EL ÁRBOL DE CIBERSEGURIDAD: UNA PROPUESTA DE FORMACIÓN AL CIUDADANO, A LAS INSTITUCIONES Y A LA SOCIEDAD

OLDA BUSTILLOS ORTEGA
https://orcid.org/0000-0003-2822-3428
obustillos@uia.ac.cr
Escuela de Ingeniería Informática, Universidad Internacional de las Américas, Costa Rica

JORGE MURILLO GAMBOA
https://orcid.org/0000-0001-5548-8283
jmurillog@uia.ac.cr
Escuela de Ingeniería Informática, Universidad Internacional de las Américas, Costa Rica

DANIEL MENA BOCKER
https://orcid.org/0009-0002-1062-6675
dfmenab@edu.uia.ac.cr
Escuela de Ingeniería Informática, Universidad Internacional de las Américas, Costa Rica

CARLOS DE LA O FONSECA
https://orcid.org/0009-0002-3413-4990
cedelaof@uia.ac.cr
Escuela de Ingeniería Informática, Universidad Internacional de las Américas, Costa Rica

Recibido: 23 de mayo del 2025 / Aceptado: 8 de junio del 2025
doi: https://doi.org/10.26439/interfases2025.n021.7986

RESUMEN. En un mundo cada vez más interconectado, la ciberseguridad se ha convertido en un pilar fundamental para proteger la información crítica y garantizar la privacidad de las personas, las instituciones y la sociedad en general. El aumento de ciberamenazas, tales como accesos no autorizados, inyecciones de código malicioso y ataques a sistemas críticos, subraya la necesidad de un enfoque integral para la seguridad digital. Este estudio se basa en definiciones y directrices del estándar en ciberseguridad ISO/IEC 27032:2023, la guía curricular ACM/IEEE CSEC2017 y el cuerpo de conocimiento de TI empresarial IEEE-CS (EITBOK). En relación con ello, se plantea el modelo del árbol de la ciberseguridad como propuesta formativa integral destinada a fortalecer

las competencias en el ámbito de seguridad de la información. La analogía del árbol proporciona un marco conceptual que distribuye herramientas estratégicas en sus componentes: follaje, tronco y raíces. Este enfoque permite enfrentar los desafíos de un entorno cibernético en constante evolución, lo que optimiza los procesos de identificación, prevención y mitigación de ciberamenazas, y contribuye simultáneamente al fortalecimiento de una sociedad digital resiliente y segura.

PALABRAS CLAVE: árbol / ciberseguridad / ciberamenaza / formación / seguridad

THE CYBERSECURITY TREE: A TRAINING PROPOSAL FOR CITIZENS, INSTITUTIONS, AND SOCIETY

ABSTRACT. The cybersecurity tree: a training proposal for citizens, institutions, and society in an increasingly interconnected world, cybersecurity has become a fundamental pillar for protecting critical information and ensuring the privacy of individuals, institutions, and society at large. The increase in cyberthreats, such as unauthorized access, malicious code injections, and attacks on critical systems, underscores the need for a comprehensive approach to digital security. This study is based on definitions and guidelines from the ISO/IEC 27032 cybersecurity standard, the ACM/IEEE CSEC2017 curriculum guide, and the IEEE-CS Enterprise IT Body of Knowledge (EITBOK). The "Cybersecurity Tree" model is proposed as a comprehensive training proposal aimed at strengthening information security competencies. The tree analogy provides a conceptual framework that distributes strategic tools across its components: foliage, trunk, and roots. The tree analogy provides a conceptual framework that distributes strategic tools across its components: foliage, trunk, and roots. This approach allows us to address the challenges of a constantly evolving cyber environment, optimizing processes for identifying, preventing, and mitigating cyberthreats, while simultaneously contributing to strengthening a resilient and secure digital society.

KEYWORDS: cybersecurity / cyberthreat / security / training / tree

INTRODUCCIÓN

Orígenes de internet y del ciberespacio

Internet se puede entender como un sistema global de redes digitales interconectadas de dominio público que conecta miles de millones de servidores, computadoras y otros dispositivos. Esto facilita el intercambio de información, eficiente y accesible (International Organization for Standardization [ISO], 2023).

En la década de 1960, se desarrollaron los protocolos TCP (*transmission control protocol*) e IP (*internet protocol*), con los que surgió la red internet. En los años 80, la comunicación vía satélite transformó la radiotelevisión y aparecieron nuevos retos de una comunidad digital con un exceso de información (De-Moragas, 2012). Hasta finales de dicha década, la informática se limitaba a operadores especializados y computadoras ubicadas en centros de procesamiento cerrados, conocidos como casas de cristal, a los que el personal general no tenía acceso (What is the Enterprise IT BOK?, 2017).

Luego, en 1990, se desarrolló la World Wide Web (WWW), lo que permitió acceder a la red informática mundial. Junto con ello, se creó el protocolo de transferencia de hipertexto (*hypertext transfer protocol*, HTTP) para la vinculación y acceso a información. La navegación libre se realizó mediante el localizador uniforme de recursos (*uniform resource locator*, URL) y la creación de enlaces a páginas web (Tim Berners-Lee, 2025).

Ya para el 2000, internet —o la WWW junto con el protocolo TCP/IP— se constituyó como la infraestructura ideal para la publicación y difusión de información que permitió el intercambio de información y la interacción en el ciberespacio (Pinheiro, 2000). A partir de ello, surgieron los motores de búsqueda Yahoo! y Lycos para facilitar la exploración y recuperación de información a través del uso de directorios donde se catalogaba la información según las descripciones proporcionadas por las páginas WWW. Luego, aparecieron los navegadores Google y Altavista, cuya búsqueda de información se apoyaba en palabras clave (Manuel et al., 2006).

Para el 2004, surgen las redes sociales Twitter, Facebook y YouTube, lo que ocasionó cambios que aceleraron el uso del ciberespacio en toda la población (De-Moragas, 2012). Casi diez años después, en el 2016, la Autoridad de Conducta Financiera del Reino Unido aportó un entorno regulatorio del ciberespacio y la gobernanza de internet como una herramienta estratégica para fomentar la participación multidisciplinaria y la colaboración entre distintos actores. Desde entonces, fueron adoptados por reguladores de sectores, tales como finanzas, salud, telecomunicaciones y protección de datos, incluyendo el ámbito de la inteligencia artificial (Moraes, 2024).

A partir del 2020, se incrementó la adopción de tecnologías de seguridad cibernética con una tasa promedio de reconocimiento de riesgos de más del 80 % para

violaciones de datos, *malware*, acceso no autorizado y ataques a la red de diferentes números de usuarios (Zhou et al., 2024). El fácil acceso a recursos de salud en línea, incluidos los generados por grandes modelos de lenguaje (*large language models*, LLM), ha cambiado significativamente la manera en que las personas buscan información relacionada sobre salud y prácticas de autocuidado. En países de ingresos bajos y medios, el 35 % de los adultos utilizan internet para estos fines, favorecidos por el creciente acceso a dispositivos digitales y la expansión del acceso a internet (Clark et al., 2024).

Definiendo la ciberseguridad

La ciberseguridad es una disciplina de las ciencias de la computación que combina aspectos tecnológicos, humanos, informativos y procedimentales para asegurar el funcionamiento de sistemas informáticos. Comprende la creación, operación, análisis y evaluación de dichos sistemas y orienta el diseño de programas de formación (Joint Task Force on Cybersecurity Education, 2017, p. 16).

