Artículos de reflexión

El fenómeno de la interconectividad y la ciberseguridad: una introducción al objeto del derecho de la ciberseguridad[1]

The Interconnectivity Phenomena and Cybersecurity: an introduction to the object of study of Cybersecurity Law

Rodolfo Núñez Robinson [2]
Universidad Católica del Perú, Perú
legal@daegis.info

Análisis Jurídico – Político
vol. 7, núm. 13, p. 15 - 43, 2025
Universidad Nacional Abierta y a Distancia, Colombia
ISSN: 2665-5470
ISSN-E: 2665-5489
Periodicidad: Semestral
revista.analisisjuridico@unad.edu.co

Recepción: 01 agosto 2024
Aprobación: 14 octubre 2024

DOI: https://doi.org/0.22490/26655489.8268

URL: https://portal.amelica.org/ameli/journal/702/7025402001/

Resumen: No cabe duda de que el fenómeno de la interconectividad es sumamente útil: nos permite alcanzar nuestros objetivos y acceder a información de manera inmediata. Sin embargo, estamos poco conscientes del alto costo que conlleva, debido a las brechas y vulnerabilidades generadas por el crecimiento exponencial de las tecnologías digitales y su desarrollo, lo que amplía cada vez más el catálogo de activos susceptibles a ciberataques. La interconectividad es una realidad imparable, por lo que resulta imprescindible aprender a gestionar los riesgos cibernéticos desde una perspectiva técnica y con un enfoque interdisciplinario que nos permita comprender el objeto de estudio del Derecho de la Ciberseguridad. Con este propósito, en el presente trabajo se explicarán los riesgos y amenazas cibernéticas, así como la evolución internacional —tanto en normas internacionales, comunitarias, técnicas y de estandarización— de esta emergente rama jurídica. Posteriormente, se abordará el término ciberseguridad desde diversas perspectivas jurídicas en los países líderes en la materia, y se establecerán los principios y usos comerciales que deben respetarse al analizarla

Notas de autor

2 Abogado y especialista en Derecho Procesal (Programa de Segunda Especialidad) por la Pontificia Universidad Católica del Perú. Asimismo, se ha especializado en Gestión de Riesgos de Ciberseguridad por la Universidad de Harvard. Es socio cofundador de la Consultora Delta Aegis, especializada en Derecho y Ciberseguridad. Maestrando en el LLM de Ciberseguridad, Ciberterrorismo y Derecho Internacional por la Universidad de la Paz de las Naciones Unidad y el Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia. Sus intereses investigativos se centran en Derecho Procesal (arbitraje, proceso civil y prueba) así como Derecho Procesal Constitucional y Ciberseguridad. Ha escrito más de una decena de artículos publicados en revistas especializadas y libros. También es conferencista nacional e internacional en universidades y foros académicos de alto nivel. Correo electrónico legal@daegis.info ORCID: 0009-0006-6533-9832.

jurídicamente (*lex artis*), lo cual servirá como parámetro de control al examinar este tipo de casos.

Palabras clave: amenazas cibernéticas, cibercrímenes, ciberseguridad, gestión de riesgos, riesgos cibernéticos.

Abstract: There is no doubt that the interconnectivity phenomenon is extremely useful: it allows us to achieve our objectives and access information immediately. However, we are poorly aware of the high cost it entails, due to the breaches and vulnerabilities generated by the exponential growth of digital technologies and their development, which increasingly broadens the catalogue of assets susceptible to cyber-attacks. Interconnectivity is an unstoppable reality, making it essential to learn how to manage cyber risks from a technical perspective and with an interdisciplinary approach that allows us to understand the object of study of Cybersecurity Law. With this purpose in mind, this paper will explain cyber risks and threats, as well as the international evolution of this emerging branch of law, in terms of international, communitarian, technical and standardisation norms. Subsequently, the term cybersecurity will be addressed from different legal perspectives in the leading countries in the field, and the principles and commercial uses that must be complied with when analysing it legally (lex artis) will be established, which will serve as a control parameter when examining this type of case.

Keywords: cybercrimes, cybersecurity, cyber threats, cyber risks, risk management.

1. Introducción: la interconectividad y los riesgos asociados

La interconectividad es la capacidad de estar en un estado permanente de conexión con el internet y con otros usuarios; permite alcanzar objetivos y acceder a la información de manera inmediata. En solo treinta años, hemos pasado de dedicar horas a buscar en una enciclopedia sobre, por ejemplo, monstruos marinos —un tema que de niño me encantaba investigar— a simplemente escribir el término en un buscador y tener acceso a documentales, videos e incluso transmisiones en vivo de submarinos explorando las profundidades del océano.

De hecho, es útil hacer una pausa para reflexionar sobre el impacto de la interconectividad y el internet en la vida diaria.

Probablemente todos tengamos un celular que permite comunicarnos con otras personas. Sin embargo, la tecnología actual convierte estos dispositivos en sucedáneos de computadoras que están siempre conectados a internet, con todos nuestros datos, incluyendo la ubicación. El internet está en todas partes, y a veces ni siquiera nos damos cuenta: ya sea en unos audífonos, un reloj, un computador portátil, el rastreador de nuestros animales, una máquina de resonancia magnética, nuestra Smart house, los sistemas industriales de control (SCADA), un misil, los controles de un avión, nuestros automóviles o los sistemas de defensa nacional. Todo está conectado a internet y, por lo tanto, es un potencial objetivo para un ciberataque.

No hay duda de la infinita utilidad de la interconectividad, pero se está soslayando el altísimo costo que conlleva, debido a las brechas generadas por el crecimiento exponencial de las tecnologías digitales y su desarrollo. De hecho, se ha configurado un panorama diverso de riesgos y amenazas cibernéticas[3], situación que se agrava notablemente por la falta de sistemas de ciberseguridad y, lo que es peor, por la escasa sensibilización hacia la cultura de ciberseguridad tanto en las personas como en las organizaciones, especialmente en sus líderes.

Esto es conocido como la superficie de ataque[4], definida como la suma de los diferentes puntos de acceso (vectores de ataque) por donde un atacante puede intentar penetrar un sistema y extraer información (United States Government Accountability Office, 2024, p. 18). Lo curioso —o alarmante, para ser más exactos— es que, dado que ahora todo está interconectado a través de internet, la superficie de ataque se ha vuelto global: cualquier persona puede llevar a cabo un ciberataque sobre cualquier dispositivo desde cualquier parte del mundo, atacando la información disponible o

cualquier otro objetivo de interés para el ciberdelincuente, cuyas motivaciones varían dependiendo del actor.

Este crecimiento exponencial de la superficie de ataque se ha denominado superficie de ataque global[5]. Al respecto, Douglas y Richard (2016) destacan la peligrosidad de esta preocupante tendencia, señalando que la superficie de ataque global está compuesta por el conjunto total de todas las vulnerabilidades en la ciberseguridad a lo largo de todos los sistemas, redes y organizaciones. En otras palabras, se trata de un fenómeno macro que está en constante expansión y representa una nueva realidad que ha llegado para quedarse (p. 10).

