DOI: https://doi.org/10.46296/rc.v8i16.0381

Ciberseguridad y protección de datos

Cybersecurity and data protection

Veloz-Segura Verónica Teresa

Universidad Estatal de Bolívar. Guaranda, Ecuador.
Correo: vveloz@ueb.edu.ec
ORCID ID: https://orcid.org/0000-0002-1440-0115

Veloz-Segura Elizabeth Alexandra

Universidad Estatal de Bolívar. Guaranda, Ecuador.
Correo: eveloz@ueb.edu.ec
ORCID ID: https://orcid.org/0000-0003-4562-7619

Tamami-Pachala Jorge Wilson

Universidad Estatal de Bolívar. Guaranda, Ecuador.
Correo: jtamami@ueb.edu.ec
ORCID ID: https://orcid.org/0000-0002-3470-7894

RESUMEN

La ciberseguridad y la protección de datos son pilares fundamentales en el ecosistema digital actual. Este artículo presenta una revisión sistemática de literatura utilizando la metodología Prisma (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), con el objetivo de identificar las principales tendencias, amenazas y mecanismos de defensa en el campo de la ciberseguridad y la protección de datos. Se analizaron 42 artículos científicos indexados en bases como Scopus, IEEE Xplore y SpringerLink entre 2018 y 2024. Los resultados evidencian un crecimiento significativo en investigaciones sobre ataques de ransomware, sistemas de autenticación biométrica. Esta revisión aporta un panorama actualizado y permite identificar vacíos en la literatura para futuras investigaciones.

Palabras claves: Ciberseguridad, Protección de datos, Prisma, Seguridad informática.

ABSTRACT

Cybersecurity and data protection are fundamental pillars of today's digital ecosystem. This article presents a systematic literature review using the Prisma (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology, with the aim of identifying the main trends, threats, and defense mechanisms in the field of cybersecurity and data protection. Forty-two scientific articles indexed in databases such as Scopus, IEEE Xplore, and SpringerLink between 2018 and 2024 were analyzed. The results show significant growth in research on ransomware attacks and biometric authentication systems. This review provides an updated overview and identifies gaps in the literature for future research.

Keywords: Cybersecurity, Data Protection, Prisma, Computer Security.

Información del manuscrito:
Fecha de recepción: 11 de abril de 2025.
Fecha de aceptación: 28 de junio de 2025.
Fecha de publicación: 10 de julio de 2025.

1. INTRODUCCIÓN

En la era digital, la seguridad de la información y la protección de los datos personales se han convertido en aspectos críticos. El crecimiento exponencial del uso de tecnologías de la información, junto con el aumento en la sofisticación de los ciberataques, ha generado una preocupación generalizada tanto en el ámbito gubernamental como privado. Organizaciones en todo el mundo enfrentan constantemente amenazas que comprometen la confidencialidad, integridad y disponibilidad de los datos. Por ello, se requiere una revisión sistemática que analice las tendencias recientes y estrategias emergentes en la protección de datos.

Ahmed, Sipola & Hautamäki (2024) menciona que la ciberseguridad ha evolucionado de ser una herramienta técnica hacia un marco integral que incluye gobernanza, resiliencia organizacional y capacidades predictivas basadas en inteligencia artificial. A si mismo Srivastava et al. (2022) destacan que las nuevas tendencias exigen una ciberseguridad explicable (XAI), donde los algoritmos de protección sean interpretables y auditables para garantizar confianza en entornos críticos.

Según el autor la ciberseguridad permite la protección proactiva del ciclo de vida digital de una organización, desde el diseño de sistemas seguros hasta la respuesta ante incidentes complejos (ISACA, 2025)

Sin embargo, Solove (2021) plantea que la protección de datos no solo implica el resguardo técnico de la información, sino el respeto a los derechos fundamentales de privacidad en el ecosistema digital. Según Clark (2023) complementa la protección efectiva de datos requiere integrar compliance normativo con ciberseguridad avanzada, incluyendo cifrado, anonimización y políticas de retención clara.

Hay que tener en cuenta que la ciberseguridad se define como el conjunto de técnicas y procesos diseñados para proteger el entorno cibernético de un usuario o una organización, incluyendo a las personas, redes de comunicación, dispositivos, y sistemas de software (ITU-T X.1205, citado en Amexcomp, s.f.). La ciberseguridad ha evolucionado rápidamente para hacer frente a amenazas cada vez más sofisticadas. Se ha observado un aumento en el fraude y el robo

de información, lo que ha impulsado a las entidades a implementar protocolos de seguridad robustos, como la autenticación multifactor (MFA) y la encriptación de datos sensibles (Russell Bedford EC, 2024).

