CIENCIA Y TECNOLOGÍA

CENDITEL
NODO MERIDA

CIBERSEGURIDAD

EN LA ERA DE LA CONVERGENCIA TECNOLÓGICA

REPÚBLICA BOLIVARIANA DE VENEZUELA | Ministerio del Poder Popular para CIENCIA Y TECNOLOGÍA

[2022 - 2030]

Ciberseguridad en la era de la convergencia tecnológica

Nuevos retos y oportunidades para salvaguardar la información digital

Daniel Quintero
María Alejandra Rujano
Carlos González
Aida Andrade
Jesús Erazo
Santiago Roca
Pablo Sulbarán
Yazmary Rondón
María Eugenia Acosta

República Bolivariana de Venezuela
Ministerio del Poder Popular para Ciencia y Tecnología (MINCYT)
Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL)

Ciberseguridad en la era de la convergencia tecnológica

Nuevos retos y oportunidades para salvaguardar la información digital

Presidente de CENDITEL
Oscar González

Directora de Investigación en Tecnologías Libres
María Alejandra Rujano

Editor
Jesús Erazo

Revisión
Yazmary Rondón, Santiago Roca, María Eugenia Acosta, Aida Andrade, Daniel Quintero, Jesús Erazo, Carlos González y María Alejandra Rujano

Diseño Gráfico
Gabriel Martínez

Ilustración
Miguel Albornoz

Diagramación
Pablo Sulbarán
Jesús Erazo

Datos para la catalogación bibliográfica

Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL)
Ciberseguridad en la era de la convergencia tecnológica
Colección: Oscar Varsavsky
Serie: Pensamiento crítico sobre la contemporaneidad tecnológica
Noviembre 2025, Primera Edición
Depósito Legal: ME2024000252
ISBN: 978-980-18-4963-62
Sitio oficial: https://convite.cenditel.gob.ve/libros/

Ciberseguridad en la era de la convergencia tecnológica

Nuevos retos y oportunidades para salvaguardar la información digital

No cabe duda de que mientras no cambie la actual estructura de poder, es absurdo creer que pueda imponerse un nuevo estilo tecnológico, pero lo que parece cada vez mas claro es que si ese nuevo estilo no ha sido por lo menos discutido y en lo posible sometido a pruebas prácticas aprovechando circunstancias favorables, un cambio de estructura de poder nos encontrará sin otros instrumentos técnicos que los ofrecidos por esta sociedad occidental que ha dejado de parecernos digna de imitarse, no es que el militante deba convertirse en tecnólogo, pero debe aprender a rechazar la falsa conciencia técnica-económica que absorbe todos los días y a percibir sus alternativas…

No creemos que se llega a una nueva sociedad mediante una mejor selección de tecnologías, pero aunque no es condición suficiente, es necesaria: la tecnologías “modernas” producen la misma alienación, dependencia y desequilibrio aunque no haya empresarios privados que agreguen a esas lacras la explotación.

Estilos Tecnólogicos 1974

Oscar Varsavsky (1920 - 1976)

Índice general

Prólogo

En plena era digital, las Tecnologías de la Información y Comunicación (TIC), se han constituido en una herramienta fundamental para todos los sectores de la sociedad, facilitando la creación, procesamiento, almacenamiento y transmisión de la información. Desde el uso cotidiano de Internet y las plataformas digitales hasta servicios avanzados como la computación en la nube y la tecnología de cadena de bloques, la población mundial deposita una confianza cada vez más grande en los sistemas digitales.

Ahora bien, uno de los principales retos se encuentra en la interconexión de estos sistemas informáticos. Los datos independientemente de que sean personales, empresariales, industriales, científicos, gubernamentales y militares circulan a través de redes físicas y digitales que requieren el uso de hardware y software interconectados; y es en esta comunicación, donde se presenta un punto álgido referente a las vulnerabilidades de la protección de los datos. Los fallos de seguridad o puertas traseras de estos sistemas pueden ser aprovechados por intrusos para ingresar a los mismos y realizar ataques cibernéticos o ciberataques, resultando comprometida la integridad y confidencialidad de la información, representando de esta manera un arduo trabajo de Ciberseguridad para proteger estos sistemas.

Aunado a lo anterior, los avances en Inteligencia Artificial (IA), computación cuántica, Internet de las Cosas (IoT por sus siglas en inglés) y otras tecnologías emergentes, si bien pueden representar, la sofistificacion de los sistemas de procesamiento y almacenamiento de la información, no obstante, esta convergencia tecnológica – donde se integran éstas y otras tecnologías – crea una red de interdependencias que puede resultar en una mayor superficie o zona eficaz de ataque, haciendo más desafiante y compleja la protección o salvaguarda de los datos.

Bajo estas condiciones, por un lado, los sistemas de Ciberseguridad no solo deben actuar ante amenazas ya conocidas, sino también prever los nuevos retos que la convergencia tecnológica traerán consigo. Por el otro lado, deben aprovechar la integración de las tecnologías emergentes para desarrollar soluciones de seguridad modernas, innovadoras o pioneras para la protección de datos.

Ahora bien, honrando la tradición y filosofía de CENDITEL centrada en el conocimiento como bien público y el reconocimiento de la no neutralidad de las tecnologías, en esta quinta edición del Libro de la Colección Oscar Varsavsky, en la cual el eje central es **Ciberseguridad en la era de la convergencia tecnológica. Nuevos retos y oportunidades para salvaguardar la información digital**, busca explorar la Ciberseguridad desde diversos ángulos, desde su impacto en los sectores como la ingeniería civil y la industria hasta plantear reflexiones sobre su afectación o incidencia social e implicaciones éticas, pasando por los desafíos del uso de la criptografía cuántica e incluso examinando cómo puede ser utilizada como herramienta pedagógica en los procesos de enseñanza y aprendizaje.

En tal sentido, en la primera sección del libro **Ciberseguridad Estratégica, Sostenibilidad e Identidad**, Daniel Quintero a través de su ensayo *Teorización estratégica sobre la defensa cibernética de la Nación*, propone que el concepto de defensa cibernética venezolano sea valorado, enriquecido y complementado en un debate abierto, que se nutra de actores civiles, militares, públicos y privados. A continuación, María Alejandra Rujano con su contribución titulada *Cibersostenibilidad: Un nuevo paradigma estratégico en la era digital*, explora la cibersostenibilidad como un modelo táctico emergente que la sociedad y las organizaciones deben integrar para equilibrar el avance tecnológico con la protección ecológica y la equidad social. Seguidamente, Carlos González con su contribución *Suplantación de la identidad digital en la era de la Inteligencia Artificial. En pos de la autenticidad en un mundo virtualizado*, muestra las tres principales aristas de la suplantación de identidad en espacios digitales: la suplantación clásica, la creación de ejércitos de perfiles falsos y la introducción de la IA generativa, con la finalidad de modelar el pensamiento de la sociedad.

La segunda sección centrada en **Ciberseguridad, Economía y Proyecciones Futuras**, inicia con el ensayo de Aida Andrade titulado *Ciberseguridad como motor económico: Definiciones, condición actual y tendencias*, el cual muestra que la Ciberseguridad ha evolucionado de un nicho técnico a un sector económico estratégico con un impacto macroeconómico y una relevancia ineludibles, destacando que su crecimiento es un reflejo de la digitalización global y la creciente conciencia de los riesgos asociados. Ahora bien, dentro de sus proyecciones a futuro, Jesús Erazo presenta *Consideraciones sobre criptografía cuántica y su futuro en el campo de la Ciberseguridad*, quien se centra en la computación cuántica y su rama especializada, la criptografía cuántica, con la finalidad de explorar una tecnología con un potencial transformador para el futuro de la Ciberseguridad.

En la tercera sección **Ciberseguridad e Intersección Tecnológica**, el autor Santiago Roca a través de su escrito *Ciberseguridad e Inteligencia Artificial: Una mirada desde el Ciberpoder*, explora diferentes modos de convergencia entre el ciberpoder y la Ciberseguridad, tomando como referencia la IA como exponente tecnológico relevante en la actualidad. Del mismo modo, Pablo Sulbarán en *Ciberseguridad aplicada a los sistemas de control industrial: Caracterización, vulnerabilidades, estrategias y expectativas*, hace una descripción del estado del arte de los Sistemas de Control Industrial (SCI) en el marco de la Ciberseguridad, analizando la arquitectura de los SCI y cómo la misma deriva en vulnerabilidades a nivel de Ciberseguridad.

Por último, el la cuarta sección titulada **Ciberseguridad en Educación y Formación**, Yazmary Rondón a través de su ensayo *Formando ciudadanos digitales críticos: El papel de la Ciberseguridad en la Educación*, busca exponer un desarrollo teórico de la situación actual, por medio de experiencias en esta área, en los niveles de educación primaria, secundaria y universitaria. Además, realiza un análisis de las competencias digitales necesarias, ventajas, desventajas, políticas y recomendaciones, tanto en la formación dirigida hacia los niños y jóvenes como usuarios vulnerables, como hacia las instituciones para el manejo eficiente

y seguro de la información derivada de sus procesos académicos y administrativos. En el cierre de esta sección, María Eugenia Acosta, con su trabajo teórico titulado *Drones y Ciberseguridad en la enseñanza de la Ingeniería Civil*, propone abrir una discusión sobre ¿Cómo formar ingenieros civiles conscientes del valor y los riesgos de los datos que utilizan en sus prácticas profesionales?. Desde esta perspectiva, plantea que uno de los grandes desafíos para las próximas generaciones de profesionales es dominar las herramientas tecnológicas emergentes y comprender los marcos legales, técnicos y culturales que rodean la producción de datos en contextos complejos.

En tal sentido, el presente libro no solo aborda temas de defensa nacional, geopolítica y sostenibilidad estratégica, también ofrece una visión actualizada de la Ciberseguridad en el contexto económico y la investigación de tecnologías futuras, así como su interacción con otras tecnologías avanzadas y su aplicación a sistemas industriales. Además, su relevancia en el ámbito educativo, ya sea para la formación de ciudadanos digitales o en la enseñanza de disciplinas técnicas específicas, se hace necesaria la apropiación del conocimiento de esta tecnología para valorar las implicaciones y retos asociados, porque debemos recordar que ninguna tecnología es neutral.

Jesús Erazo
Correo: jerazo@cenditel.gob.ve
Editor del Libro

Ciberseguridad Estratégica, Sostenibilidad e Identidad

Teorización estratégica sobre la defensa cibernética de la Nación

Daniel Quintero[1]

Introducción

Las amenazas cibernéticas para la defensa

Para iniciar este análisis es importante exponer una mirada inicial sobre la temática, Leiva (2017) manifiesta que la ciberdefensa debe ser considerada un bien público, que amerita su establecimiento como un nuevo Eje Estratégico, para visualizarse como una nueva dimensión que coadyuve a potenciar este factor como capacidad estratégica. En tal sentido, para entender esa dimensión emergente se requiere una valoración del avance que han tenido los fenómenos amenazantes para el pensamiento estratégico en las últimas décadas, Pontijas (2023) plantea: "La creciente vulnerabilidad cibernética de las sociedades modernas obliga a estas a dotarse de capacidades y desarrollar estándares de seguridad, protección y respuesta ante las complejas y crecientes amenazas en dicho ámbito" (p. 13). Precisamente, la volatilidad de los cambios es lo que dificulta más el establecer medidas efectivas contra las amenazas, ya que la mutabilidad digital abre caminos pero también genera desequilibrios, en el informe "Global Cybersecurity Outlook 2025" se indica:

> – La escalada de tensiones geopolíticas contribuye a un entorno más incierto. – La mayor integración y dependencia de cadenas de suministro más complejas está generando un panorama de riesgos más opaco e impredecible. – La rápida adopción de tecnologías emergentes contribuye a nuevas vulnerabilidades, ya que los ciberdelincuentes las aprovechan eficazmente para lograr mayor sofisticación y escala. – Simultáneamente, la proliferación de requisitos regulatorios en todo el mundo añade una importante carga de cumplimiento para las organizaciones. Todos estos desafíos se ven exacerbados por una creciente brecha de habilidades, lo que dificulta enormemente la gestión eficaz de los riesgos cibernéticos. (World Economic Forum, 2025, p. 2)[2]

[1]Historiador y abogado egresado de la Universidad de Los Andes (ULA). Actualmente se desempeña como docente en la ULA, y como investigador en el Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL). Autor y director de publicaciones académicas y de divulgación científica. dquintero@cenditel.gob.ve

[2]**En su idioma original**: "Escalating geopolitical tensions and increasingly sophisticated cyberthreats pose significant risks to critical infrastructure, which depends on networks of interconnected devices and legacy systems. The ongoing conflict in Ukraine exemplifies these vulnerabilities, with critical sectors such as energy, telecommunications, water and heating repeatedly targeted by both cyber and physical attacks. These attacks often focus on disrupting control systems and compromising data, highlighting the critical risks associated with operational technology (OT). As cyberthreats continue to evolve, they not only threaten system functionality but also jeopardize human safety, increasing the severity and consequences of disruptions to vital infrastructure".

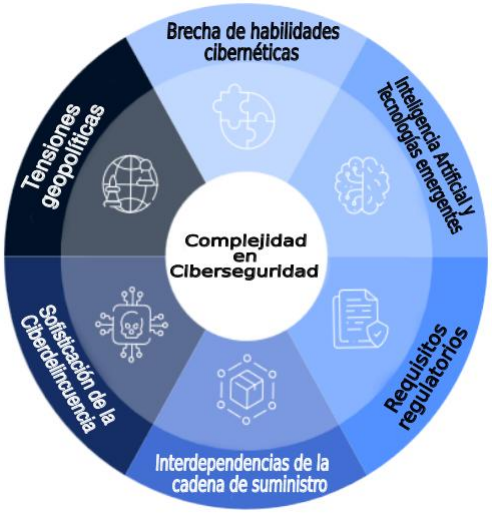

Figura 1: Factores que agravan la complejidad de la ciberseguridad.
Fuente: Elaboración del autor tomado como base World Economic Forum (2025, p. 2).

Valorando estas variables, se considera que el uso desenfrenado de productos tecnológicos profundiza la distancia entre los factores que agravan la complejidad de la ciberseguridad y la posibilidad de establecer un manejo responsable de los mismos (Figura 1). Esto sería un proceso que no ameritaría preocupación si fuera un simple modismo, pero en el caso de las Tecnologías de la Información y las Comunicaciones (TIC) su crecimiento es irreversible al punto de trascender como Digitalidad, generando el caldo de cultivo para conflictos, amenazas, disputas y ambiciones con actores de distinta procedencia. Aquí es preciso indicar que estos escenarios conflictivos son atendidos de forma desestructurada en muchas legislaciones nacionales latinoamericanas, porque separan lo estratégico de lo técnico creando vacíos normativos, apunta Andres (2012):

> La creciente accesibilidad a Internet de secretos, dinero e información industrial crea importantes incentivos para que individuos, grupos y Estados encuentren formas de utilizar cibercapacidades ofensivas. Esta motivación se ve incrementada por el hecho de que la atribución de ataques desde el ciberespacio es a menudo imposible y las leyes y normas internacionales relativas al ciberespionaje, el crimen y la guerra son a menudo débiles o inexistentes (p. 91).[3]

En gran medida los entes decisorios de la región se ven obligados a ceder ante las decisiones de los hegemones tecnológicos, comprometiendo su soberanía, presentándose una coyuntura disruptiva, pudiendo mencionarse: Primero, el uso desmedido de dispositivos o aplicaciones cuyas afectaciones cognitivas se desconocen. Segundo, no existe un equilibrio entre quienes producen (emporios tecnológicos) y quienes consumen (totalidad de la humanidad), lo que coloca en muy pocas manos el control de los elementos constituyentes

[3]**En su idioma original**: "The increasing Internet accessibility of secrets, money, and industry creates significant incentives for individuals, groups, and states to find ways to use offensive cyber capabilities. This motivation is heightened by the fact that attributing attacks from cyberspace is often impossible and the laws and social norms relating to cyberespionage, crime, and warfare are often weak or nonexistent".

de la *Digitalidad*. Tercero, el entrecruzamiento de las amenazas ha tocado a distintos niveles del aparato estatal, lo que ha llevado a respuestas normativas imprecisas, sesgadas o parcializadas por la falta de la Talento Humano capacitado.

Es así como se presenta un cúmulo de aspectos tecno/sociales, engranados para conformar un espectro amenazante, que inicialmente ha sido prefigurado dentro de la Seguridad Informática (no confundir con Seguridad de la Información), sin considerar un elemento clave: la diferencia entre seguridad pública o Defensa de la Nación. Esto no es una discusión semántica, ya que el hecho de atender las amenazas como un "crimen" o un "acto de guerra" cambia radicalmente el foco con que se debería asumir la problemática, explican Kott et al. (2015):

> La ciberseguridad se ha convertido en uno de los principales retos de nuestra sociedad altamente interconectada. Particulares, empresas y gobiernos están cada vez más preocupados por los costes y las amenazas que les imponen la ciberdelincuencia, el ciberespionaje y la ciberguerra. En el ámbito de la ciberdefensa, el conocimiento de la situación es especialmente importante. Se refiere a la ciencia, la tecnología y la práctica de la percepción, la comprensión y la proyección de eventos y entidades en el entorno pertinente, en nuestro caso el ciberespacio. La conciencia situacional es difícil de conseguir en campos como la aviación, la operación de plantas o la gestión de emergencias. Es aún más difícil —y mal comprendido— en el campo relativamente joven de la ciberdefensa, en el que las entidades y los acontecimientos son tan diferentes de los fenómenos físicos más convencionales. (p. 1)[4]

Por lo tanto, el encauzar correctamente los dominios disciplinares de la ciberseguridad y la ciberdefensa no ha sido tarea sencilla, porque los objetivos pueden ser disímiles pero las herramientas son en muchos casos coincidentes. Una muestra de lo anterior puede ser el llamado *malware*, que es utilizado para acciones de delincuencia pero también es central en la *ciberguerra*, este tipo de software malicioso abusa de las vulnerabilidades de programación, desde el 2018 se ha expandido un 151 %, con costes económicos que superan los seis billones de dólares cada año, afectando las infraestructuras críticas por completo o provocando la filtración de datos delicados y disminuyendo la confianza en el proveedor del sistema (Kumar et al., 2020).

Así pues, la categoría del *malware* engloba muchas modalidades, los atacantes informáticos avezados pueden apoyarse en diversidad de tácticas para cubrir sus huellas, como las APT (Amenaza Persistente Avanzada), que puede ser ajustada como estrategia

[4]**En su idioma original**: " Cyber security has emerged as one of the dominant challenges to our highly net- worked society. Individuals, corporations and Governments are increasingly con-cerned about the costs and threats imposed on them by cyber crime, cyber espionage and cyber warfare. Within the field of cyber defense, situational awareness is particularly prominent. It relates to science, technology and practice of perception, comprehension and projection of events and entities in the relevant environment—in our case cyberspace. Situational Awareness is difficult to achieve in such fields as aviation, plant operation or emergency management. It is even more difficult—and poorly understood—in the relatively young field of cyber defense where the entities and events are so unlike the more conventional physical phenomena".

de ataque silente, permaneciendo inactiva en una red durante meses antes de ser detectada, estando en capacidad de dañar la infraestructura crítica de un país (Acquaviva et al., 2017). En ese contexto, la APT ha escalado como una de las amenazas más robustas en materia cibernética, porque integra los mejores elementos para sobrepasar las defensas convencionales y estremecer los cimientos de las estructuras de cualquier Estado, al punto de dejarlo parcialmente controlado o totalmente vulnerable, profundiza Huang y Zhu (2019):

> Con la integración de las redes de comunicación y las tecnologías de la información en las infraestructuras críticas, como las redes eléctricas, los sistemas de transporte y los sistemas de distribución de agua, el uso directo de tecnologías estándar ha hecho que nuestras infraestructuras sean vulnerables a los ciberataques. Una amenaza emergente son las Amenazas Persistentes Avanzadas (APT), que son una clase de procesos de hacking multifase y multietapa, que inician sus infecciones en ciberinfraestructuras, pero que se dirigen a infraestructuras físicas específicas, como centrales nucleares y fábricas automatizadas. A diferencia de los ataques "spray-and-pray", los APT, como los ataques dirigidos, realizan un reconocimiento y adaptan sus técnicas de pirateo al sistema objetivo. (p. 52)[5]

Aquí se evidencia la capacidad destructiva que puede alcanzar el uso estratégico de un software malicioso, que por su intencionalidad sobrepasa las características típicas de un "delito informático", al ser encaminado a la implosión del objetivo atacado y estar direccionado casi siempre por actores estatales. En la literatura especializada, *Stuxnet* es considerado el primer caso públicamente conocido y documentado de una APT de origen estatal, que bajo la premisa de negación y engaño (ciber-*D&D*) violentó a profundidad los sistemas de defensa del adversario, la herramienta en cuestión tenía los elementos propios de un *gusano informático*, analizan Heckman et al. (2015):

> Los beneficios incluían un plan general de campaña de ciber-*D&D* que produjera una recopilación eficaz de inteligencia sobre las capacidades y vulnerabilidades iraníes y que, a su vez, se convirtiera en un arma para explotar los sistemas iraníes. Los servicios de inteligencia proporcionaron información detallada sobre los PLC específicos que debían atacarse, identificaron las defensas y vulnerabilidades de las infraestructuras iraníes de control del enriquecimiento y apoyaron la incorporación de capacidades de *D&D* en *Stuxnet* para evitar su detección por los sistemas defensivos de las ciberdefensas de las infraestructuras iraníes. La inteligencia proporcionó detalles esenciales para las capacidades de engaño (por ejemplo, cegando y suplantando los sistemas de control), mientras que

[5] **En su idioma original**: "With the integration of communication networks and information technologies with the critical infrastructures including power grids, transportation systems, and water distribution systems, the direct use of the off-the-shelf technologies has made our infrastructure vulnerable to cyber attacks. One emerging threat is the Advanced Persistent Threats (APTs) which are a class of multiphase and multistage hacking processes [9], initiating their infections in cyberinfrastructures yet targeting at specific physical infrastructures such as nuclear power stations and automated factories. Unlike the "spray-and-pray" attacks, APTs as the targeted attacks, perform reconnaissance and tailor their hacking techniques to the targeted system".

> las capacidades de *D&D* del software permitieron la recolección encubierta y clandestina en el objetivo durante la campaña. (p. 62)[6]

En vista de lo acotado, el conjunto de consecuencias que trajo *Stuxnet* al programa nuclear iraní lo colocan como un antecedente incuestionable de una *ciberarma* que aunque provino del entorno cibernético produjo secuelas cinéticas. Este tipo de ataques marcan la línea divisoria para que una acción empiece a ser considerada dentro de la Defensa, no pudiendo ser categorizados eventos de tal magnitud exclusivamente como criminalidad digital (aunque también lo son). Lo anteriormente expuesto remite de nuevo al debate de las dificultades de monitorear, regular y resguardarse en el espacio virtual, con el agregado que los daños no se circunscriben a lo intangible, advirtiendo Gutzwiller et al. (2017):

> De hecho, no es fácil controlar el ciberespacio, ni siquiera con los sistemas y la tecnología más avanzados. La ciberdefensa es muy asimétrica, es decir, las ventajas para el atacante son mucho más numerosas que para el defensor. En este caso, debido a que las acciones de los atacantes se producen en medio de un vasto caos de datos, las capacidades y la intención son difíciles de determinar, y mientras que los defensores están bajo constante exposición en la red, confiando en sus pares para tener éxito, los atacantes tienen éxito como lobos solitarios, y sólo necesitan una vulnerabilidad para la victoria. (p. 37)[7]

Por ello, es necesario comprender el panorama amenazante y las dimensiones que involucra, para saber cuál es la lectura estratégica que se debe dar en un entorno tan puntual como la Defensa. Además, en relación con las implicaciones referidas, hay que matizar la temática dentro del entorno nacional, entendiendo que una propuesta de Defensa Cibernética precisa lidiar con el hecho que estamos en una etapa lejana de desarrollo computacional si se compara con los hegemones tecnológicos.

Empero, la necesidad de medidas no puede limitarse a replicar posturas normativas o medidas técnicas recetadas desde los centros detentadores del poder. En efecto, la combinación de la baja concepción estatal más el subdesarrollo de las capacidades digitales de la población son un cóctel letal para mantener subsumida a una región o país bajo el control informático externo, refiriendo Shimonski et al. (2014):

[6] **En su idioma original**: "The benefits included an overall cyber-*D&D* campaign plan that produced effective intelligence collection on Iranian capabilities and vulnerabilities.That plan, in turn, was weaponized to exploit Iranian systems. Intelligence provided detailed information on the specific PLCs to be targeted, identified defenses and vulnerabilities in the Iranian enrichment control infrastructures, and supported incorporation of *D&D* capabilities into Stuxnet to prevent detection by defensive systems in the Iranian infrastructure cyber defenses.Intelligence and *D&D* capabilities supported each other. Intelligence provided essential details for deception capabilities (e.g., blinding and spoofing the control systems), while the *D&D* capabilities of the software enabled covert and clandestine collection on the target during the campaign".

[7] **En su idioma original**: "Indeed, it is no easy matter to control cyberspace, even with state of the art systems and technology. Cyber defense is very asymmetric, meaning, the advantages for the attacker are far more numerous [6] than for the defender. In this case, because attacker actions occur in vast noise in data, capabilities and intent are difficult to determine [7], and while defenders are under constant network exposure, relying on peers to succeed, attackers are successful as lone wolves, and only need one vulnerability for victory".

> Como ya se ha dicho, las amenazas crecen exponencialmente. La matemática es sencilla. A medida que más personas se conectan a la Internet pública a través de un número creciente de dispositivos que incluyen teléfonos móviles, ordenadores portátiles, tecnología portátil y tabletas, el número de posibles víctimas también crece. El vector de ataque también se amplía. Internet, alimentado por los motores de búsqueda, las redes sociales y la capacidad de conservar todo lo que recopila, es la mina de oro de un espía digital cuando realiza labores de reconocimiento. Una de las mayores amenazas actuales en Internet son los motores de búsqueda y las redes sociales. Se puede conocer virtualmente el historial de una persona, lo que le gusta, su ubicación y quiénes son sus amigos y familiares. Se puede saber dónde trabaja. Incluso puedes seguir sus movimientos día a día. Esto nos recuerda que el libro de George Orwell "1984" puede haber llegado [...] [**a 2025**] y que el Gran Hermano está vigilando. (p. 5)[8][Texto en negrita agregado por el autor del presente artículo].

Crear conciencia ciudadana sobre estos entornos amenazantes es básico, se precisa reflexionar sobre escenarios adversos que impliquen el accionar de una APT, es fundamental formar a nuestros servidores públicos sobre los riesgos del software privativo/extranjero para el manejo de información estratégica/gestión de infraestructuras críticas nacionales. En síntesis, es impostergable el apuntalar una propuesta de Defensa Cibernética, porque la preponderancia de lo informático demuestra que el *Gran Hermano* no es una posibilidad sino una realidad, quedará ver si como región o país podemos emular la gesta de Winston Smith (personaje central de la obra 1984) y luchar contra el sometimiento ciber-totalitario que propicia el capitalismo cognitivo.

Construcción fáctica de la defensa cibernética

En correspondencia a lo previo, el crecimiento tecnológico encarnó un desafío inusitado, ya que era imposible asumir una defensa bajo los parámetros del pasado. Estos cambios alteraron las concepciones básicas de la guerra, agregándose el dominio cibernético como otro campo de actuación para la Defensa, pero la falta de recursos tanto materiales como humanos junto a la elevada exigencia técnico-formativa requerida han dificultado la externalización de las capacidades de ciberdefensa (Expósito, 2022). Por tanto, al variar tanto el campo de batalla como el *objetivo estratégico* en el *ciberespacio* se presenta también la necesidad de un cambio generacional del Talento Humano capacitado, que ahora debe pensar y actuar en estos escenarios.

[8]**En su idioma original**: "As mentioned before, threats grow exponentially. The math is simple. As more people connected to the public Internet via a growing number of devices to include mobile phones, laptops, wearable technology, and pads, the number of possible victims also grows. The attack vector also extends. The Internet fueled by search engines, social media, and the ability to retain all that it collects is a digital spy's goldmine when doing reconnaissance work. Considerably, one of the biggest threats today on the Internet is in the form of search engines and social media. You can virtually learn a person's history, what they like, their location, and who their friends and family are. You can learn where they work. You can even track their movement day by day. This isa reminder that George Orwell's book "1984" may indeed have come to[...] and Big Brother is watching".

Por tanto, ante lo diversificado e integral de la amenaza, las teorías y conceptos sobre la Defensa que se venían pregonando durante años debieron pasar fácticamente por una reingeniería profunda. Precisamente, los estados que comprendieron este giro estratégico se enfocaron en el proceso pedagógico para formar a los servidores públicos de los ámbitos civil y militar para que edificaran Políticas Públicas que tocaran el fondo de la problemática, refiere Rutz (2021):

> Téngase en cuenta que todo este proceso que estamos describiendo sobre los recursos humanos necesarios para afrontar el conflicto ciberespacial con el objetivo de conseguir la paz en el ciberespacio, es en definitiva pensar en una política educativa. Dicha política podrá tener diferente lineamiento y alcance según cómo lo piense una Universidad, el Ministerio de Defensa, un sector que represente una o varias Infraestructuras Críticas (sector nuclear, petrolero, bancario o el encargado de satélites, por ejemplo), o bien cada una de las Fuerzas Armadas u otras agencias del Estado que necesiten dichos recursos. (p. 35)

Contrariamente al lento proceder de los organismos burocráticos, que de forma acompasada iniciaban el camino formativo para la capacitación o formación de especialistas para la ciberdefensa, al unísono los disímiles campos que envuelven a la *Digitalidad* daban rienda suelta a nuevas amenazas que se desplegaban vertiginosamente (incluso más peligrosas que las anteriores) y con una maleabilidad que las hacía imposibles de rastrear o controlar, según Cubeiro (2021):

> Nuevas tecnologías, a las que se suele calificar como "emergentes y disruptivas", muchas de ellas muy próximas a su eclosión, van a tener un enorme impacto sobre la Ciberdefensa: Blockchain, BigData, Inteligencia Artificial, computación cuántica, 5G, gemelo digital. Además, a nadie puede escapar que los recursos que habrán de dedicarse a este nuevo entorno de las operaciones militares van a ir progresiva y decididamente en aumento, por lo que, aunque pequeño, se trata de un sector en obligado auge y con claro porvenir. Y, es más, en esta carrera armamentística-tecnológica no debemos quedarnos atrás, pues los países que sí "hagan sus deberes" estarán en clara ventaja respecto al resto en un ámbito operativo que será cada vez más determinante en el devenir de los conflictos. (p. 103)

Hoy día el mayor acceso a las TIC volvió cotidiana e irreversible la penetración informática, pero sin preverse su desbordamiento amenazante, que ha trastocado las percepciones civiles/militares que encuentran un contendiente abstracto, difuso, asimétrico, colocando en una posición dubitativa a los estados a la hora de dar respuesta. Es decir, el volumen y complejidad de un *ciberataque* hace que sea esencial para la mayoría de las entidades el resguardar la información sensible y proteger los activos digitales, entendiendo que la ciberdefensa conlleva a una capacidad de respuesta ante la presencia de una acción agresiva en el ámbito del ciberespacio (Torrijos y Jiménez, 2021). Lo indicado por los autores previos es cierto, pero a la dimensión operativa (capacidad de respuesta) siempre debe estar direccionada por la visión estratégica.