Ante esta situación, surge la pregunta: ¿qué se debe hacer? Primero, desde una óptica técnica, es necesario comenzar a identificar y comprender las amenazas cibernéticas. Estas se componen de todo aquello que puede causar daños o pérdidas a una persona (natural o jurídica), aprovechando las vulnerabilidades de los sistemas de información o las medidas de ciberseguridad de una organización. Para efectos de este trabajo, se identifican cuatro tipos de amenazas cibernéticas:

- Amenazas externas impremeditadas: son aquellas que ocurren accidentalmente —ya sea por impericia, negligencia o simple descuido— en la relación de la organización con agentes externos, como terceros, socios comerciales, exempleados, entre otros, que en el lenguaje técnico se conocen como third-party vendors (TPV). Aunque no existe la intención de causar daño, este igual se produce y persiste.

- Amenazas externas premeditadas: son actos dolosos perpetrados por agentes externos con la intención de obtener accesos no autorizados a los sistemas de información críticos de una organización con fines ilícitos, para provecho personal y/o ideológico. Pueden involucrar a un TPV, a un exempleado insatisfecho u otros agentes criminales.

- Amenazas internas premeditadas: son actos dolosos cometidos por personas internas a la organización, con la intención de acceder de manera no autorizada a los sistemas de información —críticos o no— con fines ilícitos, buscando provecho personal y/o ideológico.

- Amenazas internas impremeditadas: son actos accidentales realizados por personas internas a la organización que pueden afectar negativamente a los sistemas, redes o datos, como

consecuencia de negligencias, impericias o errores humanos. Aunque no exista intención de causar daño, este igualmente se produce y persiste.

Las amenazas cibernéticas deben analizarse junto con los riesgos cibernéticos para realizar un análisis integral de las vulnerabilidades que son aprovechadas por los cibercriminales, quienes las explotan con el objetivo de obtener un provecho ilícito.

A diferencia de las amenazas cibernéticas, los riesgos cibernéticos son aquellos daños, pérdidas o disrupciones en las operaciones comerciales generadas por el uso de sistemas de tecnologías de la información. Estos riesgos se dividen en tres grupos principales, que a menudo son pasados por alto por las gerencias empresariales al realizar un estudio de contingencias (Falco y Rosenbach, 2022, p. 6):

- Riesgos operacionales empresariales: potenciales pérdidas directas o indirectas causadas por el personal o por el colapso (downtime) de sistemas empresariales clave, procesos y/o procedimientos.

- Riesgo reputacional: potenciales pérdidas o daños causados a la reputación o imagen pública de una organización o persona.

- Riesgos legales y de cumplimiento: potenciales pérdidas o daños derivados de acciones legales en contra de una empresa o persona por haber infringido alguna ley o marco normativo —ya sea por usuarios o entidades reguladoras—, así como responsabilidad civil, administrativa y/o penal.

Resulta alarmante que, en varios países del mundo, se reste importancia —o se ignore por completo— la gestión de riesgos cibernéticos[6], lo cual impide mitigar los potenciales daños catastróficos de los ciberataques en empresas y personas. Esto, a pesar de ser, en gran parte del mundo, una necesidad empresarial crítica que permite a los negocios y a los Estados operar con seguridad y continuidad.

Ni los riesgos ni las amenazas cibernéticas deben tomarse a la ligera debido al potencial daño catastrófico que pueden causar. Algunos ejemplos lo ilustran: ¿sabían que un ciberataque puede matar a una persona? Aunque parezca extraño que un ataque a un sistema informático pueda causar daños físicos, sucede más a menudo de lo que se piensa. En julio de 2019, en Mobile, Alabama, la clínica Springhill Medical Center fue objeto de un ataque de ransomware.

El ransomware, según el National Institute of Standards and Technology (NIST), es un tipo de malware que ataca la información

de una organización o persona y la encripta. Si se desea volver a acceder a dicha información, es necesario pagar un rescate (ransom), de lo contrario, la información se perderá para siempre o será vendida en la Deep Web al mejor postor. De acuerdo con otra definición (Falco y Rosenbach, 2022, p. 23), el ransomware es un tipo de malware que bloquea el acceso a un sistema o amenaza con divulgar información sensible a menos que se realice el pago de un rescate.

En este caso, un bebé llamado Nicko Silar nació justo cuando el Springhill Medical Center fue atacado por un ransomware. Debido a que los sistemas de la clínica estaban caídos por el ciberataque, el personal médico no pudo acceder a la historia clínica de la madre ni monitorear los signos vitales de ella y del bebé. Como resultado, no pudieron detectar que el cordón umbilical estaba ahorcando a Nicko. Aunque nació, el daño causado por la sofocación resultó en un daño cerebral irreparable, que le costó la vida nueve meses después. Todo esto fue consecuencia de un ataque a un sistema informático médico.

Otro caso ocurrió en Düsseldorf, Alemania, en septiembre de 2020. El Hospital de la Universidad de Düsseldorf fue atacado por un ransomware, lo que hizo que los sistemas del hospital dejaran de funcionar, incluyendo el sistema encargado de admitir pacientes en emergencias. Lamentablemente, durante ese ataque, una mujer de 78 años, afectada por un aneurisma aórtico, sufrió un deterioro de salud que motivó su traslado de emergencia para recibir atención médica urgente.

El centro médico más cercano era el Hospital de la Universidad de Düsseldorf. Sin embargo, al informar sobre la llegada de esta paciente, no pudieron admitirla debido al ciberataque —se informó que no estaban atendiendo emergencias—, por lo que se rechazó su ingreso y se redirigió la ambulancia al Hospital Universitario Helios de Wuppertal, a 32 kilómetros de distancia, lo que retrasó una hora el tratamiento de la paciente. Lamentablemente, murió poco después.

A nivel global, también se puede observar cómo una falla tecnológica puede afectar al mundo entero. En julio de 2024, ocurrió un problema en el software de CrowdStrike que generó una falla crítica en todos los sistemas operativos Windows. Como consecuencia, casi todas las aerolíneas a nivel mundial que operaban con Windows, los aeropuertos, las clínicas y, en general, todas las organizaciones que utilizan dicho sistema operativo no pudieron realizar sus operaciones empresariales (de hecho, 8.5 millones de dispositivos quedaron paralizados). Este evento causó daños inconmensurables, siendo que, por ejemplo, Delta Air Lines estimó una pérdida económica de USD 500 millones. En total, se calcula que los daños globales ascienden a 5.4 billones de dólares. Todo esto a raíz de una falla técnica en una actualización.

¿Cuál se considera una de las principales causas de estos eventos? Las antiguas y soberanas generaciones que ocupan los altos cargos gerenciales de las empresas, quienes no creen en las ventajas de la tecnología y dan la espalda a los potenciales riesgos catastróficos de un ciberataque en su organización. Además, prevalece una falsa sensación de seguridad, creyendo que nunca ocurrirá nada, pero cuando ocurre, ya es demasiado tarde para comenzar a adoptar medidas contra el ataque.