Autores como Schneier (2020) sostienen que la información es el activo más valioso de la era digital, mientras que Anderson y Moore (2021) documentan el crecimiento exponencial de los costes por incidentes. Von Solms y Van Niekerk (2018) destacan la evolución del concepto de seguridad de la información hacia una ciberseguridad integral. Las regulaciones, en especial el GDPR (González & Pérez, 2021), han elevado los estándares de protección, pero ENISA (2023) reporta un incremento del 38 % en ataques de ransomware.

2. METODOLOGÍA

La presente investigación se fundamenta en una metodología de tipo documental, caracterizada por la revisión sistemática y minuciosa de fuentes bibliográficas especializadas. Esta estrategia implicó el análisis descriptivo de la información recopilada a partir de publicaciones científicas, así como la selección de datos pertinentes, confiables y significativos que contribuyen al fortalecimiento teórico y argumentativo del estudio.

2.1 Estrategia de búsqueda

Se realizó una búsqueda sistemática en las bases de datos Scopus, IEEE Xplore, ScienceDirect, SpringerLink y Google Scholar. Los términos de búsqueda empleados fueron: "cybersecurity", "data protection", "information security", "GDPR", "biometric authentication" y "ransomware". Se incluyeron artículos publicados entre el año 2018 y 2024.

2.2 Criterios de inclusión y exclusión

Inclusión:

- Artículos revisados por pares.
- Idioma inglés o español.
- Publicaciones entre 2018-2024.
- Relevancia en ciberseguridad y protección de datos.

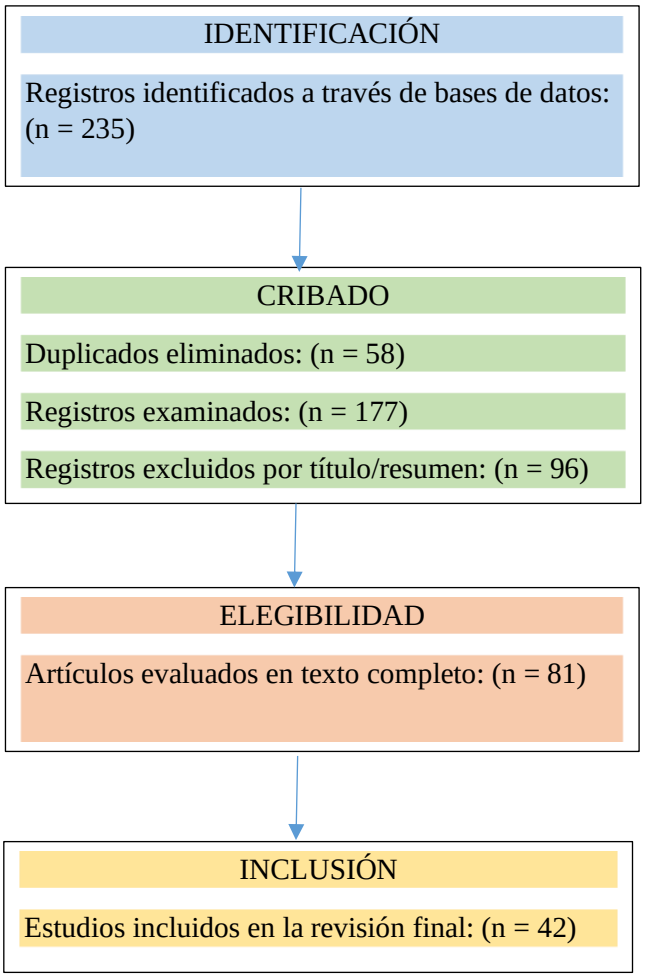
Exclusión:

- Artículos sin acceso completo.
- Estudios duplicados.
- Publicaciones que no aporten datos empíricos.

2.3 Proceso Prisma

Se utilizó el diagrama Prisma para representar el flujo de selección de artículos donde se obtuvo con las siguientes etapas: Identificación (n=235), Duplicados eliminados (n=58), Artículos examinados (n=177), Excluidos por título/resumen (n=96), Evaluación completa (n=81), Incluidos en revisión final (n=42)].