En el 2013, la Unión Europea (UE) publicó una normativa sobre ciberseguridad y, en agosto del 2015, propuso una ley para establecer requisitos de seguridad a los proveedores de servicios de internet y empresas web (What is the Enterprise IT BOK?, 2017, sección 4.2). Ese mismo mes, la Association for Computing Machinery (ACM), en colaboración con IEEE Computer Society (IEEE-CS) y otras sociedades informáticas, constituyeron el grupo de trabajo sobre educación en ciberseguridad Joint Task Force on Cibersecurity Education[1]. El propósito fue desarrollar una guía curricular completa sobre ciberseguridad que se publicó a finales del 2017 bajo el nombre de *Cybersecurity Curricula 2017* (CSEC 2017).

Por su parte, Ballestero (2020) considera que la ciberseguridad posee la capacidad de resistir acciones que comprometan la disponibilidad, autenticidad, integridad o confidencialidad de los datos y servicios. Incluye los términos *ciberdelincuencia*, *ciberterrorismo*, *ciberataque* y *ciberdefensa* (Ballestero, 2020, p. 40). En tal sentido, Cano (2020, p. 2) identificó cinco áreas clave que generan un impacto transversal en el ámbito de la ciberseguridad, las cuales parten de la pregunta: ¿quién puede provocar los diferentes tipos de ciberdelitos? Sobre ello, Ballestero (2020, pp. 40-41) ha clasificado los tipos de agentes capaces de provocar incidencias y problemas de ciberseguridad de la siguiente manera:

- agentes naturales: sin intencionalidad ni motivación, por ejemplo, un desastre natural
- agentes de perfil bajo: individuos aislados o poco organizados

1 Con aporte de las sociedades ACM, IEEE, AIS SIGSEC, IFIP.

– cibercriminales: organizaciones mafiosas o de crimen organizado
– ciberterroristas: organizaciones terroristas en acciones de propaganda y atentados
– ciberactivistas: grupos antisistemas y de extremismo radical, político o ideológico
– Estados: cuando los Gobiernos extienden conflictos físicos al ámbito virtual, campañas de desprestigio, intromisión en procesos electorales hasta acciones como la ciberguerra

El estándar ISO/IEC 2732 (2023) propone dos definiciones:

– Seguridad en internet: busca preservar la confidencialidad, integridad y disponibilidad de la información a través de la red.
– Ciberseguridad: protege a las personas, sociedades, organizaciones y naciones contra riesgos cibernéticos, con el objetivo de mantener estos riesgos en un nivel tolerable.

Educación y normativas sobre ciberseguridad

La guía curricular CSEC 2017 (Joint Task Force on Cybersecurity Education, 2017) plantea que el mundo ha enfrentado una escasez de profesionales cualificados en ciberseguridad y que, para el año 2022, ya existía una demanda inmediata y creciente de 1,8 millones de puestos vacantes en este campo. Por ello, se ha considerado fundamental que los diseñadores de cursos, talleres y planes curriculares académicos identifiquen e interactúen con expertos y proveedores de capacitación especializados a fin de explorar oportunidades de colaboración que potencien la calidad y pertinencia de los contenidos formativos en ciberseguridad (Joint Task Force on Cybersecurity Education, 2017; What is the Enterprise IT BOK?, 2017).

De acuerdo con Carrillo et al. (2019), el aumento de ciberataques ha creado una necesidad urgente de fortalecer la ciberseguridad como una especialidad académica. En tal sentido, es fundamental priorizar la inversión en docencia y desarrollo humano por encima de la tecnología (*software*, *hardware* y comunicaciones). Entonces, se hace relevante educar, capacitar y sensibilizar a todos los actores involucrados en la ciberseguridad, con el fin de garantizar la estabilidad de las organizaciones e instituciones.

La formación en ciberseguridad está emergiendo como una disciplina bien definida, con un alcance amplio y profundo que abarca diversos subcampos del ecosistema informático moderno, como el desarrollo de *software*, las redes y la gestión de bases de datos. La ciberseguridad o seguridad informática viene a proteger tanto la infraestructura computacional como los activos de la organización y la información de

los usuarios contra los riesgos del entorno digital, el cual es uno de los recursos más importantes a resguardar (Valencia-Arias et al., 2020).

Por ello, elaborar una estrategia nacional de ciberseguridad enfrenta desafíos, como una definición ambigua, falta de coordinación entre el sector privado y el Gobierno, así como una educación insuficiente para preparar a los profesionales necesarios (Arreola García, 2019). De acuerdo con la Unesco (2024), las autoridades educativas deben actualizar las funciones del docente con las competencias necesarias, reforzar la formación docente y desarrollar programas de capacitación para preparar a los maestros en el uso y manejo de inteligencia artificial (IA) y ciberseguridad para garantizar un enfoque seguro y ético.

OBJETIVOS DE LA INVESTIGACIÓN

El objetivo de este estudio es presentar el modelo del árbol de la ciberseguridad como una propuesta educativa dirigida a ciudadanos, instituciones y a la sociedad en general, con el fin de exponer la importancia de la confidencialidad, integridad y disponibilidad de la información. Cabe resaltar que no se llevó a cabo ninguna prueba de campo ni se aplicó o validó el modelo dentro del campo laboral de ninguna industria.

Los objetivos específicos de esta propuesta son los siguientes:

1. Analizar la estructura y funcionamiento del árbol identificando sus componentes (follaje, tronco y raíz).
2. Comparar el árbol con la disciplina de la ciberseguridad, es decir, analizar su estructura de capas y relacionarla con ciberamenazas, y su ubicación con el árbol.
3. Identificar iniciativas académicas aplicadas a la protección y presentación segura de los datos ubicando temas de formación en las tres áreas (follaje, tronco, raíz).

METODOLOGÍA

Para este estudio se realizaron investigaciones sobre estándares ISO y guías curriculares, y cuerpos de conocimiento de las sociedades de computación IEEE CS y ACM, además de artículos sobre educación en ciberseguridad y ciberamenazas. Se excluyeron de esta investigación los temas relacionados con seguridad social, legal o cualquier otro tema distinto a seguridad de la información en la red internet.

1. Revisión de literatura (análisis de documentos): se realizó una revisión de literatura utilizando los criterios de búsqueda en temas sobre ciberseguridad, amenazas cibernéticas y sus impactos en diversos sectores. Se accedieron

a diferentes bases de datos, tales como Google Académico, ProQuest Digital Dissertation and Theses, IEEE Xplore y Academia.edu.

2. Análisis comparativo: los hallazgos obtenidos sobre ciberseguridad y ciberamenazas fueron analizados con apoyo de figuras y cuadros comparativos. La analogía del árbol permitió la definición y comprensión de la ciberseguridad como herramienta orientadora. Finalmente, se abordaron aspectos relacionados con la formación en ciberseguridad y recomendaciones para guías curriculares.

El modelo del árbol de la ciberseguridad se justifica metodológicamente como una herramienta conceptual destinada a guiar la formación integral en esta disciplina. Ayuda a respaldar la inversión en recursos sobre seguridad de la información y facilita el análisis de riesgos y la gestión de sistemas y servicios seguros. Al integrar estos componentes, no solo se busca fortalecer las capacidades técnicas de individuos e instituciones, sino también promover una cultura de ciberseguridad a nivel general, con énfasis en la resiliencia y sostenibilidad en un entorno digital expuesto a constantes ciberamenazas.