Precisamente, esta falta de previsión y sensibilización frente a la ciberseguridad, que proviene desde un plano vertical (buy-in), impide que las empresas adopten una cultura de prevención en sus actividades diarias. No existe un convencimiento por parte de sus líderes que sea transmitido a la cultura organizacional y a sus empleados, con el objetivo de mitigar y/o evitar potenciales daños.

Esta preocupante resistencia hacia la ciberseguridad crea un ambiente altamente atractivo para los cibercriminales, quienes aprovechan las falencias de seguridad —sean físicas, digitales, lógicas y/o administrativas— para penetrar los sistemas y llevar a cabo actos delictivos, motivados por sus ideologías y/o intereses. Estos actos pueden incluir el robo de información para su venta, la ejecución de un ataque DDoS[7] para bloquear el acceso a un sistema, la publicación de un mensaje político en la red social de una entidad del Estado con la que se está en desacuerdo, el robo de secretos de Estado para ser vendidos a un país rival o, incluso, el ataque a sistemas críticos[8] para provocar un apagón en un país entero como parte del cyberwarfare.

Como se ha podido apreciar hasta este punto, la ciberseguridad es una necesidad imprescindible en el día a día. Por ello, es importante comprender y difundir la noción de esta incipiente rama jurídica que, por su naturaleza, se basa principalmente en soft law[9], ya que no existe una legislación específica en cada país que regule completamente esta materia debido a su alta tecnicidad. Para entenderlo mejor, es necesario comprender qué es la ciberseguridad.

2. Metodología o pauta de análisis

El presente trabajo tiene como finalidad plasmar y analizar el estado del arte del objeto de estudio del Derecho de la Ciberseguridad. Para ello, primero se definirá el objeto de estudio, partiendo de la premisa de que este es la ciberseguridad —como podría parecer obvio—, aunque luego se demostrará que dicha afirmación es extremadamente compleja debido al alcance inconmensurable de este campo.

Esto se demostrará mediante una revisión bibliográfica exhaustiva, seleccionando fuentes relevantes como artículos académicos, libros, informes y documentos técnicos y estandarizados que sirven como referencia a nivel mundial. Posteriormente, se sintetiza y compara la información obtenida, identificando tendencias y patrones comunes, con el fin de comprender, de la mejor manera, el estado del arte de este estudio.

3. ¿Qué es la ciberseguridad?: regulación internacional

La ciberseguridad cuenta con un sinfín de definiciones y un contenido sumamente extenso y altamente técnico. Para efectos de este trabajo, es útil conocer las diferentes maneras en que se entiende y sus principios elementales, con el fin de establecer los estándares a considerar al analizar casos desde una perspectiva jurídica.

3.1. Antecedente internacional: el Convenio sobre la Ciberdelincuencia de 2001

Una de las normas más antiguas y relevantes sobre ciberseguridad, cuyo objetivo principal fue armonizar el Derecho de la Ciberseguridad desde una perspectiva penal —mucho antes de abordar este tema desde una óptica regulatoria o civil—, es el Convenio de Budapest sobre la Ciberdelincuencia, promovido por el Consejo de Europa y firmado el 23 de noviembre de 2001.

Esta norma internacional sentó las bases para el tratamiento de los crímenes cibernéticos, destacándose la visión, hace más de 23 años, de los 31 países firmantes en ese momento, tal como se señala en el preámbulo del mencionado tratado:

> Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional;
>
> Conscientes de los profundos cambios provocados por la digitalización, la convergencia y la globalización continuas de las redes informáticas;
>
> Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes;
>
> [...] Convencidos de que el presente Convenio es necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de

> dichos actos, tal como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar eficazmente contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable. (Consejo Europeo, 2001, p. 2)

El Convenio de Budapest tuvo un profundo impacto en el mundo, especialmente en los países que lo suscribieron y en aquellos que se han ido adhiriendo —a febrero de 2024, cuenta con 93 Estados, entre partes y observadores—. De hecho, según el Consejo de Europa, este convenio ha servido como directriz y/o ley modelo para que otros países desarrollen su normativa interna en relación con la ciberdelincuencia (Consejo de Europa, 2024, p. 2), la cual forma parte integral de la ciberseguridad.

De acuerdo con el propio Consejo de Europa, el 13 de julio de 2020 se realizó un estudio integral sobre los beneficios e impactos del Convenio de Budapest en los países miembros, concluyendo empíricamente que este sirve como marco legal para la cooperación internacional, no solo en relación con la ciberdelincuencia, sino también con cualquier delito que implique pruebas electrónicas. Para llegar a esta conclusión, el informe cita varios casos de Estados que armonizaron su legislación interna con el Convenio de Budapest, con el fin de proteger a sus ciudadanos de los cibercrímenes (Consejo de Europa, 2024, pp. 6-8). A continuación, se presentan algunos casos:

- República de Cabo Verde: en 2017 se aprobó la Ley n.° 8/IX/2017 en la que se establece, entre otras disposiciones, normas penales materiales y procesales respecto a los crímenes cibernéticos a la luz de su Estrategia Nacional en Ciberseguridad.

- Croacia: en 2013 implementaron una reforma integral a su Código Penal y Procesal Penal para armonizarse con el Convenio de Budapest.

- República Dominicana: aprobó la Ley n.° 53-07, Ley de Crímenes y Delitos de Alta Tecnología, junto con otras reformas a sus normas penales en consonancia con el Convenio de Budapest.

- Finlandia: modificó su Código Penal para implementar las obligaciones contenidas en el Convenio de Budapest.

- Francia: modificó su legislación para adaptarse a la evolución de los cibercrímenes con la Ley n.° 2004-575, Ley de Confianza en la Economía Digital.

- Alemania: modificó su Código Penal en 2009, con el fin de incorporar todas las disposiciones sustantivas (delitos cibernéticos) previstas en el Convenio de Budapest; siendo esta misma reforma legislativa replicada en su Código Procesal Penal.

- Portugal: empleó el Convenio de Budapest como ley modelo para aprobar la Ley n.° 109/2009, Ley de Cibercrímenes.

Es cierto que el Convenio de Budapest no definió la ciberseguridad, pero su importancia radica en la regulación de los delitos cibernéticos que, como se verá más adelante, contienen en sus tipologías elementos que conforman el concepto de ciberseguridad desde una perspectiva principalista.

Para ello, es necesario delimitar las disposiciones sustantivas penales del Convenio de Budapest[10], con el fin de realzar las características de los delitos cibernéticos sancionados, los cuales, como veremos, son similares a las definiciones actuales de ciberseguridad. A continuación, haremos un resumen de cada tipo penal para destacar los elementos de hecho relacionados con la ciberseguridad:

- Artículo 2 – Acceso ilícito: el acceso deliberado e ilegítimo a todo o parte de un sistema informático infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

- Artículo 3 – Interceptación ilícita: la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo. En este, se incluyen las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos.