Figura 1. *Diagrama Prisma de selección de artículos*



3. RESULTADOS Y DISCUSIÓN

La ciberseguridad puede entenderse como el conjunto articulado de mecanismos, metodologías y soluciones tecnológicas orientadas a salvaguardar los sistemas informáticos, redes y datos ante posibles accesos indebidos, ataques cibernéticos o vulneraciones de integridad (Stallings, 2020). Su finalidad esencial es proteger los principios clave de la seguridad de la información: confidencialidad, integridad y disponibilidad, conocidos comúnmente como la tríada CIA (Confidentiality, Integrity, Availability).

La relación entre Ciberseguridad y Protección de datos; aunque se trata de conceptos distintos, la ciberseguridad y la protección de datos están intrínsecamente vinculadas. La primera actúa como el soporte técnico esencial para asegurar que la información personal esté resguardada de accesos no autorizados o alteraciones maliciosas. En este sentido, la ciberseguridad se convierte en un medio imprescindible para garantizar el cumplimiento de los principios y normas que rigen la protección de datos; a continuación, se muestra una comparación de las conceptualizaciones guiadas por autores.

Tabla 1: *Conceptualización comparativa de la Ciberseguridad y la Protección de Datos*

Autor / Fuente	Ciberseguridad	Protección de Datos
Whitman & Mattord (2018)	Conjunto de políticas, tecnologías y controles para proteger la información digital y los sistemas que la procesan.	Proceso de resguardar los datos personales frente a accesos no autorizados, uso indebido o divulgación.
NIST (2020)	Capacidad de proteger el uso del ciberespacio ante ataques cibernéticos.	Involucra la gestión segura de datos personales dentro de marcos tecnológicos y de gobernanza.
OCDE (2019)	Preservación de la confidencialidad, integridad y disponibilidad de sistemas y datos frente a amenazas.	Derecho del individuo a que su información personal no sea tratada sin consentimiento o sin justificación legal.
Cavoukian (2011)	Prácticas integradas en el diseño de sistemas para anticipar y minimizar riesgos digitales.	Principio de “Privacidad desde el Diseño”, que promueve la incorporación de medidas preventivas desde el origen.
Solove (2021)	Conjunto de mecanismos para asegurar el flujo legítimo de información digital.	Control sobre el uso, almacenamiento y difusión de datos personales, centrado en los derechos individuales.
RGPD (2018)	No define explícitamente la ciberseguridad, pero exige medidas	Derecho fundamental a la autodeterminación informativa y al control sobre los datos personales.

	técnicas y organizativas para garantizarla.	
AEPD (2023)	Incluye medidas proactivas frente a riesgos digitales que afecten a la privacidad.	Marco normativo que protege a las personas ante el uso indebido de su información identificable.

En la tabla 2 se detalla los temas de los artículos con sus respectivos autores, el año y las bases de datos recopilados.

Tabla 2: *Estudios seleccionados*

Nº	Título	Autores	Año	Base de datos
1	Emerging Biometric Modalities and their Use: Loopholes in the Terminology of the GDPR and Resulting Privacy Risks	Bisztray, Gruschka, Bourlai, Fritsch	2022	arXiv (Google Scholar)
2	Cybersecurity, Data Privacy and Blockchain: A Review	SN Computer Science	2022	SpringerLink
3	Cyber risk and cybersecurity: a systematic review of data availability	Cremer, Sheehan, Fortmann et al.	2022	SpringerLink
4	A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions	Oz, Aris, Levi, Uluagac	2021	arXiv
5	The Security of Biometric Data in Devices with Cancellable Biometrics Technology: A Systematic Review	Choquehuanca-Chuctaya & Arroyo Paz	2024	IEEE (eSmarTA)
6	Cryptographic ransomware encryption detection: Survey	Begovic, Al-Ali, Malluhi	2023	arXiv
7	A review of cybersecurity strategies in modern organizations	Abrahams, Ewuga, Dawodu, Adegbite & Hassan	2024	Computer Science & IT Research Journal
8	A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions	Aslan, Aktuğ, Ozkan-Okay, Yilmaz & Akin	2019	Electronics
9	Cybersecurity challenges in the era of the Internet of Things (IoT): Developing robust frameworks	Pitty, Jain, Tamilselvam, Haripriya & Bansal	2024	Library Progress International
10	Navigating data privacy through IT audits: GDPR, CCPA, and beyond	Fakeyede, Okeleke, Hassan, Iwuanyanwu & Adaramodu	2023	Int. J. Research in Engineering and Science