Se debe recalcar que la Defensa Cibernética no es un asunto unidimensional que atañe solo a un ente militar, por el contrario debe atenderse integralmente el fenómeno con la incorporación de todos los actores del Estado. En este sentido, el principal objetivo de cualquier estrategia de ciberseguridad y ciberdefensa será plantear un mando único que coordine las acciones y a los actores involucrados en la lucha contra las amenazas en el ciberespacio, organizando a instancias públicas/privadas, los técnicos, académicos, juristas, sin descuidar la cooperación internacional, en virtud del carácter global de la amenaza (Jaunarena, 2021). Lo orientado por el analista rioplatense es fundamental, solo se puede lograr una postura sólida si se integra al conjunto de actores sociales a la ciberdefensa.

En definitiva, las amenazas informáticas deben dejar de ser abordadas como excentricidades. Actualmente, muchas propuestas de ciberdefensas son comparadas con la *Línea Maginot*, que el ejército alemán simplemente pasó por alto para invadir Francia durante la Segunda Guerra Mundial, con esta analogía se quiere hacer ver que los atacantes tienen toda la libertad de movimiento, mientras que los defensores están atascados o inmóviles (Fink et al., 2014). Parece poco probable que únicamente con un esfuerzo aislado se evite redituar una suerte de *ciber-Línea Maginot*, es necesario que la dinámica ciberespacial se mantenga en constante transformación.

En otras latitudes, se ha avanzado en las percepciones estratégicas, siento interesante evaluar la experiencia europea que empezó a perfilar claramente los ámbitos de la ciberseguridad y la ciberdefensa, al punto que en el año 2020 la Comisión Europea (CE) estipuló la "Estrategia de ciberseguridad de la UE" que discurre sobre cómo aprovechar y reforzar todas las herramientas y recursos para ser tecnológicamente soberana, asomando la cooperación en materia de ciberdefensa con socios como la Organización del Tratado del Atlántico Norte (OTAN). En el continente americano en 2018, se realizó la conferencia "Ciberdefensa en las Américas: Importancia del Ciberespacio como Campo de Batalla del Siglo XXI", actividad auspiciada por la Junta Interamericana de Defensa (JID), esgrimiéndose que solo diez países del continente contaban con una Estrategia Cibernética, concluyendo que para impulsar este tipo de medidas es esencial la colaboración interna (Fuerza Armada, Gobierno e iniciativa privada) junto a la promoción de acciones Inter-Estatales. Estas conferencias son importantes, pero claramente la disgregación política continental y la sombra de control hegemónico hacen que las perspectivas de desarrollo estratégico sean limitadas.

Siguiendo la línea precitada, en distintos documentos difundidos por la Comisión Económica para América Latina y el Caribe (CEPAL) se reitera que es ineludible el fortalecer la agenda en ciberdefensa de las instituciones regionales, siendo lo apropiado una estrategia colaborativa entre el conjunto de las naciones, considerando que el monitoreo permanente de la actividad cibernética regional facilitaría las alertas tempranas para evitar ciberataques, recomendándose la creación de una red regional (R. Díaz, 2014). Una muestra de lo sugerido por el autor previo, se puede percibir en la resolución 2341 del Consejo de Seguridad de la Organización de las Naciones Unidas (ONU), que sobre el uso indebido de las TIC exhorta a los estados miembros al establecimiento o reforzamiento de las alianzas

nacionales, regionales e internacionales a fin de prevenir, proteger, mitigar e investigar las afectaciones ocasionadas por atentados contra instalaciones de infraestructura vital, así como para responder y recuperarse de ellos mediante acciones conjuntas (ONU, 2017).

De hecho, regionalmente con la creación del Consejo de Defensa Sudamericano (CDS) en 2009, se dieron señales de estar avanzándose en la adopción de políticas comunes para entablar una estrategia conjunta hacia las ciberamenazas, quedando establecido en su *Plan de Acción 2012*, dentro del punto 1.f la: "Conformación de un Grupo de Trabajo para evaluar la factibilidad de establecer políticas y mecanismos regionales para hacer frente a las amenazas cibernéticas o informáticas en el ámbito de la defensa" (CDS, 2012, p. 1)[9]. Otra instancia que ha intentado mantener un tratamiento al respecto es el MERCOSUR (Mercado Común del Sur), que por intermedio del Consejo del Mercado Común (CMC) decidió crear la Reunión de Autoridades sobre Privacidad y Seguridad de la Información e Infraestructura Tecnológica (RAPRISIT), como órgano auxiliar del prenombrado consejo. Justamente, en el año 2015 el autor de este artículo participó como parte del grupo de expertos que asesoraba a la delegación venezolana en la RAPRISIT, siendo complejo el acordar una conceptualización que integrara las particularidades normativas de cada país miembro sobre elementos vinculados a la Seguridad de la Información.

Sin duda, el escenario ideal es un entorno de colaboración, coordinación y respeto planetario, empero como se referenciaba en la aparte inicial del artículo las tensiones geopolíticas contemporáneas hacen ver que en el ámbito de la ciberdefensa el futuro será de conflicto y no de convivencia pacífica. Es urgente, retomar o mantener (según sea el caso) iniciativas como las promovidas por la Unión de Naciones Suramericanas (UNASUR) y el MERCOSUR, que permitan plantear una visión estratégica que no esté amarrada ni a las diatribas políticas regionales ni a las incidencias hegemónicas continentales y así logar evadir los rasgos que ralentizan un trabajo articulado:

> La ciberdefensa cooperativa ha sido reconocida como una estrategia esencial para luchar contra los ciberataques. Compartir información sobre ciberseguridad entre varias organizaciones y aprovechar la información cibernética acumulada para construir un sistema proactivo de ciberdefensa, no es tarea fácil para las organizaciones. Sin embargo, la construcción de este sistema de ciberdefensa se enfrenta a dos retos: (1) las organizaciones son reacias a compartir su información privada con otras, (2) incluso cuando se ponen de acuerdo sobre una solución en la que la información puede ser compartida de manera que se preserve la privacidad, la información de ciberamenazas difusas tiene que ser procesada para construir el modelo de predicción de futuros incidentes cibernéticos nuevos o desconocidos.(Badsha et al., 2019, p. 708)[10]

[9]**Nota del autor:** Durante el período 2012-2014 el autor de este artículo realizó un estudio de las Políticas Regionales sobre Ataques informáticos y su Incidencia en la vulnerabilidad de la Defensa de la UNASUR que contó con interacciones investigativas con personal del Centro de Estudios Estratégicos de Defensa de la UNASUR y de la delegación venezolana ante esa instancia. Puede ser consultado en: https://repositorio.iaen.edu.ec

[10]**En su idioma original:** "The Cooperative Cyber-defense has been recognized as an essential strategy

De lo esgrimido, se van diagnosticando nudos fácticos para hacer una construcción conceptual de la Defensa Cibernética. Junto con hacer converger posturas inter/multi/trans-disciplinares, se requiere entre otros aspectos el definir lo que es la amplitud de la amenaza propiamente dicha desde el ámbito jurídico, ya que ahí se encuentra uno de los mayores vacíos, porque un ataque a un Estado o actuaciones en perjuicio del mismo, implican el uso de "nuevas armas" informáticas, surgiendo la duda acerca de la aplicabilidad del derecho existente a estas nuevas situaciones internacionales, especialmente debido a las singulares características del ciberespacio y las ciberarmas (Pérez, 2021).

En ese sentido, cuando se insiste que es un asunto estratégico, que debería responder a una Política Pública se refiere a ese carácter in extenso. Entonces, la Defensa Cibernética es una tarea central del gobierno, debiendo articular a las organizaciones civiles y militares en el marco del derecho internacional aplicado al ciberespacio (Pérez, 2016). Lo aludido evidencia lo impostergable de realizar una conceptualización temática, que incluya la cantidad de variables, factores, ámbitos y actores involucrados, que incidirán en el entramado jurídico, administrativo, técnico que debe adecuarse al panorama de las amenazas que cambian rápidamente.

Partiendo de Grobler et al. (2016) que se apoyan en las ideas de Wilson (2007), se puede decir que al introducir lo cibernético en la estructura de Defensa, entran en juego una serie de aspectos nuevos que pueden influir en la forma en que se analizan los ataques cibernéticos: nuevas visiones de política de seguridad nacional; consideración de las operaciones psicológicas que pudieran afectar a civiles inocentes; posibles acusaciones contra el Estado por crímenes de guerra por interrupción de los sistemas informáticos críticos; y la responsabilidad del Estado por los actos ilícitos dentro de un país.

Como se puede ver, la ciberdefensa al ser un asunto estatal debería responder a categorías jurídicas que precisen sus competencias, obligaciones, responsabilidades y límites. Aunque ciertamente este es el deber ser, los hegemones informáticos actúan de forma irrestricta, con un total irrespeto al Derecho Internacional y las normas internas de los estados que no tienen los mecanismos para defenderse.

Del mismo modo que lo legal es inapelable, lo administrativo/presupuestario es obligatorio para concebir cuán lejos se puede llegar en la organización de la ciberdefensa, concuerdan Carayannis et al. (2016) que: "Debe aclararse el coste fiscal de la ayuda prevista, así como sus resultados. También debe mostrarse su estudio de viabilidad y rentabilidad" (p. 309)[11]. Conforme a lo afirmado por el catedrático heleno, estos elementos deben manejarse

to fight against cyberattacks. Cyber-security information sharing among various organizations and leveraging the aggregated cyber information to build proactive cyber defense systems is nontrivial for organizations. However,building such cyber defense system is challenged by two issues: (1) organizations are reluctant to share their private information to others (2) even when they agree on a solution where information can be shared in privacy preserving manner, the obfuscated cyberthreat information has to be processed to build the trained model for future prediction of any new or unknown cyber incident".

[11] **En su idioma original:** "It's fiscal cost of envisioned support should be clarified as are its outcomes. Its feasibility and profitability study should also be shown".

con mucha cautela, particularmente lo referido a la rentabilidad y coste fiscal. Es necesario aclarar que en materia de Defensa es muy relativo establecer la rentabilidad y limitar las inversiones de acuerdo al coste fiscal, debido a que un Estado requiere garantizar su supervivencia, ya que ante su extinción de nada le serviría el ahorro fiscal[12].

No obstante, el desarrollo de un pensamiento estratégico coadyuvará a la viabilidad, pero no puede garantizarla del todo (por lo difuso de la amenaza) y difícilmente puede establecer un criterio de rentabilidad, ya que un sistema de Defensa Cibernética amerita de profesionales capacitados, equipos óptimos e infraestructuras íntegras que requieren asignaciones presupuestarias de peso para mejorar las condiciones con las que se enfrentarán las amenazas.

De tal manera, lo presupuestario es un aspecto que al final marcará la diferencia entre las naciones que tienen el control del ciberespacio y las que son dominadas. Sin los recursos suficientes, no se cubrirán en gran medida las categorías operativas, aprecia Herring y Willett (2014):

> La defensa cibernética incluye tres categorías complementarias: "proactiva", "activa" y "regenerativa". Las actividades "proactivas" fortalecen el entorno cibernético y mantienen la máxima eficiencia para la ciberinfraestructura y las funciones de la misión. Las actividades "activas" detienen o limitan el daño de la actividad cibernética del adversario en el tiempo cibernético relevante. Las actividades "regenerativas" restauran la eficacia o la eficiencia de la misión después de un ciberataque exitoso. Estas categorías forman un continuo de actividades de seguridad cibernética que ocurren de manera continua y simultánea en las redes, integradas por un marco común de automatización que incluye la defensa cibernética activa (ACD) como un subconjunto de la defensa cibernética integrada. (p.p. 46 - 47)[13]

Cuando se dice que con asignaciones presupuestarias de relevancia se cubrirían las categorías complementarias, no se puede dejar de enunciar pilares que no son operativos sino que forman parte de la constitución del pensamiento nacional en Defensa Cibernética como: la investigación estratégica y el desarrollo de tecnología propia, en ambos casos serán el núcleo para que se fortalezca la triada: "proactiva", "activa" y "regenerativa".

[12] **Nota del Autor:** indicaba el poeta George Byron:"Apenas son suficientes mil años para formar un Estado; pero puede bastar una hora para reducirlo a polvo"(p. 423).

[13] **En su idioma original:** "Cyber defense includes three complementary categories: "proactive", "active", and "regenerative". "Proactive" activities harden the cyber environment and maintain peak efficiency for cyberinfrastructure and mission functions. "Active" activities stop or limit the damage from adversary cyber activity in cyber-relevant time. "Regenerative" activities restore mission effectiveness or efficiency after a successful cyber attack. These categories form a continuum of cyber-security activities occurring continuously and simultaneously on networks, integrated by a common framework of automation that includes Active Cyber Defense (ACD) as a subset of integrated cyber defense".

Teorización estratégica sobre la defensa cibernética de la Nación

Para elaborar un planteamiento nacional sólido en materia de ciberdefensa, es fundamental reiterar que lo estratégico debe primar indiscutiblemente sobre lo técnico. Resulta un sinsentido, el emprender acciones operativas o invertir en capacidades tecnológicas si previamente no existe una claridad de los objetivos que se persiguen, los cuales deben estar alineados de forma inequívoca con los fines superiores del Estado. Esta prelación garantiza que los recursos tecnológicos respondan a una visión integral para la Seguridad de la Nación. Sin esta orientación, se corre el riesgo de una fragmentación estratégica.

Entonces, aunque unas capacidades técnicas sólidas son necesarias para una ciberdefensa eficaz (aunque no son suficientes), las buenas tecnologías no sirven de mucho sin estrategias adecuadas para su empleo; de forma inversa, el desconocer las estrategias que debemos emplear para la defensa, nos limitará la comprensión plena de las tecnologías necesarias para aplicarlas estratégicamente (Herring y Willett, 1999). Por tanto, para establecer una estrategia en ciberdefensa que atienda estructuralmente el escenario problemático, un paso esencial es determinar:

- ¿Cómo enfrentar la vulnerabilidad?
- ¿Cuáles son los escenarios amenazantes?
- ¿Qué riesgos están latentes?
- ¿Dónde se perfila el peligro?

Para dar respuestas a estas preguntas es pertinente contextualizar la base problemática de ese entramado: vulnerabilidad/amenaza/riesgo/peligro, evaluando el nivel de inmersión en la Digitalidad de la población venezolana. Por ello, es importante hacer mención de la distribución de los suscriptores del servicio de la Internet por tipo de abonado al IV trimestre de 2024, aportada por la Comisión Nacional de Telecomunicaciones de Venezuela (CONATEL, 2024), que estima en 25.200.760 suscriptores de la Internet (incluidos los que acceden a datos por la red de telefonía móvil), como se muestra la Figura 2:

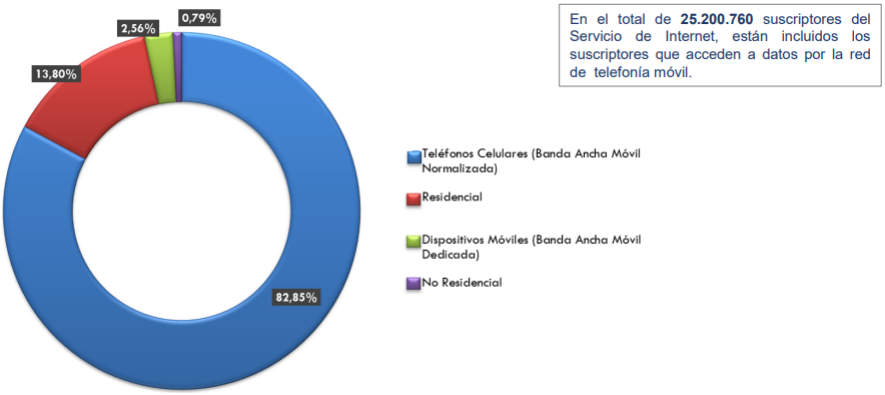

Figura 2: Internet por tipo de abonado al IV trimestre de 2024.
Fuente: CONATEL (2024).

Esto refleja la necesidad de una Política Pública sobre Defensa Cibernética venezolana, porque la cantidad de usuarios activos de la internet en nuestro país debe superar la cifra de suscriptores, probablemente rebasa los treinta millones (La diferencia radica en el hecho que en una suscripción pueden haber varios usuarios). Con un porcentaje poblacional tan alto utilizando tecnologías privativas y extranjeras la vulnerabilidad es impactante a nivel público y privado. Por otra parte, la realidad política de las últimas dos décadas ha colocado a Venezuela en el centro de las mayores confrontaciones regionales tras el fin de la Guerra Fría, siendo reiterados los desencuentros con el hegemón continental, lo que reviste una amenaza sustancial en el ámbito de la Defensa Cibernética, detallando Leetaru (2019) en un informe digital para la revista Forbes:

> En el caso de Venezuela, la idea de que un gobierno como los Estados Unidos interfiera remotamente con su red eléctrica es bastante realista. Las operaciones cibernéticas remotas rara vez requieren una presencia terrestre significativa, lo que las convierte en una operación de influencia idealmente negable. Dada la preocupación de larga data del gobierno estadounidense con el gobierno de Venezuela, es probable que Estados Unidos ya mantenga una presencia profunda dentro de las redes de la infraestructura nacional del país, por lo que es relativamente sencillo interferir con las operaciones de la red.[14]

Tomando como referencia lo explicado por el académico norteamericano, sumado a lo indicado previamente sobre el uso de APT por distintos tipos de actores y la importante expansión digital que hay en la sociedad venezolana, entonces lo informático configura una escena altamente riesgosa. Es fundamental el acelerar la conformación de un equipo inter/multi/trans-disciplinario que reflexione, analice y proponga medidas a corto, mediano y largo plazo sobre los peligros cibernéticos para el Estado venezolano. Como el escenario problemático no va a esperar a que se consolide el marco nacional, hay que en paralelo recorrer varias rutas, pero la más sustancial es madurar una idea venezolana sobre la ciberdefensa, ya que partiendo de esto se afinarán las dimensiones legales, operativas y administrativas.

Es importante destacar que en el caso nacional, la estructuración de la Dirección Conjunta de Seguridad Informática (DICOCEI) de la Fuerza Armada Nacional Bolivariana (FANB) por medio de la Resolución N° 007778 (Ministerio del Poder Popular para la Defensa, 2014) fue un primer paso para atender el problema. Antes de esta resolución ministerial no existían antecedentes normativos que hicieran mención al asunto. No obstante, tras la revisión documental de dicha resolución, se percibe que en lo relativo a la creación y activación de la DICOCEI la información es escasa, contando solo con dos artículos, detallando el primero que estará organizado por una dirección; una división de

[14] **En su idioma original:** "In the case of Venezuela, the idea of a government like the United States remotely interfering with its power grid is actually quite realistic. Remote cyber operations rarely require a significant ground presence, making them the ideal deniable influence operation. Given the U.S. government's longstanding concern with Venezuela's government, it is likely that the U.S. already maintains a deep presence within the country's national infrastructure grid, making it relatively straightforward to interfere with grid operations".

Ciber-Seguridad; una división de Ciber-Defensa; y una división de Sistemas y Tecnologías de Información. En su segundo apartado, se determina que será: "[...] el Órgano Rector en materia de CIBER-SEGURIDAD y CIBER-DEFENSA" (p. 63). Esta resolución aglutinaba dos áreas que deben ser atendidas de forma diferente aunque se vinculan (CIBER-SEGURIDAD y CIBER-DEFENSA). El combinar estas dimensiones puede afectar el objetivo y la visión estratégica, sumado al hecho que nació como un espacio circunscrito a lo militar, cuando debería ser una instancia de articulación más integradora.

Transcurrido un año, la DICOCEI daría paso a la Dirección Conjunta de Ciberdefensa (DICOCIBER) de la FANB, adscrita al Comando Estratégico Operacional, según Resolución N° 009723 (Ministerio del Poder Popular para la Defensa, 2015). Al igual que el instrumento que antecedió solo refleja dos artículos, describiendo el primero la estructura organizativa, que estará compuesta por:

- Director Conjunto;
- Sub-Director Conjunto;
- Gestión Administrativa;
- División de Operaciones Ciberdefensa;
- División de Gestión de Seguridad Informática;
- División de Investigación y Desarrollo;
- División de Redes Sociales.

Llama la atención tres aspectos diferenciados en relación a su antecesor (DICOCEI): 1. La inclinación operativa que asume; 2. Se marca distancia con el término Ciber-Seguridad; y 3. Acertadamente se promueve la investigación y desarrollo. Además, en su numeral segundo se detalla que "[...] será el Órgano Rector y Representante en materia de CIBERDEFENSA en la Fuerza Armada Nacional Bolivariana" (p. 4). En la investigación documental efectuada en distintas fuentes informáticas, se accedió a la web oficial del Comando Estratégico Operacional, observándose que en el enlace de las *Direcciones Conjuntas* (Figura 3) se hace mención a la DICOCIBER. Igualmente se pudo revisar distintas redes sociales públicas que son gestionadas por la División de Redes Sociales, que sin embargo no tienen mayor información sobre la gestión en ciberdefensa.[15]

[15]**Nota del autor:** hay que hacer la salvedad que en la web oficial de la Aviación Militar Bolivariana (AMB) se detalla un organigrama institucional, pudiendo ingresarse a un enlace que describe el Alto Mando, donde se encuentra la Dirección de Tecnología, ahí se puede apreciar la existencia de una Dirección de Ciberdefensa que tiene determinadas su misión, funciones y organización. Este constituye un buen modelo operativo/táctico por su estructura: Centro de Monitoreo y Detección; División de Guerra Cibernética; División de Guerra de Información; División de Seguridad Informática; y División de Régimen Especial de Seguridad. Asimismo, hay que destacar que en agosto de 2025 el Ejecutivo Nacional aprobó la creación de la Dirección de Ciberdefensa de la Guardia Nacional Bolivariana (GNB).

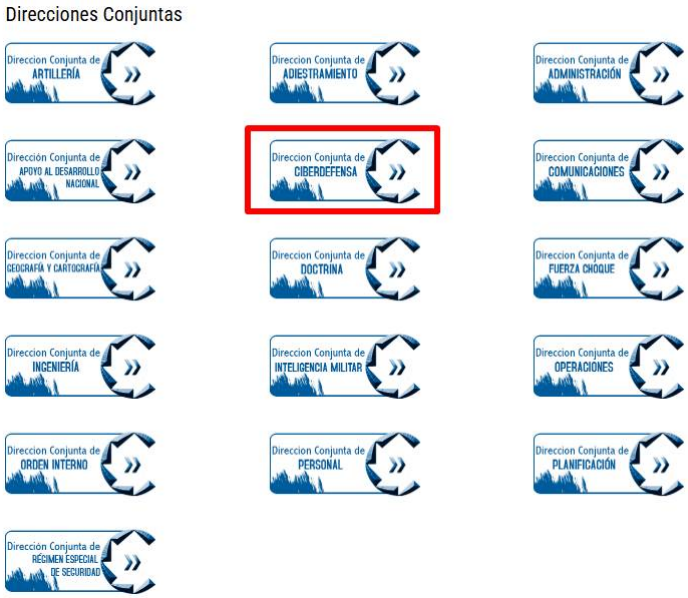

Figura 3: Direcciones Conjuntas del CEOFANB.
Fuente: CEOFANB (2025).

Como se ha referido ampliamente, el hecho que un tema se relacione a la Defensa no debe excluirlo del debate público, por el contrario la intervención de todos los sectores de la vida nacional daría un salto cualitativo a cualquier propuesta sobre ciberdefensa. En una importante investigación gestionada por K. Díaz y Zavarce (2020) sobre una propuesta de un Modelo de Organización Cibernética del Comando Cibernético Nacional, esgrimen lo siguiente:

> Lo señalado hasta aquí evidencia que no existe "salud organizacional" en las instituciones estatales dedicadas al tema de la ciberseguridad y ciberdefensa (llámese comandos, entes, organismos, consejos y comisiones) al no contarse con atributos claves como alineación estratégica, calidad en la ejecución y capacidad de renovación requeridos para minimizar situaciones organizacionales signadas por procesos burocráticos con señales de ineficiencia en el manejo de los talentos, infraestructuras y recursos disponibles, lo cual genera poca capacidad de adaptación ante las amenazas que provienen de un contexto interno y externo cada vez más politizado y radicalizado. (p. 24)

Lo planteado por los autores anteriores sobre la "salud organizacional" también ha sido observado en este artículo, que desde una visión crítica abre el espacio para presentar alternativas al respecto. Aunque con la DICOCIBER se consiguió posicionar abiertamente la temática, aún adolece el Estado venezolano de un concepto público sobre la Defensa Cibernética de la Nación, siendo oportuno generar nuestras propias teorizaciones. Asimismo, se deben sustentar los cambios en las experiencias históricas, revisando permanentemente las fortalezas o debilidades de esas estrategias y tácticas Saydjari (2021). Es decir, hay que poner en una balanza las fortalezas y carencias para poder fundamentar una propuesta de

Defensa Cibernética de la Nación que no se quede solo en una definición teórica, sino que coadyuve a los cambios que amerita el Estado.

Un aspecto interesante para analizar en el contexto que se está estudiando, es la reciente creación del Consejo Nacional de Ciberseguridad (CNC), conforme al Decreto N° 4.975 del 12 de agosto de 2024 emanado de la Presidencia de la República, publicado en Gaceta Oficial N.° 42.939. Si bien, como se explicó previamente la ciberseguridad y la ciberdefensa son ámbitos diferentes, no deja de ser una iniciativa importante desde el plano estratégico el CNC, indicando el artículo 2, que sus funciones son las siguientes:

1. Asesorar al Presidente de la República Bolivariana de Venezuela y al Consejo de Defensa de la Nación en la elaboración de la política nacional de ciberseguridad que contenga los planes y programas de seguridad informática, vigilancia tecnológica, supervisión y control de incidentes telemáticos.

2. Elevar propuestas de regulaciones, leyes y o reglamentos en materia de prevención de uso de las tecnologías de información y comunicación con fines delictivos.

3. Verificar el grado de cumplimiento de la implementación de los planes y regulaciones adoptados en materia de ciberseguridad.

4. Formular propuestas y recomendaciones sobre la política de ciberseguridad, en armonía con los intereses y objetivos de la Nación para garantizar los fines supremos del Estado.

5. Realizar la valoración continua de riesgos y amenazas en materia de seguridad informática.

6. Impulsar la constitución de una red de vigilancia durante 24 horas de incidentes telemáticos, afiliada a los pares regionales para prevenir, mitigar y/o controlar los delitos informáticos transfronterizos, de conformidad con el artículo 41 del documento de Naciones Unidas para la prevención del ciberdelito.

7. Constituir Comités de Trabajo Interinstitucionales y de Emergencia, para la atención y prevención del uso de las tecnologías de información y comunicación con fines delictivos.

8. Requerir de las personas naturales o jurídicas de carácter público y privado los datos, estadísticas e informaciones relacionados con la seguridad informática de la Nación, así como su necesario apoyo.

9. Impulsar programas de capacitación en materia de ciberseguridad con instituciones educativas, centros de investigación y entidades públicas y privadas.

10. Fomentar la formación de equipos multidisciplinarios especializados en ciberseguridad del sector público y privado.

11. Promover las inversiones necesarias para el fortalecimiento de la plataforma telemática del Estado.

12. Dictar el reglamento para su organización y funcionamiento.

13. Otras que sean decididas en el seno del Consejo, al menos por las dos terceras partes de sus miembros permanentes. (p. 2)

Tomando en cuenta que según el numeral primero el CNC asesorará al Consejo de Defensa de la Nación y que según el artículo tercero el Ministerio del Poder Popular para la Defensa forma parte del mismo, es probable que asuma algunas competencias en ciberdefensa, aunque dicha palabra no se menciona en la referida gaceta.

Tras lo visto hasta ahora, sería pertinente para el Estado venezolano la creación de una Comisión Presidencial para la Defensa Cibernética de la Nación que podría ser el punto de conexión entre el CNC y el DICOCIBER. Esta comisión debería a posteriori constituirse en un Consejo Nacional de Ciberdefensa (CND), compuesto por un equipo inter/multi/trans-disciplinar que debata y consolide nuestro concepción estratégica de Ciberdefensa. Una referencia que podría ser valorada para un futuro CND sería el modelo finlandés, que ha erigido un relacionamiento civil/militar que fortalece la Defensa Cibernética sin necesidad de ser una potencia militar de primer orden, se detalla en el portal de diseño tecnológico Huld (2025) lo siguiente:

> Varias empresas de la industria de defensa operan actualmente en Finlandia, y somos reconocidos internacionalmente por nuestra experiencia en ingeniería altamente cualificada. Los aspectos éticos de la inversión en el sector de defensa se han debatido durante mucho tiempo, pero la actitud ha cambiado en los últimos años. El ascenso de Finlandia como centro de la tecnología de defensa nórdica también ha atraído a inversores internacionales.
>
> El desarrollo de la tecnología de defensa no solo abarca los sistemas tradicionales, sino también la tecnología de software avanzada, cuyas posibilidades de aplicación están en expansión.
>
> El papel de la inteligencia artificial y la ciberseguridad en el desarrollo de la tecnología de defensa también ha aumentado significativamente. A medida que los sistemas se digitalizan y la comunicación entre dispositivos aumenta, la ciberseguridad se ha convertido en un componente fundamental de la estrategia de defensa. La inteligencia artificial, por otro lado, permite una organización más eficiente de la defensa y el análisis de datos, lo que crea nuevos tipos de soluciones de seguridad. La cooperación entre el estado, los institutos de investigación y las empresas que operan en la industria de defensa crea las condiciones para una sociedad aún más segura. El desarrollo de la tecnología de defensa forma parte de un ecosistema de seguridad más amplio que incluye, por ejemplo, la ciberseguridad, la tecnología de inteligencia y la gestión de crisis.[16]

[16] **En su idioma original:** "Several defense industry companies are currently operating in Finland, and we are internationally recognized for our highly skilled engineering expertise. The ethical aspects of

Esta referencia al modelo finlandés busca mostrar que un alto nivel estratégico en temas de Defensa Cibernética pasa por integrar a todos los actores. Es perfectamente comprensible y aceptable que los aspectos operativos/tácticos, las capacidades técnicas específicas, los protocolos de respuesta a incidentes o los métodos de inteligencia, deban permanecer en el ámbito de la reserva para no comprometer la Seguridad de la Nación.