- Artículo 4 – Ataques a la integridad de los datos: todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos, independientemente de la magnitud y extensión del daño.

- Artículo 5 – Ataques a la integridad del sistema: la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la

introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

- Artículo 6 – Abuso de los dispositivos: la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: i) cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos antes mencionados; y/o, ii) contraseñas, códigos de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático con la intención de que sean utilizados para cometer cualquiera de los delitos antes mencionados.

- Artículo 7 – Falsificación informática: la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente.

- Artículo 8 – Fraude informático: actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: i) la introducción, alteración, borrado o supresión de datos informáticos; y/o, ii) cualquier interferencia en el funcionamiento de un sistema informático con la intención de obtener ilegítimamente un beneficio económico para uno mismo o para un tercero.

- Artículo 10 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines: las infracciones de la propiedad intelectual de conformidad con las obligaciones que haya contraído en aplicación del Acta de París de 24 de julio de 1971, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

Del mismo modo, se considera como delito las infracciones de los derechos de conformidad con las obligaciones que asumidas en aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas cuando tales actos se

cometan deliberadamente, a escala comercial y por medio de un sistema informático.

Claramente, como una norma comunitaria de alcance casi global, los parámetros regulados en las disposiciones sustantivas penales del Convenio de Budapest pueden ser considerados estándares internacionales de protección cibernética, mutatis mutandis, con las reservas y declaraciones de cada país. No obstante, en este punto, es importante destacar una serie de elementos comunes en las conductas ilícitas tipificadas que hemos resumido precedentemente.

Aunque la conexión será más evidente en la sección siguiente, se puede adelantar que el impacto e influencia de este instrumento internacional en la ciberseguridad es notable, ya que, de los elementos comprendidos en dichos delitos, se aprecia que se reprocha cualquier acto que, mediante un sistema digital:

- Infrinja, penetre y/o viole medidas de seguridad digital con la obtención de obtener datos comprendidos dentro de un sistema informático, se encuentre o no interconectado con otros sistemas [confidencialidad].

- Intercepte datos informáticos en transmisiones no públicas, sean internas o externas [*confidencialidad*].

- Dañe, de cualquier manera, datos informáticos [*integridad*].

- Obstaculice (disrupción) un sistema mediante la alteración de datos informáticos [*integridad y disponibilidad*].

- Se emplee para cometer un delito o acceder a bases de datos ilícitamente [*confidencialidad e integridad*].

- Manipule y/o adultere de cualquier manera datos informáticos sin autorización, tengan o no relación con derechos de propiedad intelectual [integridad].

Al final de cada viñeta, se han introducido una o dos palabras: confidencialidad, integridad y/o disponibilidad. Esto se debe a que los delitos cibernéticos atacan, necesariamente, alguno de los tres elementos fundamentales y básicos de la ciberseguridad, conocidos como la *CIA Triad o Tríada CID* en español.

3.2. La CIA Triad

De acuerdo con Falco y Rosenbach, este es un estándar técnico aplicado en todo el mundo, que busca garantizar, como mínimo, tres principios fundamentales en la seguridad de la información (2022, pp.

44-46). Estos principios, como se podrá apreciar, también se presentan como bienes jurídicos protegidos en normativas internas de protección de datos personales, por ejemplo:

- Confidencialidad (*confidentiality*): se refiere a la prevención del acceso no autorizado a información privada y/o sensible. Como se mencionó anteriormente, el acceso puede ser premeditado —como cuando un agente, interno o externo, ingresa sin autorización a los sistemas y accede a la información de manera intencional o dolosa—, o impremeditado —cuando un agente, interno o externo, debido a descuido, impericia o negligencia, genera una vulnerabilidad o filtra información—. En pocas palabras, la confidencialidad busca mantener la información privada y/o sensible fuera del alcance de personas no autorizadas.

- Integridad (*integrity*): hace referencia a la consistencia de los sistemas, redes y datos, asegurando que no sufran alteraciones no autorizadas o no intencionadas. Esto garantiza que los sistemas, redes y datos funcionen según lo previsto cuando un usuario autorizado accede a ellos, evitando que se borren o modifiquen de manera indebida. Lo esencial es que la información se mantenga tal como la organización la necesita (sin adiciones ni eliminaciones no autorizadas), evitando modificaciones o supresiones no autorizadas.

- Disponibilidad (*availability*): la disponibilidad se refiere a la capacidad de los usuarios autorizados para acceder a sus sistemas, redes o datos cuando lo necesiten. Es decir, garantiza el acceso inmediato a los recursos cuando sea necesario para los fines correspondientes.

A pesar de ser un estándar técnico, los elementos de esta tríada están legislados en algunos países. Por ejemplo, en los Estados Unidos se cuenta con el Federal Information Security Modernization Act (FISMA), que regula estos principios bajo el concepto de information security (seguridad de la información):

> El término 'seguridad de la información' significa proteger la información y los sistemas de información contra el acceso, uso, difusión, disrupción, modificación o destrucción no autorizados, con el fin de garantizar:
>
> (A) la integridad, que significa la protección contra la modificación o destrucción indebidas de la información, incluida la no repudiación y la autenticidad de la información;

> (B) la confidencialidad, que significa preservar las restricciones autorizadas de acceso y difusión, incluidos los medios para proteger la privacidad personal y la información sujeta a derechos de propiedad; y
>
> (C) la disponibilidad, que significa garantizar el acceso oportuno y fiable a la información y su uso[11] (p. 128)

Con base en lo expuesto, es importante tener presente que la Tríada CID sirve como un parámetro de control mínimo y un estándar universalmente aceptado para determinar los niveles de ciberseguridad. Constituye el derrotero indiscutible que debe seguirse siempre al estudiar, analizar e implementar una política elemental de protección de sistemas informáticos o, en general, de nuestro entorno digital (pues, al fin y al cabo, todo es información).

Además, no debemos perder de vista que cada ciberataque infringirá alguno de estos principios, ya que, sea como causa o consecuencia, no puede haber un ataque si el ciberdelincuente no vulnera algún elemento de la tríada (dependiendo de la intención y el tipo de ataque). Estos elementos deben estar siempre presentes como mínimo en todo análisis de gestión de riesgos en el ciberespacio.

4. Estado del arte: las fuentes normativas internacionales y estándares técnicos del derecho de la ciberseguridad (y de la ciberseguridad)

Es necesario iniciar este acápite destacando el notable caso de los Estados Unidos de América. Este país, a través de su 107.º Congreso, aprobó el 27 de noviembre de 2002 la Public Law 107-305: Cyber Security Research and Development Act. Aunque esta norma no define la ciberseguridad, declara con contundencia que, desde 1997, Estados Unidos ya estaba evaluando internamente su defensa cibernética, tal como se establece en su parte considerativa (findings). En este sentido, el Congreso considera lo siguiente:

> (1) Los revolucionarios avances en la tecnología de la computación y las comunicaciones han interconectado las infraestructuras gubernamentales, comerciales, científicas y educativas —incluidas las infraestructuras críticas para la energía eléctrica, la producción y distribución de gas natural y petróleo, las telecomunicaciones, el transporte, el suministro de agua, la banca y las finanzas, y los servicios de emergencia y gubernamentales— en una vasta red interdependiente física y electrónica.
>
> (2) El aumento exponencial de la interconectividad ha facilitado la mejora de las comunicaciones, el crecimiento económico y la prestación de servicios críticos para el bienestar público, pero también ha incrementado las consecuencias de un fallo temporal o prolongado.