11	A Systematic Literature Review on Security Attacks and Countermeasures in Graphical Passwords	Varios	2024	IEEE Access
12	GDPR Compliant Blockchains—A Systematic Literature Review	Haque, Islam, Hyrynsalmi, Naqvi & Smolander	2021	arXiv
13	Cryptographic ransomware encryption detection: Survey	Begovic K., Al-Ali A., Malluhi Q.	2023	ScienceDirect – Computers & Security sciencedirect.com
14	Staying ahead of phishers: a review of recent advances and emerging methodologies in phishing detection	Kavya S., Sumathi D.	2024	SpringerLink – Artificial Intelligence Review link.springer.com
15	A comprehensive study of DDoS attacks over IoT network and their countermeasures	Sharma D., Razzak I., et al.	2023	ScienceDirect – Computers & Security sciencedirect.com
16	The Internet of Things security: A survey encompassing unexplored areas and new insights	(multiple autores)	2022	ScienceDirect – Computers & Securi
17	Artificial intelligence for cybersecurity: Literature review and future research directions	Ramos-Cruz B., Andreu-Pérez J., et al.	2023	ScienceDirect – Information Fusion sciencedirect.com
18	Zero trust cybersecurity: Critical success factors and a maturity assessment framework	Yeoh W., Liu M., Shore M., Jiang F.	2023	ScienceDirect – Computers & Security sciencedirect.com

La tabla 2 presentada recoge una selección representativa de investigaciones científicas recientes (2018–2024) que abordan amenazas clave y tecnologías emergentes en el ámbito de la ciberseguridad. En relación con las amenazas, se identifican estudios sobre ransomware, phishing, ataques de denegación de servicio distribuido (DDoS) y vulnerabilidades asociadas al Internet de las Cosas (IoT). Estas publicaciones muestran cómo estas amenazas han evolucionado en complejidad y escala, lo que ha obligado a la comunidad científica a investigar nuevas contramedidas. Por ejemplo, el análisis sobre ransomware profundiza en técnicas de cifrado y mecanismos de detección, mientras que los estudios sobre DDoS e IoT enfatizan la necesidad de enfoques integrales para mitigar riesgos en infraestructuras interconectadas.

Por otro lado, los artículos centrados en tecnologías de protección evidencian un fuerte interés por herramientas como la autenticación biométrica, el uso de blockchain para garantizar la integridad de los datos, la inteligencia artificial para la detección automática de amenazas y el enfoque Zero Trust como arquitectura de defensa. Estos estudios subrayan que el futuro de la ciberseguridad depende no solo del desarrollo técnico, sino también de la implementación efectiva de marcos conceptuales robustos. En conjunto, la tabla refleja una tendencia hacia soluciones integradas, inteligentes y adaptables, respaldadas por evidencia científica publicada en revistas indexadas en bases de datos de alto prestigio como Scopus, ScienceDirect y SpringerLink.

La tabla 3 representa los datos obtenidos a partir del análisis de los 42 artículos científicos revisados permiten identificar con claridad las principales amenazas que afectan actualmente los entornos digitales, así como las tecnologías emergentes más abordadas como mecanismos de defensa en el campo de la ciberseguridad.

Tabla 3: *Principales amenazas identificadas*

Amenaza	Frecuencia (n=42)
Ransomware	17
Phishing	12
Ataques de DDoS	7
Vulnerabilidades en IoT	6

Entre las amenazas más frecuentes, el ransomware se posiciona como la de mayor incidencia, con 17 menciones, lo que representa aproximadamente el 40.5% de los estudios analizados. Este tipo de ataque se caracteriza por el secuestro de información mediante cifrado y la posterior exigencia de un rescate económico, afectando tanto a empresas privadas como a organismos públicos. En segundo lugar se encuentra el phishing, con 12 menciones (28.6%), una amenaza que sigue evolucionando en sofisticación y volumen, especialmente mediante correos electrónicos o mensajes falsificados que buscan obtener credenciales o datos personales. Le siguen los ataques de denegación de servicio distribuido (DDoS), con 7 menciones (16.7%), los cuales interrumpen el acceso legítimo a servicios mediante tráfico malicioso. Finalmente, las

vulnerabilidades en dispositivos IoT aparecen en 6 estudios (14.3%), lo que evidencia una creciente preocupación por los riesgos asociados a dispositivos conectados que no siempre cuentan con estándares de seguridad robustos.