Propuesta y reflexiones finales

La construcción y consolidación de una estrategia nacional de ciberdefensa debería culminar en una Política Pública sólida y perdurable, no puede gestarse bajo una percepción unívoca. Entonces, es imperioso un diálogo estratégico que permite identificar vulnerabilidades críticas, anticipar amenazas complejas y alinear los objetivos de seguridad con los preceptos constitucionales.

En un estudio encabezado por Kott et al. (2015), se proponen cinco funciones principales para establecer un marco eficaz de ciberdefensa, si bien tienen una inclinación hacia lo técnico/operativo este papel de trabajo es importante para coadyuvar a fundamentar una percepción nacional. Por tanto, se toman referencialmente las ideas de estos autores pero ajustándolas y ampliándolas al contexto venezolano:

1. **Fortalecerse de los ataques:** aprender de las acciones reales que han afectado al Estado venezolano.
2. **Priorización:** plantear medidas viables dentro de la realidad venezolana que conduzcan a la mayor reducción de riesgos y protección contra los actores amenazantes.
3. **Normalización:** homologar un lenguaje compartido para investigadores, especialistas en TIC, auditores y funcionarios de seguridad que estén involucrados en áreas conexas a la ciberdefensa nacional.
4. **Diagnóstico y mitigación:** medición permanente para probar y validar la eficacia de las medidas actuales y previsualizar los próximos pasos.
5. **Prospectiva:** potenciar la investigación inter/multi/trans-disciplinar que permita la valoración de los escenarios futuros y trace las estrategias estatales para aminorar las vulnerabilidades, determinar las amenazas, evaluar los riesgos y prepararse para los peligros.

investing in the defense sector have been debated for a long time, but attitudes have changed in recent years. Finland's rise to the center of Nordic defense technology has also attracted international investors. The development of defense technology does not only concern traditional systems, but also advanced software technology, the application possibilities of which are expanding. The role of artificial intelligence and cyber security in the development of defense technology has also increased significantly. As systems become more digital and communication between devices increases, cybersecurity has become a critical part of defense strategy. Artificial intelligence, on the other hand, enables more efficient organization of defense and data analysis, which creates new types of security solutions. Cooperation between the state, research institutes and companies operating in the defense industry creates the conditions for an even safer society. The development of defense technology is part of a broader security ecosystem that includes, for example, cyber security, intelligence technology and crisis management".

Para conducir estratégicamente los cinco procesos que se explicaron previamente, se debe construir desde los preceptos de la Constitución de la República Bolivariana de Venezuela (CRBV) lo que doctrinalmente es para el Estado venezolano: la Defensa Cibernética. Precisamente, partiendo del artículo 322 de la Carta Magna se aporta una definición adaptada a la realidad venezolana, conceptualizándose de la siguiente manera (Asamblea Nacional, 2009):

> La Defensa Cibernética de la Nación es competencia esencial y responsabilidad del Estado, fundamentada en la comprensión estratégica de la Digitalidad para propender a la Defensa Integral, la protección corresponsable, el análisis prospectivo, la formación investigativa crítica y el desarrollo científico/tecnológico libre que permitan superar las vulnerabilidades y garanticen la soberanía venezolana ante las amenazas, riesgos o peligros vinculados a acciones de actores estatales o individuales mediante el uso de tecnologías disruptivas o emergentes en el espacio cibernético o entornos artificiales que pueden causar consecuencias cinéticas o afectaciones intangibles al Estado venezolano o sus ciudadanos.

Esta propuesta nace del estudio pormenorizado sobre el tema a lo largo de los años[17], pero es necesario que el concepto de Defensa Cibernética venezolano sea valorado, enriquecido y complementado en un debate abierto, que se nutra de actores civiles, militares, públicos y privados. Como se ha señalado en múltiples ocasiones, la naturaleza sensible de los asuntos vinculados a la Defensa Nacional no significa que deben quedar abstraídos de la consulta a todos los sectores. De hecho, la inclusión activa de todos los actores de la sociedad representaría un salto cualitativo fundamental en la formulación de cualquier iniciativa en materia de ciberdefensa.

Referencias

Acquaviva, J., Mahon, M., Einfalt, B., y LaPorta, T. (2017). *Optimal cyber-defense strategies for advanced persistent threats: a game theoretical analysis*. IEEE. https://ieeexplore.ieee.org/abstract/document/8069083

Andres, R. (2012). *The emerging structure of strategic cyber offense, cyber defense, and cyber deterrence*. Georgetown University Press. https://www.researchgate.net/profile/Richard-Andres-2/publication/292126434_The_Emerging_Structure_of_Strategic_Cyber_Offense_Cyber_Defense_and_CyberDeterrence/links/58a0f881aca272046aad638d/The-Emerging-Structure-of-Strategic-Cyber-Offense-Cyber-Defense-and-Cyber-Deterrence.pdf

[17] **Nota del autor:** hay que indicar que el contenido del presente artículo tomó como base los estudios doctorales del autor. Asimismo, parte de los contenidos de esa investigación sirvieron de referencia tanto para la estructuración del Curso de Ciberseguridad como la edificación de tres de sus módulos, que pueden ser visualizado en la plataforma formativa "Toparquía" de CENDITEL: https://cursos.cenditel.gob.ve/toparquia/curso-ciberseguridad.

Asamblea Nacional. (2009). *Constitución de la República Bolivariana de Venezuela*. Gaceta Oficial de la República Bolivariana de Venezuela N°5.908 Extraordinario. https://www.asambleanacional.gob.ve/storage/documentos/leyes/constituci-20220316143116.pdf

Badsha, S., Vakilinia, I., y Sengupta, S. (2019). *Privacy preserving cyber threat information sharing and learning for cyber defense*. IEEE. https://ieeexplore.ieee.org/abstract/document/8666477

Carayannis, E., Campbell, D., y Panagiotis, M. (2016). *Cyber-development, Cyber-democracy and Cyber-defense*. Springer-Verlag.

CDS. (2012). *Plan de Acción 2012*. UNASUR.

CEOFANB. (2025). *Direcciones Conjuntas*. https://ceofanb.mil.ve/direcciones-conjuntas-2

CONATEL. (2024). Servicio de Internet. IV Trimestre 2024. *Cifras del Sector de Telecomunicaciones*. https://conatel.gob.ve/wp-content/uploads/2025/08/Presentacion_Internet_IV-2024.pdf

Cubeiro, E. (2021). Ciberdefensa e I+D+i: el Ciberespacio y las operaciones militares. *Revista Ciberseguridad, seguridad de la información y privacidad*, (145), 102-104. https://revistasic.es/sic145/revistasic145.pdf

Díaz, K., y Zavarce, C. (2020). *Modelo de Organización Cibernética del Comando Cibernético Nacional*. Fondo Editorial Ediciones Oncti. https://www.oncti.gob.ve/wp-content/uploads/2022/04/LibroDigital.Modelo-organizacional-20-11-2020.pdf

Díaz, R. (2014). *Estado de la ciberseguridad en la logística de América Latina y el Caribe*. CEPAL. https://repositorio.cepal.org/bitstream/handle/11362/47240/1/S2100485_es.pdf

Expósito, J. (2022). La externalización de la ciberdefensa: Viabilidad y eficiencia de la externalización de competencias propias de las fuerzas armadas. *Revista Ejército*, (971), 38-44. https://ejercito.defensa.gob.es/Galerias/multimedia/revista-ejercito/2022/971/accesible/Revista_Ejercito_971_marzo_2022.pdf

Fink, G., Haack, J., McKinnon, A., y Fulp, E. (2014). Defense on the move: ant-based cyber defense. *IEEE Security y Privacy*, *12*(2), 36-43. https://ieeexplore.ieee.org/abstract/document/6798536/

Grobler, M., Jansen van Vuuren, J., y Zaaiman, J. (2016). Preparing South Africa for cyber crime and cyber defense. *Journal of Systemics, Cybernetics and Informatics*, *11*(7), 32-41. https://researchspace.csir.co.za/items/df536132-0af2-408b-a915-90bfb8c9ae08

Gutzwiller, R., Hunt, S., y Lange, S. (2017). *A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts*. IEEE. https://ieeexplore.ieee.org/abstract/document/7497780

Heckman, K., Stech, F., Thomas, R., Schmoker, B., y Tsow, A. (2015). *Cyber denial, deception and counter deception*. Springer. https://doi.org/10.1007/978-3-319-25133-2

Herring, M., y Willett, K. (1999). A concept for strategic cyber defense. *IEEE Military Communications. Conference Proceedings (Cat. No. 99CH36341)*, *1*, 458-463. https://ieeexplore.ieee.org/abstract/document/822725

Herring, M., y Willett, K. (2014). Active cyber defense: a vision for real-time cyber defense. *Journal of Information Warfare*, *13*(2), 46-55. https://www.jstor.org/stable/26487121

Huang, L., y Zhu, Q. (2019). Adaptive strategic cyber defense for advanced persistent threats in critical infrastructure networks. *ACM SIGMETRICS Performance Evaluation Review*, *46*(2), 467-488. https://dl.acm.org/doi/abs/10.1145/3305218.3305239

Huld. (2025). *The Importance of Defence Technology is Growing – Finland Positions at the Forefront of International Development*. https://huld.io/news/the-importance-of-defence-technology-is-growing-finland-positions-at-the-forefront-of-international-development/

Jaunarena, H. (2021). Ciber defensa. *CEDEF*, (49). http://repositorio.ub.edu.ar/bitstream/handle/123456789/9584/CEDEF_octubre_2021.pdf?sequence=1&isAllowed=y

Kott, A., Wang, C., y Erbacher, R. (2015). *Cyber Defense and Situational Awareness*. Springer. https://doi.org/10.1007/978-3-319-11391-3

Kumar, G., Saini, D., y Cuong, N. (2020). *Cyber Defense Mechanisms: Security, Privacy, and Challenges*. CRC Press.

Leetaru, K. (2019). *Could Venezuela's Power Outage Really Be A Cyber Attack?* Forbes Magazine. https://www.forbes.com/sites/kalevleetaru/2019/03/09/could-venezuelas-power-outage-really-be-a-cyber-attack/?sh=1e7aed19607c

Leiva, R. (2017). Ciberdefensa,¿ hacia un nuevo eje estratégico? *Revista Ensayos Militares*, *3*(1), 77-92. https://revistaensayosmilitares.cl/index.php/acague/article/view/4/4

Ministerio del Poder Popular para la Defensa. (2014). *Resolución N.º 007778 de 2014. Creación y activación la Dirección Conjunta de Seguridad Informática de la Fuerza Armada Nacional Bolivariana (DICOCEI)*. Gaceta Oficial de la República Bolivariana de Venezuela Nº 40.557, de fecha 08 de diciembre 2014.

Ministerio del Poder Popular para la Defensa. (2015). *Resolución N.º 009723 de 2015. Creación y activación la Dirección Conjunta de Ciberdefensa de la Fuerza Armada Nacional Bolivariana (DICOCIBER)*. Gaceta Oficial de la República Bolivariana de Venezuela Nº 40.655, de fecha 07 de mayo 2015.

ONU. (2017). *Uso indebido de la tecnología de la información y las comunicaciones*. https://www.un.org/counterterrorism/es/cybersecurity

Pérez, I. (2016). Educational networking: human view to cyber defense. *Information Technologies and Learning Tool*, *52*(2). https://lib.iitta.gov.ua/704842/1/1398-5331-1-PB.pdf

Pérez, I. (2021). La legítima defensa del Estado frente a ataques cibernéticos según el Derecho internacional. *Global strategy reports*, (25). https://global-strategy.org/la-legitima-defensa-del-estado-frente-a-ataques-ciberneticos-segun-el-derecho-internacional/

Pontijas, J. (2023). *Unión Europea: ciberseguridad y ciberdefensa*. Instituto Español de Estudios Estratégicos. https://www.ieee.es/Galerias/fichero/docs_analisis/2023/DIEEEA04_2023_JOSPON_Europa.pdf

Rutz, G. (2021). Ciberdefensa como campo intelectual: aproximaciones a los desafíos de la acción pedagógica relativa a sus dominios. *Revista Espectros*, (7). http://espectros.com.ar/wp-content/uploads/Ciberdefensa-como-campo-intelectual_aproximaciones-

a-los-desaf%C3%ADos-de-la-acci%C3%B3n-pedag%C3%B3gica-relativa-a-sus-dominios_por-Guillermo-Rutz.pdf

Saydjari, O. (2021). Cyber defense: art to science. *Communications of the ACM*, *47*(3), 52-57. https://dl.acm.org/doi/abs/10.1145/971617.971645

Shimonski, R., J., Z., y A Bishop, A. (2014). *Cyber reconnaissance, surveillance and defense.* Elsevier eBooks. https://doi.org/10.1016/c2013-0-13412-5

Torrijos, V., y Jiménez, D. (2021). ¿Seguridad sin fronteras, seguridad en abstracto? tendencias en el estudio de la ciberseguridad y la ciberdefensa. *Revista Política y Estrategia*, (138). https://www.politicayestrategia.cl/index.php/rpye/article/view/957/631

World Economic Forum. (2025). *Global Cybersecurity Outlook 2025.* https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

Cibersostenibilidad: Un nuevo paradigma estratégico en la era digital

María Alejandra Rujano[1]

Introducción

En la era digital, la cibersostenibilidad (*Cybersustainability* en inglés, también conocida como Tecnología de la Información Verde o *Green IT*[2]) es un paradigma, disciplina y conjunto de prácticas que busca armonizar el desarrollo y uso de las tecnologías digitales con la protección del medio ambiente y la sostenibilidad a largo plazo. Su objetivo es minimizar la huella ecológica negativa del ecosistema digital mientras se maximiza su potencial como herramienta para impulsar la sostenibilidad en otros sectores de la economía y la sociedad. Es un concepto que va más allá de la eficiencia energética, e incluye la ética, la resiliencia y el impacto social de las tecnologías, promoviendo un cambio en la visión del mundo hacia la responsabilidad planetaria.

A diferencia de la ciberseguridad, que es una disciplina reactiva (o preventiva) enfocada en gestionar el riesgo digital y cuya función es proteger activos, sistemas e información de amenazas externas, brechas y ataques, asegurando la Confidencialidad, Integridad y Disponibilidad (CIA, por sus siglas en inglés) de dichos activos (Kidd, 2024), la cibersostenibilidad es una disciplina estratégica y proactiva que abarca una perspectiva más amplia del impacto a futuro, tanto en el ámbito digital (*bits*) como físico (recursos naturales) (Richards et al., 2011).

El término cibersostenibilidad es un concepto relativamente reciente, un neologismo que combina dos ideas preexistentes: ciber (del griego *kybernetiké*, "arte de gobernar", que dio origen a la cibernética[3] y al prefijo moderno relacionado con el mundo digital y la informática) (Gaitán, 2015), y la sostenibilidad (del latín *sustinere*, "sostener"). Sin embargo, no existe una persona o un documento específico que se considere el acuñador del término, a diferencia de la sostenibilidad que se popularizó con el Informe Brundtland (1987), en el cual se estableció una definición clara y concisa del concepto, que ha servido como guía para políticas y acciones a nivel global.

[1]Ingeniero Industrial egresada de la Universidad Yacambú, Magister en Modelado en Simulación de Sistemas y Doctora en Gestión para la Creación Intelectual. Actualmente se desempeña como Investigadora en el Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL). Autora y editora de publicaciones académicas y de divulgación científica. mrujano@cenditel.gob.ve

[2]Es un conjunto de prácticas y metodologías enfocadas en reducir el impacto ambiental asociado con el desarrollo, uso y desecho de la infraestructura y los servicios de Tecnología de la Información y Comunicación (TIC).

[3]Es la ciencia que estudia las analogías entre los sistemas de control y comunicación en los seres vivos (animales, humanos) y las máquinas (computadoras, robots).

En consecuencia, la cibersostenibilidad surgió orgánicamente en el ámbito tecnológico y empresarial a medida que varias tendencias se volvieron cercanas, como la adopción masiva de la nube (*Cloud computing*), el *Big Data*, la Inteligencia Artificial (IA) y el Internet de las Cosas (IoT), las cuales pusieron de manifiesto el enorme impacto ambiental (consumo energético, *e-waste*[4]) de la infraestructura tecnológica (Bartczak y Block, 2025). Este enfoque fue una respuesta necesaria a la convergencia de dos crisis interconectadas: el reconocimiento de la huella ecológica masiva del sector de las Tecnologías de la Información y Comunicación (TIC) y la creciente necesidad de resiliencia digital para gestionar los procesos de sostenibilidad. Por ello, el término fue adoptado gradualmente por consultoras, académicos y líderes industriales para nombrar un conjunto de desafíos y soluciones que ya existían en la práctica, buscando una viabilidad no solo económica, sino también ecológica y ética, de la sociedad de la información.

En este sentido, la integración de la ciberseguridad en la cibersostenibilidad se articula de dos formas complementarias, la primera de ellas como habilitador crítico de la sostenibilidad (rol estratégico), donde la ciberseguridad es la garantía de resiliencia que protege los sistemas operacionales que gestionan los recursos y el medio ambiente, y la segunda como contribuyente al impacto ecológico (rol operacional), que exige que los equipos de ciberseguridad minimicen su propia huella de carbono[5], ya que los servicios de control (servidores redundantes, *logs* y *firewalls*) consumen energía y generan chatarra electrónica, promoviendo la búsqueda de una ciberseguridad sostenible por diseño que reduzca las emisiones de CO_2 sin comprometer el nivel de riesgo y protección (Psico-smart, 2024).

Es así, que la palabra cibersostenibilidad sirve para reconocer el riesgo de que la tecnología, si no se gestiona de forma responsable, socava los Objetivos de Desarrollo Sostenible (ODS) (Naciones Unidas, 2018). Este riesgo se materializa de múltiples maneras, desde el agotamiento de los recursos naturales y el aumento de las emisiones de carbono (afectando directamente al ODS 13: Acción por el Clima, y ODS 12: Producción y Consumo Responsables) debido a infraestructuras ineficientes y la generación masiva de chatarra electrónica, hasta la afectación del bienestar humano (ODS 3: Salud y Bienestar) y la exacerbación de las desigualdades (ODS 10: Reducción de las Desigualdades) si los modelos digitales promueven el consumo irreflexivo y dañan el equilibrio social y psicológico.

Este ensayo explora la cibersostenibilidad como un nuevo paradigma estratégico que las organizaciones y la sociedad deben adoptar para armonizar el progreso digital con los límites planetarios y la justicia social. Para lograrlo, primero se muestra un marco de convergencia entre ciberseguridad y sostenibilidad, para conocer la interdependencia crucial entre la protección de los activos digitales y la continuidad de los procesos de desarrollo sostenible; luego se plantean los pilares tecnológicos que sustentan este enfoque, identificando la infraestructura digital y las herramientas que deben optimizarse, y finalmente, se presentan

[4]Es una abreviatura del inglés *electronic waste*, que en español se traduce como basura electrónica, desechos electrónicos o chatarra electrónica.

[5]Es un indicador ambiental que mide el impacto total de una actividad, individuo, empresa, producto o evento en el cambio climático.

los desafíos y riesgos de la cibersostenibilidad en el ecosistema digital, para guiar a las organizaciones en el desarrollo de estrategias de resiliencia digital que protejan los logros de la sostenibilidad.

Marco de convergencia entre ciberseguridad y sostenibilidad

La cibersostenibilidad no es solo un tema técnico, es un cambio de mentalidad que reconoce que no puede haber una transformación digital exitosa en un mundo que se deteriora, ni una transformación verde sin el poder habilitador de la tecnología digital. Por lo tanto, la cibersostenibilidad es un concepto fundamental en la intersección de la digitalización, la ciberseguridad y la sostenibilidad, cuya relevancia radica en establecer que la resiliencia y la seguridad de los sistemas digitales son condiciones indispensables para que los beneficios de la digitalización perduren y no se vean comprometidos por riesgos asociados a la hiperconectividad. De esta manera, la ciberseguridad y la sostenibilidad han trascendido su papel como preocupaciones secundarias (que a menudo se olvidan o subestiman) para convertirse en requisitos operativos y estratégicos ineludibles en la gestión empresarial contemporánea, como se muestra en la Figura 1.

Figura 1: Representación de la cibersostenibilidad.
Fuente: Elaboración propia (2025).

El diagrama de Venn muestra cómo la digitalización actúa como herramienta para la eficiencia, la sostenibilidad define el propósito responsable, y la ciberseguridad garantiza la protección y la seguridad de la información, donde la intersección de estos tres dominios da forma a la cibersostenibilidad, como el objetivo final de un futuro digital ético y resiliente. Las intersecciones representan los puntos en los que dos bases deben colaborar para generar valor o establecer una exigencia que contribuye al núcleo de la cibersostenibilidad, como se muestra en la Tabla 1.

Tabla 1: Dominios de la cibersostenibilidad.

Digitalización y Sostenibilidad: permiten habilitar soluciones verdes, al centrarse en cómo la tecnología digital impulsa los objetivos ambientales y sociales.	**Eficiencia de recursos:** La tecnología (IoT, IA y Big Data) permite optimizar el consumo de energía, agua y materiales en industrias, agricultura y ciudades, haciendo los procesos más eficientes y reduciendo el desperdicio.
	Descarbonización: El uso de herramientas digitales (smart grids o redes inteligentes) facilita la integración de energías renovables y la gestión de la demanda energética para reducir las emisiones de carbono.
	Transparencia y medición: Las plataformas digitales permiten monitorear, medir y reportar el impacto ambiental en tiempo real, lo que es esencial para la toma de decisiones sostenibles.
Digitalización y Ciberseguridad: promueven la gestión de riesgos y herramientas, al abordar la necesidad de proteger el proceso de transformación digital.	**Resiliencia operacional:** La ciberseguridad debe asegurar la continuidad del negocio y la capacidad de recuperación ante ataques. Esto es necesario para que la digitalización pueda sostenerse a largo plazo.
	Eficiencia energética: Las prácticas de ciberseguridad deben ser eficientes en el uso de recursos. Por ejemplo, la optimización de centros de datos y el uso de algoritmos criptográficos ligeros reducen el consumo energético.
	Gestión de riesgos: La digitalización introduce nuevos riesgos (Ejemplo, vulnerabilidades en el IoT) y la ciberseguridad proporciona las herramientas para identificarlos y tratarlos, como evaluación de vulnerabilidades.
Sostenibilidad y Ciberseguridad: protegen la infraestructura crítica, garantizando que tanto la seguridad como las operaciones se realicen bajo un marco de responsabilidad.	**Infraestructura crítica:** La sostenibilidad exige proteger la infraestructura crítica (Ejemplo, sistemas de agua, energía, smart grids) de los ciberataques, ya que su fallo tendría un impacto ambiental y social grave.
	Ética y gobernanza: Esta intersección impone una exigencia de ética, asegurando que los sistemas de seguridad y los datos se gestionen de manera justa, transparente y respetuosa con los derechos humanos.
	Larga vida útil: La ciberseguridad, al proteger los sistemas de fallos y ataques, prolonga la vida útil de los equipos digitales, lo que es una forma directa de contribuir a la sostenibilidad.

Fuente: Elaboración propia, a partir de Patagonia (2025) y Henen (2025)

El dominio del rendimiento de recursos en la cibersostenibilidad se ve actualmente amenazado por la alarmante cantidad de agua consumida por tecnologías clave, como la IA, particularmente en sus centros de datos. Aunque la IA es una herramienta para optimizar el consumo de agua en industrias, agricultura y ciudades, como se menciona en el primer domino, sus propios procesos, especialmente el entrenamiento y la operación de grandes modelos en centros de datos, demandan cantidades significativas de agua para la refrigeración. Esto crea una paradoja de la sostenibilidad, ya que la tecnología que habilita soluciones verdes y eficientes en el uso del agua, a su vez, genera una nueva huella hídrica que debe ser gestionada bajo el principio de optimización del rendimiento de recursos (dentro del dominio de digitalización y ciberseguridad), buscando optimizar el uso de recursos en la propia infraestructura digital para que la digitalización y sostenibilidad sea responsable.

Al respecto, Richards et al. (2011) destacaron que existe un costo ambiental escondido asociado con el almacenamiento masivo de datos que no se refleja en el precio que paga el usuario. Esto genera la peligrosa percepción de que los datos digitales son gratuitos, no sólo en términos económicos, sino también medioambientales. Sin embargo, esta visión errónea tiene graves consecuencias, evidenciadas por el crecimiento exponencial de la información digital, por ejemplo, cada mes, miles de millones de fotos se suben solo a Facebook y cada minuto, se añade una cantidad masiva de contenido de video a plataformas como YouTube. Este crecimiento desmedido e invisiblemente costoso ignora el impacto real que tienen los centros de datos necesarios para albergar toda esta información.

Asimismo, Parra (2025) investiga el precio que paga el planeta por cada palabra generada con IA y argumenta que:

> Generar un texto de 100 palabras en ChatGPT consume, en promedio, 519 mililitros de agua, el equivalente a una botella. Este consumo, que puede parecer mínimo en la escala de una sola consulta, se magnifica cuando se analiza el impacto a gran escala. (...) Cada respuesta de 100 palabras también implica un consumo promedio de 0,14 kilovatios-hora (kWh), suficiente para alimentar 14 bombillas LED durante una hora. Multiplicado por millones de usuarios, el impacto es abrumador (s. p).

Como señala el autor, al escalar estos mínimos consumos a los millones de usuarios que utilizan la tecnología a nivel global, la carga ambiental se vuelve desproporcionadamente alta. Esto sugiere que el consumo masivo de agua y electricidad por parte de la IA subraya la urgencia del dominio de la digitalización y ciberseguridad, específicamente su punto sobre eficiencia energética, la cual establece que las prácticas digitales y de ciberseguridad deben ser eficientes en el uso de recursos. El desafío de los modelos de IA es que sus centros de datos son los principales responsables de este consumo.

Por lo tanto, para que la digitalización sea verdaderamente sostenible, es imperativo 1) implementar la optimización de centros de datos, buscando métodos de refrigeración más eficientes y de ciclo cerrado que minimicen el uso del agua, y 2) desarrollar y emplear algoritmos criptográficos ligeros y modelos de IA más eficientes en el uso de energía, reduciendo así la huella eléctrica por cada unidad de cómputo.

Ahora bien, si no se abordan estos costos internos de manera ética, la tecnología que supuestamente promueve la sostenibilidad se convierte en una fuente significativa de impacto ambiental por sí misma. En este sentido, Achuthan et al. (2025) también indica que:

> (...) la ciberseguridad aumenta la huella de carbono mediante el uso de una serie de algoritmos criptográficos de procesamiento, las criptomonedas, los atacantes con capacidades avanzadas que agotan los recursos, y el desarrollo de sistemas de detección y prevención de intrusiones de alta sobrecarga. Esto resulta en una compensación (o compromiso) entre energía, rendimiento y seguridad (p. 2)[6].

[6]Cita textual traducida al español

Esta compensación implica un desafío fundamental ya que es necesario encontrar un equilibrio óptimo donde la búsqueda de la máxima protección digital no consuma excesivos recursos energéticos (afectando la sostenibilidad), pero donde la eficiencia energética no degrade la capacidad de respuesta y la eficacia de la seguridad (afectando la resiliencia). Es decir, este dilema obliga a tomar decisiones conscientes sobre el diseño de la infraestructura digital, favoreciendo soluciones de baja huella de carbono sin comprometer la confidencialidad, integridad y disponibilidad de los sistemas críticos.

Por ejemplo, la minería de *Bitcoin*, un proceso de seguridad basado en la Prueba de Trabajo (en inglés, *Proof of Work*), es el caso más extremo de esta compensación, ya que su consumo de energía puede:

> (...) rivalizar o incluso superar el consumo anual total de electricidad de países pequeños. Es necesario estudiar estas compensaciones y desarrollar mecanismos para equilibrarlas dependiendo de los requisitos de la aplicación. Así, se propone el concepto de ciberseguridad sostenible o verde no sólo para aumentar la vida útil de los sistemas informáticos sino también para incorporar prácticas sostenibles en el ciclo de vida de la ciberseguridad y al mismo tiempo ser resilientes a las ciberamenazas (Achuthan et al., 2025, p. 2)[7].

Bajra et al. (2024) también opina que "Las criptomonedas basadas en PoW como *Bitcoin* emiten aproximadamente 0,86 toneladas métricas de carbono por transacción, lo que equivale a consumir 1000 kWh de electricidad, lo que las hace 27 veces más intensivas en carbono que las transacciones PoS" (p. 1)[8]. Esta desproporción en el consumo energético y las emisiones contaminantes resalta la urgencia de la migración a protocolos más eficientes para el futuro de las finanzas descentralizadas. La alta huella de carbono del PoW, impulsada por la intensa competencia minera y la necesidad de *hardware* especializado y constante refrigeración, se contrapone directamente a los principios de cibersostenibilidad que buscan reducir activamente el *e-waste* y el consumo energético global de las infraestructuras digitales. Por lo tanto, el uso extendido de la Prueba de Participación (PoS, por sus siglas en inglés) representa un avance crucial hacia una tecnología *blockchain* más viable y respetuosa con el medio ambiente (Bit2me, 2025).

En este orden de ideas, el Centro de Ciberseguridad Industrial (2025) adapta los principios ambientales tradicionales al mundo digital y tecnológico, para proponer una hoja de ruta llamada 3R de la cibersostenibilidad, enfocándose en el uso responsable y eficiente de los recursos de *hardware* y *software*, como se muestra en la Tabla 2.

[7] Cita textual traducida al español.
[8] Cita textual traducida al español.

Tabla 2: Las 3R de la cibersostenibilidad.

R	Concepto	Objetivo	Ejemplos prácticos
Reducir	Disminuir el consumo energético y la necesidad de nuevos equipos (*hardware*).	Minimizar la huella de carbono digital y el gasto de energía y recursos naturales.	Reducir el brillo de las pantallas; usar el modo oscuro; eliminar correos masivos; priorizar reuniones virtuales; optimizar el código de software para que sea menos pesado.
Reutilizar	Extender la vida útil de los equipos y activos digitales, dándoles nuevos usos.	Evitar la generación de residuos electrónicos (*e-waste*) y la fabricación de nuevos dispositivos.	Reparar y actualizar computadores y servidores en lugar de desecharlos; reutilizar componentes; comprar tecnología de segunda mano o reacondicionada; usar *software* libre.
Reciclar	Clasificar, depurar y optimizar los recursos digitales y físicos al final de su vida útil.	Asegurar que los materiales valiosos sean recuperados y que los datos inútiles no consuman energía de almacenamiento.	Borrar archivos y bases de datos obsoletas; clasificar y optimizar recursos digitales; llevar equipos electrónicos dañados a centros de reciclaje especializados (puntos limpios).

Fuente: Elaboración propia, a partir de Centro de Ciberseguridad Industrial (2025).