ANALIZANDO LA CIBERSEGURIDAD

El auge de la ciberseguridad

La necesidad de ciberseguridad surgió con el desarrollo de las primeras computadoras centrales de las instituciones públicas y universidades, en las que las redes de computadoras eran utilizadas por docentes y alumnos para investigación y para el envío de correos electrónicos y archivos. Entonces, para proteger estos dispositivos y misiones, se implementaron múltiples niveles de seguridad.

La seguridad informática, que trascendía la mera protección física de los dispositivos de cómputo, tuvo un punto de partida significativo con la publicación de un informe en febrero de 1970 para el Departamento de Defensa de los Estados Unidos, denominado Informe RAND R-609. Este buscó definir los diversos controles y mecanismos esenciales para garantizar la protección de los sistemas de procesamiento de datos computarizados (Joint Task Force on Cybersecurity Education, 2017).

Entre 1980 y 2000, la red de internet se incrementó exponencialmente y conectó a millones de dispositivos. Esto generó que la seguridad de la información dependiera de la concienciación de individuos y organizaciones que se enfrentaban a filtraciones de datos, ataques cibernéticos, vulneraciones en protocolos y sistemas de seguridad, tanto del sector privado como del público (Ganesan et al., 2016; Von Solms & Van Niekerk, 2013).

A partir del año 2000, la computación en la nube (*cloud computing*) vino a establecerse como un recurso esencial, al estilo *commodity*. Sin embargo, cada vez que un

usuario subía datos a la nube, perdía el control sobre ellos, lo quiera o no. Esto planteó desafíos en materia de seguridad y privacidad (Garrison & Nova, 2017).

En la década del 2010, surgió la propuesta del agente de seguridad para el acceso a la nube (*cloud access security broker*, CASB), con el propósito de garantizar la protección tanto de la información como de los usuarios (Mendoza, 2014). En una encuesta del 2024, aplicada por la empresa PurpleSec (2025), sobre seguridad de la información, más del 50 % de todos los ciberataques se dirigen a pequeñas y medianas empresas (pymes), y más del 66 % de estas reportaron al menos un incidente entre 2018 y 2020. En el caso de las grandes empresas, se registra un promedio anual de ciento treinta brechas de seguridad por organización, con un preocupante aumento del 27,4 % en la cantidad de incidentes año tras año. A nivel individual, aproximadamente 71,1 millones de personas son víctimas de ciberdelitos cada año, lo que evidencia la creciente magnitud y alcance de las amenazas digitales en todos los niveles.

Para el 2020, Nigeria y Sudáfrica reportaron ocho millones de ataques de *malware* en sus aplicaciones y se detectaron ciento dos millones de programas potencialmente no deseados. Además, las notificaciones falsas sobre servicios de correo electrónico se convirtieron en métodos comúnmente utilizados por personas malintencionadas con el propósito de recopilar nombres de usuario y contraseñas (Okonkwo & Udo, 2022).

Por otro lado, el crecimiento acelerado de los dispositivos de internet de las cosas (IoT) ha llamado la atención de los cibercriminales —como cámaras domésticas conectadas a internet—, lo que pone de manifiesto la urgencia de reforzar los mecanismos de protección de estos dispositivos (Morales Suárez et al., 2019). Otro caso es sobre robo de fondos bancarios con un deterioro significativo de la imagen corporativa de las entidades involucradas (González et al., 2020). Por ejemplo, en los Gobiernos, el aumento de los ciberataques ha generado una creciente preocupación sobre la posible participación de los Estados nación en una guerra cibernética. Esto ha ocasionado que los sistemas de información se volvieran aún más vulnerables, enfrentando el riesgo de ser víctimas del cibercrimen y de las ciberamenazas sin contar con las medidas de protección adecuadas (Joint Task Force on Cybersecurity Education, 2017, pp. 16-17).

De acuerdo con Mayle (2018), los autores de ataques cibernéticos suelen ocultar la identidad y el origen de su ubicación. Individuos y grupos operan en el ciberespacio sin respetar fronteras y, en los últimos años, los ataques contra las infraestructuras de información se han vuelto más frecuentes y complejos, y los perpetradores son cada vez más profesionales. El número de incidentes que afectan la ciberseguridad sigue en aumento, lo que pone en riesgo la información, la red, la seguridad de los usuarios y la de los Gobiernos. Las amenazas provienen principalmente de dos categorías: operaciones de ciberguerra y actividades del cibercrimen (Arreola García, 2019).

Impacto económico del cibercrimen

La actividad delictiva en internet es mucho más amplia que solo el cibercrimen, ya que prácticamente todos los elementos de la actividad delictiva humana se han trasladado al ciberespacio. Un alto funcionario británico informó que la mitad de todos los delitos denunciados en el Reino Unido están relacionados con el cibercrimen (Lewis, 2018, p 6).

En el 2014, un estudio del Center for Strategic and International Studies (CSIS) de Washington D. C. estimó que el cibercrimen le cuesta a la economía mundial aproximadamente 500 000 millones de dólares, lo que representa cerca del 0,7 % del ingreso global. Esta cifra supera los ingresos nacionales de muchos de los países, lo que demuestra que el cibercrimen es una actividad altamente lucrativa. Unos años después, la estimación del cibercrimen ascendía a 600 000 millones de dólares, un 0,8 % del PBI mundial (Lewis, 2018). De igual manera, de acuerdo con Moreno González (2019), en América Latina, el costo del cibercrimen al 2019 osciló entre los 15 000 y 30 000 millones de dólares.

De acuerdo con un estudio de Fernando Ballestero (2020), existen dos tipos de empresas: aquellas que han sido víctimas de un ataque informático en el último año y aquellas que aún no son conscientes de haberlo sufrido. Los ciberdelincuentes se aprovechan del incremento del teletrabajo, el auge del comercio electrónico y el envío masivo de mensajes, donde muchas instituciones y organizaciones carecen de sistemas de protección adecuados (Ballestero, 2020).

Ante el incremento de ciberamenazas y ciberataques en las últimas décadas, los Gobiernos y las instituciones académicas deben responder ampliando la oferta de programas educativos e integrando la ciberseguridad en los marcos curriculares. La ciberseguridad es un campo emergente y las instituciones académicas ya están creando diversos programas educativos para satisfacer la demanda de profesionales calificados (Joint Task Force on Cybersecurity Education, 2017, pp. 16-18).

La formación en ciberseguridad

La incorporación de los principios fundamentales de la ciberseguridad debe establecerse desde las fases iniciales de cualquier plan de estudios especializado con el propósito de dotar de un marco conceptual sólido que facilite la comprensión de la terminología esencial, el entorno de las ciberamenazas, las vulnerabilidades y los principios de la seguridad de la información. En esa línea, la educación es fundamental, pero debe actualizarse para acceder a material educativo de manera segura. Los estudiantes deberían aprender principios y buenas prácticas de ciberseguridad en las escuelas del futuro (De-Moragas, 2012).

Un análisis de artículos publicados reveló que la seguridad de la red y la protección de los datos se posicionaron como los temas más críticos para el sector público y

el privado (Cano, 2011). De acuerdo con Valencia-Arias (et al., 2020), la mayor cantidad de publicaciones sobre ciberseguridad se agrupan en dos áreas principales:

– la seguridad de la red (*network security*) que asegura la estructura del sistema

– la seguridad de los datos (*security of data*) que protege la información crítica

Esto es un indicador de que la educación en ciberseguridad es cada vez un tema más relevante, pues impulsa avances en desarrollos e investigaciones en ambas áreas. En la Figura 1, se brinda un insumo clave para la definición de áreas temáticas a ser incorporadas en programas académicos sobre formación en ciberseguridad.