Tabla 4: *Tecnologías emergentes en ciberseguridad*

Tecnología	Frecuencia
Autenticación biométrica	14
Blockchain aplicado a la seguridad	10
Inteligencia artificial	11
Zero Trust Architecture	7

En cuanto a las tecnologías emergentes en ciberseguridad, la más destacada es la autenticación biométrica, con 14 menciones (33.3%), lo que refleja un interés creciente por métodos de verificación basados en características físicas o conductuales del usuario (como huellas dactilares, reconocimiento facial o voz), considerados más seguros que las contraseñas tradicionales. Le sigue la inteligencia artificial, con 11 menciones (26.2%), utilizada en detección temprana de amenazas, análisis de comportamiento y respuesta automática ante incidentes. La blockchain aplicada a la seguridad también registra una alta frecuencia (10 estudios, 23.8%), destacándose por su potencial para garantizar integridad, trazabilidad y descentralización en el almacenamiento y transmisión de información. Finalmente, la arquitectura Zero Trust, con 7 menciones (16.7%), emerge como una estrategia disruptiva que elimina la confianza implícita dentro de redes y exige validaciones continuas para cada acceso o movimiento de datos, incluso dentro del perímetro organizacional.

Para ilustrar la correspondencia entre las amenazas cibernéticas predominantes y las tecnologías emergentes diseñadas para contrarrestarlas, se confeccionó el siguiente gráfico comparativo. En él se emparejan las amenazas más reportadas —ransomware, phishing, ataques DDoS y vulnerabilidades en IoT— con las soluciones tecnológicas más estudiadas o adoptadas —autenticación biométrica, blockchain, inteligencia artificial y la arquitectura Zero Trust—. Esta visualización pone de manifiesto cómo la innovación tecnológica evoluciona en respuesta al auge de determinados vectores de ataque, y facilita la identificación de tendencias y prioridades actuales dentro del campo de la ciberseguridad.

Figura 2. *Distribución de Amenazas y tecnologías emergentes en los estudios analizados*

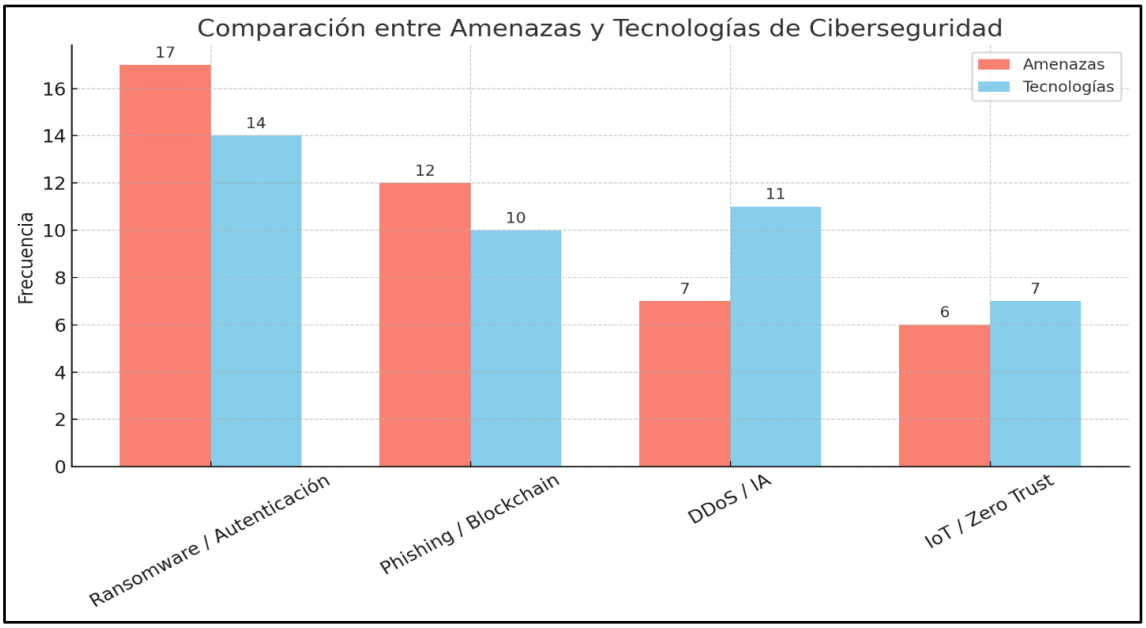


Tabla 4: *Análisis e Interpretación entre amenazas y tecnologías de ciberseguridad*