Como se observa, la cibersostenibilidad busca extender la vida útil de la tecnología para combatir la obsolescencia programada, ya que esta práctica es una de las mayores generadoras de residuos electrónicos y de consumo energético innecesario. Esta cultura obliga a los usuarios a desechar *hardware* funcional o ligeramente defectuoso debido a fallos inducidos (como la interrupción del soporte de *software*, la dificultad intencional de la reparación, entre otros), lo cual contraviene el principio de reutilizar. Al exigir la compra constante de nuevos dispositivos, la obsolescencia programada dispara la demanda de recursos y aumenta el consumo energético, lo cual la cibersostenibilidad busca activamente mitigar a través de la promoción de un *software* más eficiente y duradero.

Pilares tecnológicos de la cibersostenibilidad

La cibersostenibilidad es un enfoque que utiliza las tecnologías emergentes para fomentar la productividad y el uso responsable de los recursos, al mismo tiempo que trabaja para minimizar el impacto negativo ambiental y social de la propia tecnología a lo largo de su ciclo de vida. Este doble objetivo exige una gestión proactiva de los nuevos desafíos de seguridad inherentes a estas herramientas, asegurando que la innovación no comprometa la integridad ni la estabilidad. Aunque no existe un conjunto único y universalmente aceptado de bases tecnológicas, los elementos clave se centran en cómo la tecnología puede ser segura, eficiente y ética a largo plazo.

En este sentido, estas bases se articulan en tres ejes interconectados que se enfocan en la optimización de recursos, que combate la ineficiencia, la ociosidad y la sobreasignación de *hardware*; la transición energética, que asegura que la demanda de la infraestructura digital sea satisfecha por energías renovables (y fuentes de carga base de bajas emisiones como la nuclear); y la economía circular, que usa la digitalización para transformar los modelos de producción de un enfoque lineal a uno completamente circular.

Es así que la ejecución y viabilidad de estas esferas de acción dependen de las tecnologías habilitadoras digitales como la IA, IoT, Blockchain, Analítica de datos, Computación en la nube y Gemelos digitales, que son las encargadas de convertir los principios teóricos en una práctica segura, eficiente y económicamente viable (Nicoletti y Apolloni, 2023). Por lo tanto, el estudio de la cibersostenibilidad debe enfocarse en la integración de estos principios con dichas tecnologías para crear un futuro digital verdaderamente sostenible.

Precisamente, en relación a la optimización de recursos tecnológicos, el *Software* Libre (SL) o de Código Abierto (*Open Source*) se establece como una pieza fundamental en las sociedades modernas. Albers (2025), explica que el SL contribuye significativamente a la cibersostenibilidad y a la eficiencia al promover la reutilización, prolongar la vida útil del *hardware*, reducir la dependencia tecnológica y fomentar el desarrollo de soluciones más ligeras y eficientes. La Tabla 3 describe los mecanismos por los que el software libre optimiza las infraestructuras de TI.

Tabla 3: Beneficios del software libre a la cibersostenibilidad.

Extensión de la vida útil del hardware (Reutilización)	**Requerimientos más bajos:** Muchos sistemas operativos y aplicaciones de SL, como Linux, son más ligeros y eficientes que sus contrapartes privativas. Esto permite que equipos antiguos o con recursos limitados (menos RAM, procesadores más lentos) puedan seguir siendo plenamente funcionales. **Lucha contra la obsolescencia programada:** Al permitir que el *hardware* funcione correctamente durante más tiempo, se reduce la necesidad de comprar nuevos equipos constantemente, disminuyendo la generación de basura electrónica (*e-waste*) y la huella de carbono asociada a la fabricación. **Optimización del código:** La libertad de estudiar y modificar el código fuente permite a la comunidad eliminar funcionalidades innecesarias o *bloatware* (software no deseado o innecesario que viene preinstalado por el fabricante o proveedor), enfocándose en el rendimiento y la eficiencia energética del software, lo que se traduce en un menor consumo de energía del *hardware* que lo ejecuta.

Continúa en la siguiente página

Eficiencia operacional y reducción de costos	**Sin costos de licencia:** La naturaleza gratuita del SL reduce drásticamente los costos operativos para individuos, empresas y gobiernos. Este ahorro financiero permite reasignar presupuestos a otras áreas, como la mejora de la infraestructura o la formación, promoviendo un uso más eficiente de los recursos económicos. **Personalización y adaptabilidad:** El código abierto permite a los usuarios personalizar y adaptar el software a sus necesidades específicas. Esta adaptación resulta en una solución más precisa y eficiente, ya que solo se implementan los módulos y recursos realmente necesarios, evitando el gasto de recursos computacionales en funcionalidades no utilizadas, lo que reduce la huella de código ((impacto ambiental y energético de un *software*). **Interoperabilidad:** El SL se adhiere frecuentemente a estándares abiertos, lo que facilita la comunicación y la integración con diferentes sistemas y *hardware*, evitando el bloqueo del proveedor y la necesidad de adquirir *hardware* o *software* específico e incompatible.
Fomento de la colaboración y la soberanía tecnológica	**Comunidad y desarrollo sostenible:** La colaboración global de desarrolladores asegura una mejora continua y una corrección de errores más rápida, lo que lleva a un software más estable y seguro (un aspecto clave de la cibersostenibilidad). Además, promueve la soberanía tecnológica, dando a los países y organizaciones el control sobre sus sistemas sin depender de un único proveedor, lo que garantiza la continuidad operativa y la adaptación a largo plazo. **Transparencia y seguridad:** La disponibilidad del código fuente permite la auditoría por parte de múltiples expertos. Esto aumenta la seguridad al reducir las vulnerabilidades y fallos (*bugs*), minimizando el riesgo de ciberataques que podrían interrumpir operaciones y provocar un uso ineficiente de recursos al tener que invertir en remediaciones costosas y a veces insostenibles.

Fuente: Elaboración propia, a partir de Albers (2025).

Otro aspecto fundamental que González y Cervantes (2024) destacan es la convergencia entre la economía circular y la digitalización, que busca optimizar los procesos de producción, extender la vida útil de los productos y facilitar la recirculación de materiales. En este sentido, los autores explican que:

> La economía circular propone un cambio fundamental en cómo se gestionan los recursos, enfocándose en mantener el valor de los productos, materiales y recursos durante el mayor tiempo posible mediante la reutilización, reparación y reciclaje. Este modelo contrasta con el enfoque lineal tradicional de "tomar-hacer-desechar", que represente la economía lineal. Paralelamente, la digitalización ofrece herramientas avanzadas como el Internet de las Cosas (IoT), la inteligencia artificial (IA) y el blockchain, que pueden optimizar y escalar las prácticas de la economía circular (p. 12).

De lo anterior, se aprecia que el verdadero aporte estratégico de esta convergencia reside en cómo las tecnologías permiten superar las barreras de trazabilidad y gestión de la complejidad del modelo circular, que por sí solo, no puede resolver eficientemente. Es así como la digitalización actúa como un catalizador de eficiencia que facilita la transición de las empresas desde el concepto teórico a la implementación rentable de la economía circular. Al mitigar problemas críticos como la incertidumbre, el fraude y los altos costos de clasificación,

la tecnología no solo posibilita el modelo circular, sino que lo hace económicamente viable a gran escala. Por ejemplo, sin IA y *Big Data*, las empresas tendrían dificultades logísticas y de inventario al tratar de gestionar miles de flujos de retorno de productos diferentes. Por consiguiente, se realiza una fundamentación de las tecnologías clave de la cibersostenibilidad, sintetizadas en la Tabla 4.

Tabla 4: Fundamentos tecnológicos de la cibersostenibilidad.

Optimización de recursos: Se centra en "hacer más con menos", reduciendo directamente el consumo energético y la huella de carbono de la infraestructura TI.	***Hardware* optimizado:** Uso de procesadores de bajo consumo (Ejemplo, arquitecturas ARM), GPUs eficientes para cargas específicas como IA, y unidades de estado sólido (SSDs) que consumen menos que los discos duros tradicionales. **Refrigeración avanzada:** Implementación de sistemas de refrigeración líquida para centros de datos, o el uso de *free-cooling* (aprovechar el aire exterior) para reducir el consumo energético en climatización. **Virtualización y consolidación:** Ejecutar múltiples sistemas operativos y aplicaciones en un solo servidor físico. Esto maximiza la utilización del *hardware*, reduce la cantidad de servidores necesarios y, por ende, el consumo de energía y espacio. **Contenedores y orquestadores:** Tecnologías como Docker y Kubernetes (proyectos de código abierto) permiten empaquetar aplicaciones de forma ligera y gestionar su despliegue de manera eficiente, escalando recursos automáticamente según la demanda y evitando el exceso de capacidad. **Arquitecturas de software sostenibles:** Desarrollar aplicaciones y algoritmos que sean computacionalmente eficientes. Un código optimizado que requiere menos ciclos de CPU consume menos energía.
Transición energética: No solo se trata de consumir menos, sino de utilizar energía más limpia y gestionarla de forma responsable.	**Alimentación con energías renovables:** Migrar los centros de datos y las infraestructuras críticas a fuentes de energía como la solar, eólica o hidroeléctrica. Algunos *hyperscalers* (grandes proveedores de servicios de computación en la nube) como Google, Microsoft y Amazon, si bien ya operan con energía renovable, ahora están apostando por la energía nuclear (DW, 2024). **Gestión inteligente de la energía (*Power Management*):** Uso de *software* y *hardware* que permita poner en estado de reposo (hibernación) los equipos cuando no estén en uso, o ajustar dinámicamente la frecuencia del procesador (DVFS, en inglés *Dynamic Voltage and Frequency Scaling*) según la carga de trabajo. **Diseño de centros de datos sostenibles:** Implementar diseños que maximicen la eficiencia, medidos por el indicador PUE (en inglés *Power Usage Effectiveness*). Un PUE cercano a 1.0 indica un alto rendimiento.

Continúa en la siguiente página

Economía circular: Aborda la sostenibilidad desde la perspectiva del ciclo de vida completo del hardware, desde la extracción de materiales hasta su fin de vida.	**Diseño modular y reparable:** Fabricar dispositivos (portátiles, servidores, *smartphones*) que sean fáciles de desmontar, reparar y actualizar, extendiendo su vida útil. **Reutilización y remanufactura:** Fomentar mercados de equipos TI reacondicionados y certificados. Un servidor o un portátil remanufacturado tiene una huella de carbono significativamente menor que uno nuevo. **Reciclaje y gestión de residuos electrónicos (*e-waste*):** Implementar sistemas eficaces y responsables para el reciclaje de componentes electrónicos, recuperando metales preciosos y tierras raras, y evitando que los desechos tóxicos contaminen el medio ambiente. **Modelos de Producto como Servicio (PaaS):** En lugar de vender *hardware*, las empresas lo ofrecen como un servicio. Esto incentiva al fabricante a crear productos duraderos, eficientes y fáciles de reciclar, ya que el equipo vuelve a sus manos al final del contrato.
Tecnologías habilitadoras: Es el principio con mayor potencial, ya que utiliza la tecnología no solo para ser más sostenibles internamente, sino para permitir que otros sectores lo sean.	**IoT:** Los sensores IoT permiten monitorizar en tiempo real el consumo energético de edificios, optimizar rutas de transporte para reducir emisiones, gestionar de forma inteligente el agua en la agricultura o detectar fugas en infraestructuras, entre otros. **IA y analítica de datos (*Big Data*):** La IA puede predecir la demanda energética para ajustar la generación, optimizar complejas cadenas de suministro para reducir desperdicios, o modelar los efectos del cambio climático para una mejor preparación. **Computación en la nube (*Cloud Computing*):** La nube centraliza los recursos computacionales, logrando economías de escala masivas en eficiencia energética. Es mucho más eficiente que miles de servidores locales subutilizados en empresas individuales. **Gemelos digitales (*Digital Twins*):** Crear réplicas virtuales de sistemas físicos (Ejemplo, una ciudad, una fábrica) para simular y probar estrategias de sostenibilidad (como cambios en el tráfico o procesos de producción) sin riesgo y con un costo mínimo. **Cadena de bloques (*Blockchain*):** Garantizar la transparencia y la trazabilidad en las cadenas de suministro, al registrar cada paso del ciclo de vida de un producto o servicio, desde su origen hasta el consumidor/cliente. Esto permite a las empresas cuantificar huella de carbono, prevenir fraudes y falsificaciones, y fortalecer la confianza de sus clientes.

Fuente: Elaboración propia.

La consecución de la cibersostenibilidad trasciende la simple adopción de tecnologías ecológicas o seguras de forma aislada, pues requiere la integración sinérgica de sus tres pilares, articulados por las tecnologías habilitadoras y un cambio cultural y de procesos profundo en las organizaciones. Esta sinergia implica que la eficiencia del código (optimización de recursos) debe alimentar la seguridad (minimización de vulnerabilidades), mientras que la digitalización (con tecnologías como la IA y el *Big Data*) debe optimizar el uso de energías renovables y habilitar modelos de economía circular para el hardware. El éxito,

por ende, depende de un pensamiento sistémico donde la sostenibilidad deja de ser un costo operativo para convertirse en un criterio de diseño estratégico desde el inicio del ciclo de vida tecnológico.

Desafíos y riesgos de la cibersostenibilidad en el ecosistema digital

Los principales desafíos y riesgos de la cibersostenibilidad se agrupan en cinco áreas temáticas interconectadas que reflejan la complejidad del ecosistema digital, a saber: la desigualdad en el acceso y uso de la tecnología (brecha digital), la falta de talento y concientización (riesgo humano), la evolución de las amenazas cibernéticas (riesgo sistémico), los riesgos de ciberseguridad en infraestructuras verdes (riesgo operacional), el *greenwashing* digital (ética social) y la regulación y cumplimiento normativo (riesgo de gobernanza). A continuación se explican cada una de ellas.

Desigualdad en el acceso y uso de la tecnología

La brecha digital no es un problema monolítico, sino una compleja serie de barreras que, en conjunto, representan una seria amenaza para la sostenibilidad inclusiva, al dejar fuera del progreso a miles de millones de personas. Para Albero (2025), esta se manifiesta principalmente en tres dimensiones:

1. **Barrera de acceso:** Representa la disparidad física y económica para conectarse. La falta de infraestructura de telecomunicaciones en zonas rurales o de bajos ingresos, sumada a los costos elevados de dispositivos y servicios de banda ancha, condena a comunidades enteras al aislamiento informativo. Desde la perspectiva de la sostenibilidad, esto significa que las poblaciones más vulnerables no pueden acceder a herramientas digitales esenciales para la resiliencia climática (como alertas tempranas de desastres) o para la eficiencia energética (como los medidores inteligentes), entre otras, imposibilitando la participación equitativa en la economía digital verde.

2. **Déficit de uso:** Viene dada por la falta de habilidades y la alfabetización digital, ya que superar la barrera física no es suficiente para utilizar la tecnología de forma efectiva. Una persona puede tener un *smartphone*, pero si carece de la formación básica, no puede aprovechar aplicaciones de salud, educación o empleo, y es más susceptible a riesgos de ciberseguridad. En términos de cibersostenibilidad, esta diferencia es crítica; sin alfabetización digital básica, los individuos no pueden participar en la gobernanza de datos ni proteger su identidad, debilitando así el ámbito social de las empresas.

3. **Brecha de calidad de uso o aprovechamiento:** Esta dimensión se refiere a la incapacidad de aplicar los conocimientos digitales para lograr beneficios tangibles y significativos, tanto a nivel individual como organizacional. No se trata solo de saber usar una aplicación, sino de entender cómo usar la red para emprender, innovar, o tomar decisiones informadas sobre sostenibilidad. En el contexto de la cibersostenibilidad, esto se traduce en:

- Un **riesgo de ineficiencia**, dado que si las organizaciones no saben cómo utilizar las herramientas digitales para optimizar cadenas de suministro o reducir el consumo energético de sus propias TI, se anula el potencial ambiental de la digitalización.
- Un **riesgo ético**, en tanto que los usuarios que carecen de conocimientos avanzados sobre privacidad y ética digital son más propensos a ser manipulados o a caer en el consumo digital irresponsable (como el uso excesivo y no optimizado de la nube).

Para ampliar esta idea, un informe de la Unión Internacional de Telecomunicaciones (UIT), organismo de las Naciones Unidas (ONU), revela que la brecha digital entre los países menos adelantados y el resto del mundo no muestra signos de reducirse, con 2.6 mil millones de personas sin acceso a Internet (ITU, 2023). Esto supone un obstáculo directo para el cumplimiento de los ODS, particularmente en áreas clave como la educación (ODS 4), el trabajo decente (ODS 8) y la reducción de las desigualdades (ODS 10). Esta exclusión es altamente desproporcionada en países de bajos ingresos y áreas rurales, donde la falta de acceso perpetúa un ciclo de pobreza y desigualdad de oportunidades al limitar el acceso a capacitación y mercados laborales. Además, esta desconexión masiva merma la cibersostenibilidad inclusiva, ya que restringe la recopilación de datos globales precisos y vuelve inaccesibles las soluciones tecnológicas verdes (como la agricultura de precisión) precisamente para las comunidades que más podrían beneficiarse de ellas. Por lo tanto, cerrar esta triple desigualdad digital es un imperativo ético y estratégico para garantizar un desarrollo global verdaderamente equitativo.

Falta de talento y concientización

Existe una escasez global de profesionales con el perfil dual que combine conocimiento de ciberseguridad y experiencia en sostenibilidad. Esto se agrava con el desafío de la concientización organizacional, donde a menudo el personal ve la ciberseguridad como un impedimento para la eficiencia operativa en lugar de un escudo protector para los activos sostenibles. La falta de una cultura cibersostenible convierte el error humano en uno de los principales vectores de ataque. Esta situación, puede deberse a que históricamente la ciberseguridad se ha centrado en proteger la información y los activos tecnológicos (confidencialidad, integridad, disponibilidad), mientras que la sostenibilidad se ha centrado en los criterios ESG[9] (ambiental, social, gobernanza), lo que ha proliferado una falta de currículos y certificaciones que integren la eficiencia energética de las TI, la gestión de la basura electrónica (e-waste) o la cadena de suministro sostenible con protocolos de seguridad.

Al respecto, el *Fortinet Training Institute*, en su informe global 2025 sobre la brecha de habilidades en ciberseguridad, señala que el 48 % de los líderes anticipan que la falta de personal con experiencia en IA es su mayor desafío para implementar soluciones de

[9]Son un conjunto de estándares utilizados por los inversores y las partes interesadas (*stakeholders*) para medir y evaluar el desempeño de una empresa en áreas críticas que van más allá de los resultados financieros tradicionales.

ciberseguridad. Dado que la IA es crucial para optimizar procesos y reducir el consumo energético (un pilar de la cibersostenibilidad), esta escasez técnica agrava aún más la brecha de sostenibilidad, creando una paradoja: la tecnología más necesaria para la eficiencia ambiental no puede ser desplegada de forma segura por falta de personal capacitado.

De igual manera, el informe identifica claramente la falta de conciencia de seguridad (56 %), la falta de capacitación (54 %) y la falta de productos de ciberseguridad necesarios (50 %), como las principales causas del déficit de seguridad Fortinet (2025). Esta tríada de factores demuestra que los controles técnicos más avanzados son inútiles si el factor humano es débil. La concientización se convierte en la línea de defensa más crítica, ya que el error humano es el vector de ataque más explotado, capaz de anular cualquier inversión en sistemas de IA o firewalls para comprometer tanto los datos corporativos como la infraestructura clave de cibersostenibilidad.

De acuerdo con Rashotte (2024), "Hay una escasez mundial de casi 4 millones de expertos en ciberseguridad, y se prevé que este déficit aumente en medio de un incremento de la demanda de ciberprofesionales." (s. p). Esta dificultad masiva y creciente no es solo un problema de recursos humanos, sino un riesgo sistémico que afecta directamente la capacidad de las organizaciones para operar de manera segura y sostenible, ya que los equipos existentes están sobrecargados y son más propensos al error, lo que también conlleva a una sobrecarga laboral que incrementa el *burnout*[10], reduce la capacidad de respuesta ante incidentes críticos y debilita la postura de ciberseguridad a largo plazo.

Es así como una posible solución a esta crisis no se limita solo a contratar, sino a inversión en capacitación masiva, programas de *upskilling* (mejora de habilidades) y *reskilling* (recapacitación o reentrenamiento), y la búsqueda activa de talento. Sin embargo, para que estos esfuerzos sean efectivos a escala global, deben enmarcarse en un ecosistema de colaboración que involucre a múltiples actores:

- **Alianzas estratégicas público-privadas:** Es fundamental establecer una colaboración estrecha entre el sector empresarial, las instituciones gubernamentales y el sector educativo.
- **Diversificación proactiva de las reservas de talento:** La búsqueda activa de talento debe ir más allá de los canales tradicionales y centrarse en grupos subrepresentados, como las mujeres y las minorías.
- **Compartir conocimiento y recursos abiertos:** La colaboración debe extenderse al intercambio de conocimiento y herramientas que beneficien a toda la comunidad de ciberseguridad.

[10]Es un estado de agotamiento físico, emocional y mental que resulta de un estrés laboral crónico que no ha sido gestionado con éxito. Es un concepto reconocido por la Organización Mundial de la Salud (OMS) como un fenómeno ocupacional (no una condición médica).

Evolución de las amenazas cibernéticas

La evolución de las amenazas cibernéticas se puede resumir en varias fases, donde cada era introdujo nuevas tácticas, motivos y objetivos. A continuación, la Tabla 5 ilustra esta evolución desde los inicios de la computación hasta la era actual, marcada por la IA y la cibersostenibilidad.

Tabla 5: Evolución de las amenazas cibernéticas.

Era / Período aproximado	**Tipo de amenaza**	**Objetivo**	**Táctica clave**
Experimental (1970-1980)	Virus primitivos y ataques informáticos por curiosidad.	Demostrar capacidad técnica; bromas.	Ingeniería social básica, difusión por disquete o redes incipientes.
Red y propagación (1990-2000)	Gusanos, *malware* de propagación masiva DDoS primitivos.	Interrupción del servicio, daño a la infraestructura.	Explotación de vulnerabilidades de red (Internet), *spam* masivo, adjuntos de correo electrónico.
Crimen organizado (2000-2010)	*Spyware* (software espía), *botnets* (Red de *bots*), *keyloggers* (capturadores de teclas), *phishing* (suplantación de identidad) financiero, *malware* dirigido a bancos.	Ganancia financiera directa (robo de datos bancarios, credenciales).	Creación de redes de *bots* para control remoto, *phishing* sofisticado, troyanos bancarios.
Rescate y espionaje (Desde 2010)	*Ransomware* (secuestro de datos), Amenazas Persistentes Avanzadas (APT), *malware* en sistemas OT/ICS.	Rescate financiero masivo y dirigido, espionaje industrial y geopolítico, sabotaje de infraestructura.	Cifrado de datos, ataque a la cadena de suministro, explotación de vulnerabilidades de día cero, ataques dirigidos a infraestructura crítica.
Convergencia y la IA (Actualidad)	Ataques impulsados por IA (generación masiva de *phishing* avanzado, *deepfakes* (contenido falso)), *malware* polimórfico, ciberataques a sistemas de cibersostenibilidad (redes inteligentes, IoT).	Manipulación de la opinión pública, evasión de defensas de seguridad, impacto ambiental o social (a través de OT), robo de datos a escala masiva.	Uso de IA para automatizar la ofuscación de código, ataques de ingeniería social hiperpersonalizados, explotación de la gran superficie de ataque del IoT.

Fuente: Elaboración propia, a partir de Codecademy (2025) y New Charter (2024).

Como se observa, esta expansión y sofisticación representa una presión constante y creciente sobre la capacidad de defensa de las organizaciones, donde los sistemas tradicionales se vuelven obsoletos rápidamente. La convergencia con la IA y el IoT ha transformado la ciberseguridad en un riesgo sistémico que, si no se gestiona adecuadamente, puede derivar en pérdidas económicas exponenciales que superan los costos de rescate y recuperación, dañar irreparablemente la confianza ante los actores clave (*stakeholders*), y comprometer la gobernanza corporativa al exponer a los directivos a una mayor responsabilidad legal por el

incumplimiento de las normativas de seguridad de datos.

En consecuencia, el ritmo al que se desarrollan las amenazas cibernéticas (IA, *deepfake*s, *ransomware*, etc.) es mucho más rápido que el de la actualización legislativa. Esto obliga a las organizaciones a cumplir con estándares que son legalmente obligatorios, pero que a menudo resultan insuficientes para protegerse contra los sofisticados ataques de la era de la IA, dejando una brecha de cumplimiento práctico que es difícil de cerrar.

Riesgos de ciberseguridad en infraestructuras verdes

Para Estévez (2024), el avance hacia la sostenibilidad impulsado por la transición a fuentes de energía renovables (solar, eólica, hidráulica) es un eje fundamental para el desarrollo global. No obstante, a medida que estas infraestructuras verdes se digitalizan y se interconectan (como las redes inteligentes o *smart grids*), su vulnerabilidad ante las ciberamenazas se incrementa significativamente. La ciberseguridad se convierte así en un componente esencial, ya que un ataque exitoso podría interrumpir el suministro de energía limpia, causando daños económicos y ambientales graves, e incluso obligando a recurrir a fuentes de energía más contaminantes, lo que socavaría directamente los ODS. La convergencia de ambas áreas refleja una realidad en la que proteger el futuro sostenible depende intrínsecamente de proteger su infraestructura digital.

Las infraestructuras verdes son objetivos atractivos para actores malintencionados. Entre las principales amenazas se encuentran los ataques a las redes inteligentes, que buscan manipular datos para causar apagones o sobrecargas, y los ataques de denegación de servicio (DDoS). Las plantas solares y eólicas también son vulnerables, pues los atacantes pueden obtener el control remoto de los sistemas SCADA para alterar o cesar la generación de energía, o manipular datos operativos. Además, la compleja cadena de suministro de tecnología verde es un factor de ataque, donde se puede introducir software malicioso (*malware*) o componentes comprometidos en el software de control, poniendo en riesgo la integridad de la infraestructura desde su origen.

Proteger estas infraestructuras presenta desafíos únicos, incluyendo su complejidad y escalabilidad, ya que gestionan redes diversas (TI, tecnologías de operación (OT) y sistemas de control industrial (ICS)) dispersas geográficamente, muchas veces operando con sistemas heredados (*legacy*) y vulnerables. Otro desafío clave es la limitación de recursos, donde los presupuestos ajustados en proyectos de sostenibilidad suelen priorizar la expansión sobre la ciberseguridad, dejando los sistemas insuficientemente protegidos. Además, la regulación y el cumplimiento normativo presentan lagunas, evolucionando lentamente en comparación con la rápida sofisticación de las amenazas. Para enfrentar estos retos, el autor propone estrategias como la implementación del modelo de seguridad *Zero Trust* (confianza cero), la micro-segmentación y la segmentación de redes.

Greenwashing digital

Otro de los riesgos directos para la cibersostenibilidad que debilita la confianza y la autenticidad de los esfuerzos ecológicos es el *greenwashing* digital (Lavado o *marketing* verde), que hace referencia a la práctica de promocionar o comunicar de manera engañosa que un producto, servicio o la operación de una empresa tecnológica es más sostenible, neutra en carbono o amigable con el medio ambiente de lo que realmente es. En este sentido, O'Brien (2025) expone que:

> Un ejemplo famoso es "Dieselgate" del fabricante de automóviles alemán Volkswagen, que comercializó sus vehículos diésel como de bajas emisiones y respetuosos con el medio ambiente. En realidad, los coches estaban equipados con un software que engañaba las pruebas de emisiones y liberaba hasta 40 veces más óxido de nitrógeno de lo permitido en Estados Unidos (s. p)[11].

Este riesgo de lavado verde afecta directamente la capacidad de las organizaciones para gestionar su cibersostenibilidad de forma ética y transparente. Cuando una empresa promueve métricas de sostenibilidad engañosas sobre sus operaciones digitales (por ejemplo, el bajo consumo de energía de un servicio en la nube), desacredita el principio de gobernanza (criterios ESG) y desvía la atención de los riesgos reales, como la huella de carbono de los centros de datos o la generación masiva de basura electrónica (e-waste). Este engaño no solo pone en peligro la reputación ante los *stakeholders* y los inversores que buscan sostenibilidad verificable, sino que también impide la adopción de soluciones de seguridad verdaderamente eficientes al desincentivar la inversión en tecnologías que aborden honestamente el impacto ambiental de las TIC.

En este orden de ideas, Green Digital (2025) detalla los engaños sobre el lenguaje de la sostenibilidad, al explicar la evolución del *greenwashing*, que comenzó con la versión 1.0 (maquillaje verde), donde la falsedad era burda y fácil de detectar (como una etiqueta ecológica sin certificaciones), luego pasó al 2.0 (alta gama), caracterizado por la omisión selectiva de información y la promoción de métricas insignificantes para distraer la atención de los impactos ambientales más graves, hasta llegar al 3.0 (simulaciones digitales) como la era de la evasión tecnológica y psicológica que utiliza la IA para crear afirmaciones tan complejas y ambiguas que resultan prácticamente imposibles de verificar para el consumidor o el regulador.

Cumplimiento normativo

La gestión del cumplimiento normativo constituye la mayor fuente de complejidad y riesgo crítico para la cibersostenibilidad, ya que obliga a las organizaciones a equilibrar las crecientes exigencias de seguridad con las de transparencia en su desempeño ambiental y social. En este contexto, las empresas están obligadas a adoptar y regirse por los criterios ESG, que abarcan las siguientes dimensiones:

[11] Cita textual traducida al español.

- **E (Ambiental):** Implica la gestión de riesgos relacionados con el clima, la reducción activa de la huella ecológica, la eficiencia energética, la gestión de residuos y la economía circular.
- **S (Social):** Se centra en la relación de la empresa con sus empleados, proveedores, clientes y comunidades, incluyendo aspectos como los derechos humanos, la diversidad, la igualdad, la salud y seguridad laboral.
- **G (Gobernanza/Gobierno corporativo):** Aborda la forma en que una empresa es dirigida y controlada, asegurando la transparencia, la ética, la autonomía corporativa y las políticas de cumplimiento, lo cual es fundamental para gestionar la responsabilidad legal ante riesgos y garantizar la integridad de los datos reportados sobre el desempeño ambiental y social (evitando así el *greenwashing* digital).

En este punto, KPMG (2023) explica lo siguiente:

> Los datos ESG provienen de cuatro fuentes principales: de terceros, informados, derivados y funcionales, y los que son propiedad de la empresa. Se están realizando esfuerzos significativos en los informes ESG y asegurar su presentación, pero ¿puede confiarse en que los datos son precisos y confiables?. La ciberseguridad es un factor crítico para garantizar informes ESG confiables. Trabaja para proteger los datos en sus orígenes mientras se recopilan, en tránsito y después de que se han analizado e informados. Además, también se requiere el cumplimiento de la privacidad de datos cuando los datos personales se procesan en la generación de informes ESG (p. 10).