Figura 1

Temas de investigación sobre ciberseguridad

Nota. Adaptado de "Tendencias investigativas en educación en ciberseguridad: un estudio bibliométrico", por A. Valencia-Arias, M. C. Bermeo Giraldo, Y. Acevedo-Correa, L. F. Garcés-Giraldo, J. Quiroz-Fabra, M. L. Benjumea-Arias & J. Patiño-Vanegas, 2020, *Revista Ibérica de Sistemas e Tecnologias de Informaçạo*, (E29), p. 236.

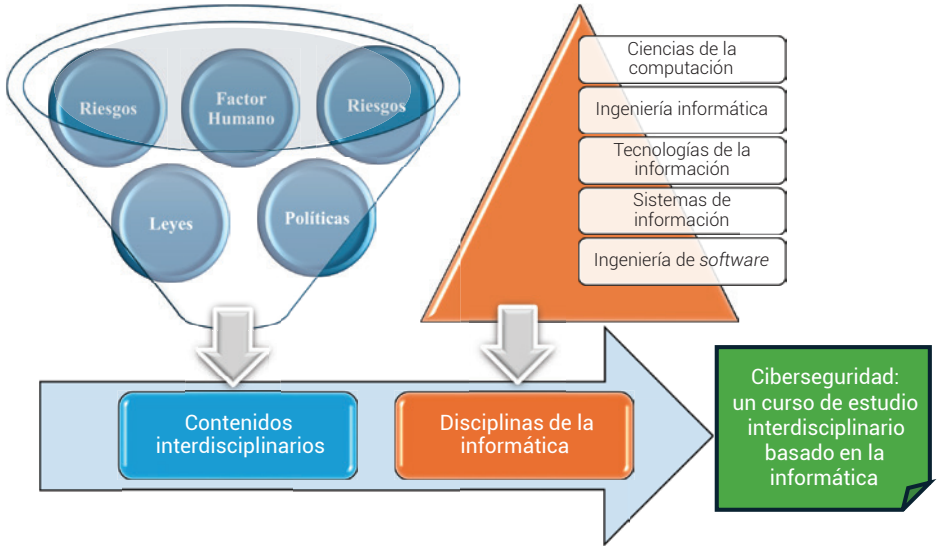
En la Figura 1, se comparan los periodos 2014 y 2016 al mostrar la tendencia creciente en todos los temas en ambos periodos. Sin embargo, se resaltan los dos primeros resultados (seguridad de la red y de los datos) como consideraciones relevantes que reflejan temas clave a tomar en cuenta a la hora de planificar nuevos cursos o talleres sobre ciberseguridad. En este contexto, la ciberseguridad y la ciberdefensa adquieren una relevancia significativa, pues es esencial gestionar los ataques cibernéticos o cibercrímenes (Cano, 2008).

También las organizaciones IEEE y ACM, con su guía CSEC 2017, ampliaron la iniciativa educativa con recomendaciones sobre un currículo académico en ciberseguridad. La propuesta (Figura 2) interrelaciona las cinco disciplinas y constituyen la

base estructural de un programa completo sobre ciberseguridad (Joint Task Force on Cybersecurity Education, 2017, p. 18).

Figura 2

Estructura de la disciplina de ciberseguridad según el CSEC 2017



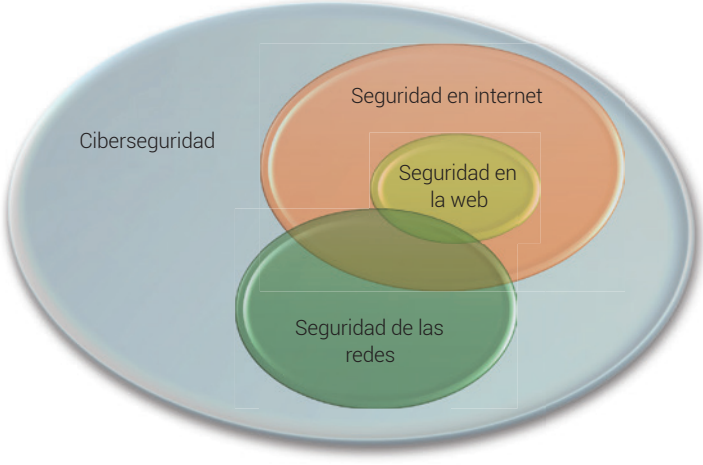
Nota. Adaptado de *Cybersecurity Curricula 2017*, por Joint Task Force on Cybersecurity Education, 2017, Association for Computing Machinery, IEEE Computer Security, Association for Information Systems Special Interest Group on Information Security and Privacy, International Federation for Information Processing Technical Committee on Information Security Education, p. 18 (https://doi.org/10.1145/3184594).

En la Figura 2, se propone una mezcla de contenidos interdisciplinarios con elementos de las cinco disciplinas de la computación. Este es un enfoque holístico determinante para el diseño de un currículo interdisciplinario con un enfoque en ciberseguridad (Joint Task Force on Cybersecurity Education, 2017).

Adicionalmente, el estándar ISO/IEC 27032 (ISO, 2023) ofrece otro aspecto relevante sobre la formación en el tema de ciberseguridad, como el análisis de su interacción e impacto, desde la perspectiva de la seguridad en la red internet, la web y la seguridad en las redes empresariales. En la Figura 3, se ilustran estas interrelaciones como parte del dominio de la ciberseguridad.

Figura 3

Relaciones entre seguridad en internet, web, redes y ciberseguridad



Nota. Adaptado de *ISO/IEC 27032:2023. Cybersecurity—Guidelines for Internet Security*, por International Organization for Standarization, 2023, p. 12 (https://www.iso.org/standard/76070.html).

De acuerdo con la Figura 3, cada dispositivo se conecta con otro y se crea un entorno propicio para el intercambio de información. La seguridad abarca exhaustivamente todos los tipos de interrelaciones presentes en una organización, incluyendo acceso desde redes de área local (LAN), redes de área amplia (WAN), redes de área personal (PAN) y redes inalámbricas (WLAN). Todas ellas requieren de una gestión en ciberseguridad (ISO, 2023).

Por lo anterior, es relevante mencionar que existe el riesgo de experimentar un gasto significativo en adquirir tecnología para la ciberseguridad, en lugar de invertir en docencia y desarrollo de la capacidad humana, así como la necesidad de fortalecer las instituciones de formación y crear programas adecuados para gestionar la ciberseguridad de manera eficaz y ética. Entonces, cabe recordar que el propósito final de la formación de profesionales en las diferentes áreas de seguridad es la de reducir los riesgos relacionados con el uso de internet para las organizaciones, empresas, usuarios y ciudadanos, con el fin de garantizar la disponibilidad y la fiabilidad de los servicios ofrecidos a través de esta plataforma (ISO, 2023).

