido este como dominio interconectado, transnacional y dinámico en el que confluyen sistemas técnicos, actores humanos, contenidos informacionales y operaciones automatizadas. Su ámbito de aplicación es ecosistémico, dinámico y proactivo. Asume como referente la red abierta y permanentemente expuesta, abandona la noción de perímetro como categoría operativa central, e incorpora dimensiones que la seguridad informática clásica ignoraba: la inteligencia sobre amenazas, la atribución de adversarios, la cooperación intersectorial e internacional, y la articulación con políticas públicas de seguridad nacional. El paradigma de la ciberseguridad se consolida desde finales de la década de 1990 y alcanza su madurez tras Stuxnet.

La ciberresiliencia, por último, designa el conjunto de capacidades organizacionales y sistémicas para anticipar, soportar, recuperarse y adaptarse frente a eventos cibernéticos adversos. Su ámbito de aplicación es adaptativo, sistémico y orientado a la continuidad. Asume como referente un escenario en el que los incidentes consumados son inevitables y la atención se desplaza desde la prevención absoluta —imposible— hacia la minimización de su impacto, la rápida recuperación y el aprendizaje organizacional. Este paradigma se consolida durante la década

de 2010 y constituye el horizonte normativo dominante en los instrumentos europeos contemporáneos como NIS 2, DORA y CRA.

La transición entre los tres paradigmas no es excluyente sino acumulativa. La ciberresiliencia no descarta los controles de la ciberseguridad ni renuncia a las medidas técnicas de la seguridad informática; los integra y los reorienta en función de un objetivo organizacional ampliado. Una analogía útil es la propuesta por Cano Martínez (2017, pp. 23-29): así como en la medicina contemporánea la salud no se entiende ya como mera ausencia de enfermedad sino como estado dinámico de bienestar que comprende prevención, tratamiento y rehabilitación, la ciberresiliencia no se entiende como mera ausencia de incidentes sino como capacidad sostenida de operar en un entorno hostil mediante la integración articulada de prevención, respuesta y aprendizaje.

Para facilitar la comprensión sintética de la evolución descrita, el cuadro siguiente sistematiza los rasgos distintivos de los tres paradigmas conceptuales:

Seguridad informática	Ciberseguridad	Ciberresiliencia
Período: hasta mediados de 1990.	Período: 1995-2015.	Período: 2015 en adelante.
Ámbito: organizacional, estático, reactivo.	Ámbito: ecosistémico, dinámico, proactivo.	Ámbito: adaptativo, sistémico, orientado a la continuidad.
Referente: sistema cerrado con perímetro defendible.	Referente: red abierta y permanentemente expuesta.	Referente: entorno hostil con incidentes inevitables.
Eje conceptual: triada CIA (confidencialidad, integridad, disponibilidad).	Eje conceptual: defensa en profundidad e inteligencia sobre amenazas.	Eje conceptual: anticipación, soporte, recuperación y adaptación.
Marco normativo dominante: políticas internas y BS 7799.	Marco normativo dominante: ISO/IEC 27000, Convenio de Budapest, leyes nacionales sobre delitos informáticos.	Marco normativo dominante: Directiva NIS 2, DORA, Cyber Resilience Act, NIST CSF 2.0.
Perfil profesional: administrador de sistemas.	Perfil profesional: CISO técnico-estratégico.	Perfil profesional: Chief Resilience Officer.

Esta evolución conceptual encuentra, por lo demás, un correlato preciso en la transformación de las profesiones del sector. El administrador de sistemas clásico, encargado de

configurar y mantener el funcionamiento técnico de la infraestructura, fue desplazado en la década de 1990 por el oficial de seguridad informática o CISO técnico, encargado de implementar políticas, controles y procesos de seguridad. Durante la década de 2000, el CISO se transformó en una figura organizacional crecientemente estratégica, encargada de articular la seguridad con las decisiones del negocio y de reportar al consejo de administración. En la década actual emerge la figura del Chief Resilience Officer o equivalente, encargado de la resiliencia operativa en sentido integral, que abarca ciberseguridad, continuidad del negocio, gestión de crisis y respuesta regulatoria coordinada. Esta evolución de los perfiles profesionales constituye, también, una manifestación del cambio paradigmático que el presente capítulo ha intentado documentar.