Por lo tanto, esta necesidad de integrar el cumplimiento normativo en ciberseguridad con el reporte ESG crea una convergencia regulatoria que impone una carga sin precedentes sobre la G de gobernanza. Este cruce implica que la ciberseguridad deja de ser solo una función tecnológica para convertirse en un imperativo de liderazgo y transparencia. Para el reporte ambiental y social, las empresas deben recopilar datos verificables sobre su consumo energético, gestión de *e-waste* y prácticas laborales en la cadena de suministro. Si la infraestructura de TI que almacena o procesa estos datos es comprometida por un ciberataque, la integridad de dichos informes se anula. En tal caso, un fallo de ciberseguridad no solo causa una brecha de seguridad (o fallo de integridad), sino que también provoca un incumplimiento en el reporte ESG, exponiendo a la empresa a sanciones por datos de sostenibilidad no fiables.

Para Brown (2024) esta integración "(...) no sólo les ayuda a coordinar y gestionar mejor sus esfuerzos de cumplimiento normativo, sino que también les permite adoptar un enfoque de doble materialidad para evaluar y gestionar el riesgo empresarial." (s. p)[12]. Esto significa que las empresas no solo deben reportar cómo los riesgos externos (ejemplo, el cambio climático) afectan a sus finanzas, sino también cómo sus propias operaciones (incluyendo la tecnología) afectan a las personas y al planeta. Es así que para que los informes ESG sean

[12]Cita textual traducida al español.

creíbles, los datos de sostenibilidad deben ser auditables.

Asimismo, es necesario comprender que el cumplimiento en ciberseguridad es la disciplina que obliga a seguir estándares, marcos de referencia y regulaciones diseñados específicamente para salvaguardar los sistemas y la información sensible de las organizaciones. En este caso, esta adhesión se divide en dos categorías esenciales. Por un lado, el cumplimiento obligatorio abarca aquellas regulaciones y normas impuestas por entidades gubernamentales o regulatorias, dirigidas especialmente a sectores con infraestructuras críticas. Un ejemplo de esto, es el Reglamento General de Protección de Datos (RGPD), promulgado por la Unión Europea, que ha elevado significativamente las responsabilidades de las organizaciones que manejan información personal. Por otro lado, existe el cumplimiento voluntario, que consiste en la adopción de certificaciones y estándares por iniciativa propia de la empresa. Estas certificaciones, como ISO 14001 (mencionado aquí como ejemplo de gestión medioambiental, que también aplica a seguridad), buscan demostrar proactivamente la competencia técnica y el compromiso de la organización con el cumplimiento de normas específicas de la industria o de mejores prácticas internacionales.

Sobre este tema, como la cibersostenibilidad es un concepto emergente que integra la ciberseguridad con los objetivos de sostenibilidad, no existe actualmente una única ley internacional de cibersostenibilidad. En relación a la gobernanza, cada región, sector y gobierno cuenta con normativas relacionadas con la ciberseguridad que desempeñan un papel fundamental en la configuración de la prácticas de seguridad.

En Venezuela, el marco legal si bien no aborda la cibersostenibilidad de manera explícita, sí establece responsabilidades críticas en materia de ciberseguridad y gobernanza que impactan la fiabilidad de los datos. Leyes como la Ley Especial Contra Delitos Informáticos (2001), Ley de Mensaje de Datos y Firmas Electrónicas (2001), Ley Orgánica de Telecomunicaciones (2011), Ley de Infogobierno (2013), Ley Orgánica de Ciencia, Tecnología e Innovación (2022) y el Plan de la Patria 2019-2025, junto con decretos que rigen la protección de infraestructuras críticas nacionales, obligan a las instituciones públicas y a ciertas entidades privadas estratégicas a mantener estándares robustos de seguridad digital.

Consideraciones finales

La cibersostenibilidad se establece como un paradigma estratégico esencial, cuyo fin es armonizar el progreso tecnológico con la preservación ambiental y la equidad social. Su implementación va más allá de la adopción de herramientas eficientes, pues requiere una profunda transformación mental que integre la ciberseguridad, la optimización de recursos y la economía circular desde la fase de diseño de la infraestructura digital. En consecuencia, adoptar este modelo no solo busca la eficiencia operativa, sino que también implica una responsabilidad colectiva de largo plazo, asegurando que el desarrollo y el uso de la tecnología estén guiados por un propósito ético y una conciencia sobre los límites planetarios.

El camino hacia un ecosistema digital verdaderamente sostenible exige una

transformación cultural y colaborativa, donde la ética, la inclusión y la resiliencia se consoliden como bases de toda iniciativa tecnológica. Para superar los desafíos planteados, las organizaciones deben priorizar la gobernanza, establecer alianzas estratégicas e invertir en la capacitación de profesionales con un perfil dual que combine conocimientos técnicos con principios de sostenibilidad. Solo esta integración sistémica y sinérgica permitirá construir un futuro digital que, además de ser seguro y eficiente, esté genuinamente alineado con la justicia social y el bienestar de las generaciones futuras.

Referencias

Achuthan, K., Sankaran, S., Roy, S., y Raman, R. (2025). Integrating sustainability into cybersecurity: insights from machine learning based topic modeling. *Discover Sustainability*, *6*(44). https://doi.org/10.1007/s43621-024-00754-w

Albero, V. (2025). *¿Qué es la brecha digital y cómo cerrarla con nuevas competencias digitales?* Adr Formación. https://www.adrformacion.com/blog/que_es_la_brecha_digital.html#:~:text=Educaci%C3%B3n%20y%20formaci%C3%B3n%20en%20competencias,plenamente%20en%20la%20sociedad%20digital.

Albers, E. (2025). *On the Sustainability of Free Software*. FSFE. https://fsfe.org/freesoftware/sustainability/sustainability.en.html

Bajra, U., Rogova, E., y Avdiaj, S. (2024). Cryptocurrency blockchain and its carbon footprint: Anticipating future challenges. *Technology in Society*, *77*. https://doi.org/10.1016/j.techsoc.2024.102571

Bartczak, J., y Block, S. (2025). *Cómo el uso de la inteligencia artificial impacta al ambiente y qué puedes hacer al respecto*. Foro Económico Mundial. https://es.weforum.org/stories/2025/06/como-el-uso-de-la-inteligencia-artificial-impacta-al-ambiente-y-que-puedes-hacer-al-respecto/

Bit2me. (2025). *¿Qué es Prueba de participación / Proof of Stake (PoS)?* Bit2me Academy. https://academy.bit2me.com/que-es-proof-of-stake-pos/

Brown, C. (2024). *Manage Cybersecurity as Part of the ESG Strategy*. Directors & Boards. https://www.directorsandboards.com/board-issues/cyber-risk/manage-cybersecurity-as-part-of-the-esg-strategy/

Centro de Ciberseguridad Industrial. (2025). *Ciberseguridad y Sostenibilidad Industrial en 2025: Un nuevo estándar para proteger recursos esenciales*. Centro de Ciberseguridad Industrial. https://www.cci-es.org/ciberseguridad-y-sostenibilidad-industrial/

Codecademy. (2025). *La evolución de la ciberseguridad*. Codecademy. https://www.codecademy.com/article/evolution-of-cybersecurity

DW. (2024). *Amazon, Google y Microsoft apuestan por la energía nuclear*. Deutsche Welle. https://www.dw.com/es/amazon-google-y-microsoft-apuestan-por-la-energ%C3%ADa-nuclear/a-70537579

Estévez, M. (2024). *Ciberseguridad en la sostenibilidad: protección de las infraestructuras verdes*. Izertis. https://www.izertis.com/es/-/blog/ciberseguridad-sostenibilidad-proteccion-infraestructuras-verdes

Fortinet. (2025). *2025 Cybersecurity Skills Gap. Global Research Report.* Fortinet Training Institute. https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/ftnt-skills-gap-report-2025.pdf

Gaitán, A. (2015). Cibernética en la guerra contemporánea: definición de nuevos escenarios estratégicos y operacionales. *Estudios en Seguridad y Defensa*, *10*(20), 117-131. https://esdegrevistas.edu.co/index.php/resd/article/view/41/315

González, M., y Cervantes, M. (2024). *Convergencia de la Economía Circular y la Digitalización: Caminos para un Futuro Sostenible* [Documento en línea/Capítulo de libro en línea]. Red de Investigación Latinoamericana en Competitividad Organizacional (RILCO). https://www.rilco.org/wp-content/uploads/2024/12/Libro_Innovacio%CC%81n_digital_20241105.pdf

Green Digital. (2025). *Greenwashing 2.0 y 3.0.* Green Digital. https://www.greendigitalcomunicacion.com/greenwashing-2-0-y-3-0/#:~:text=Greenwashing%203.0:%20o%20la%20era,la%20marca%20cae%20en%20picada.

Henen, B. (2025). Cybersecurity in the Digital Era: Between Digital Transformation and Protection Challenges. *Law and World*, *11*(35), 111-125. https://doi.org/10.36475/11.3.8

ITU. (2023). *Los últimos datos sobre conectividad mundial muestran un crecimiento, si bien persisten las brechas.* Comunicado de Prensa, ITU. https://www.itu.int/es/mediacentre/Pages/PR-2023-11-27-facts-and-figures-measuring-digital-development.aspx

Kidd, C. (2024). *What's The CIA Triad? Confidentiality, Integrity, & Availability, Explained.* Splunk Blog. https://www.splunk.com/en_us/blog/learn/cia-triad-confidentiality-integrity-availability.html

KPMG. (2023). *Ciberseguridad en ESG.* KPMG. https://assets.kpmg.com/content/dam/kpmg/co/sac/pdf/2023/11/KPMG%20-%20Cybersecurity%20in%20ESG.pdf

Naciones Unidas. (2018). *¿Sabes cuáles son los 17 objetivos de desarrollo sostenible?* Naciones Unidas. https://www.un.org/sustainabledevelopment/es/2018/08/sabes-cuales-son-los-17-objetivos-de-desarrollo-sostenible/

New Charter. (2024). *Cyber Security. From Evolution To Current Trends.* New Charter. https://www.newchartertech.com/cyber-security-from-evolution-to-current-trends/

Nicoletti, B., y Apolloni, A. (2023). Framework of IoT, Blockchain, Digital Twins, and Artificial Intelligence Solutions in Support of the Digital Business Transformation of Logistics 5.0 (Chapter 12). En *Supporting Technologies and the Impact of Blockchain on Organizations and Society* (pp. 195-219). IGI Global. https://www.researchgate.net/publication/373697485_Framework_of_IoT_Blockchain_Digital_Twins_and_Artificial_Intelligence_Solutions_in_Support_of_the_Digital_Business_Transformation_of_Logistics_50

O'Brien, C. (2025). *What is Greenwashing in Marketing?* Digital Marketing Institute. https://digitalmarketinginstitute.com/blog/greenwashing-in-marketing

Parra, S. (2025). *La sed de ChatGPT: la IA consume una cantidad de agua alarmante.* National Geographic España. https://www.nationalgeographic.com.es/ciencia/agua-que-gasta-chatgpt-y-otros-modelos-ia_23812

Patagonia. (2025). *Twin transition: cómo la transformación digital puede impulsar la sostenibilidad*. Patagonia. https://itpatagonia.com/que-es-twin-transition-principios-sustentables/

Psico-smart. (2024). *Rol de la ciberseguridad en la transformación digital*. Psico-smart. https://blogs-es.psico-smart.com/articulo-rol-de-la-ciberseguridad-en-la-transformacion-digital-34224

Rashotte, B. (2024). *Por qué cerrar la brecha de habilidades cibernéticas requiere un enfoque colaborativo*. Foro Económico Mundial. https://es.weforum.org/stories/2024/07/por-que-cerrar-la-brecha-de-habilidades-ciberneticas-requiere-un-enfoque-colaborativo/

Richards, B., Walker, S., y Blair, L. (2011). Cyber-Sustainability: leaving a lasting legacy of human wellbeing. *Researchgate*. https://doi.org/10.14236/ewic/HCI2011.18

Suplantación de la identidad digital en la era de la inteligencia artificial. En pos de la autenticidad en un mundo virtualizado

Carlos González[1]

Introducción

Las redes sociales, que en realidad son servicios de red social, han jugado un papel cada vez más preponderante dentro del ámbito de la comunicación y la socialización de los seres humanos. Con el paso de los años, no solo ha ido aumentando la importancia de estas funcionialidades en cuanto a la interacción humana, sino que se han convertido en el ágora del Siglo XXI.

En este sentido, Moreno et al. (2024) han establecido que la función de interconexión inicialmente asociada a los operadores de redes sociales, se ha convertido en el vehículo conductor de las discusiones que derivan en toma de decisiones sobre la forma en que el conglomerado asumirá los asuntos públicos de su país.

Si bien ya comenzaba a ser preocupante la presencia de comunicaciones mediadas principalmente por elementos tecnológicos, el temor creció a medida que comenzaron a surgir funcionalidades de Inteligencia Artificial (IA). En un principio, estas nuevas herramientas se utilizaron como apoyo para la creación de contenidos, sin embargo, con el advenimiento de la IA generativa, capaz de crear archivos multimedia, textos estructurados y en general una amplia gama de potenciales contenidos, la situación alcanzó niveles cada vez más complejos.

Las circunstancias han escalado de nivel, de tal forma que la preocupación por la identidad en el ámbito digital, ha tenido que lidiar con distintas y cada vez más complejas amenazas en un período de tiempo bastante corto (Estella, 2025).

La suplantación de identidad, que comenzó de manera artesanal, robando datos de personas para construir perfiles falsos, ha devenido hoy en día en la creación de verdaderos ejércitos de perfiles falsos, ya no solo con la intención de hacerse pasar por otras personas, sino influir en el pensamiento colectivo. Esto, aparte de plantear dilemas morales y éticos, urge la necesidad de tomar acciones para enfrentar de manera consciente el desafío que representa hoy en día, la intervención de la IA en los servicios de red social.

[1]Licenciado en Administración egresado de la Universidad de Los Andes (ULA), MSc. en Educación mención Informática y Diseño Instruccional. Actualmente se desempeña como investigador en el Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL). cgonzalez@cenditel.gob.ve

El propósito de presente trabajo, es mostrar las tres principales aristas de la suplantación de identidad en espacios digitales, comenzando con la suplantación clásica, en la cual una persona busca suplantar a otra persona o a una organización a través de la creación de perfiles falsos, siguiendo con la creación de ejércitos de perfiles falsos para manejarlos e interactuar con otros usuarios, y finalmente la introducción de la IA generativa como herramienta no solo para crear perfiles falsos, sino para gestionarlos, generando contenidos de manera autónoma, con la finalidad de modelar el pensamiento de la sociedad.

Finalmente, se hará una breve reseña acerca de cuáles son las principales potencialidades a desarrollar en la sociedad actual, para lidiar con la presencia de este tipo de interacción no humana o mediada por la IA, para posteriormente presentar una reflexión acerca de los principales retos que implica esta nueva realidad.

El mundo digital o ciberespacio como herramienta de socialización

Desde tiempos inmemoriales, los seres humanos han socializado, constituyendo esta actividad el pilar fundamental del desarrollo de las civilizaciones (Santamaría, 2015). Esta actividad permaneció imperturbable, solamente cambiada por los métodos para desarrollarla. Sin embargo, con el advenimiento de la Internet, y particularmente desde que se lanzaron las plataformas de red social, el ágora o espacio de socialización donde se comparte con otras personas, ha trascendido, en lo que se denomina genéricamente como redes sociales.

El concepto de red social, el cual fue desarrollado por John Barnes, hace más de setenta años, se refiere a los vínculos existentes entre las personas que están en contacto (Ahmed et al., 2024). Sin embargo, el mismo autor establece que ese concepto fue tomado por las plataformas digitales para ser llevado al ámbito virtual. Es así como surge la confusión entre servicios de red social y redes sociales.

Queda establecido entonces, que el mundo digital o ciberespacio, está constituido por las funcionalidades computacionales que permiten la expresión de las personas en este ámbito, y como consecuencia se han constituido como un contexto, primero alternativo, y luego principal de las relaciones sociales entre los seres humanos (Muros, 2011).

El concepto de identidad digital

La identidad es un derecho humano, vinculado con la posibilidad de individualizar en una persona ciertas características que la hacen única (Santamaría, 2015). Este concepto, el cual se encuentra bien establecido en el ámbito físico, no es tan obvio dentro de espacios mediados por tecnologías informáticas o espacios digitales.

En este sentido, Muros (2011), establece que en el ámbito digital, la identidad no solamente depende de lo que la persona es, sino de lo que pretende o desea ser. Este añadido trae consigo implicaciones distintas a lo que es la identidad física. Por ejemplo, en los espacios digitales se comparten fotografías, datos personales, aficiones, se muestra el círculo

de amistades y familiares, entre otras características, las cuales, en conjunto conforman el concepto de identidad digital.

Del mismo modo, en el ámbito digital, las personas tienen una reputación. Según Santamaría (2015), esta reputación depende de cómo se manejen todos los aspectos que conforman la identidad digital. Esto significa que todo lo que es mostrado a través de servicios de red social, y que conforman el concepto de identidad digital, definen igualmente la reputación de las personas.

Como consecuencia de lo anterior, dentro del presente escrito se entenderá como identidad digital, un concepto construido a partir de lo que establecen Santamaría (2015) y Muros (2011). La identidad digital es un conjunto de datos e información propios de cada persona que participa en las dinámicas de los distintos servicios de red social, lo cual, en conjunto configura un perfil de comportamiento, el cual define la reputación de cada persona en el ciberespacio.

Suplantación de la identidad digital

Como se ha explicado anteriormente, la identidad digital trasciende los aspectos físicos del concepto, incluyendo todos los datos compartidos en la red. En este sentido Martínez (2024) afirma que cualquier acción orientada a utilizar sin permiso los datos que conforman la identidad digital de otra persona, configura una suplantación. Si se utiliza el nombre de la persona, su fotografía, incluso vivencias o experiencias ajenas presentadas como propias, esto se considera suplantación de identidad.

Por otra parte, Santamaría (2015), establece, debido al carácter social y cambiante de la información digital, es necesario tener especial cuidado al momento de tomar decisiones sobre aquello que se comparte en el ciberespacio. Esto se debe a que lo compartido en este ámbito, constituye la reputación de cada persona. Como consecuencia de lo anterior, es lógico pensar, según Muros (2011), que existan personas interesadas en hacer pasar datos de la identidad digital ajena como propios, para realizar actividades reprobables e incluso ilícitas a nombre de otras personas.

Por esta razón, Gabaldón y Pereira (2008) deja claro que la suplantación de la identidad digital se realiza siempre con fines inconfesables, generalmente para cometer acciones ilegales a nombre de terceras personas, arruinando su reputación. Es por esto que cada vez más la legislación de distintos países, toma en cuenta esta práctica como un delito.

Métodos de suplantación de identidad digital: Del robo de información a la ultrasuplantación o *deepfake*

La suplantación de identidad en el ámbito digital, ha sido una preocupación creciente a partir del momento en que los individuos comenzaron a interactuar a través de servicios de correo electrónico, mensajería, entre otros. La necesidad de corroborar la verdadera

identidad de quienes interactúan en el ciberespacio, ha pasado de mera preocupación a una necesidad ineludible (Martínez, 2024).

Hoy en día no es solo necesaria la certeza acerca de quién está detrás de otros dispositivos tecnológicos afirmando ser alguien en particular, principalmente para evitar que una persona suplante la identidad de otra con el fin de realizar engaños (Montaperto, 2018). En el ámbito actual, donde la mayoría de transacciones comerciales son llevadas a cabo a través de medios digitales, es vital la protección de la identidad en este ámbito, principalmente para evitar que terceras personas suplanten la identidad de otras o de empresas, para obtener un beneficio de manera fraudulenta.

En este sentido, Gabaldón y Pereira (2008) establecen que pueden existir dos tipos de suplantación de identidad: el robo de la identidad de una persona o empresa existente, y también la creación de perfiles completamente falsos, ambos casos con el propósito de obtener un beneficio de forma fraudulenta.

Como consecuencia de lo anteriormente expuesto, puede entonces construirse un hilo narrativo, orientado hacia el entendimiento de la evolución de la suplantación de identidad, comenzando como una práctica realizada por simple diversión, pasando por el uso indebido de una identidad ajena para dañar la reputación del legítimo propietario de la misma, hasta la creación de perfiles falsos para promover fraudes financieros y sociales masivos.

Finalmente, la mayor preocupación radica en la práctica de algunos delincuentes informáticos, los cuales utilizan desde la suplantación de medios tradicionales, tales como tarjetas de débito o crédito, hasta el hurto de la identidad digital a empresas financieras, para intentar "pescar" incautos, constituyendo el método de *phishing*, palabra del inglés deformada deliberadamente para convertirla en el concepto ya establecido, y que ha pasado de manera informal al idioma castellano como un anglicismo (Gabaldón y Pereira, 2008).

Todas las modalidades expuestas, tienen en común la intención de causar daño. El espectro pernicioso de estas prácticas varía desde daños menores o confusión con fines de diversión malsana, pasando por la vulneración de la reputación de las personas, hasta llegar a la posibilidad de la comisión de estafas financieras (Montaperto, 2018).

En un mundo cada vez más dependiente de la interacción digital, las crecientes preocupaciones sobre la veracidad de la identidad de personas y empresas se erigen como limitantes tóxicas de las relaciones interpersonales, en un vicioso crescendo que pone en peligro la confianza en la interacción humana en la era digital, pues las herramientas para llevar a cabo este tipo de actividades generan resultados, principalmente a través de las funcionalidades de Inteligencia Artificial (IA), que dificultan cada vez más el discernimiento entre lo real y lo falso (Martínez, 2024).

A partir de este momento, se hará un esbozo de las principales modalidades de la suplantación de la identidad digital en la actualidad, a través de la explicación de casos

particulares vinculados con cada una de las formas.

La información se presentará en forma de progresión, posicionando en primer término la suplantación como método de engaño u ocultamiento de la verdadera identidad, pasando luego a los daños a la reputación por venganza, posteriormente se presentará el caso de secuestro de la identidad profesional, para finalmente mostrar los peligros de esta práctica en el ámbito educativo.

Suplantación para el engaño

Tal como se ha establecido, la suplantación de identidad apunta principalmente hacia la estafa. Las herramientas que ofrece hoy en día la IA, permiten la creación de fotografías, audio e incluso vídeo, incluso con funcionalidades gratuitas, fácilmente accesibles a través de una simple búsqueda en línea (Estella, 2025).

Ya no es necesario robar fotografías, basta con una sola de ellas compartida por un usuario, para que a través de una IA generativa, se puedan desarrollar diversas imágenes de esa persona. Basta con grabar un fragmento de conversación, para que este mismo tipo de herramientas pueda crear un audio con las voz de la persona grabada. Del mismo modo, se pueden generar vídeos.

Si bien este tipo de herramientas de IA generativa aun no ha alcanzado un nivel que le permita eludir los análisis profundos, a simple vista las creaciones fabricadas usando estas herramientas, pueden confundir incluso al ojo más entrenado (Ramos, 2024).

En este punto, es necesario enfatizar que quienes desarrollan este tipo de actividades, lo hacen generalmente con un propósito pernicioso, sin embargo Ramos (2024), establece que esto no fue siempre así, ya que este tipo de representaciones se utilizan para dar vida — por ejemplo — a personajes históricos que expliquen de primera mano sus acciones a un público ávido de conocerlos directamente a través de sus protagonistas.

Esta dicotomía entre las buenas y malas intenciones ha creado una corriente, la cual ha separado el *deepfake* o ultrasuplantación entre "bueno y malo". Sin embargo, el mísmo término de ultrasuplantación, tal como lo describe Estella (2025), guarda intrínsecamente una connotación negativa, pues el término en español está compuesto por la palabra suplantación, lo cual indica una actitud perniciosa. Igualmente en el inglés, el término incluye la palabra *fake*, la cual significa literalmente falso.

En este sentido, debe entenderse la ultrasuplantación como un término que busca fines inconfesables, ya que los intentos de darle una connotación positiva, chocan directamente con el contexto para el que fueron creados. Valga elejemplo anterior, cuando se le da vida a un personaje histórico, no se pretende suplantarlo, ni que las personas que lo vean, piensen que ha vuelto a la vida.

En consecuencia, la ultrasuplantación o *deepfake*, es la base sobre la cual descansa todo un entramado de engaño con distintos fines, los cuales varían desde la venganza o intención de dañar la integridad o reputación de una persona, hasta la comisión de los delitos más graves.

Venganza digital o daños a particulares

El daño a la reputación motivado por distintas causas, es una de las primeras capas de los efectos de la suplantación digital. Las personas maliciosas buscan confundir al entorno del objetivo del ataque, de tal forma que se conviertan en motivo de burlas, escarnio público forjado, e incluso ser potencialmente convertidos en protagonistas de escándalos de índole sexual (Estella, 2025).

La venganza suele ser una de las principales motivaciones para realizar una ultrasuplantación orientada hacia una persona en particular. Es común ver cómo han aumentado la cantidad de fotografías, audios e incluso vídeos, en los cuales las personas involucradas aparecen en actividades que nunca han realizado, u ofreciendo declaraciones inexistentes (Ramos, 2024).

En este sentido, y pese a que comienza a existir la percepción de que una persona que aparezca en actitudes potencialmente reñidas con sus características habituales, podría ser víctima de este tipo de situaciones, el nivel de realismo de estas ultrasuplantaciones es cada vez más impactante. Por esta razón, existe una tendencia gradualmente creciente a dudar de los archivos multimedia que son difundidos de manera no convencional.

Sin embargo, más allá de la necesidad de corroborar la veracidad de una publicación que podría exponer o vulnerar la reputación de las personas, es necesario lograr un nivel de interacción tal, que permita retomar la confianza que generaban las relaciones interpersonales directas (Martínez, 2024).

Esto es de vital importancia, principalmente debido a que en la actualidad, la sociedad digital está aislando a las personas (Estella, 2025). Esto se puede corroborar, a través de la creciente desconfianza que generan las interacciones a través de redes sociales. Esto incluso ha llegado a generar desconfianza a niveles donde los actores de la interacción en el ciberespacio se cuestionan temas tales como ¿es realmente mi amigo quien escribe?.

La duda genera un estado de permanente vigilancia y escepticismo, envenenando o haciendo tóxicas las relaciones digitales. Tal como lo expone Martínez (2024), la pérdida de confianza entre los actores digitales podría erosionar la socialización entre las personas, principalmente entre los jóvenes, quienes de manera progresiva han comenzado a generar paranoias vinculadas con la posible falsedad de la identidad de las personas con quienes interactúan.

Estella (2025), va más allá, sugiriendo que la falta de certeza sobre las identidades

digitales, y el temor a ser víctimas de algún tipo de ultrasuplantación, podría provocar daños psicológicos, trascendiendo el simple menoscabo de la reputación, lo que podría ser un elemento disociativo de la socialización.

Finalmente, Gabaldón y Pereira (2008), aseveran que incluso una venganza o intención de daño personal podría causar daños profundos en el ámbito financiero, puesto que los ciberdelincuentes podrían causar, ya sea de manera intencional o indirecta, una vulneración del patrimonio de la persona atacada, ya sea generando situaciones que le causen pérdidas en su erario, o indirectamente, debido a que los afectados necesiten invertir dinero para revertir los daños causados a su reputación.

Secuestro de identidad profesional

Una capa más profunda de la suplantación de identidad, está dada por el secuestro de la identidad de los profesionales o figuras públicas de peso. Tal como es estableció anteriormente, Ramos (2024) estableció que existe una visión que podría tener una connotación positiva sobre la ultrasuplantación, poniendo como ejemplo la generación de recursos multimedia protagonizados por personajes históricos con fines educativos.

En el caso de la suplantación de identidad profesional, los *deepfake* podrían ser usados para mostrar a figuras públicas, o de peso dando declaraciones, o proclamando hallazgos científicos totalmente falsos. Esto sube las apuestas en cuanto al peligro intrínseco a este tipo de actividades ilícitas. Un político dando una declaración explosiva en una ultrasuplantación, podría ser desvirtuado, sin embargo en el ínterin, las declaraciones falsas podrían generar situaciones caóticas.

En este punto, aparece un riesgo inminente señalado por Estella (2025), quien afirma que una declaración falsa atribuida a una personalidad de renombre puede tener consecuencias incalculables, los cuales pueden ir desde la histeria colectiva, hasta otro tipo de acciones que podrían resultar nocivas para toda la sociedad.

En el caso de la recreación de figuras históricas con la intención de crear un ambiente inmersivo, generalmente con fines pedagógicos, ya se podrían presentar efectos contraproducentes tales como dudas sobre la veracidad de la representación de los personajes, su voz si se trata de quienes vivieron antes de la invención de las grabaciones, entre otras, el caso de usar figuras de renombre existentes podría tener consecuencias devastadoras (Ramos, 2024).

Esta situación evidencia el peligro potencial del uso de la IA generativa con fines apartados de la moral y la ética con fines de manipular la opinión pública, lo cual trasciende de manera evidente la vulneración de los derechos de quien está siendo objeto de la ultrasuplantación, trascendiendo lo personal, hasta escalar a un problema social.

Identidad digital en la educación

Uno de los puntos más importantes dentro de la sociedad en el cual impacta directamente la suplantación de identidad es la educación. Según Toro (2024), los archivos multimedia generados a través de ultrasuplantación, son un peligro inminente para los estudiantes, especialmente los más jóvenes.

Los más jóvenes, especialmente niños y adolescentes, pese a que están inmersos en el ámbito digital y sus interacciones sociales se basan principalmente en las plataformas de servicios de red social, por el mismo hecho de dar por sentado que este tipo de interacción es la norma, podrían terminar por no utilizar ningún filtro discrecional que les permita discernir entre una creación digital y la realidad (Toro, 2024).

Por otra parte, dentro del ámbito educativo, específicamente en el ámbito de la educación en línea, es vital el concepto de la identidad. Tanto los estudiantes como los facilitadores deben tener la seguridad de que son ellos con quienes efectivamente está interactuando la comunidad educativa. En este sentido, cobra particular importancia el concepto del yo digital, presentado por Muros (2011).

Este concepto se refiere principalmente a la convergencia obligatoria entre la identidad física de las personas y su identidad digital, principalmente cuando se trata de actividades como la educación mediada por tecnologías informáticas. Cuando se está aprendiendo, los estudiantes deben ser ellos mismos quienes interactúen con las actividades en línea, del mismo modo, los facilitadores deben ser quienes personalmente se encarguen de orientar el proceso educativo.

Estas dos aristas, son de vital importancia al momento de comprender la trascendencia del concepto de identidad en el ámbito de la educación. La primera de ellas, evoca la necesidad de preparar a todos los involucrados en el proceso de enseñanza – aprendizaje para una realidad en la cual, los estímulos recibidos a través de los sentidos, los cuales son generados y presentados por y a través de medios digitales, podrían no ser lo que parecen.

