La ciberseguridad: conceptos principales, su evolución, el desarrollo de tecnologías emergentes en el mundo y los desafíos al respecto en América Latina

Cybersecurity: Key concepts, Its evolution, the development of emerging technologies worldwide, and the challenges in Latin America

Contralmirante Luis Vera Torres. Se graduó de la Escuela Naval del Perú en 1992 como Alférez de Fragata. Es calificado en guerra de superficie e ingeniería de armas. Ha seguido los cursos Básico de Inteligencia, Básico de Estado Mayor y Comando y Estado Mayor en la Escuela Superior de Guerra Naval; y el curso Alto Mando y la Maestría de Seguridad y Defensa en el Centro de Altos Estudios de la República Bolivariana de Venezuela. Sirvió a bordo del B.A.P. *Sánchez Carrión*, B.A.P. *Mariátegui*, como Jefe de Armamento del B.A.P. *De Los Heros*, B.A.P. *Villavisencio* y B.A.P. *Aguirre*; fue Segundo Comandante del B.A.P. *Aguirre* y Comandante del B.A.P. *Pisco*. Se ha desempeñado como Segundo Comandante de la Estación de Misiles, Oficial Inspector del Área de Armamento del Proyecto 55 (B.A.P. *Aguirre*), Oficial de la Secretaría de la Comandancia General de la Marina, Comandancia General de Operaciones del Pacífico, Segundo Comandante de la Estación Naval de Paita, Oficial Secretario del Jefe del Estado Mayor General de la Marina, Jefe del Proyecto de Construcción del Buque Multipropósito n.º 1 B.A.P. *Pisco*, Sub Director de la Dirección General del Personal de la Marina. En el 2020, con el grado de Contralmirante, fue designado al Ministerio de Defensa como Asesor del Ministro; en 2021, como Agregado de Defensa y Naval en la Embajada del Perú en la República Italiana; en 2023, como Jefe de la División de Operaciones Frente Externo del Estado Mayor Conjunto de las Fuerzas Armadas; y, actualmente, se desempeña como Comandante de Ciberdefensa.

Resumen: El presente artículo examina la evolución de la ciberseguridad, un campo en constante cambio que surge en la década de 1950 y se ha desarrollado a la par de los avances tecnológicos. Se exploran los conceptos fundamentales de la ciberseguridad y se analizan los desafíos actuales a nivel global y regional, con especial atención en América Latina, donde las brechas en infraestructura y la falta de cultura de seguridad presentan retos significativos. Además, se evalúa el impacto de las tecnologías emergentes, como la inteligencia artificial y el aprendizaje automático, en la mejora de los sistemas de protección y en la detección de amenazas. Este estudio proporciona una visión integral de las vulnerabilidades en el ciberespacio y la importancia de la cooperación internacional en la mitigación de riesgos.

Palabras clave: Ciberseguridad, inteligencia artificial, ciberdelitos, América Latina, tecnologías emergentes, seguridad de la información.

Abstract: *This article examines the evolution of cybersecurity, a dynamic field that emerged in the 1950s and has progressed alongside technological advancements. It explores fundamental concepts in cybersecurity and analyzes current global and regional challenges, with particular emphasis on Latin America, where gaps in infrastructure and a lack of security culture present significant challenges. Additionally, the impact of emerging technologies, such as artificial intelligence and machine learning, on improving protection systems and threat detection is evaluated. This study provides a comprehensive view of vulnerabilities in cyberspace and the importance of international cooperation in mitigating risks.*

Keywords: *Cybersecurity, artificial intelligence, cybercrime, Latin America, emerging technologies, information security.*

Introducción

La ciberseguridad básicamente aparece en los años 50 y ha evolucionado de una manera acelerada con los avances tecnológicos hasta nuestros días, avances que, definitivamente, han transformado muchos aspectos de la industria, defensa y el quehacer cotidiano de las personas, sin que algunas veces nos demos cuenta de que ejecutamos acciones de ciberseguridad en los dispositivos electrónicos que usamos y que están conectados a una señal de internet.

La ciberseguridad es un campo multidisciplinario que se ocupa de proteger los sistemas informáticos, redes y datos contra accesos no autorizados, ataques cibernéticos y robo de información. A lo largo de los años, como se mencionó anteriormente, ha experimentado una evolución significativa para adaptarse a las cambiantes amenazas y tecnologías que abordaré más adelante.