La pregunta que orienta el resto del presente volumen surge naturalmente de este recorrido: ¿cuál es el marco jurídico —internacional, regional y nacional— que el derecho contemporáneo ha articulado para gobernar la ciberseguridad en su acepción ampliada y la ciberresiliencia como paradigma vigente?; ¿cómo ha respondido específicamente el ordenamiento jurídico ecuatoriano a este desafío?; ¿qué brechas estructurales persisten y qué políticas públicas resultan necesarias para colmarlas? El esfuerzo sistemático por responder a estas preguntas constituye, precisamente, el propósito de los capítulos que siguen.

Reflexiones finales del capítulo

El presente capítulo ha recorrido las cinco grandes etapas que articulan la genealogía de la ciberseguridad contemporánea, desde su precursor en la criptografía militar de la primera mitad del siglo XX hasta su consolidación como categoría jurídica y estratégica autónoma en la actualidad. Tres ideas conviene retener como hilo conductor del libro entero.

La primera es la naturaleza dialéctica de la relación entre tecnología y derecho. Cada salto tecnológico relevante —el computador electrónico, la red distribuida, el ataque a infraestructuras físicas mediante medios digitales, la interconexión masiva de productos— ha generado una respuesta normativa correlativa, generalmente con un retraso significativo respecto del fenómeno técnico. Este desfase, que algunos autores denominan cyber-legal lag, constituye una característica estructural y permanente del campo, no un defecto coyuntural superable mediante mayor diligencia legislativa. El autor ha sostenido en obra anterior que esta asimetría temporal exige del jurista del

derecho digital una vigilancia epistemológica permanente, dado que la subsunción correcta de un fenómeno tecnológico nuevo bajo una categoría jurídica clásica raramente puede asumirse como evidente (Páez Rivadeneira, 2025, pp. 112-130).

La segunda es la transición desde modelos individuales de protección hacia modelos cooperativos y sistémicos. La ciberseguridad contemporánea es, ineludiblemente, un bien público cuya garantía depende de la articulación entre el Estado, el sector privado, la comunidad técnica y los organismos internacionales. Ningún actor, por poderoso que sea, puede proveerla de manera autárquica; ningún ordenamiento, por sofisticado que se encuentre, puede prescindir de la cooperación transfronteriza.

La tercera es la progresiva juridificación de un fenómeno que, durante décadas, perteneció exclusivamente al dominio técnico. Lo que en 1988 era una emergencia gestionada por un puñado de ingenieros en Pittsburgh constituye, en 2026, una compleja red de obligaciones jurídicas, regímenes sancionatorios, estándares técnicos vinculantes, tratados internacionales y políticas públicas nacionales. Esta transformación impone al jurista contemporáneo la obligación de dominar un cuerpo de conocimiento que excede los confines clásicos del derecho positivo y exige diálogo permanente con la ingeniería, la administración pública y las relaciones internacionales. El presente manual ha sido concebido, precisamente, como instrumento de ese diálogo.

Preguntas de autoevaluación

1. ¿Cuál es el contenido del principio de Kerckhoffs y por qué resulta relevante para la ciberseguridad contemporánea?

2. Explique en qué sentido el trabajo desarrollado en Bletchley Park durante la Segunda Guerra Mundial constituye un antecedente de la ciberseguridad moderna.

3. ¿Por qué el teorema de Cohen sobre la indecidibilidad del problema de detección de virus es relevante para entender las limitaciones de la industria antivirus?

4. Identifique las cuatro consecuencias estructurales que el gusano de Morris generó para la disciplina de la ciberseguridad.

5. ¿Qué tres innovaciones organizacionales introdujo el modelo CERT/CC desarrollado en Carnegie Mellon en 1988?

6. Distinga, con base en lo expuesto en el capítulo, entre el caso del virus ILOVEYOU y el caso de Stuxnet en cuanto a sus implicaciones jurídico-doctrinales.