En este sentido, Murguía Serrano et al. (2025) plantean la necesidad de preparar a todos los involucrados tanto en la creación como en la detección de contenidos contentivos de ultrasuplantación. En el caso de la creación, la preparación iría orientada principalmente hacia la generación de competencias para reconocer y utilizar las principales herramientas creadoras de deepfakes. En el caso de la detección, es necesario formar individuos críticos, capaces de utilizar herramientas digitales para verificar la autenticidad de los contenidos digitales.

La manipulación de la opinión pública: Un ejército en las sombras

En la primera parte de este escrito, se presentó un análisis sobre la suplantación de identidad de personas o instituciones reales, con la finalidad de engañar a las personas, al intentar hacer pasar la identidad falsa como si fuese la original, mostrando distintas aristas

o casos del problema. Sin embargo, esta situación trasciende con creces lo esbozado.

Existe la tendencia de crear cuentas falsas para interactuar en los principales servicios de red social, sin embargo, como lo establecen Curry y Gradecki (2025), la creación manual de una gran cantidad de cuentas y perfiles falsos, sería una actividad muy engorrosa. Por esta razón, se crearon funcionalidades en la IA generativa, que permiten la creación de múltiples perfiles que pueden ser manejados en simultáneo.

Los "*sock puppets*", personajes sintéticos a gran escala

Los *sock puppets*, que traducido literalmente significa marioneta de calcetín, es un término que ha aparecido para describir los perfiles falsos en los servicios de red social. No se trata solamente de generarlos, ya que su mera existencia no tendría sentido.

Se trata de marionetas porque pueden ser controladas, y tal como lo explican Curry y Gradecki (2025), se utilizan para actuar como un verdadero ejército, no portando armas, sino ideas que son dirigidas a través de ellos. Los tópicos de conversación, las impresiones, puntos de vista y opiniones sobre un tema, son dirigidos a través de estos perfiles, que actúan como verdaderas legiones romanas asumiendo su famosa formación de combate en tortuga.

Del mismo modo, los mencionados autores dejan claro que no solamente se trata de manejar o manipular la opinión a través del trabajo coordinado de cuentas falsas. También, hoy en día existe la posibilidad de crear a través de funcionalidades de IA generativa, una marioneta hiperreal, que a simple vista puede parecer una persona. Gracias a esto, es posible generar personas que no existen, comprar seguidores generados por IA, para inflar sus números, y de esta forma generar *influencers* que comenzarán a captar humanos reales, para apoyar y diseminar las ideas promovidas por la marioneta informática.

En este punto, es necesario destacar que los *sock puppets*, comparten características particulares, principalmente evidenciadas por sus rasgos lingüísticos (Kumar et al., 2016). Principalmente, los perfiles falsos que actúan en conjunto, generalmente lanzan la misma frase una y otra vez en distintas publicaciones, construyen las frases y la estructura de sus mensajes de una manera estandarizada y muchas veces sin la fluidez del lenguaje humano.

Ya no se trata de cuentas creadas para simular un gran número de seguidores o interacciones con "me gusta". Se han convertido en redes de "personas artificiales" que simulan opiniones, interacciones, e incluso pueden simular comunidades enteras (Curry y Gradecki, 2025), todo con un solo fin: el posicionamiento de ideas y mensajes orientados por quienes manejan a las marionetas virtuales.

Tendencias fabricadas o *astroturfing*

Los ejércitos de bots o sock puppets, como ya se ha mencionado, tienen como finalidad posicionar en los servicios de red social ciertas narrativas, políticas comerciales específicas,

e incluso un pretendido apoyo a ideologías políticas (García et al., 2019).

En este sentido, es necesario acotar que la forma que se utiliza en el ámbito de los servicios de red social para posicionar las ideas promocionadas por los actores interesados en influir a través de los perfiles falsos o *sock puppets*, viene dada por el intento de hacer creer a las personas reales que existe una masa crítica de personas en favor de una idea, ya sea política, social, comercial, o simplemente la percepción sobre cualquier tema en particular (García et al., 2019).

El uso de ejércitos de perfiles falsos, interactuando a través de los servicios de red social para construir una narrativa favorable a determinados grupos económicos o de poder, es conocida como *astruturfing*,o por su equivalente en español que podría ser campaña de opinión orquestada. De esta forma, se busca distorsionar la opinión pública, en favor de ideas o productos de interés para ciertos grupos (Arce-García y Said-Hung, 2022).

Del mismo modo, los autores señalan que existen empresas dedicadas no solo a la creación de cuentas falsas de manera masiva. Las empresas existentes se dedican igualmente a construir campañas, de acuerdo a las solicitudes de sus clientes. La intención de este tipo e campañas es generar a través de ejércitos de perfiles falsos, para convertir una narrativa determinada en tendencia predominante, simulando un apoyo inexistente (Curry y Gradecki, 2025).

Ataques coordinados para la desinformación

El *astroturfing* o campañas para la desinformación diseñadas para inundar las redes con noticias falsas, tendencias artificiales e incluso discursos de odio, son amplificados por miles de perfiles falsos para dar la ilusión de consenso (Arce-García y Said-Hung, 2022). Este tipo de campañas se hacen de manera organizada, no dejan nada al azar, y generalmente buscan ocasiones particulares, en las cuales puedan desplegar su actividad desinformativa.

Esto, según Curry y Gradecki (2025), apunta generalmente hacia la pulverización de las opiniones que son desfavorables a las tendencias creadas artificialmente. Para lograr esto, no solo es necesario programar opiniones y respuestas favorables al tema que se desea posicionar. Es necesario igualmente que se maneje una masa que genere opiniones contrarias a las tendencias rivales.

En este sentido, García et al. (2019) realizan una argumentación que conduce a presumir la vital importancia de las cuentas con opiniones contrarias a los rivales. Muchas veces el vituperio y los discursos radicalmente opuestos a la temática que se desea convertir en tendencia, generan una sensación de apoyo más contundente que el apoyo.

Esto genera, según Arce-García y Said-Hung (2022), una especie de "fuenteovejuna digital", en la cual las personas no se unen para combatir una injusticia, sino a un comendador ficticio (persona, entidad o ideología) expuesto como agresor, o lo que es peor, acusado injustamente de causar perjuicios, para lograr unión en torno a su condena social. Esto

genera peligros inminentes y plantea debates morales profundos. Del mismo modo, puede causar a partir de una idea o discurso falaz, el cambio de opinión sobre determinada temática que afecta a toda una comunidad.

Interferencia en procesos democráticos

En el caso de la política el ataque de enjambres de cuentas falsas puede causar efectos muy perniciosos en cuanto a la búsqueda del bien común. La manipulación generada por los *sock puppets*, enfilados contra una determinada ideología a través de prácticas de *astroturfing*, puede desencadenar en la manipulación de elecciones o debates públicos a través de la creación de perfiles que polarizan y dividen a la ciudadanía, haciendo que tomen partido por opciones que no necesariamente encarnan las legítimas aspiraciones del colectivo (Arce-García y Said-Hung, 2022).

Los espacios digitales han ganado terreno especialmente en el último lustro (García el al., 2025). Durante ese período, esencialmente la población más joven ha hallado un espacio de interacción social, que ha reemplazado paulatinamente los espacios tradicionales. De este modo, los debates políticos, especialmente aquellos vinculados a la realización de procesos de elecciones, están inevitablemente marcados por las tendencias surgidas de la interacción digital.

De lo anterior, se desprende una serie de preocupaciones acerca de la posibilidad real de interferencias no en procesos electorales en sí, sino en la formación de opiniones acerca de los mismos (Arce-García y Said-Hung, 2022). Esto genera una realidad inquietante, puesto que en este escenario, la intrusión en contextos comiciales no se basa en vulnerar la integridad de los datos de la votación, sino en hacer que las personas voluntariamente, elijan opciones que en realidad no son su elección, sino que han sido impuestas por la interacción digital.

Esto desvirtúa el debate público, imposibilitando la distinción entre la voz ciudadana genuina y la propaganda automatizada, y en última instancia amenaza la salud de las democracias al socavar la integridad de los procesos de formación de opinión (Arce-García y Said-Hung, 2022). El proceso de formación de criterios políticos, está entonces, intoxicado por cámaras de eco y burbujas informativas (o desinformativas) radicalizadas, donde la discusión y argumentos se ve dominada por actores no humanos.

La “Internet Muerta”: El ocaso de la interacción auténtica

Hasta este momento se han delineado dos aspectos sobre creación de identidades falsas están directamente mediadas por seres humanos. En el caso de la suplantación para intentar hacerse pasar por otra persona, incluso una empresa, se hace de manera dirigida hacia particulares. En el segundo caso, se crean perfiles masivos para influir en el desarrollo de ideas en los servicios de red social, con la pretensión de imponer una visión.

Estas dos primeras visiones tienen en común, que si bien pueden utilizar funcionalidades de IA para generar los perfiles falsos y/o ejércitos de identidades inexistentes de manera

creíble e incluso capaz de confundir a la mayoría de las personas, siempre son humanos los que dirigen el proceso valiéndose de las herramientas generativas para lograr sus propósitos.

Sin embargo, en este punto cabe una pregunta: ¿Es el contenido que veo en Internet generado por humanos? Esta interrogante no es un desafío hipotético, sino la consecuencia de una realidad palpable. Las granjas de *bots* tradicionales — por citar un ejemplo — donde se manejan miles de cuentas, dependen de la automatización simple y la mano de obra humana para operarlas. Sin embargo, los algoritmos de IA pueden elevar la sofisticación y la capacidad de engaño de estas operaciones.

Más allá de la credibilidad del engaño, el hecho de que la generación de contenido, ideas, narrativas críticas, documentos, e incluso la orientación del pensamiento que se desea posicionar sea llevado a cabo por un algoritmo y no por humanos, cambia la ecuación y crea retos mayores.

El crecimiento de esta tendencia ha creado un nuevo concepto, el cual si bien en un principio se consideró meramente una teoría conspirativa, está siendo repensado desde ópticas distintas, pues está presente y cada vez gana más terreno, se trata de la "Internet Muerta", que es descrita por Walter (2024), como un escenario en el cual una proporción significativa del contenido y las interacciones en línea son generadas por IA sin supervisión humana, diluyendo la experiencia de interacción humana, sustituyéndola por una fascinación derivada de la interacción con algoritmos.

Esta situación crea una creciente preocupación acerca de la desaparición de las relaciones humanas legítimas, sustituyéndolas por conexiones meramente digitales, con el agregado de estar constituidas no por interacción digital con otros humanos, sino con IA, creando una fascinación por el intercambio con estos algoritmos, creados deliberadamente para crear descargas de dopamina (entre otros neurotransmisores), para generar adicción por ciertos tipos de contenidos (Walter, 2024).

En este sentido, a continuación se presentan las principales características de la denominada Internet Muerta, de tal modo que se pueda comprender el alcance de este fenómeno, a la vez que se muestran los nuevos retos que aparecen debido a esta creciente tendencia.

Contenido generativo masivo

Cualquier persona que haya interactuado con una funcionalidad de IA, puede corroborar que son capaces de producir textos, imágenes, video, entre otros, al tiempo que los analiza en cuestión de segundos. Esta capacidad permite la creación de contenido masivo en tiempos ínfimos (Özgürel et al., 2024).

Por otra parte, las funcionalidades de IA generativa pueden crear contenido que es de alta calidad, por ejemplo, fotografías y vídeos de alta resolución que podrían engañar fácilmente a cualquier usuario desprevenido, convirtiéndose en una amenaza para la integridad de la

información que se encuentra en línea (Walter, 2024).

Se pueden generar en segundos *blogs*, artículos, hilos de la red "X" y comentarios en foros creados por IA para simular actividad, llenar espacios vacíos o manipular algoritmos de SEO. Esto es solo una parte de lo que puede hacer un algoritmo generativo. Debido a la velocidad conque crece este tipo de contenidos masivos, es válido dudar de cualquier publicación que no esté respaldada por la credibilidad de la evidencia presentada para respaldar lo que se presenta.

Por otra parte, Walter (2024) establece en los resultados de su investigación, que el flujo de contenidos e interacciones en línea están siendo tomados por asalto por la IA, haciendo que la interacción entre seres humanos en estos espacios sea cada vez menor.

En este punto, la mayor preocupación radica en cómo se puede discernir cuál contenido es creado por humanos realmente. No existe un control sobre la identidad de un creador no solo de historias, sino de obras artísticas tales como pinturas, fotografías e incluso obras literarias. No es posible establecer cómo la interacción con creaciones hechas por no humanos podría afectar la psiquis de quienes sí lo son.

Interactores no humanos

Cuentas que responden automáticamente a publicaciones, simulan conversaciones o generan opiniones en todos los ámbitos del quehacer humano sin un propósito creativo. Los humanos pueden creer que se trata de interacciones legítimas y de este modo crear opiniones sesgadas. Se trata de creaciones de los algoritmos, que al ser confundidas con creaciones humanas, distorsionan la percepción de quienes interactúan con éstas (Walter, 2024).

Cuando un humano interactúa con bots de IA, que simulan comportamientos humanos, están generando empatía o rechazo por opiniones, imágenes o vídeos que no guardan relación alguna con actividad humana. Cabe preguntarse dónde se dirige la atención de una persona cuando se enfrasca en conversaciones, diatribas o admiración por supuestas creaciones humanas, que en realidad no lo son.

En este sentido, Özgürel et al. (2024) establece que la interacción de seres humanos con una contraparte no humana, podría comenzar a generar sentimientos de empatía por actitudes y formas de abordar distintos temas que no son intrínsecas a la condición humana, en tanto que se trata de entidades artificiales, sustentadas en componentes no biológicos, se trata de la sustitución del sistema límbico de los seres biológicos por el sistema de circuitos de silicio.

Cabe entonces la pregunta ¿Puede un sistema artificial emular humanidad? Responder esta interrogante puede ser un reto en la actualidad debido a que las funcionalidades de IA están programadas a través del *machine learning* y el *deep learning* para emular respuestas que creen empatía. En este sentido, es de vital importancia cuestionar las interacciones digitales no verificadas, para intentar interactuar apropiadamente con humanos y con IA.

Entornos de aprendizaje contaminados

En la actualidad, las plataformas de aprendizaje en línea se basan en la idea de aprendizaje colaborativo, debido a que este concepto sintetiza el núcleo del proceso de aprendizaje, representado por conceptos tales como cognición, metacognición, emociones y motivación (Genimon Vadakkemulanjanal et al., 2025). En este sentido, se hace vital para llevar adelante un proceso de enseñanza – aprendizaje correctamente dirigido, una gestión adecuada de los procesos cognitivos.

Durante los años recientes, ha comenzado una tendencia, la cual de manera progresiva ha incluido la IA en estos procesos centrales de la educación, así lo establecen (Arámbulo Ayala de Sánchez et al., 2024), al afirmar que incluso la UNESCO ha manifestado la necesidad de incluir la IA de manera decisiva en el proceso educativo, dando paso al concepto de educación 4.0 en el cual la integración de tecnologías avanzadas es un punto vital.

Con el advenimiento de la IA generativa, muchos procesos educativos automatizados a través de plataformas de aprendizaje, han logrado ser optimizados a través de *software*, funcionalidades en línea, y otras tecnologías, han comenzado a utilizar herramientas generativas avanzadas para realizar el trabajo que antes realizaban los humanos (Genimon Vadakkemulanjanal et al., 2025).

Del mismo modo en que la identidad de las personas ha sido usurpada por funcionalidades de IA avanzadas, los contenidos educativos están siendo generados de esta forma, desplazando de forma silenciosa a los humanos (Arámbulo Ayala de Sánchez et al., 2024). Es conocido que los materiales educativos, llamados también objetos virtuales de aprendizaje en el ámbito de la educación en línea, deben guardar relación con sus pares desarrollados en épocas previas a la digitalización.

Los estudiantes de todas las etapas, desde la educación inicial hasta la univesitaria, incluyendo niveles de postgrado, están comenzando a interactuar con funcionalidades no humanas, las cuales están presentes en el dominio cognitivo del proceso educativo, sino también en el afectivo y psicomotor (Genimon Vadakkemulanjanal et al., 2025).

Esto constituye un riesgo, puesto que el trabajo en conjunto de los tres dominios del ámbito educativo depende de la interacción con facilitadores que van más allá de proporcionar los datos en información (Arámbulo Ayala de Sánchez et al., 2024). Cabe cuestionarse, por ejemplo, cómo un niño que está aprendiendo nociones básicas sobre el desarrollo del lenguaje podría verse afectado al interactuar sin saberlo, con una funcionalidad no humana o no generada por seres humanos directamente.

Es necesario entonces, comenzar a desarrollar potencialidades tanto en los estudiantes como en los facilitadores, para reconocer y utilizar de manera controlada las funcionalidades educativas generadas por IA, y las actividades mediadas por este tio de tecnologías (Genimon Vadakkemulanjanal et al., 2025), de tal forma que la humanidad de los educandos no se vea afectada, planteando escenarios potencialmente riesgosos, dado que la educación impacta

directamente sobre la sociedad.

Enfrentando la triple amenaza: Acciones inminentes

A lo largo del presente escrito, se han presentado argumentos orientados a describir tres amenazas: la usurpación de identidad, los ejércitos de *bots* y la "Internet Muerta", para mostrar que juntos representan una crisis convergente para la identidad y la autenticidad digital, específicamente erosionando los conceptos de verdad, confianza y responsabilidad en un espacio donde diferenciar lo humano y lo artificial se convierte en una ardua tarea.

Como consecuencia de lo expuesto, es necesario plantear la necesidad de tomar acciones, debido a que la pasividad, tal como lo establecen Curry y Gradecki (2025), constituye una perniciosa actitud, debido a que deja potencialmente en manos de la IA, la posibilidad de construir a su medida tanto los espacios de interacción digital, como la forma en que éstos son usados. En pocas palabras, existe el riesgo de la deshumanización de la socialización.

Intentar concebir una socialización carente de humanidad sin la presencia de la IA generativa sería prácticamente imposible. Probablemente se podría hablar de usurpación de identidad y creación de *bots* o personajes falsos Özgürel et al. (2024), sin embargo, las funcionalidades capaces de generar creaciones casi humanas han llevado esto a otro nivel, puesto que sus productos son muy difíciles de distingur de los creados por humanos. Por esta razón es necesario emprender acciones orientadas hacia el discernimiento sobre el origen de todo aquello con lo que se interactúa en espacios virtuales.

Alfabetización digital crítica

En la actualidad, el concepto de alfabetización tecnológica cobra nuevas dimensiones. En un principio, se trataba únicamente de conocimiento acerca de jerga tecnológica vinculada a la computación. Sin embargo, con el advenimiento de los servicios de red social, es necesario comprender nuevos términos, esta vez relacionados con la socialización, tanto en el ámbito tradicional, como en el ámbito virtual (Arámbulo Ayala de Sánchez et al., 2024).

Es necesario entonces, que los actores en todos los ámbitos de la vida cotidiana, no solo comiencen a manejar terminología sobre informática, sino que se requiere el desarrollo de competencias digitales, las cuales según Arámbulo Ayala de Sánchez et al. (2024), permiten crear conciencia acerca de todas las implicaciones del ámbito virtual en la actualidad.

Para poder lograr una correcta alfabetización tecnológica para afrontar la realidad actual es necesario, según Genimon Vadakkemulanjanal et al. (2025), que las instituciones educativas proyecten dentro de sus programas de estudio, cursos dirigidos a la construcción de las potencialidades necesarias dentro de la era de la IA, mostrándola como una funcionalidad con la cual se puede interactuar simulando que son humanos, pero siempre teniendo presente que sus respuestas son simuladas, para comportarse como humanos.

Por otra parte, advierten también Genimon Vadakkemulanjanal et al. (2025), que la rapidez y alta precisión con que las funcionalidades de IA producen resultados de alta calidad, puede generar la falsa sensación de infalibilidad. Esto es falso, pues los algoritmos de IA, si bien generan respuestas bastante precisas, pueden cometer errores, incluso pequeños, tales como errores de ortografía.

Es necesario entonces, educar para la sospecha, con una orientación hacia el reconocimiento de señales de contenido no generado por humanos. Este tipo de formación de competencias informáticas en la era de la IA, solo será posible generando una interacción mediada por otros humanos, que serán los tutores para mediar en esta nueva forma de socialización con una forma de inteligencia creada por humanos, pero que en sí no lo es (Arámbulo Ayala de Sánchez et al., 2024).

Marcos regulatorios proactivos

Para lograr una relación saludable con las funcionalidades de IA, es necesaria la intervención del Estado, para regular la forma en que las empresas que crean y gestionan plataformas de IA se relacionan con la sociedad (Leon, 2023). Esta necesidad surge por la situación ya expuesta a lo largo del escrito, sobre la necesidad de distinguir el contenido generado por humanos, del que ha sido generado por IA.

Por otra parte, existe la preocupación acerca de lo que se puede hacer, debido a la condición de no territorialidad de muchos de estos servicios. Los Estados que pretendan regular el uso y la forma en que se realiza la interacción con las plataformas de IA, tienen por delante el reto de encontrar las fórmulas para alcanzar ese objetivo (Estella, 2025).

En este sentido Estella (2025), asegura que los sistemas de IA que se encuentran regulados, lo están bajo regulaciones orientadas hacia prohibir aquellos que presenten mayores riesgos para la sociedad. Si embargo, la metodología para determinar el grado de peligrosidad de una funcionalidad de IA, no puede medirse bajo parámetros cuantitativos. Leon (2023), asegura que la IA no debe ser regulada por representar una amenaza en sí, sino que la normativa debe estar dirigida a proteger los aspectos de los cuales se nutre este tipo de funcionalidades informáticas. La primera de ellas son los datos, pues para que un modelo de este tipo pueda funcionar, ya sea a través del *machine learning* o el *deep learning*, deben ser alimentadas con datos. En este sentido, quiénes y cómo manejen los datos que se usan para la IA deben ser objeto de la regulación.

Del mismo modo, es necesario legislar además sobre marcos éticos, los cuales establecen los parámetros éticos que sirven de marco para establecer qué debe o no debe ser hecho con la ayuda de la IA. En cuanto al manejo de los datos personales, más allá de los usados para alimentar los algoritmos, se trata de regular qué se debe o no hacer a través de la IA y la necesidad de consentimiento por parte del dueño de los datos para establecer su uso (Estella, 2025).

En general, los autores están de acuerdo en que la regulación de la IA debe englobar las

principales variables que son intrínsecas a ella, para lo cual el rol del Estado es primordial. Es necesario que si bien las funcionalidades de IA cumplen con un proceso interno de autorregulación, no es posible descargar todo el peso de la reglamentación sobre su uso sobre ellas mismas. En este sentido, el vínculo entre el Estado y la legislación debe ser el colectivo de usuarios de los algoritmos.

Tecnologías de verificación

A medida que la IA generativa ha avanzado, la verificación que permita discernir acerca de la autenticidad de un contenido ha variado. También es cierto que el hecho de que un contenido, por ejemplo multimedia, haya sido generado con IA, no implica que no sea legítimo. Por ejemplo, se puede mejorar un escenario en una fotografía, para que el fondo aparezca atenuado, o para resaltar con enfoque algunas figuras. Esto no hace ilegítima la foto, aunque no haya sido generada por medios tradicionales (López, 2025).

En este sentido, es necesario discernir qué tipo de contenidos deben ser objeto de verificación (Ahmed et al., 2024). Para ello, existen tecnologías que permiten realizar la verificación de archivos de texto, audio, video, entre otros. Es necesario igualmente acotar que, la mayoría de estas tecnologías para reconocer contenido generado por IA, está constituido precisamente por funcionalidades de este mismo tipo.

Es vital entonces, según (Özgürel et al., 2024), conocer tanto las herramientas que permitan verificar si los contenidos han sido generados por IA, e igualmente cuáles contenidos pueden ser perjudiciales, o incluso reportan peligros para la sociedad en caso de no poder ser detectados. Estas acciones pasan por comprender el riesgo de la IA generativa, con relación a la creación de contenidos potencialmente peligrosos. En este sentido, López (2025), establece que la educación digital orientada a la comprensión de las capacidades de la IA es vital.

Reflexiones finales

Las distintas variantes que ponen en riesgo la identidad digital en la era de la IA, si bien surgen a partir del uso indiscriminado de la IA, probablemente no puedan ser detenidas del todo sin prescindir de las herramientas generativas. Esta no es una opción en la actualidad, debido a que el campo de las tecnologías informáticas se está desarrollando en esta dirección.

Es un hecho que a medida que las tecnologías basadas en IA generativa crecen, su interacción con los humanos se hace más cercana. Si a eso se le suma la posibilidad de la usurpación de identidad por parte de estas funcionalidades, además de la creación masiva de perfiles falsos que simulen interacción con humanos, y además los contenidos generados no son humanos, entonces posiblemente se podría producir una simbiosis tal entre IA y las personas, que crearía un nuevo concepto de humanidad.

Esta humanidad digital podría verse como la cristalización de las fantasías de ficción, principalmente del género *cyberpunk*. La diferencia radica, que en el mencionado género de ficción, los humanos literalmente se implantaban componentes robóticos, pero en esta

realidad, los componentes están representados por IA generativa que hace el trabajo, tradicionalmente realizado por humanos.

Es entonces pertinente preguntarse: ¿Es suficiente la acción de detectar contenidos generados por IA? Esta interrogante es válida, puesto que si bien es posible detectar y discernir el contenido generado por IA, es necesario igualmente generar un marco moral y ético que regule la forma en que los humanos utilizan estas herramientas, para evitar la creación de libros, obras artísticas e incluso piezas musicales con la ayuda de estas funcionalidades.

Haciendo la conexión con el aforismo tan difundido, que la realidad puede superar la ficción, la IA generativa se ha constituido en una especie de implante en la vida de los seres humanos. No los dota de fuerza sobrehumana o habilidades imposibles para las entidades biológicas. Por el contrario, les provee la capacidad de generar de manera prácticamente inmediata, contenidos que sería imposible lograr a través de las capacidades humanas promedio. Se trata de evitar que los seres humanos, al igual que en la ficción *cyberpunk*, se conviertan en seres híbridos, no por los implantes, sino a través de sus creaciones.

Uno de los riesgos principales de esta tendencia, es la exclusión social. No todas las personas pueden acceder a las principales funcionalidades generativas de la IA. Esto podría crear élites que como en el mencionado género de ficción, utilicen las herramientas de este tipo para eregirse.

La idea debe centrarse en reinvindicar la agencia humana. La tecnología debe ser un puente para potenciar nuestra conexión y creaciones, no un frio muro que la simule. Las personas deben reclamar su derecho a crear, con la ayuda legítima de la IA sin perder la autenticidad. El desafío es construir un futuro digital donde la autenticidad, y no el simulacro, sea el valor supremo.

Referencias

Ahmed, A., Qamar, R., Asif, R., Imran, M., Khurram, M., y Ahmed, S. (2024). The Dead Internet Theory: Investigating the Rise of AI-Generated Content and Bot Dominance in Cyberspace. *Pakistan Journal of Engineering Technology and Science (PJETS)*, *12*, 37-48. https://doi.org/10.22555/pjets.v12i1.1077

Arámbulo Ayala de Sánchez, M. C., Martinez Peñaloza, M. Y., y Ramírez, P. (2024). Competencias digitales y la alfabetización en inteligencia artificial en estudiantes universitarios. *PHHOMINUM Revista de Ciencias Sociales y Humanas*. https://doi.org/10.47606/ACVEN/PH0312

Arce-García, S., y Said-Hung, E. (2022). Astroturfing y debate político español desde las redes sociales: un estudio de caso. *Sociologia, Problemas e Práticas*, (100), 107-124. https://doi.org/10.7458/SPP202210025549

Curry, D., y Gradecki, J. (2025). Epic Sock Puppet Theater: artistic tactics for mitigating online disinformation. *Artnodes E-Journal on Art, Science and Technology*, (33). https://doi.org/10.7238/artnodes.v0i33.418111

Estella, A. (2025). La regulación de las deepfakes (ultrasuplantaciones) en el reglamento de la UE sobre Inteligencia Artificial. *Revista de Administración Pública*, *226*, 261-290. https://doi.org/10.18042/cepc/rap.226.11

Gabaldón, L. G., y Pereira, W. (2008). Usurpación de identidad y certificación digital: propuestas para el control del fraude electrónico. *Sociologias*, *10*(20), 164-190.