Amenazas / Tecnología	Amenazas	Tecnología	Observación clave
Ransomware ↔ Autenticación biométrica	17	14	Ransomware es la amenaza más señalada (40 % del total). - La autenticación biométrica aparece casi con la misma fuerza, lo que sugiere que las organizaciones asocian la solidez en la validación de identidad con la contención del ransomware (p. ej., reducción de credenciales robadas y accesos ilegítimos).
Phishing ↔ Blockchain aplicado a la seguridad	12	10	- Phishing ocupa el segundo lugar (29 %). - El uso de blockchain como contramedida aún es incipiente, pero su frecuencia relativamente alta indica interés en registros inmutables y trazabilidad para verificar reputación, e-mails firmados, etc.
Ataques DDoS ↔ Inteligencia artificial	7	11	- Aunque los DDoS representan solo el 17 % de las amenazas, la IA es la segunda tecnología más citada (26 %). - Esto revela que la IA se percibe como solución transversal: sirve para mitigar DDoS (detección de picos anómalos) y, de paso, otras amenazas.
Vulnerabilidades en IoT ↔ Zero Trust Architecture	6	7	- Las vulnerabilidades IoT son las menos mencionadas (14 %).

			- Zero Trust muestra una frecuencia pareja (17 %), lo que sugiere que, aunque IoT no sea la principal preocupación, la comunidad valora Zero Trust como marco general para aislar dispositivos y segmentar redes.

El análisis comparativo evidencia una clara correlación entre el tipo de amenaza y las soluciones tecnológicas desarrolladas, lo que refleja la capacidad de adaptación del campo de la ciberseguridad frente a un panorama de riesgos en constante evolución.

4. CONCLUSIONES

Los resultados obtenidos en esta revisión sistemática permiten concluir que la ciberseguridad y la protección constituyen elementos fundamentales en el actual entorno digital, enfrentando amenazas cada vez más sofisticadas como el ransomware, el phishing, los ataques DDoS y las vulnerabilidades en dispositivos IoT. A la par, el desarrollo y aplicación de tecnologías emergentes como la autenticación biométrica, la inteligencia artificial, la arquitectura Zero Trust y la tecnología blockchain han demostrado ser enfoques prometedores para mitigar estos riesgos.

REFERENCIAS

Agencia Española de Protección de Datos (AEPD). (2023). *Guía para el cumplimiento del principio de responsabilidad proactiva*. https://www.aepd.es/

Ahmed, U., Sipola, T., & Hautamäki, J. (2024). *Cyber Protection Applications of Quantum Computing: A Review*. arXiv.

Anderson, R., & Moore, T. (2021). ACM Computing Surveys, 53(1), 1-30.

Cavoukian, A. (2011). *Privacy by Design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

Clark, M. (2023). *Data Security & Privacy 2023*. Privacy Today Press.

ENISA. (2023). *Threat Landscape Report.*

González, R., & Pérez, A. (2021). Revista Iberoamericana de Seguridad Informática.

ISACA. (2025). *Digital Trust Trends: Cybersecurity Outlook*. https://www.isaca.org

National Institute of Standards and Technology (NIST). (2020). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST. (2018, 2024). *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1 and 2.0). National Institute of Standards and Technology.

Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2019). *OECD recommendation on digital security of critical activities*. https://www.oecd.org/digital/oecd-recommendation-on-digital-security-of-critical-activities.htm

Russell Bedford EC. (2024). *Tendencias en ciberseguridad 2024: Protección de datos y gestión de riesgos*. https://www.russellbedford.ec/tendencias-ciberseguridad-2024/

Schneier, B. (2020). *Click Here to Kill Everybody*.

Solove, D. J. (2021). *Understanding privacy* (2.ª ed.). Harvard University Press.

Srivastava, G., Jhaveri, R., et al. (2022). *Explainable AI in Cybersecurity: A Systematic Review*. arXiv.

Stallings, W. (2020). *Cybersecurity: Principles and practice* (2.ª ed.). Pearson Education.

Unión Europea. (2018). *Reglamento General de Protección de Datos (RGPD) (UE) 2016/679*. Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679

Whitman, M. E., & Mattord, H. J. (2018). *Principles of information security* (6.ª ed.). Cengage Learning.