7. ¿Cuáles son las tres proposiciones doctrinales que Stuxnet estableció empíricamente y que han reconfigurado el derecho de la ciberseguridad?

8. Compare las características distintivas de la Directiva NIS (2016), la Directiva NIS 2 (2022) y el Reglamento DORA (2022).

9. ¿Qué innovaciones aporta el Cyber Resilience Act respecto del régimen previo de responsabilidad por seguridad de productos digitales?

10. Explique las diferencias conceptuales entre seguridad informática, ciberseguridad y ciberresiliencia, y justifique por qué la transición entre estos paradigmas no es excluyente sino acumulativa.

Actividad práctica

Localice y lea integralmente el dictamen In re Robert Tappan Morris (United States Court of Appeals, Second Circuit, 928 F.2d 504, 1991), que confirmó la condena del autor del gusano de Morris bajo la Computer Fraud and Abuse Act. Identifique:

1. El criterio jurídico mediante el cual el tribunal estableció el dolo del autor.

2. La interpretación judicial del concepto de «acceso no autorizado» en el contexto del incidente.

3. Las analogías o disanalogías con la tipificación del artículo 234 del Código Orgánico Integral Penal ecuatoriano sobre acceso no consentido a sistemas informáticos.

Elabore un comentario crítico de dos mil palabras que examine si la doctrina sentada por el tribunal estadounidense en 1991 resultaría aplicable, mutatis mutandis, en el marco del ordenamiento jurídico ecuatoriano contemporáneo.

Lecturas complementarias recomendadas

Sobre criptografía y antecedentes históricos:

- Singh, S. (1999). The Code Book: The Secret History of Codes and Code-Breaking. London: Fourth Estate.
- Hodges, A. (1983). Alan Turing: The Enigma. London: Burnett Books.
- Copeland, B. J. (Ed.). (2006). Colossus: The Secrets of Bletchley Park's Codebreaking Computers. Oxford: Oxford University Press.

Sobre la era de los primeros virus y el gusano de Morris:

- Cohen, F. (1987). Computer Viruses: Theory and Experiments. Computers & Security, 6(1), 22-35.
- Spafford, E. (1989). The Internet Worm Program: An Analysis (Purdue Technical Report CSD-TR-823). West Lafayette: Purdue University.
- Eichin, M. W. & Rochlis, J. A. (1989). With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988. Proceedings of the IEEE Symposium on Security and Privacy, 326-343.

Sobre Stuxnet y la era de la ciberguerra:

- Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York: Crown Publishers.
- Langner, R. (2013). To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve. Arlington: The Langner Group.
- Sanger, D. E. (2012). Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power. New York: Crown Publishers.

Sobre el marco regulatorio europeo contemporáneo:

- Markopoulou, D., Papakonstantinou, V. & de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review, 35(6), 1-11.
- Schmitz-Berndt, S. (2023). Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. Journal of Cybersecurity, 9(1), tyad009.
- Bygrave, L. A. (2022). Internet Governance by Contract. Oxford: Oxford University Press.

Sobre el marco ecuatoriano y latinoamericano:

- Acurio del Pino, S. (2016). Delitos Informáticos: Generalidades. Quito: Editora Jurídica del Ecuador.
- Páez Rivadeneira, J. J. (2025). Inteligencia Artificial Jurídica: de la Práctica a la Epistemología. Quito: Corporación de Estudios y Publicaciones (CEP).
- Páez Rivadeneira, J. J. (2026). Consultor de Protección de Datos. Quito: CETID (en prensa).
- Saín, G. (2015). Delito y nuevas tecnologías: Fraude, narcotráfico y lavado de dinero por Internet. Buenos Aires: Editores del Puerto.
- Cano Martínez, J. J. (2017). Inseguridad de la información: una visión estratégica. Bogotá: Alfaomega.

Referencias bibliográficas

Las referencias siguen el estilo de la American Psychological Association (APA), séptima edición.

Acurio del Pino, S. (2016). *Delitos informáticos: generalidades*. Quito: Editora Jurídica del Ecuador.

Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3.ª ed.). Indianapolis: Wiley.

Bamford, J. (2008). *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*. New York: Doubleday.

Brunnstein, K. (1990). Klassifikation und Beschreibung von Computer-Viren. *Datenschutz und Datensicherung*, *14*(2), 41-63.

Bygrave, L. A. (2022). *Internet governance by contract*. Oxford: Oxford University Press.

Cano Martínez, J. J. (2017). *Inseguridad de la información: una visión estratégica*. Bogotá: Alfaomega.

Castells, M. (2001). *La galaxia Internet: reflexiones sobre Internet, empresa y sociedad*. Madrid: Plaza & Janés.

Cohen, F. (1985). *Computer viruses* (Tesis doctoral). University of Southern California, Los Ángeles.

Cohen, F. (1987). Computer viruses: theory and experiments. *Computers & Security*, *6*(1), 22-35. https://doi.org/10.1016/0167-4048(87)90122-2

Copeland, B. J. (Ed.). (2006). *Colossus: the secrets of Bletchley Park's codebreaking computers*. Oxford: Oxford University Press.

Diffie, W. & Landau, S. (2007). *Privacy on the line: the politics of wiretapping and encryption* (ed. ampliada). Cambridge: MIT Press.

Eichin, M. W. & Rochlis, J. A. (1989). With microscope and tweezers: an analysis of the Internet virus of November 1988. *Proceedings of the IEEE Symposium on Security and Privacy*, 326-343.

Falliere, N., Murchu, L. O. & Chien, E. (2011). *W32.Stuxnet Dossier* (Versión 1.4). Cupertino: Symantec Security Response.

Hodges, A. (1983). *Alan Turing: the enigma*. London: Burnett Books.

Langner, R. (2013). *To kill a centrifuge: a technical analysis of what Stuxnet's creators tried to achieve*. Arlington: The Langner Group.

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies, 22*(3), 365-404.

Markopoulou, D., Papakonstantinou, V. & de Hert, P. (2019). The new EU cybersecurity framework: the NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review*, *35*(6), 1-11.

Ministerio de Telecomunicaciones y de la Sociedad de la Información [MINTEL]. (2021). *Plan Ecuador Digital 2021-2025*. Quito: MINTEL.

Páez Rivadeneira, J. J. (2025). *Inteligencia artificial jurídica: de la práctica a la epistemología*. Quito: Corporación de Estudios y Publicaciones (CEP).

Páez Rivadeneira, J. J. (2026). *Consultor de protección de datos*. Quito: Centro de Estudios Tecnológico en Informática y Derecho (CETID) [en prensa].

Saín, G. (2015). *Delito y nuevas tecnologías: fraude, narcotráfico y lavado de dinero por Internet*. Buenos Aires: Editores del Puerto.

Sanger, D. E. (2012). *Confront and conceal: Obama's secret wars and surprising use of American power*. New York: Crown Publishers.

Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations* (2.ª ed.). Cambridge: Cambridge University Press.

Schmitz-Berndt, S. (2023). Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. *Journal of Cybersecurity*, *9*(1), tyad009.

Singh, S. (1999). *The code book: the secret history of codes and code-breaking*. London: Fourth Estate.

Solove, D. J. (2008). *Understanding privacy*. Cambridge: Harvard University Press.

Spafford, E. (1989). *The Internet worm program: an analysis* (Purdue Technical Report CSD-TR-823). West Lafayette: Purdue University.

Téllez Valdés, J. (2008). *Derecho informático* (4.ª ed.). México: McGraw-Hill.

Welchman, G. (1982). *The Hut Six story: breaking the Enigma codes*. New York: McGraw-Hill.

West-Brown, M., Stikvoort, D., Kossakowski, K. P., Killcrece, G., Ruefle, R. & Zajicek, M. (2003). *Handbook for computer security incident response teams (CSIRTs)* (2.ª ed.). Pittsburgh: Software Engineering Institute, Carnegie Mellon University.

Zetter, K. (2014). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. New York: Crown Publishers.

FIN DEL CAPÍTULO 1