De acuerdo con "What is the Enterprise IT BOK?" (2017), la formación en seguridad no debe restringirse exclusivamente al personal encargado del diseño, implementación y supervisión de los sistemas de protección, sino que debe abarcar a todo el personal de la organización. Una parte considerable de las brechas de seguridad se origina en acciones realizadas por los propios empleados. Las amenazas a la seguridad no pueden

ser neutralizadas completamente mediante soluciones tecnológicas —como *software* o *hardware*—, por lo que resulta fundamental incorporar estrategias orientadas a la gestión y formación del factor humano. La formación del equipo de ciberseguridad debe ser la más exhaustiva y de carácter continuo, así como los programas de capacitación. Además, deben incluir a todos los niveles del personal de puestos operativos, procesos y procedimientos de seguridad de la información (What is the Enterprise IT BOK?, 2017, parte 1, sección 5, Security Education and Training).

EL MODELO DEL ÁRBOL DE CIBERSEGURIDAD

Esta investigación presenta el modelo del árbol de la ciberseguridad como propuesta para fortalecer las competencias en el ámbito de seguridad de la información. La analogía del árbol ofrece un marco conceptual estructurado en tres componentes: follaje, tronco y raíces. Esta división facilita la identificación de las áreas clave sobre seguridad física y lógica, lo que sirve como base para la planificación de inversiones estratégicas en *software* y *hardware*. Finalmente, el modelo se complementa con la incorporación de temas de educación sobre la ciberseguridad en cada uno de estos tres componentes.

Cabe resaltar que el modelo del árbol ya ha sido utilizado por el IEEE-CS, pero orientado a ubicar los cuerpos de conocimiento de las TIC dentro de la *Guía de Tecnología de la Información Empresarial* (EITBOK) (What is the Enterprise IT BOK?, 2017).

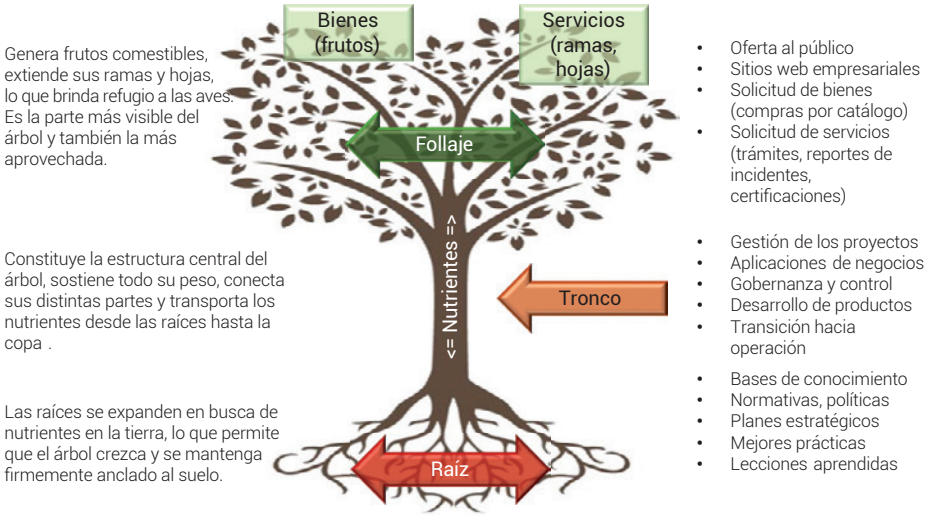
La analogía del árbol

Un árbol está compuesto por tres partes: raíces, tronco y follaje (ramas, hojas y frutos). Cada parte tiene una función específica que contribuye a su crecimiento y supervivencia, las cuales interactúan entre sí.

- Las raíces: absorben el agua y nutrientes para alimentar los demás componentes. Las raíces crecen buscando alimento, hacen crecer y desarrollar el árbol. Ayudan a engrosar el tronco, extender las ramas, aumentar el follaje y dar frutos.
- El tronco transporta sustancias desde las raíces hacia las ramas y las hojas (estas últimas realizan la fotosíntesis para generar energía). Es la parte principal del árbol, porque soporta el peso total. Al engrosar el tronco, este permite extender las ramas y aumentar el follaje. Un buen tronco evita que se fracture el árbol y se desplome.
- El follaje es lo que se aprecia a la distancia. Con el follaje viene la floración y los frutos comestibles. Es la mayor parte utilizable del árbol al extenderse y dar sustento a muchas formas de vida, como insectos, aves y hasta mamíferos, pues comen, anidan y se protegen en ella.

Figura 4

Componentes típicos de un árbol y analogía con una empresa



Al comparar esta estructuración del árbol con la de una empresa u organización, las raíces representarían los valores y conocimientos fundamentales (la base primordial), el tronco sería la infraestructura que los sostiene junto a las ramas que representan las diferentes áreas de desarrollo (o proyectos), y el follaje con hojas y frutos serían los resultados visibles y aprovechables. En resumen, tenemos la analogía del árbol aplicado a la organización de la siguiente forma:

– La raíz es la base de la empresa. Estas bases representan el conocimiento contenido en reglamentos, normativas, leyes, políticas, planes estratégicos, además de documentos sobre procesos y procedimientos junto a las mejores prácticas y lecciones aprendidas con la experiencia. Asociamos a la raíz con la seguridad de los datos, pues gestiona la información crítica y vital de la empresa. Los datos críticos, así como los componentes de ciberseguridad ubicados en la raíz, no deben contratarse a terceros (*outsourcing*, en inglés).

– El tronco comunica y sostiene el peso de la organización. Aquí se gestionan los proyectos y la gestión de las aplicaciones de negocios. El tronco incorpora los sistemas y aplicaciones (presupuestos, gobernanza y control) que se desarrollan "en vivo". También la gestión de proyectos innovadores, desarrollo de productos y de transición (mover de desarrollo hacia producción). Algunos procesos o proyectos pueden ser ejecutados vía subcontratación u *outsourcing* siempre que no manejen información crítica. Asociamos al tronco con la seguridad de la red por ser la que comunica todo.

– El follaje es la puerta principal de acceso al público. Acá se ubica el catálogo de bienes y servicios en forma de sitios web empresariales. Gracias al follaje, los usuarios usan la autogestión vía consultas en red. También pueden elaborar solicitudes de bienes (compras por catálogo) y de servicios (trámites, reporte de incidentes, impresión de documentos y certificaciones digitales, por ejemplo). Asociamos al follaje con la seguridad de internet y seguridad en la web, por ser la que brinda acceso al usuario.

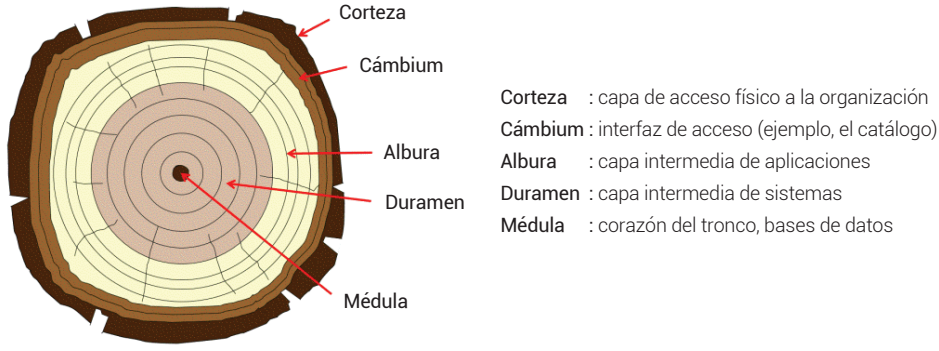
La analogía del árbol, apoyada en la Figura 4, comienza a ofrecernos un marco mental que permite ubicar los distintos elementos de la ciberseguridad en cada una de sus tres partes. Esta analogía se abordará con mayor profundidad más adelante en esta investigación.