Conceptos claves[1]

a) Ciberseguridad: Conjunto de prácticas y medidas para proteger sistemas, redes y datos de amenazas cibernéticas.

b) Amenaza cibernética: Posible peligro o ataque informático que puede comprometer la seguridad de la información.

---

1 Castro, S. *Principios de Ciberguerra.*

c) Ciberataque: Un intento de comprometer la seguridad de un sistema informático, a menudo con intenciones maliciosas.

d) Ciberdelito: Actividades criminales realizadas en línea, como el robo de datos o el fraude cibernético.

e) Confidencialidad: Garantizar que la información solo sea accesible para las partes autorizadas.

f) CSIRT *(computer security incident response team)*: Se traduce como equipo de respuesta a incidentes de seguridad informática.

g) Prueba de penetración *(penetration test)*: Una evaluación de seguridad en la que los probadores intentan encontrar vulnerabilidades y explotarlas sin conocimiento previo de la infraestructura objetivo. Los casos de prueba están limitados, ya que no se explota la funcionalidad interna de la aplicación.

h) SOC *(security operations center)*: Se traduce como centro de operaciones de seguridad. Es un centro de monitoreo y gestión de seguridad cibernética compuesto por un equipo de expertos en seguridad, que supervisa continuamente la infraestructura de tecnología de la informática (TI) y redes en busca de amenazas y actividades maliciosas, con el propósito de detectar, analizar y responder a incidentes de seguridad en tiempo real, además de gestionar políticas de seguridad y coordinar la respuesta a incidentes.

i) Anti *malware*: Estrategias y medidas que tienen como objetivo la protección contra *malware*, que incluye virus, *spyware*, *ransomware* y otros programas maliciosos. La protección contra el *malware* implica la instalación y actualización regular de *software* de seguridad (como antivirus y anti *malware*) para detectar y eliminar amenazas.

j) *Firewall*: Barrera de seguridad que controla el tráfico de red y protege contra intrusiones no autorizadas.

k) *Malware*: *Software* malicioso diseñado para dañar, robar o infiltrarse en sistemas informáticos.

l) *Phishing*: Técnica de engaño en línea para obtener información confidencial, como contraseñas, a través de correos electrónicos falsos y/o haciéndose pasar por entidades legítimas.

m) *Ransomware*: Tipo de malware que cifra archivos y exige un rescate para su liberación.

n) Sistema anti *spam*: Herramienta que detecta y bloquea correo no deseado o mensajes no solicitados, a menudo utilizado en la lucha contra el correo basura.

o) *Hacktivistas*: Individuos o grupos que utilizan habilidades de *hacking* para promover causas sociales o políticas.

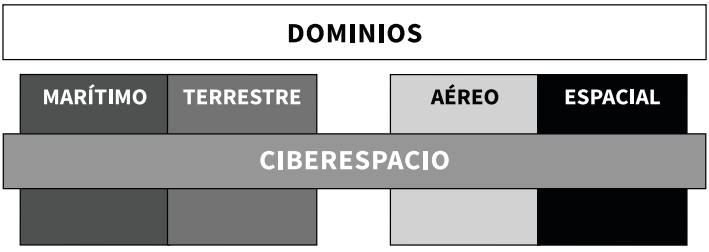
p) *Exploit*: Es un *software*, un fragmento de datos o una secuencia de comandos que aprovecha un error o una vulnerabilidad de una aplicación o sistema para provocar un comportamiento involuntario o imprevisto. Su nombre deriva del verbo inglés *to exploit*, que significa "usar algo en beneficio propio". Básicamente, esto significa que el objetivo de un ataque padece un defecto de diseño que permite a ciertas personas crear los medios para acceder a él y utilizarlo en su propio interés.

Evolución de la ciberseguridad

Con la creación de las redes informáticas, módems y demás, en los años sesenta se va afianzando la ciberseguridad, sin embargo, podríamos mencionar que existieron dos etapas: la primera, antes de que apareciera la Internet, y la segunda, luego de la Internet. Durante la primera etapa, por ejemplo, para perpetrar los hurtos de información o dañar los equipos, necesariamente se deberían llegar físicamente a ellos, por lo que en esa época eran considerados como un robo cualquiera y no como hoy en día que se lo cataloga como un ciberataque.