> (3) Un Grupo de Trabajo Conjunto del Departamento de Defensa concluyó, tras un ejercicio de guerra de la información realizado por Estados Unidos en 1997, que los resultados "demostraban claramente nuestra falta de preparación para un ataque cibernético y físico coordinado contra nuestras infraestructuras militares y civiles críticas[12] .(p. 116, el destacado es del autor).

Esta norma, además de evidenciar el trabajo interno realizado para asegurar la seguridad nacional en todos los ámbitos (incluida la ciberseguridad, que, si hoy en día es algo novedoso, imagínense en 1997), crea fondos para otorgar financiamiento y becas a personas que realicen investigaciones en ciberseguridad, incluyendo el financiamiento del National Institute of Standards and Technology (NIST), que es, indiscutiblemente, la agencia más importante en materia de tecnología y ciberseguridad en el mundo.

Entonces, ¿qué es la ciberseguridad? Comencemos citando un documento parcialmente desclasificado el 9 de noviembre de 2014[13], emitido por la Casa Blanca el 8 de enero de 2008, titulado Cybersecurity Policy (U), contenido en la National Security Presidential Directive/NSPD-54 y la Homeland Security Presidential Directive/HSPD-23. Esta directiva establece la política, estrategia, lineamientos e implementación de acciones para asegurar el ciberespacio en Estados Unidos, donde se define la ciberseguridad de la siguiente manera:

> Ciberseguridad significa prevención de daños, protección y restauración de computadoras, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas, comunicaciones por cable y comunicaciones electrónicas, incluida la información contenida en ellos, para garantizar su disponibilidad, integridad, autenticación, confidencialidad y no-repudio[14]. (p. 3)

De acuerdo con esta definición, la ciberseguridad tiene un propósito no solo preventivo, sino también reactivo, abarcando una serie de elementos tecnológicos, como las computadoras, los sistemas y servicios de telecomunicaciones y, en general, todo tipo de comunicaciones electrónicas. Asimismo, se incluye en el ámbito de protección el hecho de que estas herramientas contienen y distribuyen información, por lo que se debe garantizar su disponibilidad, integridad, autenticación, confidencialidad y no repudio.

Esta misma definición ha sido adoptada por el Committee on National Security Systems (CNSS) en el documento técnico CNSSI n.° 4009, del 6 de abril de 2015 y replicada en el documento actualizado en marzo de 2022. Dicho documento, denominado Committee on National Security Systems (CNSS) Glossary, ha

servido como base para el NIST y está avalado directamente por el Cyber Security Research and Development Act.

De acuerdo con una de las definiciones del NIST, la ciberseguridad puede definirse sencillamente como la habilidad de proteger o defender el uso del ciberespacio de un ciberataque[15]. Esta definición, aunque es homogénea en otros documentos técnicos como el NIST SP 800-39 de marzo de 2011 y el NIST SP 800-30 de septiembre de 2012 —y es la más conocida y empleada—, no es la única que maneja este instituto. Además de la definición mencionada, el NIST tiene cinco otras definiciones de ciberseguridad para tener en cuenta:

> Prevención de daños, protección y restauración de ordenadores, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas, comunicaciones por cable y comunicaciones electrónicas, incluida la información contenida en ellos, para garantizar su disponibilidad, integridad, autenticación, confidencialidad y no repudio[16]. (contenida en los documentos CNSSI 4009-2015, NIST SP 1800-10B, NIST SP 1800-25B , NIST SP 1800-26B, NIST SP 800-160 Vol. 2 Rev. 1, NIST SP 800-37 Rev. 2, NIST SP 800-53 Rev. 5, NIST IR 8401 y NIST IR 7621 Rev. 1).
>
> Prevención de daños, protección y restauración de ordenadores, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas, comunicaciones por cable y comunicaciones electrónicas, incluida la información contenida en ellos, para garantizar su disponibilidad, integridad, autenticación, confidencialidad y no repudio[16]. (contenida en los documentos CNSSI 4009-2015, NIST SP 1800-10B, NIST SP 1800-25B , NIST SP 1800-26B, NIST SP 800-160 Vol. 2 Rev. 1, NIST SP 800-37 Rev. 2, NIST SP 800-53 Rev. 5, NIST IR 8401 y NIST IR 7621 Rev. 1).
>
> El proceso de proteger la información mediante la prevención, detección y respuesta a los ataques[17]. (Contenida en los documentos NIST SP 800-160 Vol. 2 Rev. 1, NIST Cybersecurity Framework Version 1.1, NIST IR 8183, NIST IR 8183 Rev. 1, NIST IR 8183A Vol. 1, NIST IR 8183A Vol. 2, NIST IR 8183A Vol. 3).
>
> Medidas y controles que garantizan la confidencialidad, integridad y disponibilidad de la información procesada y almacenada por una computadora.[18] (Contenida en el documento CNSSI 4009-2015).
>
> [...] La prevención de daños, el uso no autorizado, la explotación y, en caso de que fuese necesario, el restablecimiento de los sistemas electrónicos de información y comunicaciones, así como de la información que contienen; con el fin de reforzar la confidencialidad, integridad y disponibilidad de dichos sistemas.[19] (Contenido en el documento NIST IR 8074 Vol. 2).
>
> "Prevención de daños, protección y restauración de computadoras, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas, comunicaciones por cable y comunicaciones electrónicas, incluida la

> información que contienen, para garantizar su disponibilidad, integridad, autenticación, confidencialidad y no repudio."[20]
>
> (Contenido en el documento NIST IR 8323r1).

Todas estas definiciones son aceptadas globalmente en los países donde rigen los más altos estándares internacionales, dependiendo del tema técnico específico y del enfoque que se le quiera dar a la ciberseguridad. Por ejemplo, para la Cybersecurity & Infrastructure Security Agency (CISA), la agencia de ciberdefensa de los Estados Unidos, la ciberseguridad se define como: "[...] el arte de proteger redes, dispositivos y datos de accesos no autorizados o usos delictivos y la práctica de garantizar la confidencialidad, integridad y disponibilidad de la información"[21] (2021).

Por su parte, el Subcommittee SC 27, Information security, cybersecurity and privacy protection del Joint Technical Committee 1 del International Organization for Standardization (ISO) y la International Electrotechnical Commission (IEC) definen la ciberseguridad en la sección 3.6 del documento técnico ISO/IEC 27032:2023[22], publicado en junio de 2023, como: "*salvaguardar a las personas, la sociedad, las organizaciones y las naciones frente a los ciber riesgos*"[23]; entendiendo por "*salvaguardar*", según dicha entidad, "*mantener los ciber riesgos a un nivel tolerable*"[24] (2023).