La estructura de capas del tronco

En la Figura 5, se presenta un corte transversal de un tronco que permite identificar las diferentes zonas o capas de un árbol, las cuales utilizaremos en la analogía (Emedec, 2021).

Figura 5

Estructura por capas del tronco de un árbol



Nota. De *La estructura del árbol*, por Emedec, 2021, sección "Estructura del tronco" (https://www.emedec.com/la-estructura-del-arbol/).

Al analizar la sección transversal de la figura del tronco, se identifican las distintas capas estructurales que lo conforman. Se aprecian tres grandes zonas (destacadas en tonos de colores), las cuales denominaremos capas del tronco y son las siguientes:

1. Corteza y cámbium: capas exteriores que brindan acceso físico y lógico al público. Las aplicaciones web comparten la información en sentido bidireccional, viajando desde el follaje, por esta capa exterior, hasta la raíz. Se

otorgan permisos restringidos de solo lectura a usuarios, clientes y público. La información que viaja por esta capa utiliza vistas de bases de datos para mostrar copias del origen y sin que el usuario pueda modificar o borrar los datos reales. Un ataque en esta capa exterior solo dañaría una copia (vista) de la información y no impactaría los datos reales ubicados en la médula.

2. Albura y duramen: capas intermedias del tronco donde se otorga el acceso a sistemas y aplicaciones asociados a procesos de negocio y servicios. Los usuarios deben registrarse previamente para obtener autorización de ingreso. La capa intermedia verifica y asigna los niveles de acceso correspondientes. Este es un ambiente con acceso restringido y con monitoreo constante. Ejemplos: registro de solicitudes de un servicio, compras y pagos en línea, completar formularios para solicitar trámites.

3. Médula: capa interna que contiene información sensible y crítica de las bases de datos. En estas capas internas del tronco, se diseña y aplica un esquema de acceso con restricciones muy estrictas para proteger los datos sensibles (raíz). Toda la información que transite en esta capa debe ser tratada con esquemas de seguridad de los más altos niveles. Solamente un número muy limitado de usuarios, computadoras y bases de datos tienen conexión directa a la raíz. Asimismo, las aplicaciones encargadas de actualizar la información clave (agregar, modificar o eliminar datos) deben contar con medidas de seguridad y monitoreo constantes. Las bases de datos clave conforman la médula de la organización y es donde se debe presupuestar la mayor inversión en *software*, *hardware*, comunicaciones y ciberseguridad. Todos los artefactos configurados y conectados a esta capa interna del tronco (incluso capas intermedias) deben estar sujetos a auditorías periódicas de seguridad, incluyendo, como mínimo, pruebas de acceso y vulnerabilidad. Ejemplos: test de penetración (PenTest) y escaneo de vulnerabilidades (VulScan Test).

En síntesis, la estructura en capas del árbol ofrece un marco conceptual útil para el diseño de programas de capacitación orientados tanto a la operación diaria del personal como a la formación técnica en áreas críticas, tales como la identificación y respuesta ante ciberataques y la prevención de accesos no autorizados.

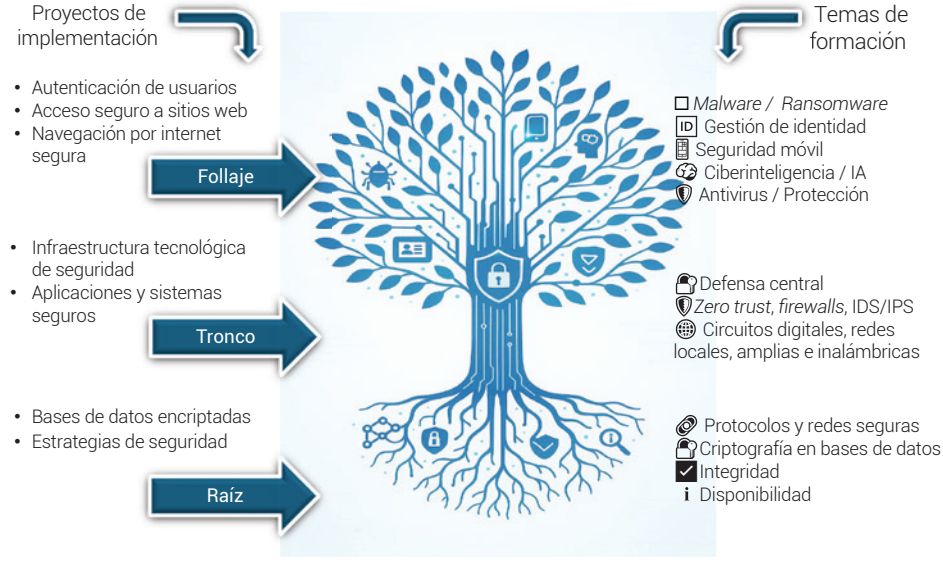
En las capas externas —la corteza y la albura— pueden establecerse controles preventivos y mecanismos de contención adicionales, con el objetivo de impedir la penetración de amenazas hacia la capa más interna —la médula—, que representa los activos más sensibles del sistema. Esta perspectiva facilita una comprensión jerarquizada de las defensas en profundidad y su implementación estratégica en entornos organizacionales.

Propuesta de un árbol de ciberseguridad

Una estrategia de ciberseguridad debe contemplar tanto la probabilidad de ocurrencia de eventos de riesgo menor (capas exteriores) como la magnitud de un posible impacto mayor. La analogía de los tres componentes del árbol (follaje, tronco y raíces), junto con la estructura por capas del tronco, ofrecen un marco de referencia eficaz para proponer estrategias y arquitecturas de ciberseguridad, además de brindar pautas para la formación del personal con el objetivo de llevar a cabo una gestión segura de ciberseguridad en la organización (Figura 6).

Figura 6

Propuesta de árbol de ciberseguridad



Procedemos a analizar cada uno de los componentes de la Figura 6:

1. Las raíces simbolizan los principios fundamentales de la organización, incluyendo las bases de datos, las estrategias de seguridad, los datos críticos y la gestión de riesgos. Se debe evitar cualquier acceso remoto a esta zona. Solamente por red local deben actualizar las bases de datos corporativas. Por tanto, se debe invertir en diseño e implementación de varios niveles de seguridad para el acceso físico y lógico a la raíz.
   - Proyectos de implementación: productos para encriptación de datos críticos.

- Temas de formación: protocolos, criptografía, manejo de integridad y disponibilidad segura de aplicaciones, sistemas, servicios con datos críticos.
- Componentes de ciberseguridad:
  - Protocolos y redes seguras. Conexiones protegidas como SSL/TLS (capa de *sockets* seguros en la capa de transporte), VPN (redes virtuales privadas).
  - Criptografía. Protección de datos mediante cifrado y encriptación segura.
  - Integridad. Garantiza que la información no ha sido modificada.
  - Disponibilidad. Asegura que la información esté accesible cuando se necesite.