En la segunda etapa, con la creación de la Internet, a finales de los años sesenta, la ciberseguridad va formándose tal como se la conoce en estos tiempos, ya que aparece un nuevo dominio para los ciberdelincuentes, este nuevo dominio es el "ciberespacio", que es el único dominio creado por el hombre y, coincidentemente, transversal a los dominios naturales, como el marítimo, el aéreo, el terrestre y el espacial, como se observa en la Figura 1.

Figura 1
Dominio transversal del ciberespacio.



Nota: Elaboración propia.

Desde que nace la Internet, la evolución del dominio denominado "ciberespacio" fue creciendo y, por lo tanto, el controlar la información y los accesos a ella se convirtieron en una preocupación y un objetivo, por lo que este acceso al inicio solo era posible en un determinado tiempo y por personas encargadas especialmente de ello, lo que restringió el acceso ante un supuesto robo de información o inserción de información errónea para un determinado fin, ya que los perpetradores podrían ser fácilmente detectados.

Con la creación de la Internet y el Aparnet, la primera red de computadoras en los años setenta, el profesor Robert Tappan Morris creó el primer virus con un programa informático llamado Creeper, que podía moverse a través de la red. Para evitar esto, el programador Ray Tomlinson, el creador del correo electrónico, creó el programa denominado Reaper, que se encargaba de perseguir y eliminar a los Creeper. Por ello, se le considera al Reaper como el primer antivirus de *software* malicioso (*malware*), con lo que se creaba los primeros "troyanos" y "gusanos informáticos".

En 1987, nacieron los primeros programas maliciosos; frente a ello, el programador John McAfee crea el *software* Virus scan y funda su compañía, McAfee. En 1988, el Gobierno de los Estados Unidos se convierte en el primer Estado en acusar y sentenciar a tres años de libertad condicional al profesor Robert Tappan Morris bajo la Ley de Abuso y Fraude Informático. El profesor Tappan adujo que quería evidenciar las deficiencias de seguridad que había detectado en las redes informáticas propias, (podría considerarse lo que hoy se le conoce como *pen testing* para la detección de vulnerabilidades de una red). En los años posteriores de la década de los noventa, los virus y los antivirus tuvieron cierto protagonismo inicial y los Gobiernos comenzaron a tomar conciencia de la importancia de la seguridad de las redes para proteger lo más importante: "la información", sensible y no sensible, dependiendo del usuario que la maneja. En el 2002, el Presidente de los Estados Unidos George W. Bush dio la orden de asumir la responsabilidad de proteger toda la tecnología de la información (TI), sensible para ese país; aun así, las organizaciones criminales se posicionaban fuertemente financiando ataques cibernéticos no solo en los Estados Unidos, sino también en todo el mundo, por lo que los Gobiernos comenzaron a tomar medidas férreas contra la ciberdelincuencia.

La ciberseguridad avanzó notablemente desde sus inicios hasta nuestros días; sin embargo, los virus y los programas maliciosos que se usan para ataques cibernéticos, lamentablemente, avanzaron con ellos y son cada día más sofisticados. Por ello, nos enfrentamos a grandes desafíos, en los que la prevención y la respuesta inmediata automática ante cualquier incidente o

vulnerabilidad serán temas importantes para poder tener un sistema eficiente ante ciberataques en este complejo y cambiante mundo cibernético.

Según un informe de investigación de la firma Markets, el mercado de ciberseguridad global crecerá a USD 345,400 millones para el 2026. El crecimiento del mercado se puede atribuir a la creciente concientización de los Estados y las organizaciones a nivel mundial y al aumento de sus inversiones en infraestructura de ciberseguridad, con el objetivo de proteger su información sensible e importante.

Ataques cibernéticos relevantes en el mundo y en América Latina

Con la finalidad de conocer algunos de los ciberataques, he considerado a continuación solo algunos de una larga lista, que, a mi criterio, son relevantes:

a) El nacimiento de Anonymous, 2003: Anonymous es un colectivo *hacktivista* internacional descentralizado, que lleva a cabo ciberataques como un medio para llamar la atención sobre sus puntos de vista políticos o para exponer objetivos de alto perfil.

b) Operación Aurora, 2009: La operación Aurora fue una serie de ataques cibernéticos que se originaron en China y se dirigieron a la información de propiedad intelectual de más de treinta empresas del sector privado de Estados Unidos de América, incluidas Google, Yahoo y Adobe. Este incidente sacó a la luz las capacidades de las operaciones cibernéticas como herramienta para realizar espionaje industrial a gran escala.