Hasta este punto, solo en Estados Unidos, se puede apreciar cómo se va configurando el estándar técnico de lo que constituye la ciberseguridad y la lex artis. Sin embargo, otro lugar geográfico que debe considerarse al estudiar esta materia es la Unión Europea.

Para esta comunidad internacional, la ciberseguridad se define de manera sencilla en la Regulación (UE) 2019/881 del Parlamento y del Consejo Europeo, del 17 de abril de 2019, que crea la European Union Agency for Cybersecurity (ENISA)[25]: "'*ciberseguridad*' *significa las actividades necesarias para proteger las redes y los sistemas de información, a los usuarios de dichos sistemas y a otras personas afectadas por las ciberamenazas*"[26].

Esta definición es empleada en toda la Unión Europea y fue adoptada por la Directiva (UE) 2022/2555 del Parlamento y del Consejo Europeo, del 14 de diciembre de 2022, que regula un alto nivel común de ciberseguridad en toda la Unión, entre otros aspectos.

Entidades europeas, como el Telecommunication Standardization Sector de la International Telecommunication Union (ITU-T), en el documento denominado Series X: Data Networks, Open System Communications and Security de abril de 2008 (X.1205), definen la ciberseguridad de la siguiente manera:

> La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardias de seguridad, directrices, enfoques de gestión de riesgos, estrategias, formación, buenas prácticas, garantías y tecnologías que pueden utilizarse para proteger el entorno cibernético y los activos de las organizaciones y los usuarios. Los activos de la organización y del usuario incluyen los dispositivos informáticos conectados, el personal, la infraestructura, las aplicaciones, los servicios, los sistemas de telecomunicaciones y la totalidad de la información transmitida y/o almacenada en el entorno cibernético. La ciberseguridad tiene como objetivo garantizar la consecución y el mantenimiento de las condiciones de seguridad de los activos de la organización y del usuario frente a los riesgos de seguridad relevantes en el ciber entorno. Los objetivos generales de seguridad comprenden los siguientes:
>
> - Disponibilidad
> - Integridad, que puede incluir autenticidad y no repudio
> - Confidencialidad.[27] (p. 2)

Cabe precisar que, para la ITU-T, el ciber entorno o entorno cibernético (cyber environment) "incluye usuarios, redes, dispositivos, todo tipo de software, procesos, información almacenada o en tránsito, aplicaciones, servicios y sistemas que puedan conectarse directa o indirectamente a las redes"[28] (2008, p. 2).

Por su parte, hay que destacar que la propia ENISA define la ciberseguridad en el documento titulado Definition of Cybersecurity – Gaps and overlaps in standarisation, publicado en diciembre de 2015, de la siguiente manera:

> La ciberseguridad se referirá a la seguridad del ciberespacio, entendiendo por ciberespacio el conjunto de enlaces y relaciones entre objetos accesibles a través de una red generalizada de telecomunicaciones, y al conjunto de objetos en sí mismos cuando presenten interfaces que permitan su control remoto, el acceso remoto a datos, o su participación en acciones de control dentro de dicho ciberespacio. La ciberseguridad deberá, por tanto, comprender el paradigma CIA para las relaciones y objetos dentro del ciberespacio y extender ese mismo paradigma CIA para abordar la protección de la privacidad de las personas jurídicas (personas y empresas), y para abordar la resiliencia (recuperación ante un ataque)[29]. (p. 7)

Si bien la ENISA adopta dicha definición, es fundamental destacar que reconoce que el Derecho de la Ciberseguridad abarca un concepto tan amplio que actualmente se puede clasificar en cinco rubros, conocidos técnicamente como los dominios de la ciberseguridad (domains)[30], y cada uno de ellos tiene un concepto y desarrollo distinto:

- Seguridad de las comunicaciones: protección contra una amenaza a la infraestructura técnica de un ciber sistema que pueda conducir a una alteración de sus características para llevar a cabo actividades no previstas por sus propietarios, diseñadores o usuarios[31].

- Seguridad de las operaciones: protección contra la corrupción intencionada de procedimientos o flujos de trabajo que tendrán resultados no previstos por sus propietarios, diseñadores o usuarios[32] (2015, pág. 11).

- Seguridad de la información: protección contra la amenaza de robo, supresión o alteración de los datos almacenados o transmitidos dentro de un ciber sistema[33].

- Seguridad física: protección contra las amenazas físicas que pueden influir o afectar al bienestar de un ciber sistema. Algunos ejemplos podrían ser el acceso físico a servidores, la inserción de hardware malicioso en una red o la coacción de usuarios o sus familias[34].

- Seguridad pública o nacional: Protección contra una amenaza cuyo origen está en el ciberespacio, pero que puede amenazar activos físicos o cibernéticos de forma que el atacante obtenga un beneficio político, militar o estratégico. Algunos ejemplos podrían ser Stuxnet o ataques DOS a gran escala contra servicios públicos, comunicaciones, sistemas financieros u otras infraestructuras públicas o industriales críticas[35]. (2015, pp. 11-12)

Con todo lo expuesto, y para finalizar este extenso desarrollo sobre el objeto de estudio de esta incipiente rama jurídica, surge la pregunta de si realmente es posible —o, mejor dicho, necesario— definir el término ciberseguridad para delimitar el objeto de esta materia.

Se coincide con ENISA en que no es necesario —e incluso podría ser incorrecto— definir la ciberseguridad de manera rígida. Lo ideal es generar definiciones contextuales que se adapten al modelo y al ámbito que se desee proteger en cada documento técnico, como se ha visto en las diversas interpretaciones de la ciberseguridad y los enfoques desde sus dominios. Como señala ENISA:

> No es necesaria una definición de la ciberseguridad en el sentido convencional que solemos aplicar a las definiciones de cosas sencillas como la autenticación de una identidad (un mecanismo de seguridad que permite verificar la identidad proporcionada). El problema es que la ciberseguridad es

> un término envolvente, no siendo posible elaborar una definición que abarque todo lo que realmente engloba este término. Por ello, debería considerarse una definición contextual, basada en una que sea relevante, encaje y que ya esté siendo utilizada por una organización o SDO[36] en concreto. (2015, p. 28)

En ese sentido, más que ofrecer una definición adicional a las ya existentes, las cuales son altamente técnicas y consensuadas entre naciones y organismos nacionales e internacionales, se considera que el derrotero que debe guiar el análisis y entendimiento del Derecho de la Ciberseguridad es la búsqueda de maneras y mejores prácticas que garanticen un uso seguro de las computadoras, redes y/o sistemas, y que, al mismo tiempo, permitan salvaguardar la información contenida, con el fin de asegurar la confidencialidad, integridad y disponibilidad (la tríada).