2. El tronco representa la infraestructura tecnológica que sustenta la seguridad, incluyendo los cortafuegos (*firewalls*) y el acceso seguro a redes locales e inalámbricas. En las ramas se implementan diversas estrategias de defensa, como la autenticación multifactor y los sistemas de detección de intrusos (*intrusion detection system*/*intrusion prevention system*, IDS/IPS). Adicionalmente, se pueden considerar estrategias de seguridad para el acceso a la red del tipo *zero trust*[2] para evitar aplicaciones con acceso directo a la información crítica.
   - Proyectos de implementación: infraestructura de seguridad (ejemplo, *firewalls*) con aplicaciones y sistemas para integrar conceptos de acceso y comunicación seguros, así como diseño e implementación de redes virtuales seguras (VLAN).
   - Temas de formación: soporte técnico y programación en defensa central, *zero trust*, configuración de muros de fuego (*firewalls*), arquitecturas de redes telemáticas (físicas e inalámbricas y VLAN) y detección IDS/IPS.
   - Componentes de ciberseguridad.
     - Defensa central (*zero trust*, *firewall*). Incluye equipos de la infraestructura de seguridad de acceso como *firewalls*, IDS/IPS (sistemas de detección de intrusiones y sistemas de prevención de intrusiones) y *zero trust* (exige una verificación de identidad estricta para cada usuario y dispositivo que intente acceder a los recursos de la red).

2 *Zero trust* es una estrategia de seguridad de red que establece que ningún usuario o dispositivo debe tener acceso a sistemas de TI o cargas de trabajo sin una necesidad explícita (Akamai, 2025).

- Circuitos digitales. Estructura conectada de redes (locales y remotas).

3. El follaje, junto a las hojas y frutos, representan los esquemas de autenticación primarios que permiten el acceso desde los sitios web y la generación de confianza en el usuario mediante un acceso seguro a la información de la organización.
   - Proyectos de implementación: autenticación de usuarios, acceso seguro a sitios web y navegación cifrada en internet utilizando túneles cifrados (VPN).
   - Temas de formación: diseño de sitios web con esquemas de autenticación y navegación segura. Gestión de ciberamenazas del tipo *malware*, *ramsonware*, seguridad móvil, configuración de antivirus y uso de IA para ciberseguridad.
   - Componentes de ciberseguridad.
     - *Malware*/*ransomware*, como variante de *malware* (*software* malicioso). Infectan computadoras, dispositivos o redes. Protección contra amenazas informáticas que comprometan la integridad, disponibilidad y confidencialidad.
     - Gestión de identidad. Control de accesos y verificación de usuarios.
     - Seguridad móvil para protección de dispositivos móviles e IoT.
     - Ciberinteligencia/IA. Uso de inteligencia artificial para detectar, prevenir y responder a amenazas.
     - Antivirus/protección de *endpoint* (protección de dispositivos como computadoras, portátiles, teléfonos móviles y tabletas contra amenazas maliciosas y ciberataques).

El integrar elementos de ciberseguridad usando la analogía de un árbol permite fortalecer cada componente y garantizar un entorno digital más seguro y resiliente. Además, este modelo sirve como herramienta de apoyo para la formación en seguridad dirigida al personal de las distintas áreas y divisiones de la organización. Entonces, una capacitación efectiva en ciberseguridad, basada en la analogía del árbol, debe utilizar un lenguaje común y no técnico, accesible para todo el personal, de modo que puedan comprenderlo y aplicarlo según su área de responsabilidad.

El árbol como modelo para educar en ciberseguridad

La analogía del árbol, tanto en su estructura vertical (raíces, tronco y follaje) como en sus capas concéntricas (corteza, albura y médula), constituye un marco conceptual

robusto para el diseño e implementación de estrategias de ciberseguridad y programas de formación especializados. Esta representación permite visualizar de forma jerarquizada y funcional los distintos niveles de protección para desarrollar temas de formación orientados a una comprensión integral del enfoque de defensa en profundidad.

- Las raíces simbolizan los fundamentos de la seguridad organizacional (bases de datos, políticas estratégicas, activos críticos y procesos de gestión de riesgos).
- El tronco representa la infraestructura tecnológica que sustenta y conecta el sistema, incluyendo mecanismos como cortafuegos, redes seguras y controles de acceso.
- El follaje, junto con las hojas y frutos, refleja los puntos de interacción con el entorno externo, como los sistemas de autenticación y los canales de acceso a información desde interfaces públicas o sitios web, fundamentales para la generación de confianza en los usuarios.

Adicionalmente, con la analogía de la estructura de capas del tronco —desde la corteza hasta la médula—, permite establecer temas de formación sobre controles escalonados que refuercen la protección en las distintas capas de acceso a la información y lo sistemas de una organización.

- En las capas externas (corteza): formación sobre el acceso del público a través de aplicaciones web utilizando vistas de las bases de datos donde se muestran copias controladas de los datos originales, lo que reduce el riesgo de modificación o eliminación.
- La capa intermedia (albura): formación sobre acceso a sistemas y aplicaciones asociados a procesos de negocio y servicios donde se ubican mecanismos de prevención y contención diseñados para bloquear intentos de intrusión.
- La médula, como núcleo central: temas de formación sobre identificación de los activos más sensibles que deben ser resguardados con los controles más estrictos, donde solamente un número muy limitado de usuarios, computadoras y bases de datos tienen conexión directa.

Esta doble analogía no solo orienta la arquitectura técnica de seguridad, sino que también ofrece directrices claras para el desarrollo de capacidades en el personal: desde la capacitación operativa para llevar a cabo tareas cotidianas hasta la formación técnica especializada en detección de amenazas, respuesta ante incidentes y prevención de accesos no autorizados.

En conjunto, la propuesta del árbol de ciberseguridad junto a la estructura de capas del árbol constituye una base conceptual robusta para la gestión segura y

estratégica de la ciberseguridad en entornos organizacionales complejos. Además, ofrece directrices claras para el diseño de programas formativos en distintos niveles: desde la capacitación técnica y profesional hasta talleres prácticos dirigidos tanto a personal no especializado como a directivos, lo que promueve una cultura de seguridad integral en todos los niveles de la organización.

CONCLUSIONES

A partir del modelo del árbol de la ciberseguridad, se reafirma la importancia de contar con un enfoque estructurado, progresivo y formativo para abordar los desafíos actuales de la seguridad digital. A diferencia de enfoques fragmentados o centrados exclusivamente en aspectos técnicos, esta propuesta integra dimensiones pedagógicas, operativas y estratégicas, con una perspectiva integral que facilita las inversiones en formación y adquisición de tecnologías de seguridad coherentes con los estándares internacionales, tales como ISO/IEC 27032, CSEC 2017 y EITBOK.

La analogía del árbol no solo permite estructurar jerárquicamente los componentes clave de la ciberseguridad (follaje, tronco y raíces), sino que también establece una lógica formativa que orienta el desarrollo de competencias en función de los distintos niveles de exposición y responsabilidad, válido a nivel individual o a nivel personal dentro de una organización. De esta manera, el modelo del árbol de ciberseguridad no solo responde a la imperante necesidad de reforzar la seguridad digital en un entorno cada vez más interconectado, sino que también contribuye de forma sustantiva a la consolidación de una cultura organizacional centrada en la prevención, la resiliencia y la gestión sostenible de los sistemas de información.

Un ejemplo de aplicación del modelo en un entorno real consiste en realizar un inventario de los productos de *software* y *hardware* presentes en una organización. Posteriormente, cada uno de estos elementos se clasifica dentro de los tres componentes del modelo. A partir de esta lista, se seleccionan aquellos elementos relacionados directa o indirectamente con la ciberseguridad y se repite el ejercicio de categorización. Es probable que diferentes personas tengan opiniones distintas respecto a la ubicación de cada componente; sin embargo, esta diversidad de criterios forma parte del proceso formativo, ya que promueve una comprensión más profunda y un mayor conocimiento sobre las herramientas de ciberseguridad disponibles en la organización.