c) Stuxnet, 2010: Stuxnet era un gusano informático extremadamente sofisticado que explotaba múltiples vulnerabilidades de Windows. Supuestamente creado por un programa encubierto entre Estados Unidos e Israel, apuntó y destruyó centrifugadoras en la instalación de enriquecimiento de uranio en Natanz, Irán, causando daños sustanciales al programa nuclear de ese país.

d) EternalBlue y ataques de *ransomware*, 2017: EternalBlue es un *exploit* que utiliza vulnerabilidades en la implementación de Windows del protocolo *server message block* (SMB). Fue filtrado por el grupo de piratas informáticos Shadow Brokers en abril del 2017. Dos importantes brotes de *ransomware* en todo el mundo, WannaCry y NotPetya, utilizaron este *exploit* para afectar a equipos sin parches.

e) El *hackeo* a Twitter, 2020: Uno de los incidentes de ciberseguridad más sensacionales de este año se desarrolló cuando las cuentas de numerosos

usuarios de Twitter de alto perfil fueron pirateadas, incluidas las de Barack Obama, Elon Musk y Bill Gates; lo que demuestra que los humanos son el eslabón más débil en la cadena de ciberseguridad.

f) Conti, 2020-2022: Es una organización del crimen organizado transnacional, que presuntamente tiene su origen en Rusia. Se la detectó por primera vez el en 2020 y se cree que es la sucesora del grupo de *ransomware* Ryuk. Este grupo de *ransomware* fue el de mayor recaudación en el 2021, con unos ingresos estimados de al menos USD 180 millones. Conti suele utilizar la modalidad doble extorsión, también conocida como *doxing*, que consiste en exfiltrar información confidencial de sus víctimas, previo al cifrado, para luego extorsionarlas amenazándolas con publicarla a menos que paguen el monto de dinero exigido.

g) Guacamaya, 2022: De acuerdo con Vicens (2022), Guacamaya se trata de un grupo de *hacktivistas* centroamericano cuyo objetivo principal es infiltrarse en empresas mineras y petroleras, en la Policía y en diversas agencias reguladoras latinoamericanas, con el fin de revelar la injusticia en general, como delitos penales contra la población, el territorio local y el planeta. Critica abiertamente el "imperialismo norteamericano" y su agresión a los pueblos de América. Este grupo *hacktivista* tiene como objetivos a Gobiernos, entidades estatales, militares y empresas extractivas, con el fin de motivar presuntamente mayor transparencia de la información sobre iniciativas de los Estados o de las instituciones mencionadas y, así, darle a la ciudadanía detalles que no se advierten directamente. El modo de operar de este grupo es identificar vulnerabilidades comunes o típicas en las infraestructuras de las instituciones objetivo, como fallas en la actualización o configuración del sistema operativo o aplicaciones específicas, las cuales son explotadas para tener acceso privilegiado a la información residente en dispositivos tecnológicos, y luego revelarla y publicarla en diferentes medios de acceso público.

Dentro de sus acciones más destacadas se encuentran ataques al sector público en Chile, México, Perú, El Salvador y Colombia, donde, debido a este ataque de *ransomware,* se reveló información sensible de Gobiernos, instituciones militares y empresas del sector extractivo.

A continuación, en la Tabla 1, se puede apreciar una comparación entre los dos últimos grupos mencionados: Conti, que opera alrededor del mundo, y Guacamaya, que básicamente opera en América Latina:

Tabla 1
Comparación de las operaciones entre las organizaciones Conti y Guacamaya.

CARACTERÍSTICAS	CONTI	GUACAMAYA
Modalidad	Crimen organizado	*Hacktivista*
Procedencia	Se presume de Rusia	Se presume de Centroamérica
Técnicas utilizadas	*Phishing* con documentos adjuntos maliciosos, explotación de vulnerabilidades ya existentes, descifrar contraseñas y fuerza bruta.	*Ransomware*, explotación de vulnerabilidades en equipos, tales como: fallas en la actualización, configuración del sistema operativo o aplicaciones.
Ámbito de ataque	Entidades del Estado y empresas escogidas claves que afecten el normal funcionamiento de un país y a los ciudadanos.	Entidades estatales, inteligencia militar, empresas extractivas como mineras y petroleras, seguridad nacional.
Organización	Organización a nivel mundial con fines económicos y de extorsión.	Organizado en defensa de una causa común: el bienestar social e intereses nacionales.
Objetivos	Generar incertidumbre, caos, inestabilidad y ganancias monetarias.	Generar mayor transparencia de los Gobiernos y las empresas extractivas.
Filosofía de operación	Hacking como forma desestabilizadora y de generación de recursos económicos ilícitos.	*Hacking* como forma de resistencia.
Finalidad	Contención, cifra los datos para asegurar el pago, exfiltra y cifra la información.	Exfiltración de información sensible.