García, J., Huicab, Y., Landeros, K., y Vargas, T. (2019). Transformando la educación en ciberseguridad: integrando tecnología educativa para formar profesionales resilientes en la universidad. *Ava Cient*, *5*(1), 22-32. http://avacient.chetumal.tecnm.mx/index.php/revista/article/view/49/50

Genimon Vadakkemulanjanal, J., Athira, P., Anit Thomas, M., Dawn, J., V., T., y P., M. (2025). *Impact of Digital Literacy, Use of AI tools and Peer Collaboration on AI Assisted Learning: Perceptions of the University students*. https://www.scielo.br/j/soc/a/TSw5QX8TVH3s7BQyppCBQrb/?format=html&lang=es

Kumar, S., Leskovec, J., Cheng, J., y Subrahmanian, V. S. (2016). An Army of Me: Sockpuppets in Online Discussion Communities. *Proceedings of the 25th International Conference on World Wide Web*, 1249-1259. https://cs.stanford.edu/~srijan/pubs/sockpuppets-www2017.pdf

Leon, C. (2023). La carrera por la regulación de la inteligencia artificial. *Revista Latinoamericana de Economía y Sociedad Digital*, (4). https://doi.org/10.53857/RLESD.04.2023.05

López, L. (2025). Inteligencia artificial generativa y confianza en los medios. Un análisis de la detección de IA en noticias usando GPTZero. *Vivat Academia. Revista de Comunicación*, (158), 1-17. https://doi.org/10.15178/va.2025.158.e1556

Martínez, G. (2024). Suplantación de identidad digital: Hacia una necesaria tutela penal. *Estudios de Deusto Revista de Derecho Público*, *72*. https://doi.org/10.18543/ed7212024

Montaperto, J. (2018). *Suplantación de identidad: Un análisis sobre su falta de regulación en el ordenamiento jurídico argentino* [Trabajo Final de Graduación]. Universidad Siglo 21. Córdoba, Argentina. https://www.pensamientopenal.com.ar/doctrina/90107-suplantacion-identidad-analisis-sobre-su-falta-regulacion-ordenamiento-juridico

Moreno, A., Castillero, E., y Serna, A. (2024). El impacto de las redes sociales en la campaña política: elecciones generales de 2023 en España. *RED MARKA Revista de Marketing Aplicado*, *28*, 56-76. https://doi.org/10.17979/redma.2024.28.1.10114

Murguía Serrano, J. Y., De la Toba Noriega, C. E., Campos Zatarain, S., Aramburo Contreras, L. Y., y Díaz Lucas, G. Á. (2025). Deepfakes: Revisión sistemática de tecnologías, impacto y estrategias de detección. *RITI Journal*, *13*(29). https://riti.es/index.php/riti/article/view/335

Muros, B. (2011). El concepto de identidad en el mundo virtual: el yo online. *REIFOP*, *14*. http://www.aufop.com

Özgürel, G., Özsezgin, İ., Ünal, A., y Çilesiz, E. (2024). Dead internet theory in theoretical framework and its possible effects on tourism. *LIFENTYU Journal of Lifestyle & SDG'S Review*, *25*. https://sdgsreview.org/LifestyleJournal/article/view/4327

Ramos, F. (2024). Deepfake: Análisis de sus implicancias tecnológicas y jurídicas en la era de la Inteligencia Artificial. *Derecho global. Estudios sobre derecho y justicia*, *9*(27). https://doi.org/10.32870/dgedj.v9i27.754

Santamaría, F. (2015). Identidad y reputación digital: Visión española de un fenómeno global. *Revista Ambiente Jurídico*, *17*, 11-44. https://dialnet.unirioja.es/descarga/articulo/6101297.pdf

Toro, G. (2024). *Deepfake una amenaza para niños, niñas y adolescentes ecuatorianos en el mundo digital* [Trabajo Final de Graduación]. Universidad Regional Autónoma de Los Andes. Ecuador. https://rraae.cedia.edu.ec/vufind/Record/UNIANDES_9ec0ac2d5ef4105e7c977b7db7c50c15?sid=2939340&lng=ga

Walter, Y. (2024). Artificial influencers and the dead internet theory. *AI & Society*, *40*, 239-240. https://doi.org/10.1007/s00146-023-01857-0

Ciberseguridad, Economía y Proyecciones futuras

Ciberseguridad como motor económico: Definiciones, condición actual y tendencias

Aida Andrade[1]

Introducción

En la sociedad digital del siglo XXI, la ciberseguridad ha dejado de ser un tema exclusivo de expertos en informática para convertirse en un eje transversal que impacta la economía, la política y la vida cotidiana. Según el Jonker et al. (2025),la ciberseguridad consiste en usar diferentes herramientas tecnológicas, procedimientos y normas para defender a los usuarios, los sistemas informáticos y la información de los ataques en el entorno digital. Para una empresa, la ciberseguridad es un componente crucial dentro de su plan general de gestión de riesgos, ya que se enfoca específicamente en manejar y mitigar las amenazas cibernéticas. Esta definición refleja su naturaleza multidimensional, abarcando desde la seguridad de infraestructuras críticas hasta la privacidad de los usuarios.

La ciberseguridad ha trascendido su concepción original como una mera necesidad técnica para convertirse en un pilar fundamental del desarrollo económico global. En un mundo cada vez más interconectado, donde la digitalización permea todos los estratos de la sociedad y la economía, la protección de la información y los sistemas se erige como un sector estratégico con un impacto macroeconómico innegable. Este ensayo explora la evolución de la ciberseguridad hacia un sector económico crucial, analizando su influencia en la estabilidad macroeconómica y su papel esencial en la resiliencia empresarial, incorporando perspectivas que humanizan su relevancia en la vida cotidiana y la confianza digital.

El crecimiento exponencial de la digitalización ha posicionado a la ciberseguridad como uno de los sectores económicos de mayor dinamismo. De acuerdo con Shivarkar (2025), el tamaño del mercado global de ciberseguridad fue de USD 268,13 billones en 2024, se calculó en 301,91 billones en 2025 y se espera que alcance alrededor de USD 878,48 billones para 2034. El mercado se está expandiendo a una sólida tasa de crecimiento anual compuesta del 12,6 % durante el período de pronóstico de 2025 a 2034. Este auge responde a factores como el aumento de ciberataques, que costaron 9,22 billones de dólares en 2024 (Golombick, 2025), y la adopción de regulaciones como el Reglamento General de Protección de Datos (RGPD) en la Unión Europea, que exigen mayores inversiones en protección digital (Costagliola, 2025).

Además, la ciberseguridad se ha convertido en un generador de empleo especializado. Un informe de International Information System Security Certification Consortium (2023), estima que en 2023 habría una deficiencia de trabajadores del sector del 12,6 % y afirma que

[1]Economista y Licenciada en Educación egresada de la Universidad de Los Andes. Actualmente se desempeña como Investigadora en el Centro de Desarrollo e Investigación en Tecnologías Libres (CENDITEL). Autora de publicaciones académicas y de divulgación científica. aandrade@cenditel.gob.ve

esta deficiencia persistirá producto de la necesidad de trabajadores de ciberseguridad, la cual se mantiene independientemente de la capacidad de las organizaciones para contratar la suficiente cantidad de trabajadores, destacando la demanda de roles como analistas de threat intelligence y arquitectos de seguridad cloud. Países como Israel y Estonia han integrado la ciberseguridad en sus políticas de desarrollo económico, creando ecosistemas donde startups, universidades y gobiernos colaboran para impulsar innovación (Andrew, 2016).

Este sector, en su vertiginoso crecimiento, no solo genera empleos altamente especializados, también impulsa la innovación tecnológica y la creación de valor en diversas industrias. Como lo señala Lee (2025) el gasto mundial en ciberseguridad está proyectado para superar los 213 mil millones de dólares en 2025, reflejando la creciente dependencia de las organizaciones en infraestructuras digitales y la conciencia de los riesgos asociados. Esta inversión masiva no es un costo superfluo, es más bien una inversión en la continuidad de las operaciones, la protección de la propiedad intelectual y la confianza del consumidor. Desde una perspectiva macroeconómica, la ciberseguridad actúa como un catalizador de la productividad y un mitigador de riesgos sistémicos. Los ciberataques, con su capacidad de paralizar infraestructuras críticas, robar datos sensibles y erosionar la confianza pública, pueden tener repercusiones devastadoras en la economía. Un estudio del World Economic Forum (2023) destacó que los ciberataques representan una de las principales amenazas a la estabilidad global, con un costo estimado que podría alcanzar billones de dólares anualmente, afectando el comercio, las finanzas y la cadena de suministro. Proteger estas vulnerabilidades es, por ende, una salvaguarda de la propia economía.

La importancia económica de la ciberseguridad trasciende el ámbito tecnológico. Fallos en seguridad, como el ataque a Colonial Pipeline en 2021, que provocó escasez de combustible en EE.UU. y el trámite de pago fue de $ 4.4 millones (Kerner, 2022), demuestran su vinculación con la estabilidad de cadenas de suministro y mercados financieros. Según James (2025) las pequeñas y medianas empresas (pymes) representan el 43 % de las víctimas de ciberataques, muchas de las cuales enfrentan quiebras por falta de preparación. En contraste, las empresas que priorizan la ciberseguridad no solo mitigan riesgos, adicionalmente ganan ventajas competitivas, lo cual refleja un paradigma donde la ciberseguridad ya no es un gasto, es una inversión en reputación y sostenibilidad. (Llanos, 2025).

Más allá de las cifras y las proyecciones, la ciberseguridad posee una dimensión profundamente humanizada. Cada violación de datos personales representa una intromisión en la privacidad y la tranquilidad de los individuos, afectando su confianza en las plataformas digitales que sustentan gran parte de su vida moderna. La seguridad de las transacciones bancarias, la privacidad de las comunicaciones en línea y la protección de los datos de salud son aspectos que, aunque mediados por la tecnología, impactan directamente en el bienestar y la dignidad de las personas. Como argumenta Admass et al. (2023), la ciberseguridad no se trata solo de proteger computadoras, se trata de proteger a las personas. Se trata de cómo la tecnología afecta la sociedad, la política y la economía. Este enfoque nos recuerda

que la ciberseguridad no es un fin en sí misma, en realidad es un medio para garantizar un entorno digital seguro y confiable para todos.

En el ámbito de la resiliencia empresarial, la ciberseguridad es un diferenciador clave y una condición imperativa para la supervivencia en el mercado actual. Las empresas que invierten proactivamente en medidas de ciberseguridad además de minimizar la probabilidad de sufrir ataques, están mejor equipadas para recuperarse rápidamente en caso de que ocurran. La capacidad de una empresa para mantener la continuidad de sus operaciones frente a un ciberataque, proteger la integridad de sus datos y preservar la confianza de sus clientes y socios es un indicador directo de su resiliencia. Un informe de Catalan (2025) sobre el costo de las violaciones de datos reveló que tener un plan de respuesta a incidentes de ciberseguridad bien establecido y probado permite a las empresas reducir considerablemente los gastos derivados de una filtración de datos y acelerar el tiempo necesario para recuperarse del ataque. Esta evidencia subraya que la ciberseguridad no es simplemente una estrategia de prevención, representa una pieza clave en la planificación para manejar riesgos y mantener la operación. La inversión en talento, tecnología y procesos de ciberseguridad permite a las empresas mitigar los riesgos reputacionales y financieros asociados a los ciberincidentes, asegurando su sostenibilidad a largo plazo.

La ciberseguridad ha evolucionado de un nicho técnico a un sector económico estratégico con un impacto macroeconómico y una relevancia ineludibles. Su crecimiento es un reflejo de la digitalización global y la creciente conciencia de los riesgos asociados. Al salvaguardar infraestructuras críticas, promover la innovación y proteger la privacidad de los individuos, la ciberseguridad se convierte en un motor de la productividad y la estabilidad económica. En el contexto empresarial, esto se traduce en la habilidad vital para no solo resistir los contratiempos, pero además para escalar y florecer dentro del exigente entorno digital actual. Reconocer y fortalecer este sector es fundamental para construir un futuro digital seguro, confiable y equitativo para todos.

Contexto actual de la ciberseguridad

Actualmente, la ciberseguridad, como ya se ha mencionado, ha trascendido su rol meramente técnico para consolidarse como un pilar fundamental de la economía global y absolutamente necesario para la resiliencia social y empresarial. La hiperconectividad inherente a la Cuarta Revolución Industrial ha transformado cada aspecto de la vida cotidiana y la actividad económica en un vasto ecosistema digital, donde la protección de la información y los sistemas además de una necesidad, es una condición ineludible para la confianza y la continuidad.

El crecimiento del sector de la ciberseguridad en su arista económica ha sido exponencial, impulsado por una confluencia de factores que incluyen la proliferación de amenazas cibernéticas cada vez más sofisticadas, la creciente digitalización de todos los sectores productivos y la implementación de marcos regulatorios más estrictos a nivel global. Diversos expertos proyectan basto crecimiento del mercado global de ciberseguridad,

esta expansión no se limita a la venta de software y hardware; abarca una vasta gama de servicios que incluyen consultoría, gestión de riesgos, respuesta a incidentes, educación y capacitación, y desarrollo de soluciones avanzadas como inteligencia artificial para la detección de amenazas. La inversión en ciberseguridad se ha convertido en una partida presupuestaria inevitable para organizaciones de todos los tamaños, desde pequeñas y medianas empresas hasta corporaciones multinacionales y gobiernos, reconociendo que el costo de un ciberataque exitoso supera con creces la inversión preventiva.

En el ámbito empresarial, las inversiones en ciberseguridad ya no son opcionales. Grandes corporaciones destinan entre 6 % y 14 % de su presupuesto IT a seguridad digital (Fimlaid, 2025), mientras que emprendimientos como startups de firewalls basados en IA atraen capital de riesgo. Solo en 2021, se invirtieron $ 643 billones en venture capital para ciberseguridad, un 92 % que en 2020 (Asociación Chilena Administradora de Fondos de Inversión, 2021), evidenciando la confianza en su rentabilidad. El crecimiento económico de la ciberseguridad es un reflejo de su papel crítico en la sociedad digital. Su mercado en expansión, la demanda laboral y las inversiones masivas confirman su relevancia. Sin embargo, persisten desafíos, como la equidad en el acceso a tecnologías seguras para economías emergentes (Comisión Económica para América Latina y el Caribe, 2013).

Desde una perspectiva macroeconómica, el sector de la ciberseguridad es un receptor de capital y un generador activo de valor. Contribuye significativamente al Producto Interno Bruto (PIB) a través de la creación de empleos de alta cualificación, el fomento de la innovación tecnológica y la exportación de servicios y soluciones. La demanda de profesionales en ciberseguridad supera con creces la oferta, evidenciando que existe una escasez mundial de profesionales en el campo de la ciberseguridad, contándose por millones los puestos de trabajo sin cubrir. Esto destaca la imperiosa necesidad de invertir en la formación y el desarrollo de nuevas habilidades en esta área (International Information System Security Certification Consortium, 2023). Este déficit, si bien es un desafío, también representa una oportunidad para el desarrollo de capital humano y la especialización en economías emergentes. Además, al proteger la infraestructura digital crítica (energía, finanzas, telecomunicaciones), la ciberseguridad salvaguarda la estabilidad económica nacional e internacional, mitigando el riesgo de interrupciones masivas que podrían paralizar cadenas de suministro, mercados financieros y servicios esenciales.

La humanización de la ciberseguridad reside en su impacto directo sobre la vida de las personas. Detrás de cada cifra de inversión o de cada estadística de ataque, hay individuos cuyas vidas son afectadas. La violación de datos personales, el robo de identidad o el fraude financiero no son meras transacciones en una base de datos; son eventos que pueden generar estrés, ansiedad y pérdidas económicas significativas para las víctimas. La ciberseguridad, en su esencia más profunda, se trata de proteger la privacidad, la seguridad y la dignidad de los ciudadanos en el entorno digital. Como lo expresa UNESCO (2025), existe la privacidad de la información, la cual se extiende más allá del individuo a la sociedad en su conjunto, en la medida en que también se refiere a cómo la privacidad afecta el flujo de información en la sociedad y cómo esto afecta el desarrollo de los individuos como

ciudadanía", y la ciberseguridad es su guardián en la era digital. La capacidad de realizar transacciones bancarias en línea con confianza, de comunicarse de forma segura con seres queridos, de acceder a servicios de salud digital o de participar en la vida cívica sin temor a la manipulación o el espionaje, son aspectos que la ciberseguridad habilita y protege. El crecimiento de este sector, por lo tanto, se traduce en una mayor capacidad colectiva para construir un espacio digital más seguro y confiable, fomentando la participación y la innovación sin el lastre constante del miedo al ciberdelito.

Ciberseguridad y economía digital

La transformación digital ha redefinido los paradigmas económicos globales, posicionando al comercio electrónico como uno de los motores más dinámicos del crecimiento económico. Según el Centro Nacional de Planeamiento Estratégico (2025), los medios de pago digital siguen ganando fuerza año tras año debido a su comodidad y practicidad. Ya en 2021, el valor de las transacciones realizadas a nivel mundial a través de este tipo de servicios de pago alcanzó los 7,5 billones de dólares estadounidenses y se estima que para 2027 este se sitúe en torno a los 15,2 billones. Sin embargo, este auge viene acompañado de un incremento exponencial en los riesgos cibernéticos, que amenazan con la seguridad de los datos y con la estabilidad financiera de empresas y consumidores.

En este contexto, la ciberseguridad emerge como un componente estratégico para la sostenibilidad del ecosistema digital. La relación intrínseca entre la ciberseguridad y el comercio digital se ha consolidado como un eje central en la economía contemporánea. En un entorno donde las transacciones, interacciones y modelos de negocio se digitalizan a una velocidad sin precedentes, la integridad y la confianza en el ciberespacio se vuelven condiciones necesarias para la viabilidad y el crecimiento del comercio electrónico.

El auge del comercio digital ha redefinido las dinámicas de mercado, ofreciendo conveniencia, accesibilidad y una expansión sin precedentes del alcance geográfico para empresas y consumidores. Sin embargo, esta vasta interconexión inherentemente amplía la superficie de ataque para ciberdelincuentes, convirtiendo cada plataforma de comercio electrónico en un objetivo potencial. La dependencia de infraestructuras digitales para la gestión de inventarios, procesamiento de pagos, logística y atención al cliente expone a las empresas a una mirada de vulnerabilidades. Como señala Bagul (2015), el mercado global de comercio electrónico, valorado en 17.1 billones de dólares en 2022, se proyecta que experimentará un crecimiento masivo, alcanzando los 80.5 billones de dólares para el año 2030. Esta expansión representa una impresionante Tasa de Crecimiento Anual Compuesta (CAGR) del 26.5 %. Esta expansión económica, si bien prometedora, exige una infraestructura de seguridad robusta para sostener la confianza del consumidor y la estabilidad operativa.

La interdependencia entre ciberseguridad y comercio digital

El comercio digital depende de tres pilares fundamentales: infraestructura tecnológica, confianza del consumidor y marcos regulatorios. La ciberseguridad opera como un eje transversal que fortalece estos pilares mediante: la protección de datos sensibles se refiere a los derechos de las personas cuyos datos se recogen, se mantienen y se procesan, de saber qué datos están siendo referidos y usados y de corregir las inexactitudes (Comisión Económica para América Latina y el Caribe, 2025). La disponibilidad de servicios, que mitiga ataques de denegación de servicio (DDoS) que podrían paralizar plataformas de e-commerce (De Neira et al., 2023). Y el cumplimiento normativo, que facilita la adhesión a regulaciones como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea (2016), evitando sanciones millonarias por incumplimiento. Un estudio presentado por Sutherland (2016) reveló que más de la mitad (58 %) de los consumidores cree que las marcas afectadas por una filtración de datos no son confiables y el 70 % dejaría de comprar en una marca que sufriera incidente de seguridad, evidenciando el impacto directo de la ciberseguridad en la confianza del cliente.

Proteger las transacciones y los datos significa proteger la capacidad de las personas para participar de manera segura y confiada en la economía digital, para acceder a bienes y servicios esenciales y para mantener la privacidad de sus vidas. Como lo articula Anderson (2021), la seguridad no es un producto, es más bien un proceso social. Se trata de las relaciones de confianza que construimos y mantenemos. En el comercio digital, esta confianza se materializa en la expectativa de que los datos y las transacciones estarán protegidos.

En este contexto, la ciberseguridad emerge no como un centro de costos, en realidad surge como una inversión estratégica y un diferenciador competitivo crucial para el comercio digital. Las empresas que priorizan la ciberseguridad construyen una base de confianza sólida con sus clientes, fomentan la lealtad y se posicionan como líderes en un mercado cada vez más consciente de los riesgos. La implementación de medidas de seguridad avanzadas, la capacitación continua del personal y el desarrollo de planes de respuesta a incidentes robustos, además de minimizar las pérdidas potenciales, permiten una recuperación más rápida y eficiente, asegurando la continuidad del negocio y la resiliencia empresarial.

Costos económicos de los ataques cibernéticos: Un análisis multidimensional

La creciente digitalización de la sociedad y la economía ha catapultado a los ataques cibernéticos a la vanguardia de las preocupaciones globales, siendo amenazas tecnológicas, resaltan como vectores de costos económicos multidimensionales con profundas implicaciones para la estabilidad financiera y el bienestar humano. Adentrémonos en la complejidad de estos costos, desglosándolos en sus componentes directos, indirectos y sistémicos, y subrayando la dimensión social inherente a cada incidente cibernético.

Los costos económicos de los ataques cibernéticos son notoriamente difíciles de cuantificar en su totalidad debido a su naturaleza difusa y sus ramificaciones a largo plazo. Sin embargo,

una aproximación multidimensional permite apreciar su verdadera magnitud. En primer lugar, se encuentran los costos directos, que son aquellos inmediatamente atribuibles a la respuesta y recuperación del incidente. Estos incluyen la investigación forense para identificar la causa y el alcance del ataque, la remediación de sistemas y la restauración de datos, los gastos legales derivados de litigios o asesoramiento, y las multas regulatorias impuestas por incumplimientos de normativas de protección de datos (como el GDPR en Europa o la CCPA en California). Además, las organizaciones deben asumir los costos de notificación a las partes afectadas, la provisión de servicios de monitoreo de crédito para las víctimas de robo de identidad, y, en algunos casos, el pago de rescates en ataques de ransomware. El informe titulado *Cost of a Data Breach Report 2025* (International Business Machines, 2025c) es una referencia clave en este ámbito, indicando que el costo medio de un ataque o violación de datos a nivel mundial se elevó a 4.4 millones de dólares en 2024, lo que demuestra tanto la mayor dificultad de estos incidentes como las graves consecuencias económicas que conllevan.

Los ciberataques generan impactos económicos multidimensionales, afectando desde microempresas hasta economías nacionales (World Economic Forum, 2025). Entre estos costos directos podemos mencionar que de acuerdo a las estimaciones realizadas por Statista, la industria del comercio digital perdió 41 billones de dolares en estafas de pago en linea a nivel mundial en el año 2022 (Kumar, 2025). Las multas regulatorias: Meta multada con 1,2 mil millones de euros por GDPR (McCallum, 2023). Los gastos en recuperación: $ 4,88 millones de coste medio global de una filtración de datos en 2024: un aumento del 10 % respecto del año anterior (International Business Machines, 2025c) y el famoso caso Colonial Pipeline: $ 4.4 millones en rescate, más $ 80 millones en mitigación (Niccum, 2021).

En segundo lugar, los costos indirectos de los ataques cibernéticos son a menudo más cuantiosos y de mayor alcance, afectando la viabilidad a largo plazo de las organizaciones. La pérdida de ingresos por interrupción del negocio es un factor crítico; el tiempo de inactividad de los sistemas puede paralizar operaciones esenciales, desde la producción hasta las ventas y la logística. Un ataque de denegación de servicio (DDoS) o un *ransomware* que cifra datos vitales puede detener completamente las operaciones, resultando en pérdidas millonarias por cada hora de interrupción. La pérdida de propiedad intelectual o datos sensibles es otro costo indirecto devastador, ya que el robo de secretos comerciales, diseños de productos o estrategias de negocio puede comprometer la ventaja competitiva de una empresa. Más allá de lo tangible, el daño reputacional es un costo incalculable. La confianza del cliente, una vez erosionada por una violación de datos o un incidente de seguridad, es extremadamente difícil de recuperar. (Giraldo, 2025) comenta que la percepción de seguridad es un factor decisivo para los consumidores, y un incidente cibernético puede llevar a una pérdida significativa de clientes y socios comerciales. Esta pérdida de confianza se traduce en una disminución de la cuota de mercado, dificultades para atraer nuevos clientes y un impacto negativo en la valoración de la empresa. De igual modo, el aumento de las primas de seguros cibernéticos y la disminución de la productividad del personal, que debe desviar recursos para abordar el incidente, también contribuyen a los costos indirectos. Se puede reseñar evidencias de estos costos indirectos, hasta ahora y entre otros se ha documentado el cierre de PYMES: 60 % en 6 meses post-ataque (Melero, 2025).

Adicionalmente, la expansión del comercio digital trae consigo la sombra creciente de los costos sistémicos de la ciberseguridad, los cuales van más allá de las pérdidas directas por ataques. Estos costos impactan la economía digital de formas profundas y a menudo subestimadas, afectando la confianza, la innovación y la estabilidad. Uno de los principales costos es la erosión de la confianza del consumidor. Las brechas de datos minan la fe de los usuarios en las plataformas de comercio electrónico, llevándolos a reducir su participación y ralentizando el crecimiento económico (Sánchez y Montoya, 2016). Esta desconfianza obliga a las empresas a invertir fuertemente en seguridad solo para mantener el *status quo*.

Otro factor relevante es la regulación excesiva y fragmentada. La proliferación de normativas como el RGPD o la CCPA, aunque necesarias, impone una carga significativa a las empresas, especialmente a las PYMES. El cumplimiento con múltiples marcos regulatorios desvía recursos valiosos que podrían destinarse a la innovación, y esta fragmentación también dificulta la cooperación global contra el cibercrimen (Naciones Unidas, 2013). Por otro lado, la distorsión en la asignación de recursos es un costo sistémico crucial. Las empresas se ven forzadas a destinar una porción creciente de sus presupuestos a la ciberseguridad, a menudo de forma reactiva. Esto desvía capital de la investigación y desarrollo, la mejora de la experiencia del cliente o la expansión a nuevos mercados, comprometiendo la competitividad a largo plazo y la innovación (Santos, 2024). De igual forma, la ciberseguridad provoca interrupciones en las cadenas de suministro digitales. Dado que el comercio digital se apoya en una red interconectada de proveedores y socios, un ciberataque a un eslabón débil puede tener efectos dominó, paralizando operaciones de múltiples empresas y causando pérdidas masivas y daños reputacionales (Urciuoli, 2022). La interconexión hace que la vulnerabilidad de uno se convierta en un riesgo sistémico.

Estrategias de mitigación

El auge del comercio digital ha traído consigo una inevitable escalada en la sofisticación y frecuencia de los ciberataques. Dada la magnitud de los costos sistémicos asociados, es crucial que las organizaciones implementen estrategias de mitigación robustas y proactivas. Estas no solo deben responder a incidentes, deben fortalecer la resiliencia digital, proteger los activos críticos y preservar la confianza del usuario. Entre las estrategias de mitigación más comunes tenemos:

Enfoque multi-capas en la seguridad tecnológica

La base de la mitigación es un enfoque de seguridad multi-capas, integrando diversas tecnologías y controles para crear barreras redundantes que dificulten la penetración y limiten el daño. Esto incluye:

- **Firewalls y sistemas de detección/prevención de intrusiones (IDS/IPS)** Funcionan como la primera línea de defensa, monitoreando y filtrando el tráfico de red en busca de actividades maliciosas (International Business Machines, 2025b). Los IDS alertan, mientras que los IPS pueden bloquear activamente las amenazas.

- **Cifrado de datos** Es fundamental proteger los datos sensibles en reposo y en tránsito (Chala, 2019). Esto asegura que, incluso si la información es interceptada, permanezca ilegible sin la clave de descifrado.
- **Gestión de identidades y accesos (IAM)** Implementar controles estrictos sobre quién accede a qué recursos y con qué privilegios es crucial (International Business Machines, 2025a). Esto implica la autenticación multifactor (MFA) y el principio de mínimo privilegio, donde los usuarios solo tienen los permisos necesarios para sus tareas.

Concienciación y capacitación del factor humano

- **Factor humano** es a menudo el eslabón más débil, con la ingeniería social y el phishing como métodos comunes de ataque. Por ello, la concienciación y capacitación continua del personal son estrategias de mitigación vitales (Rifa, 2024).
- **Programas de formación regulares** Educar a los empleados sobre los riesgos de seguridad, las políticas de la empresa y las mejores prácticas (por ejemplo, cómo identificar correos electrónicos de phishing o la importancia de contraseñas fuertes) reduce significativamente los incidentes causados por errores humanos (Calle et al., 2024).
- **Simulacros de *phishing*** Realizar simulacros controlados ayuda a evaluar la efectividad de la capacitación y a identificar áreas donde se necesita reforzar el conocimiento (Cabezas y Fiallos, 2024).

Gestión de riesgos y resiliencia organizacional

Las organizaciones deben adoptar una gestión de riesgos cibernéticos proactiva e incorporar la resiliencia en su cultura:

- **Evaluación de riesgos continua** Identificar, analizar y evaluar constantemente las vulnerabilidades y amenazas permite priorizar las inversiones en seguridad (Asociación Bancaria y de Entidades Financieras de Colombia, 2022). Esto incluye auditorías periódicas y pruebas de penetración.
- **Planificación de la respuesta a incidentes y recuperación ante desastres (DRP)** Desarrollar y probar planes detallados para responder a un ciberataque minimiza el tiempo de inactividad y el impacto financiero. Un DRP bien diseñado asegura la continuidad del negocio (Saeed, 2022).
- **Colaboración e intercambio de inteligencia** Participar en comunidades de intercambio de información sobre amenazas permite a las organizaciones estar al tanto de las últimas tácticas de los atacantes y adaptar sus defensas de manera proactiva (Rego y Pérez, 2017).

Seguridad en el Ciclo de Vida del Desarrollo de Software (SDLC)

Para el comercio digital, donde el software es central, es crucial integrar la seguridad desde las etapas iniciales del desarrollo, lo que se conoce como *Security by Design* (Díaz et al., 2013). Además, se deben considerar:

- **Pruebas de seguridad regulares** Incluir revisiones de código, análisis estáticos y dinámicos de aplicaciones (SAST/DAST) y pruebas de penetración a lo largo del SDLC ayuda a identificar y corregir vulnerabilidades antes del despliegue del software (GitLab platform, 2024).
- **Uso de componentes seguros** Priorizar el uso de librerías y marcos de trabajo con historiales de seguridad probados y mantenerlos actualizados es vital para evitar vulnerabilidades conocidas en componentes de terceros (Asociación Bancaria y de Entidades Financieras de Colombia, 2022).

Las estrategias de mitigación contra los ciberataques en el comercio digital son complejas y requieren una inversión continua en tecnología, capacitación y procesos. Al adoptar un enfoque integral que abarque la seguridad multi-capas, la concienciación del factor humano, la gestión de riesgos y la seguridad integrada en el ciclo de vida del software, las organizaciones pueden construir una postura de defensa robusta. Esta proactividad protege los activos y operaciones, al tiempo que refuerza la confianza de los consumidores, un elemento indispensable para el éxito sostenido en el dinámico panorama del comercio digital. Adicionalmente, para mitigar los riesgos cibernéticos, las inversiones deben ser multidimensionales, abarcando tecnología, el factor humano, investigación y desarrollo (I+D), y marcos regulatorios eficaces.

Tecnología e infraestructura resiliente

La escalada constante en la sofisticación de las amenazas cibernéticas exige que el sector del comercio digital vaya más allá de las medidas de seguridad tradicionales, como *firewalls* y antivirus. Para construir una infraestructura verdaderamente resiliente, es fundamental invertir en tecnologías avanzadas que permitan una defensa proactiva y adaptable. Las áreas clave de inversión incluyen la Inteligencia Artificial (IA) y el *Machine Learning* (ML), así como la anticipación a la amenaza de la computación cuántica con la criptografía post-cuántica.

IA y ML en ciberseguridad

La integración de la IA y el ML representa un cambio de paradigma en la ciberseguridad. Estas tecnologías cambian el juego, al pasar de un enfoque reativo a uno proactivo, permitiendo la identificación en tiempo real de anomalías y amenazas emergentes. Los sistemas basados en IA y ML pueden analizar grandes volúmenes de datos de red, comportamiento de usuarios y registros de eventos a una velocidad y escala inalcanzables para el análisis humano. Esto facilita la identificación de actividades sospechosas, como intentos de *phishing* sofisticados, *malware* polimórfico o ataques de día cero, antes de que

causen un daño significativo (Raji et al., 2023). La dependencia creciente resalta la IA y el ML como una ventaja competitiva, y como un requisito fundamental para la supervivencia en el actual panorama de amenazas.