Al promover el desarrollo continuo de capacidades en el capital humano especializado, esta propuesta incide positivamente en la construcción de una sociedad digital más segura, resiliente ante ciberamenazas y preparada para enfrentar los desafíos del ciberespacio.

Como recomendación final y para futuras investigaciones, se sugiere utilizar este modelo como base para realizar una evaluación cualitativa, mediante encuestas,

entrevistas o pruebas piloto, que permitan validar y medir su eficacia en un entorno real.

REFERENCIAS

Akamai. (2025). *What is zero trust*. https://www.akamai.com/glossary/what-is-zero-trust

Arreola García, A. (2019). Desafíos a las estrategias de ciberseguridad. *Revista del Centro de Estudios Superiores Navales*, *40*(4), 25-53. https://cesnav.uninav.edu.mx/cesnav/revista_pdf/2019/2019-4.pdf

Ballestero, F. (2020). La ciberseguridad en tiempos difíciles. *Información Comercial Española. Boletín Económico*, (3122), 39-48. https://doi.org/10.32796/bice.2020.3122.6993

Cano, J. (2008). Cibercrimen y ciberterrorismo: dos amenazas emergentes. *Information Systems Control Journal*, 1-6. https://www.researchgate.net/publication/238781406_Cibercrimen_y_Ciberterrorismo_Dos_Amenazas_Emergentes.

Cano, J. (2011). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. *Sistemas. Asociación Colombiana de Ingenieros de Sistemas*, (119).

Cano M., J. J. (2020). Seguridad y ciberseguridad 2009-2019. Lecciones aprendidas y retos pendientes. *Sistemas*, (155), 81-94. https://doi.org/10.29236/sistemas.n155a6

Carrillo, J. J. M., Zambrano, N. A., Cantos, J. S. M., & Bravo, M. Z. (2019). Ciberseguridad y su aplicación en las instituciones de educación superior. *Revista Ibérica de Sistemas e Tecnologias de Informação*, *E20*, 438-448. https://www.proquest.com/docview/2318537201/fulltextPDF/85B311F112D34AA7PQ/1?accountid=45277

Clark, O., Reynolds, T. L., Ugwuabonyi, E. C., & Joshi, K. P. (2024). Exploring the impact of increased health information accessibility in cyberspace on trust and self-care practices. *SaT-CPS 2024: Proceedings of the 2024 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems* (pp. 61-70). Association for Computing Machinery. https://doi.org/10.1145/3643650.3658611

De-Moragas, M. (Ed.). (2012). *La comunicación: de los orígenes a internet*. Gedisa.

Emedec, S. (2021, 30 de julio). *La estructura del árbol*. https://www.emedec.com/la-estructura-del-arbol/

Ganesan, R., Jajodia, S., Shah, A., & Cam, H. (2016). Dynamic scheduling of cybersecurity analysts for minimizing risk using reinforcement learning. *ACM Transactions on Intelligent Systems and Technology (TIST)*, *8*(1), 1-21. https://doi.org/10.1145/2882969

Garrison, J., & Nova, K. (2017). *Cloud native infrastructure. Patterns for scalable infrastructure and applications in a dynamic environment*. O'Reilly.

González, A., Idrobo, S., & Villamarín, A. (2020). *Gestión de seguridad del activo intangible*. Universidad Internacional SEK. https://www.academia.edu/43066543/Maestr%C3%ADa_en_Ciberseguridad

International Organization for Standarization. (2023). *ISO/IEC 27032:2023. Cybersecurity—Guidelines for internet security* (2.ª ed.). https://www.iso.org/standard/76070.html

Joint Task Force on Cybersecurity Education. (2017). *Cybersecurity Curricula 2017*. Association for Computing Machinery; IEEE Computer Security; Association for Information Systems Special Interest Group on Information Security and Privacy; International Federation for Information Processeing Technical Committee on Information Security Education. https://doi.org/10.1145/3184594

Lewis, J. (2018). *Economic impact of cybercrime—No slowing down*. CSIS https://www.academia.edu/38817793/Economic_Impact_of_Cybercrime_No_Slowing_Down

Manuel, V., Gonçalves, B., & Carrapatoso, E. M. (2006). Rumo a uma web mais inteligente resumo. *EduSer*, *2*(2), 201-227.

Mayle, C. (2018). *Ciberseguridad CERTAL 2018*. Academia. https://www.academia.edu/44956544/Ciberseguridad_CERTAL_2018

Mendoza, M. A. (2014). *Seguridad en la nube para empresas: ¿qué son los CASB?* We Live Security. https://www.welivesecurity.com/la-es/2014/09/24/seguridad-nube-empresas-que-son-casb/

Moraes, T. (2024). Ethical AI regulatory sandboxes: Insights from cyberspace regulation and internet governance. En *TAS '24: Proceedings of the Second International Symposium on Trustworthy Autonomous Systems* (pp. 1-10). Association for Computing Machinery. https://doi.org/10.1145/3686038.3686049

Morales Suárez, A. C., Díaz Ávila, S. S., & Leguizamón Páez, M. Á. (2019). Mecanismos de seguridad en el internet de las cosas. *Vínculos*, *16*(2), 288-297. https://doi.org/10.14483/2322939x.15758

Moreno González, J., Albornoz, M. M., & Maqueo Ramírez, M. S. (2019). Ciberseguridad: estado de la cuestión en América Latina. *Revista de Administración Pública,*

1(148), 23-46. https://revistas-colaboracion.juridicas.unam.mx/index.php/rev-administracion-publica/article/download/38396/35294

Okonkwo, I. E., & Udo, B. (2022). Utilising BIMI-VMC as a cybersecurity tool for brand protection. *Academia Letters*, Artículo 4690. https://doi.org/10.20935/al4690

Pinheiro, M. (2000). *Redesignando a WWW o papel do design na democratização da World Wide Web*. Pontifícia Universidade Católica do Rio de Janeiro.

PurpleSec. (2025). *2024 Cybersecurity Statistics*. The Ultimate List Of Cybersecurity Stats Data, & Trends. https://purplesec.us/resources/cybersecurity-statistics/

Tim Berners-Lee. (2025, 12 de junio). En *Wikipedia*. https://es.wikipedia.org/wiki/Tim_Berners-Lee

Unesco. (2024). *Marco de competencias para docentes em matéria de IA*. https://unesdoc.unesco.org/ark:/48223/pf0000393813

Valencia-Arias, A., Bermeo Giraldo, M. C., Acevedo-Correa, Y., Garcés-Giraldo, L. F., Quiroz-Fabra, J., Benjumea-Arias, M. L., & Patiño-Vanegas, J. (2020). Tendencias investigativas en educación en ciberseguridad: un estudio bibliométrico. *Revista Ibérica de Sistemas e Tecnologias de Informacąo*, (E29), 225-239. https://www.researchgate.net/publication/341220536

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

What is the enterprise IT BOK? (2017, 22 de diciembre). En *EITBOK. Guide to the Enterprise IT Body of Experience*. http://eitbokwiki.org/What_is_the_Enterprise_IT_BOK%3F

Zhou, Y., Wang, Q., & Li, G. (2024). Intelligent talent information system guarantee based on cyberspace security technology. En *ICCSIE '24: Proceedings of the 2024 9th International Conference on Cyber Security and Information Engineering* (pp. 123-130). Association for Computing Machinery. https://doi.org/10.1145/3689236.3689867