Tecnologías emergentes

Luego de hacer un breve recuento en el párrafo anterior sobre algunos de los ataques cibernéticos en el mundo y la comparación entre los principales grupos de ciberdelincuentes que han delinquido en América Latina, se puede evidenciar que las amenazas cibernéticas se vuelven cada vez más sofisticadas, con ataques como el *ransomware* y el *phishing*; por ello, la ciberseguridad se centró en la búsqueda de tecnologías automáticas de detección y respuesta en tiempo real ante estas sofisticadas amenazas, adaptándose a tecnologías emergentes, como la inteligencia artificial (IA) y el aprendizaje automático (ML).

Con la llegada de la IA y el ML, la ciberseguridad ha evolucionado hacia enfoques más predictivos y proactivos, utilizando algoritmos para detectar

patrones de comportamiento malicioso, predecir y prevenir ataques con respuesta automatizada a incidentes, como una perfecta integración entre ambas tecnologías, las mismas que se usan en todo el mundo y ya, hace algunos años, en América Latina, donde son herramientas indispensables para una eficiente seguridad cibernética.

Como contraparte a lo mencionado anteriormente, estas tecnologías también podrían ser utilizadas, en la actualidad o en un futuro cercano, para perpetrar delitos por los cibercriminales; no solo en delitos comunes, sino que el riesgo para los Estados podría darse con la construcción y uso de armas cibernéticas por parte de los ciberdelincuentes, lo que las convierte al final en un gran desafío mundial.

Desafíos en América Latina

América Latina enfrenta una serie de desafíos en el ámbito de la ciberseguridad, que van desde la falta de infraestructura, falta de conocimiento, falta de conciencia, escasa cultura de seguridad, falta de recursos, hasta la creciente sofisticación de las amenazas cibernéticas. El afrontar con éxito estos desafíos demandará un enfoque integral que deberá considerar inversiones en educación, capacitación, infraestructura y, no menos importante, la cooperación internacional.

Según el informe del Observatorio de Ciberseguridad de la Organización de Estados Americanos[2] la comunidad de respuesta en América Latina a incidentes está experimentando cambios significativos debido a los tipos y complejidad de los ataques que necesita combatir. Asimismo, no es muy uniforme la madurez de sus capacidades y hay mucha necesidad de mejoras.

En cuanto a la evaluación y contribución de expertos, en el citado informe se señala que la seguridad informática en América Latina continuará evolucionando, al considerarse que existen países que tienen mayores incidencias de ataques cibernéticos que otros; por lo que es importante construir canales de cooperación a diferentes niveles entre los Gobiernos e instituciones internacionales, ya que se pronostica la multiplicación de los *ransomware* y el *phishing,* entre otros tipos de ataques.

Es importante señalar que los Gobiernos no son ajenos a las amenazas y al riesgo de proliferación de los ataques cibernéticos. El proteger los servicios e infraestructura sensible y básica para hacer frente a los incidentes

2 Informe de Ciberseguridad del Observatorio de la Ciberseguridad en América Latina y el Caribe.

informáticos se convierte en un desafío importante para mantener a un país conectado de forma segura.

Como información relevante contenida en el informe, en la parte del análisis de los perfiles de países, sobre el Perú se menciona textualmente lo siguiente:

Mientras que los servicios de gobierno electrónico y comercio electrónico continúan expandiéndose en el Perú, la conciencia social de la seguridad cibernética es generalmente baja. La Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) ofrece literatura en línea sobre este tema, pero no hay una amplia campaña de sensibilización que esté actualmente vigente. Muchas universidades nacionales y empresas privadas ofrecen educación y capacitación en seguridad cibernética. Sin embargo, suele carecerse de tecnología adecuada y personal educativo con experiencia. [3]

Como ideas generales de los desafíos que enfrenta Latinoamérica, se resume lo siguiente:

a) En cuanto a tecnología, la región está avanzando en términos de adopción de tecnologías de ciberseguridad; sin embargo, todavía enfrenta desafíos en términos de infraestructura y recursos.

b) La importancia de alinear las políticas de ciberseguridad con las regulaciones internacionales es un desafío en Latinoamérica.

c) Es innegable que existe carencia de profesionales capacitados en ciberseguridad en la región, lo que dificulta la implementación efectiva de estrategias de seguridad.

d) Algunos países latinoamericanos enfrentan amenazas específicas, como el cibercrimen organizado y ataques dirigidos a sectores clave, como el financiero y el energético.