4. Conclusiones

Como se ha podido observar, la interconectividad ha generado un profundo cambio en el paradigma que solía regir nuestra vida cotidiana. Ahora, casi todo está conectado a internet, y, si bien esto nos permite acceder a la información de manera inmediata y sencilla, también ha ampliado la superficie de ataque de los cibercriminales a un alcance global.

Debido a ello, hoy en día, un ciberataque puede ocurrir desde un continente a otro sin necesidad de desplazarse físicamente; basta con una computadora, una red, sistemas y, por supuesto, acceso a internet. Por esta razón, y ante la creciente frecuencia de los ciberataques y nuestra dependencia de la tecnología, el Derecho ha ido adaptándose a los cambios tecnológicos, dando lugar a una incipiente rama jurídica: el Derecho de la Ciberseguridad.

Esta novedosa disciplina regula la ciberseguridad, pero, al ser un tema eminentemente técnico, existen una multitud de definiciones y posturas yuxtapuestas sobre lo que este concepto significa. De hecho, como se ha visto, la normativa internacional (en su mayoría soft law) aborda la ciberseguridad desde distintas perspectivas (como mejores prácticas de protección, un conjunto de herramientas para proteger, entre otros), y, además, abre la puerta al estudio de subramas (dominios), que son en sí mismos campos completos de conocimientos técnicos que escapan al ámbito jurídico.

En atención a esto, lo más importante a considerar al intentar comprender el objeto de estudio del Derecho de la Ciberseguridad es proporcionar definiciones contextuales que se adapten al objetivo y las necesidades específicas, siempre ceñidos al derrotero indiscutible fijado por la Tríada CID.

Referencias

Committee on National Security Systems. (2022). *CNSSI 4009*. Committee on National Security Systems. https://tinyurl.com/bdzmny3v

Committee on National Security Systems. (2015). *Committee on National Security Systems (CNSS) Glossary - CNSSI No. 4009*. Committee on National Security Systems.

Congreso de Los Estados Unidos de América. (2002). *Cyber Security Research and Development Act*. Congreso de los Estados Unidos de América. https://tinyurl.com/yck6mua6

Congreso de Los Estados Unidos de América. (2014). *Federal Information Security Modernization Act*. Public Law 113-282. https://tinyurl.com/84my2m7v

Consejo Europeo. (2001, 23 de noviembre). *Convenio sobre la ciberdelincuencia*. Consejo Europeo. https://tinyurl.com/bdxu2tyk

Consejo Europeo. (2024, 8 de febrero). *Consejo Europeo*. https://tinyurl.com/6x846c9f

CrowdStrike. (2024). *EXECUTIVE SUMMARY: CrowdStrike Preliminary Post Incident Review (PIR): Content Configuration Update Impacting*. CrowdStrike.

Cybersecurity & Infrastructure Security Agency. (2021, 1 de febrero). *What is cybersecurity?*https://tinyurl.com/yck76dzx

European Union Agency for Network and Information Security. (2015). *Definition of cybersecurity - Gaps and overlaps in standardisation*. European Union Agency for Network and Information Security.

Falco, G. y Rosenbach, E. (2022). *Confronting cyber risk: An embedded endurance strategy for cybersecurity*. Oxford University Press.

Gelsi, S. (2024, 31 de julio). *MarketWatch*. https://tinyurl.com/575ckp73

International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2023). *ISO/IEC 27032:2023: Cybersecurity — Guidelines for Internet security*. International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC).

International Telecommunication Union. (2008). *SERIES X: DATA NETWORKS, OPEN SYSTEM - Recommendation ITU-T X.1205 (Overview of Cybersecurity)*. International Telecommunication Union.

La Casa Blanca de los Estados Unidos de América. (2008). *Homeland Security Presidential Directive/HSPD-23. Cybersecurity Policy*. La Casa Blanca de los Estados Unidos de América.

La Casa Blanca de los Estados Unidos de América. (2008). *National Security Presidential Directive/NSPD-54. Cybersecurity Policy*. La Casa Blanca de los Estados Unidos de América.

Magee, T. (2024, 24 de julio). *Raconteur*. https://tinyurl.com/2t9meenb

National Institute of Standards and Technology. (2011). *NIST SP 800-29*. National Institute of Standards and Technology. https://tinyurl.com/9d969e34

National Institute of Standards and Technology. (2012). *NIST SP 800-30*. National Institute of Standards and Technology. https://tinyurl.com/3c5h5c8r

National Institute of Standards and Technology. (2015). *NIST IT 8074 Vol. 2*. National Institute of Standards and Technology. https://tinyurl.com/4rmwb5nt

National Institute of Standards and Technology. (2016). *NIST IR 7621 Rev. 1*. National Institute of Standards and Technology. https://tinyurl.com/bdfdp3z2

National Institute of Standards and Technology. (2018). *NIST Cybersecurity Framework V. 1.1*. National Institute of Standards and Technology. https://tinyurl.com/59ncac9x

National Institute of Standards and Technology. (2018). *NIST SP 800-37 Rev. 2*. National Institute of Standards and Technology. https://tinyurl.com/365jbd6t

National Institute of Standards and Technology. (2019a). *NIST IT 8183*. National Institute of Standards and Technology. https://csrc.nist.gov/pubs/ir/8183/upd1/final

National Institute of Standards and Technology. (2019b). *NIST IR 8183A Vol. 1*. National Institute of Standards and Technology. https://csrc.nist.gov/pubs/ir/8183/a/v1/final

National Institute of Standards and Technology. (2019c). *NIST IT 8183A Vol. 2*. National Institute of Standards and Technology. https://tinyurl.com/yc52kd63

National Institute of Standards and Technology. (2019d). *NIST IT 8183A Vol. 3*. National Institute of Standards and Technology. https://csrc.nist.gov/pubs/ir/8183/a/v3/final

National Institute of Standards and Technology. (2019e). *NIST SP 800-160 Vol. 2, Rev. 1*. National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final

National Institute of Standards and Technology. (2022). *Ransomware: Small Business Cybersecurity Corner*. https://tinyurl.com/4re4r9sn

National Institute of Standards and Technology. (2020a). *NIST SP 1800-25B*. National Institute of Standards and Technology. https://tinyurl.com/33hd2byu

National Institute of Standards and Technology. (2020b). *NIST SP 1800-26B*. National Institute of Standards and Technology. https://tinyurl.com/4b4hamv5

National Institute of Standards and Technology. (2022a). *NIST IR 8401*. National Institute of Standards and Technology. https://csrc.nist.gov/pubs/ir/8401/final

National Institute of Standards and Technology. (2022b). *NIST SP 1800-10B*. National Institute of Standards and Technology. https://tinyurl.com/mrtpke7k

National Institute of Standards and Technology. (2023). *NIST IR 8323r1*. National

National Institute of Standards and Technology. (2024). *Protecting controlled unclassified information in nonfederal systems and organizations*. Departamento de Comercio de los Estados Unidos de América. https://csrc.nist.gov/pubs/ir/8323/r1/final

Parlamento y Consejo Europeo. (2019). *Regulación (UE) 2019/881 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.° 526/2013*. Parlamento y Consejo Europeo.