3 Informe de Ciberseguridad del Observatorio de la Ciberseguridad en América Latinay el Caribe, p. 84, 2.

Conclusiones

a) El ciberespacio tiene características únicas que lo diferencian de los otros espacios, y que sus usos podrían estar contenidos en cualquier otro dominio de manera particular en uno o en todos a la vez.

b) No puede haber una estrategia nacional de seguridad que no incluya la ciberseguridad, debido a que es un domino transversal a todos.

c) La convergencia de tecnologías aceleradas y exponenciales está creando cambios disruptivos en el planeta, como la inteligencia artificial (IA) y el aprendizaje automático (ML).

d) La automatización con inteligencia artificial (IA) y el aprendizaje automático (ML) ha revolucionado la forma en que abordamos la ciberseguridad, y está permitiendo una detección más rápida y precisa de amenazas, así como respuestas automáticas ante ataques cibernéticos.

e) Los estrategas deben conocer y entender la coincidencia de las tecnologías emergentes disruptivas: IA y ML, para explotar sus capacidades en beneficio propio con la finalidad de optimizar la detección y respuesta inmediata ante amenazas.

f) La concientización de los Estados y organizaciones globales apunta cada vez más al convencimiento de que se debe invertir en sistemas eficientes de seguridad para la protección de su principal activo, "la información", debido a los diversos ciberataques ocurridos y que vienen aconteciendo a nivel mundial.

g) América Latina aún tiene trabajo por hacer para fortalecer su postura cibernética y protegerse de las amenazas cibernéticas en constante evolución. Es fundamental abordar estos desafíos de manera colaborativa y centrada en la innovación para garantizar un entorno digital seguro y protegido en la región.

h) La ciberseguridad ha evolucionado significativamente en América Latina con un enfoque creciente en la adopción de tecnologías, como la IA y el ML, para mejorar la detección y la respuesta ante amenazas cibernéticas. Sin embargo, persisten desafíos en términos de cumplimiento normativo, escasez de talento y amenazas únicas en la región.

Referencias

1. Castro, S. *Principios de Ciberguerra*.
2. JID. Junta Interamericana de Defensa. (2020). *Ciberamenaza, entender el concepto de ciberamenazas y analizar el panorama actual y las tendencias*..
3. JID. Junta Interamericana de Defensa. (2020). *Ecosistema ciberespacial, entender el rol de la ciberdefensa militar en el contexto nacional e internacional.*
4. JID. Junta Interamericana de Defensa. (2020). *Ecosistema ciberespacial, entender la importancia de la cooperación público-privada, la gestión de riesgos de terceros, la información en la ciberdefensa y concienciar sobre los riesgos de ciberseguridad asociados a situaciones de pandemia*.
5. Gobierno de España, Presidencia. (2013). *Estrategia de ciberseguridad nacional*.
6. Gobierno del Perú. Presidencia del Consejo de Ministros, Secretaría de Gobierno y Transformación Digital. (2023). *Foro de seguridad y confianza digital*.
7. OEA. Organización de Estados Americanos (2023). *Retos y estrategias: Las consideraciones de los ataques* ransomware *en las Américas.* (10).
8. Secure C. *El mercado de ciberseguridad crecerá a USD 345,400 millones en el 2026*.https://blog.camelsecure.com/el-mercado-de-ciberseguridad-crecer%C3%A1-a-usd-3454-mil-millones-en-2026.
9. Ciberamenazas y Tendencias. Análisis de las ciberamenzas nacionales e internacionales, de su evolución y tendencias futuras. (23), 2023.
10. Estrategias Nacionales de Ciberseguridad: Lecciones aprendidas y reflexiones desde las Américas y otras regiones. 2022.
11. Guía de Ciberdefensa. *Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar.*
12. Introducción a la ciberdefensa. Perspectiva militar e integral. 2020.
13. Saavedra, B. Jefe del Programa de Ciberseguridad, Centro William J. Perry de Estudio Hemisféricos de Defensa.