Parlamento y Consejo Europeo. (2022). *Directiva (UE) 2022/2555 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.° 910/2014 y la Directiva (UE) 2018/1972*. Parlamento y Consejo Europeo.

United States Government Accountability Office. (2018). *Weapon systems cybersecurity*. United States Government Accountability Office.

Bibliografía consultada

BornCity. (2024, 28 de julio). BornCity. https://tinyurl.com/55tjyejd

Brooks, R. (2023, 17 de marzo). The CIA Triangle and Its Real-World Application. Netwrix. https://tinyurl.com/42azcjh8

Douglas, H. y Richard, S. (2016). How to measure anything in cybersecurity risk. Wiley.

Núñez Robinson, R. (2024, 21 de junio). Los delitos cibernéticos (cibercrímenes) en el Perú: El tipo de modalidad delictiva más relevante en el Perú y el mundo. Ius 360. https://tinyurl.com/7ev2sfcy

Ralston, W. (2020, 11 de noviembre). The untold story of a cyberattack, a hospital and a dying woman. WIRED. https://tinyurl.com/5xxjc89p

Srinivasan, S. y Ni, L. K. (2023). Ransomware attack at Springhill Medical Center. Harvard Business Review.

Notas

1 El presente trabajo académico es una reflexión sobre el uso masivo de la tecnología y la necesidad de encontrar nuevas formas de protección.

3 El término exacto, y sobre el cual mucho se ha escrito, es *Cyberthreat Landscape y Cyber Risks*.

4 El término exacto es *Attack Surface*.

5 El término exacto es *Global Attack Surface*.

6 El término exacto en inglés es *Cyber Risk Management*.

7 *Distributed Denial of Service*.

8 Como el Sistema denominado *Supervisory Control and Data Acquisition* - SCADA.

9 Recordemos que el *soft law* son un conjunto de reglas colectivas que no son vinculante, pero que se emplean como parámetros y/o estándares que regulan las prácticas de un mercado específico.

10 Sin considerar las declaraciones ni reservas realizadas por otros países, sino únicamente el texto original del referido Convenio.

11 Traducción libre de "*(3) The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide— "(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; "(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and*

proprietary information; and "(C) availability, which means ensuring timely and reliable access to and use of information".

12 Traducción libre de "*The Congress finds the following:*

(1) Revolutionary advancements in computing and communications technology have interconnected government, commercial, scientific, and educational infrastructures—including critical infrastructures for electric power, natural gas and petroleum production and distribution, telecommunications, transportation, water supply, banking and finance, and emergency and government services—in a vast, interdependent physical and electronic network.

(2) Exponential increases in interconnectivity have facilitated enhanced communications, economic growth, and the delivery of services critical to the public welfare, but have also increased the consequences of temporary or prolonged failure.

(3) A Department of Defense Joint Task Force concluded after a 1997 United States information warfare exercise that the results 'clearly demonstrated our lack of preparation for a coordinated cyber and physical attack on our critical military and civilian infrastructure'".

13 Cabe resaltar que el resto del documento será desclasificado el 5 de enero de 2043.

14 Traducción libre de "(f) 'cybersecurity" means prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation".

15 Traducción libre de "*The ability to protect or defend the use of cyberspace from cyberattacks*".

16 Traducción libre de "*Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation*".

17 Traducción libre de "*The process of protecting information by preventing, detecting, and responding to attacks*".

18 Esta era la definición de seguridad de la computación (computer security) que fue reemplazada por el término ciberseguridad. El texto original traducido libremente es el siguiente: "*Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a*

computer. Rationale: Term has been replaced by the term 'cybersecurity'".

19 Traducción libre de "*the prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems*".

20 Traducción libre de "*Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation*".

21 Traducción libre de "*Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information*".

22 Este reemplaza el estándar técnico anterior contenido en la ISO/IEC 27032:2012.

23 Traducción libre de "*safeguarding of people, society, organizations and nations from cyber risks*".

24 Traducción libre de "*Safeguarding means to keep cyber risk at a tolerable level*".

25 Dicha norma deroga la Regulación (UE) n.° 526/2013, *Cybersecurity Act*.

26 Traducción libre de "'*cybersecurity' means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats*".

27 Traducción libre de "*Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following*:

- *Availability*
- *Integrity, which may include authenticity and non-repudiation*
- *Confidentiality*".

28 Traducción libre de "cyber environment: This includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks".

29 Traducción libre de "*Cybersecurity shall refer to security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalised telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that Cyberspace. Cybersecurity shall therefore encompass the CIA paradigm for relationships and objects within cyberspace and extend that same CIA paradigm to address protection of privacy for legal entities (people and corporations), and to address resilience (recovery from attack)*".

30 Aunque desde un punto de vista más técnico, los dominios de la ciberseguridad son ocho, de acuerdo con el Certified Information Systems Security Professional (CISSP), una de las más prestigiosas certificaciones en ciberseguridad del mundo: i) Domain 1. Security and Risk Management; ii) Domain 2. Asset Security; iii) Domain 3. Security Architecture and Engineering; iv) Domain 4. Communication and Network Security; v) Domain 5. Identity and Access Management (IAM); vi) Domain 6. Security Assessment and Testing; vii) Domain 7. Security Operations; y, viii) Domain 8. Software Development Security.

31 Traducción libre de "*Protection against a threat to the technical infrastructure of a cyber system which may lead to an alteration of its characteristics in order to carry out activities which were not intended by its owners, designers or users*".

32 Traducción libre de "*Protection against the intended corruption of procedures or workflows which will have results that were unintended by its owners, designers or users*".

33 Traducción libre de "*Protection against the threat of theft, deletion or alteration of stored or transmitted data within a cyber system*".

34 Traducción libre de "*Protection against physical threats that can influence or affect the well-being of a cyber system. Examples could be physical access to servers, insertion of malicious hardware into a network, or coercion of users or their families*".

35 Traducción libre de "*Protection against a threat whose origin is from within cyberspace, but may threaten either physical or*

cyber assets in a way which will have a political, military or strategic gain for the attacker. Examples could be 'Stuxnet' or wide-scale DOS attacks on utilities, communications, financial system or other critical public or industrial infrastructures".

36 Standard Developing Organization

Rodolfo Núñez Robinson

El fenómeno de la interconectividad y la ciberseguridad: una introducción al objeto del derecho de la ciberseguridad[1]

The Interconnectivity Phenomena and Cybersecurity: an introduction to the object of study of Cybersecurity Law

Análisis Jurídico – Político
vol. 7, núm. 13, p. 15 - 43, 2025
Universidad Nacional Abierta y a Distancia, Colombia
revista.analisisjuridico@unad.edu.co

ISSN: 2665-5470
ISSN-E: 2665-5489

DOI: https://doi.org/0.22490/26655489.8268