Computación cuántica y criptografía post-cuántica

Mirando hacia el futuro, el avance de la computación cuántica plantea un desafío significativo a la seguridad criptográfica actual. Los algoritmos de encriptación que hoy en día protegen la mayoría de las transacciones de comercio digital, como RSA y la Criptografía de Curvas Elípticas (ECC), podrían volverse vulnerables frente a computadoras cuánticas suficientemente potentes. Esto amenaza la confidencialidad y la integridad de los datos a largo plazo, incluyendo información financiera y personal almacenada durante años. En respuesta a esta amenaza inminente, instituciones clave como el National Institute of Standards and Technology (NIST) están liderando la iniciativa para desarrollar y estandarizar algoritmos de criptografía post-cuántica (PQC), que son resistentes a los ataques de computadoras cuánticas (Sood, 2024). La adopción temprana de estas soluciones PQC es vital para que las empresas de comercio digital preparen su infraestructura y protejan sus datos sensibles de futuras amenazas cuánticas, asegurando la confianza a largo plazo en el ecosistema digital.

Desarrollo de capital humano especializado

La protección del creciente ecosistema del comercio digital enfrenta un desafío formidable: la escasez crítica de profesionales en ciberseguridad. Abordar esta carencia es fundamental para fortalecer las defensas contra los ciberataques, exigiendo un enfoque multifacético que involucre la educación formal, la capacitación continua y la certificación profesional.

Las universidades desempeñan un papel crucial en la formación de la próxima generación de expertos en ciberseguridad. Instituciones de renombre mundial como Georgia Tech y el MIT están a la vanguardia, ofreciendo programas de maestría con enfoques prácticos que preparan a los estudiantes para los desafíos del mundo real (Edwise Foundation, 2025). Estos programas imparten conocimientos teóricos y también desarrollan habilidades críticas a través de laboratorios especializados y proyectos aplicados, asegurando que los graduados estén listos para integrarse en equipos de seguridad de alto nivel.

Más allá de la educación universitaria, las certificaciones y la capacitación empresarial son pilares esenciales para el desarrollo de competencias específicas y actualizadas en ciberseguridad. Empresas líderes en tecnología, como Cisco y Microsoft, invierten significativamente en programas de certificación accesibles para una amplia audiencia (Arias, 2025). Estas certificaciones validan las habilidades prácticas y el conocimiento técnico de los profesionales, siendo altamente valoradas en la industria y facilitando su inserción y progresión laboral.

Marcos legales y gobernanza proactiva

En un panorama de amenazas cibernéticas en constante evolución, la efectividad de las defensas en el comercio digital no depende únicamente de la tecnología y el talento humano; requiere también de un marco legal robusto y una gobernanza proactiva. Las regulaciones deben ser dinámicas, adaptándose al ritmo de las nuevas vulnerabilidades y vectores de ataque, y deben fomentar la inversión en seguridad a través de mecanismos efectivos.

Regulaciones sectoriales: Un enfoque ampliado

La complejidad del ecosistema digital, especialmente en sectores críticos, demanda regulaciones que vayan más allá de los requisitos generales. Un ejemplo destacado es la Directiva NIS2 de la Unión Europea (UE). Esta directiva representa una evolución significativa de su predecesora (NIS Directive), expandiendo los requisitos de seguridad cibernética a un espectro más amplio de entidades críticas y esenciales. Incluye sectores como la energía, la salud, la banca, la infraestructura digital, el transporte y, de manera crucial para el comercio digital, ciertos servicios digitales y proveedores de servicios gestionados. La NIS2 impone obligaciones más estrictas en gestión de riesgos, notificación de incidentes y cooperación transfronteriza, buscando elevar el nivel de resiliencia cibernética en toda la UE (European Commission, 2023). Al hacer que la ciberseguridad sea una responsabilidad legal explícita para un mayor número de empresas, especialmente aquellas que operan en cadenas de suministro digitales interconectadas, se busca crear un efecto cascada positivo en la seguridad general del comercio digital.

Incentivos fiscales para empresas: Impulsando la inversión en ciberseguridad

Las regulaciones, si bien necesarias, pueden ser percibidas como una carga, especialmente por las pequeñas y medianas empresas (PYMES), que a menudo carecen de los recursos de las grandes corporaciones para implementar medidas de seguridad avanzadas. Aquí es donde los incentivos fiscales y los subsidios se convierten en una estrategia de gobernanza proactiva y efectiva. Países como Singapur han adoptado este enfoque, ofreciendo subsidios y exenciones fiscales a las PYMES que inviertan en la adopción de medidas avanzadas de ciberseguridad (Unifiedpost Group, 2023). Estos programas alivian la carga financiera mientras actúan como un catalizador para la mejora de la postura de seguridad. Al reducir el costo de la inversión en herramientas, capacitación o consultoría de ciberseguridad, los gobiernos pueden estimular a las empresas a implementar mejores prácticas y tecnologías, fortaleciendo así el eslabón más débil de la cadena de suministro digital y contribuyendo a una mayor resiliencia sistémica en el comercio digital.

Colaboración intersectorial: Una exigencia global

La naturaleza transnacional y la creciente sofisticación de los ciberataques trascienden las fronteras organizacionales y geográficas, haciendo de la colaboración intersectorial una necesidad primordial y global para la resiliencia del comercio digital. Ningún actor individual, ya sea un gobierno, una empresa o una institución académica, puede abordar

eficazmente la complejidad de las amenazas cibernéticas por sí solo. Es por ello que la cooperación entre múltiples actores, públicos, privados, académicos e internacionales, se vuelve fundamental para la defensa colectiva.

Alianzas Público-Privadas (APP): son vehículos esenciales para canalizar recursos y conocimientos entre el sector público y el privado, fortaleciendo la infraestructura crítica del comercio digital. Intercambio de inteligencia, esta base de conocimiento global organiza y describe las tácticas y técnicas adversarias conocidas, permitiendo a las organizaciones hablar un lenguaje común y compartir información sobre ciberataques de manera estructurada (Picus Security Validation Platform, 2025).

Cooperación internacional: Dada la naturaleza sin fronteras del ciberespacio, la cooperación internacional es indispensable para una defensa colectiva eficaz. Esto mediante Organismos Globales, entidades como la Unión Internacional de Telecomunicaciones (UIT), una agencia especializada de las Naciones Unidas, juegan un papel crucial. La UIT promueve el desarrollo de estándares y mejores prácticas de ciberseguridad a nivel global, con un enfoque particular en asistir a los países en desarrollo en la construcción de sus capacidades digitales y marcos de seguridad (Naciones Unidas, 2010). Esto ayuda a elevar el nivel de seguridad en regiones que podrían ser puntos débiles en la cadena global del comercio digital. De igual manera, los Tratados y Acuerdos internacionales establecen marcos legales para la persecución del cibercrimen y la cooperación judicial. El Convenio de Budapest sobre la Ciberdelincuencia (Budapest Convention) es un hito en este sentido, siendo el primer tratado internacional que aborda la ciberdelincuencia y proporciona un marco legal para la cooperación entre países en la investigación y enjuiciamiento de delitos cibernéticos (Council of Europe, 2001). Estos acuerdos son fundamentales para desmantelar redes criminales y garantizar que los ciberdelincuentes no encuentren refugios seguros.

Ciberseguridad y economía en Venezuela

La ciberseguridad se ha consolidado como una preocupación global y regional ineludible, impulsada por la creciente dependencia de las sociedades y economías del ciberespacio y el aumento exponencial de la actividad digital, un fenómeno exacerbado tras la pandemia de COVID-19 (Singh et al., 2021). Este incremento en la interconexión digital ha transformado el panorama de riesgos, haciendo que la protección de la información y los sistemas sea prioritaria. Este contexto global establece un marco de referencia urgente para comprender la situación particular de Venezuela, donde la resiliencia cibernética se entrelaza directamente con la estabilidad económica y social.

Priorizar la ciberseguridad en Venezuela es fundamental para proteger la privacidad personal de los ciudadanos, salvaguardar la infraestructura crítica del país (incluyendo sistemas de energía, telecomunicaciones y salud), fomentar la confianza en la tecnología digital, impulsar el desarrollo económico mediante la protección de la propiedad intelectual, y asegurar el cumplimiento de regulaciones internacionales esenciales para la participación en el comercio global (Rodriguez, 2016). La seguridad cibernética es vital para proteger la

infraestructura crítica del país, como los sistemas de energía, telecomunicaciones y salud, contra posibles ataques cibernéticos que podrían tener consecuencias devastadoras. Según (Donoso, 2022) garantizar la integridad de las transacciones y los sistemas informáticos es fundamental para fomentar la confianza digital, lo que se traducen en una mayor aceptación de la tecnología en todos los ámbitos. Más allá de esto, la ciberseguridad es un motor económico directo, ya que al salvaguardar la propiedad intelectual y alentar la innovación, se generan nuevos puestos de trabajo y se expanden las oportunidades comerciales en la tecnología.

Venezuela se ha posicionado entre los diez primeros países de América Latina en ataques cibernéticos, una estadística alarmante que subraya la elevada vulnerabilidad de sus instituciones y empresas frente a las amenazas digitales (Cámara Venezolana de Empresas de Tecnologías de la Información, 2023). La alta posición de Venezuela en el ranking de ciberataques de la región y la identificación explícita de su infraestructura crítica como objetivo, indican que la inversión en ciberseguridad en el país no es simplemente una cuestión de "mejores prácticas"tecnológicas, mas bien es una necesidad imperativa para garantizar la continuidad de los servicios esenciales, proteger la privacidad de los ciudadanos y preservar la soberanía digital y la estabilidad socioeconómica. Cuando un país es identificado como un objetivo principal para los ciberataques y su infraestructura crítica se menciona explícitamente como vulnerable, la ciberseguridad se eleva más allá de un problema técnico a una cuestión de resiliencia nacional. La posibilidad de que estos ataques interrumpan servicios esenciales significa que una inversión inadecuada o respuestas tardías podrían llevar a una inestabilidad social y económica generalizada. (Centro de Ciberseguridad Industrial, 2021). Esto crea un argumento convincente para que el gobierno y el sector privado venezolano traten la ciberseguridad como una prioridad y necesidad estratégica en lugar de un gasto discrecional.

Desarrollo histórico y marco regulatorio del mercado de la ciberseguridad en Venezuela

La evolución de la ciberseguridad a nivel global ha sido un proceso dinámico, desde la aparición de los primeros virus informáticos y antivirus hasta el auge del teletrabajo y el Internet de las Cosas (IoT). Estos avances han incrementado exponencialmente los objetivos de los ciberdelincuentes y la necesidad de una mayor concienciación sobre seguridad. Esta tendencia global ha, de manera inherente, influido y moldeado el desarrollo de la ciberseguridad en Venezuela. La trayectoria global de la ciberseguridad implica que Venezuela, como parte integral del ecosistema digital mundial, ha enfrentado y continúa enfrentando desafíos que trascienden sus fronteras geográficas.

En la actualidad, Venezuela cuenta con la Ley Especial Contra los Delitos Informáticos, promulgada para proteger los bienes jurídicos de las conductas delictivas cometidas a través de las Tecnologías de la Información y la Comunicación (Asamblea Nacional de la República Bolivariana de Venezuela, 2001). Esta ley marcó un hito en la legislación nacional para abordar los crímenes en el ciberespacio.

En la Gaceta Oficial n.° 42.939 del 12/08/2024, difundida por el Servicio Autónomo Imprenta Nacional y Gaceta Oficial (SAINGO) el 19/08/2024, se ha publicado el Decreto n.° 4.975, fechado 12/08/2024, mediante el cual "se crea el Consejo Nacional de Ciberseguridad, con carácter permanente, como órgano asesor y de consulta dependiente del Presidente de la República Bolivariana de Venezuela en materia de la prevención de los usos delictivos de las tecnologías de comunicación e información, cuyo funcionamiento se regirá por lo previsto en el presente Decreto." A pesar de la existencia de un marco legal, el nivel de madurez general en ciberseguridad de América Latina y el Caribe, incluyendo a Venezuela, se mantiene en un estado bajo (entre 1 y 2 en el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones - CMM) (Bravo, 2024; Observatorio de la Ciberseguridad en América Latina y el Caribe, 2016). Adicionalmente, se ha señalado que los aspectos legales en Venezuela son "parciales" y pueden "vulnerar algunos derechos fundamentales como la libertad de expresión" (Rodriguez, 2016).

Esta discrepancia sugiere una brecha significativa entre la intención legislativa y la implementación efectiva o la percepción de su aplicación, lo que podría limitar su impacto real en la mejora de la ciberseguridad nacional y la confianza de los actores privados. La presencia de leyes detalladas y un centro nacional dedicado generalmente indica un fuerte compromiso con la ciberseguridad. Sin embargo, la baja puntuación de madurez para la región y la crítica específica sobre la naturaleza "parcial" del marco legal venezolano y su posible infracción de derechos fundamentales, presentan una clara contradicción. Esto sugiere que el marco legal, aunque existente, podría no ser totalmente efectivo debido a desafíos de implementación, falta de recursos para su aplicación, o un diseño que prioriza el control sobre la colaboración y la construcción de confianza, lo que podría disuadir la participación del sector privado y la innovación.

Panorama actual de la ciberseguridad en Venezuela

Venezuela ha experimentado un aumento significativo en los ciberataques, con una estimación del 30 % de incremento en el último año, según datos atribuidos al Observatorio Venezolano de Ciberseguridad Los tipos de ataques más comunes en el país incluyen *malware*, *phishing*, ataques de denegación de servicio distribuido (DDoS) y *ransomware*. Se han documentado picos alarmantes de hasta 30 millones de ataques informáticos por minuto y ataques DDoS que alcanzan los 700 gigabytes por segundo, dirigidos contra instituciones estatales (Grupo de investigación y análisis Misión Verdad, 2024).

Es importante señalar que la verificación directa de los informes del "Observatorio Venezolano de Ciberseguridad" en los fragmentos proporcionados conduce a una mención genérica en el informe del BID sin detalles específicos del perfil de Venezuela en la página 174 (Banco Interamericano de Desarrollo, 2020). Esta limitación en la corroboración de la fuente original y la disponibilidad pública de datos específicos de ciberseguridad de dicho observatorio sugiere una posible debilidad en la transparencia de la información oficial y verificable sobre el panorama de ciberseguridad en Venezuela. Esta escasez de datos puede

obstaculizar la toma de decisiones informadas y la evaluación precisa del riesgo por parte de los actores públicos y privados. Para la rigurosidad académica, la verificación de la fuente es primordial. La atribución de una estadística específica a un observatorio de ciberseguridad no se corrobora directamente con informes detallados de dicho observatorio en los materiales proporcionados, en realidad se corrobora con otras entidades de monitoreo social. Esta brecha de datos es un hallazgo significativo en sí mismo, ya que destaca un desafío en la evaluación de la verdadera magnitud del problema y en la formulación de políticas basadas en evidencia.

Es importante señalar que la verificación directa de los informes del "Observatorio Venezolano de Ciberseguridad" en los fragmentos proporcionados conduce a una mención genérica en el informe del BID sin detalles específicos del perfil de Venezuela en la página 174 (Organización de los Estados Americanos & Banco Interamericano de Desarrollo, 2020). Esta limitación en la corroboración de la fuente original y la disponibilidad pública de datos específicos de ciberseguridad de dicho observatorio sugiere una posible debilidad en la transparencia de la información oficial y verificable sobre el panorama de ciberseguridad en Venezuela. Esta escasez de datos puede obstaculizar la toma de decisiones informadas y la evaluación precisa del riesgo por parte de los actores públicos y privados. Para la rigurosidad académica, la verificación de la fuente es primordial. La atribución de una estadística específica a un observatorio de ciberseguridad no se corrobora directamente con informes detallados de dicho observatorio en los materiales proporcionados, en realidad se corrobora con otras entidades de monitoreo social. Esta brecha de datos es un hallazgo significativo en sí mismo, ya que destaca un desafío en la evaluación de la verdadera magnitud del problema y en la formulación de políticas basadas en evidencia.

Los sectores más vulnerables a los ciberataques en Venezuela son el financiero, el gubernamental y el de salud, principalmente debido a la vasta cantidad de datos sensibles que gestionan y su criticidad para el funcionamiento del país. Estas industrias manejan grandes volúmenes de información confidencial, lo que las convierte en objetivos atractivos para los ciberdelincuentes.

La infraestructura crítica, que abarca sistemas de energía y telecomunicaciones, constituye un objetivo primordial para los ciberdelincuentes (Banco Interamericano de Desarrollo, 2020). Un ejemplo concreto es la infraestructura de CANTV, que ha reportado volúmenes de tráfico hasta cinco veces mayores de lo que su estructura puede soportar, haciéndola particularmente susceptible a ataques de denegación de servicio (Grupo de investigación y análisis Misión Verdad, 2024). La concentración de ciberataques en sectores críticos como el financiero, gubernamental, de salud y la infraestructura conlleva pérdidas económicas directas para las entidades afectadas, y también representa un riesgo sistémico significativo. Estos ataques pueden paralizar servicios esenciales, erosionar la confianza pública y exacerbar la inestabilidad en un contexto económico ya desafiante para Venezuela, con graves consecuencias para la vida cotidiana de los ciudadanos y la gobernabilidad del país. El ataque a sectores críticos significa que los ciberataques tienen consecuencias de gran alcance más allá de las pérdidas financieras inmediatas. La vulnerabilidad de CANTV es un ejemplo tangible de cómo las limitaciones de infraestructura pueden amplificar el impacto

de los ataques, lo que podría conducir a interrupciones generalizadas del servicio. Esto implica que la amenaza no es simplemente un riesgo comercial, es además una preocupación de seguridad nacional y bienestar público, que exige una estrategia de defensa coordinada y robusta.

La región de América Latina y el Caribe enfrenta una alarmante brecha de talento humano calificado en ciberseguridad, estimada en 600.000 profesionales en el año 2020 (Banco Interamericano de Desarrollo, 2020).Según estimaciones, para 2030 la demanda de profesionales en tecnología de la informacion (TI) certificados en Latinoamérica crecerá hasta diez veces en comparación con 2020. Además, el 70 % del gasto empresarial en la región estará dirigido a tecnologías enfocadas en la transformación digital. Sin embargo, la brecha de habilidades TI representa un desafío significativo, con un impacto económico estimado en 34.800 millones de dólares para el 2022 (Forbes Centroamérica, 2025).

En la Venezuela contemporánea, a pesar de que la ciberseguridad se ha convertido en una pieza fundamental del panorama nacional, especialmente en el marco de los recientes eventos electorales y el aumento de la actividad cibernética maliciosa, no se dispone de variedad de fuentes de información que hayan publicado lo documentado al respecto. Los ataques informáticos han proliferado, explotando las vulnerabilidades del sistema tecnológico del país. Lo cual ha motivado una respuesta sin precedentes por parte del Estado, que ha reconocido la necesidad de una defensa más robusta en el ciberespacio. La ministra de Ciencia y Tecnología, Gabriela Jiménez, ha destacado la seriedad de esta situación, revelando que desde el 28 de julio del 2024, mas de 106 fueron objeto de agresiones digitales, incluyendo la Presidencia de la República, el Consejo Nacional Electoral (CNE) y la CANTV (Eljuri, 2024). Este fenómeno ha sido calificado por expertos como el ataque informático más grande en la historia de la nación, tanto por su volumen, como también por la multiplicidad de las agresiones, lo que sugiere un esfuerzo coordinado y de gran envergadura (Grupo de investigación y análisis Misión Verdad, 2024). La respuesta gubernamental se ha materializado en la creación del Consejo Nacional de Ciberseguridad, una instancia diseñada para fortalecer las plataformas tecnológicas y mitigar los riesgos inherentes a la guerra híbrida moderna, en la que el ciberespacio se ha erigido como un dominio central de conflicto (Bravo, 2024).

Según Misión Verdad (2024), única fuente hallada con datos precisos, desde una perspectiva técnica, los ciberataques se han manifestado en diversas modalidades, siendo el ataque de Denegación de Servicio Distribuido (DDoS) la forma más prevalente, constituyendo el 65 % de las agresiones. Estos ataques han afectado gravemente a los servidores de instituciones estatales y los enlaces internacionales que proveen internet al país. Otros tipos de ataques incluyen el robo de información mediante correos electrónicos con software malicioso (17 %), la ampliación de DNS (6.9 %), el secuestro de rutas BGP (3.45 %), y la desfiguración de páginas web (3.44 %). La magnitud de estas agresiones es sorprendente; se han registrado picos de hasta 30 millones de ataques por minuto. Según un informe de la proveedora de servicios de telecomunicaciones Columbus, el volumen de tráfico malicioso ha llegado a ser cinco veces mayor que la capacidad máxima de 10GB de

los enlaces nacionales de CANTV. La empresa Netscout, por su parte, ha corroborado la frecuencia de estos incidentes y su carácter de "bombardeo generalizado" hacia un proveedor de telecomunicaciones singular que alberga la infraestructura del partido gobernante.

La evidencia disponible sugiere que la ciberofensiva contra Venezuela es de origen foráneo y cuenta con un significativo respaldo económico y tecnológico. Aunque el rastreo es difuso, el punto inicial de salida de los ataques fue identificado en Macedonia del Norte, nación donde operan comandos cibernéticos del Pentágono y la OTAN sin restricciones; no obstante, expertos indican que este país solo fungió como un "último punto de salida" mediante redes VPN, sugiriendo que los atacantes reales se ubicaban en otras áreas geográficas. La alta magnitud y duración de estos ataques, que superan las capacidades de un actor no estatal, refuerzan la teoría de una operación respaldada por una entidad gubernamental. En respuesta a esta crisis y como preparación ante futuros desafíos en un entorno global cada vez más digitalizado y susceptible a las "nuevas guerras híbridas", la creación del Consejo Nacional de Ciberseguridad representa un paso crucial para el Estado venezolano (Grupo de investigación y análisis Misión Verdad, 2024).

No se ha podido precisar evidencias de las consecuencias económicas que estos ataques han implicado pero al comprender por las secciones anteriores la vinculación directa entre las acciones liberticidas maliciosas y la estabilidad económica publica y privada, se puede inferir que los costos de los ciberataques recientes en el país han conducido a cuantiosas perdidas en ambos sectores. Y lo que es más importante, la afectación en el desenvolvimiento de las actividades económicas y sociales de los venezolanos se han visto altamente afectadas generando un ambiente de tensión e inseguridad digital.

Conclusiones

La ciberseguridad, en la sociedad contemporánea, ha trascendido su naturaleza meramente técnica para erigirse como un pilar fundamental del desarrollo económico y la estabilidad sistémica. Lejos de ser un gasto opcional, la protección digital se ha consolidado como una inversión estratégica que impulsa la productividad y fomenta la resiliencia en un entorno cada vez más interconectado. La capacidad de un país para salvaguardar sus infraestructuras críticas, proteger y preservar la confianza del consumidor determina su competitividad y sostenibilidad a largo plazo.

El vínculo directo entre la ciberseguridad y el sector económico se manifiesta en la prevención de costos multidimensionales que amenazan la viabilidad empresarial y la estabilidad macroeconómica. La creciente sofisticación de las amenazas cibernéticas genera pérdidas directas por concepto de remediación e indemnizaciones, así como costos indirectos derivados de la interrupción de negocios y el daño reputacional incalculable. Estos incidentes no solo comprometen la integridad de los datos, sino que erosionan la confianza del cliente, un activo intangible indispensable para el florecimiento del comercio digital. Asimismo, los costos sistémicos, como la distorsión en la asignación de recursos y las interrupciones en las cadenas de suministro, evidencian la interdependencia entre la seguridad digital y la salud

económica. Priorizar la inversión en ciberseguridad se convierte, por ende, en una obligación para fortalecer la competitividad, asegurar la continuidad operativa y mitigar los riesgos financieros.

En el contexto específico de Venezuela, la necesidad de la ciberseguridad adquiere una relevancia crítica que demanda una atención académica y estratégica urgente. La vulnerabilidad en los sistemas de ciberseguridad, especialmente tras ataques perpetrados contra instituciones y servicios públicos, tiene profundas implicaciones económicas y psicológicas para la población. A nivel económico, estos incidentes interrumpen el acceso a servicios esenciales, comprometiendo transacciones y la estabilidad financiera de los ciudadanos. A nivel psicológico, generan una sensación de inseguridad y desconfianza en las infraestructuras digitales del Estado. Es fundamental diagnosticar el estado actual de las infraestructuras digitales, la brecha de talento humano especializado y la adecuación de los marcos regulatorios. La promoción de la investigación contextualizada es una condición necesaria para construir una economía digital robusta, segura y confiable en el país, asegurando un futuro próspero y protegido.

Referencias

Admass, W., Munaye, Y., y Diro, A. (2023). Cyber security: State of the art, challenges and future directions. *Cyber Security And Applications*, (2). https://doi.org/10.1016/j.csa.2023.100031

Anderson, R. (2021). *Security engineering: A guide to building dependable distributed systems (3rd ed.)* John Wiley & Sons. https://www.cl.cam.ac.uk/archive/rja14/Papers/SEv3.pdf

Andrew, J. (2016). Experiencias avanzadas en políticas y prácticas de ciberseguridad. En M. Porrúa (Ed.). A. G. de Alba Díaz (Ed.), *Panorama general de Estonia, Israel, República de Corea y Estados Unidos*. Banco Interamericano de Desarrollo. https://publications.iadb.org/es/publications/spanish/viewer/Experiencias-avanzadas-en-pol%C3%ADticas-y-pr%C3%A1cticas-de-ciberseguridad-Panorama-general-de-Estonia-Israel-Rep%C3%BAblica-de-Corea-y-Estados-Unidos.pdf

Arias, E. (2025). *Cisco and Microsoft Cybersecurity Certifications Overview*. CISCO. https://www.cisco.com/c/en/us/training-events/training-certifications/certifications.html%20y%20https://learn.microsoft.com/en-us/credentials/browse/?type=certification&products=security

Asociación Bancaria y de Entidades Financieras de Colombia. (2022). *Guia de buenas prácticas para auditar la ciberseguridad. Asociación Bancaria y Entidades Financieras de Colombia*. Asobancaria. https://www.asobancaria.com/wp-content/uploads/2022/06/Guia%5C_de%5C_Buenas%5C_Practicas%5C_para%5C_Auditar%5C_la%5C_Ciberseguridad%5C_2022%5C_V1.pdf

Asociación Chilena Administradora de Fondos de Inversión. (2021). *Reporte Venture Capital & Private Equity 2021-2022*. ACAFI. https://acafi.cl/Reporte_Final_2021_2022.pdf

Bagul, S. (2015). E-commerce market size worth us $ 80.5 Trillion by 2030. *TECH MAG*, (5), 67-68. https://doi.org/10.26480/itechmag.05.2023.67.68

Banco Interamericano de Desarrollo. (2020). *Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe*. Inter-American Development Bank. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Bravo, S. (2024). *Ministra Gabriela Jimenez Ramírez: Venezuela se encuentra en alerta ante ataques cibernéticos*. Mincyt. https://mincyt.gob.ve/ministra-gabriela-jimenez-ramirez-venezuela-encuentra-en-alerta-ante-ataques-ciberneticos/

Cabezas, E., y Fiallos, H. (2024). Simulación de ataques fishing y Planes de Concienciación aplicables al ámbito empresarial – Un enfoque práctico para mejorar la resiliencia organizacional. *INNOVA Research Journal*, *9*(2), 95-110. https://dialnet.unirioja.es/descarga/articulo/10011858.pdf

Calle, A., Conforme, Y., Magallanes, E., y Guaranda, J. (2024). Importancia de la ciberseguridad en la investigación de mercados digitales. *Ciencia y Desarrollo*, *27*(2), 255-265. https://dialnet.unirioja.es/descarga/articulo/9604359.pdf

Cámara Venezolana de Empresas de Tecnologías de la Información. (2023). *Venezuela in LATAM Cyberattacks Top 10*. CAVEDATOS. https://cavedatos.org/blog/venezuela-in-latam-cyberattacks-top-10-spanish/

Catalan, C. (2025). *The true cost of data breaches*. Teramind. https://www.teramind.co/learn/data-exfiltration/cost-of-data-breaches/

Centro de Ciberseguridad Industrial. (2021). *La Ciberseguridad Industrial en Venezuela*. CCI. https://www.cci-es.org/maps/venezuela/

Centro Nacional de Planeamiento Estratégico. (2025). *Seguridad de las transacciones digitales*. CEPLAN. https://observatorio.ceplan.gob.pe/ficha/o40_2024

Chala, Y. (2019). *Importancia de la aplicación del mecanismo de cigrado de información en las empresas para la prevención de riesgos como ataques, plagio y pérdida de la confidencialidad* [Tesis de especialización]. Universidad Nacional Abierta y a Distancia. https://repository.unad.edu.co/bitstream/handle/10596/30745/yfchala..pdf

Comisión Económica para América Latina y el Caribe. (2013). *Economia digital para el cambio estructural y la igualdad*. CEPAL.org. https://repositorio.cepal.org/server/api/core/bitstreams/ce419364-f83a-4ef3-a9dd-91c9c295b273/content

Comisión Económica para América Latina y el Caribe. (2025). *Biblioguías – Biblioteca de la CEPAL*. CEPAL.org. https://n9.cl/e67bzr

Costagliola, D. (2025). *GDPR Explained: Key rules for data protection in the EU*. Investopedia. https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp

Council of Europe. (2001). *Convenio sobre la ciberdelincuencia. Serie de Tratados Europeos.n°185*. OAS. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

De Neira, A., Kantarci, B., y Nogueira, M. (2023). Distributed denial of service attack prediction: Challenges, open issues and opportunities. *Computer Networks*, (222). https://doi.org/10.1016/j.comnet.2022.109553

Díaz, J., Harari, I., y Amadeo, A. (2013). *Guía de recomendaciones para diseño de software centrado en el usuario*. Universidad Nacional de La Plata. https://core.ac.uk/download/pdf/296358615.pdf

Donoso, M. (2022). ¿Cuán importante es la seguridad cibernpetica para lograr la seguridad hídrica? *Revista de Ciencias Ambientales*, *56*(1), 284-297. https://www.redalyc.org/journal/1275/127550463012/html/

Edwise Foundation. (2025). *Best Universities in the USA for Computer Science and IT Studentes*. Edwisefoundation. https://edwisefoundation.com/best-universities-in-the-usa-for-computer-science-and-it-students/

Eljuri, A. (2024). *Más de 100 instituciones del Estado fueron afectadas por ataques cibernéticos desde el 28-j. Oficina de Gestión Comunicacional del Ministerio del Poder Popular para Ciencia y Tecnología*. Mincyt. https://mincyt.gob.ve/mas-de-100-instituciones-del-estado-fueron-afectadas-por-ataques-ciberneticos-desde-el-28-j/

European Commission. (2023). *Directiva NIS2: nuevas normas sobre ciberseguridad de las redes y sistemas de información*. EC. https://n9.cl/0bpihr

Fimlaid, J. (2025). *How rate hikes and cuts shape cybersecurity spend*. Nuharborsecurity.com. https://www.nuharborsecurity.com/blog/how-rate-hikes-and-cuts-shape-cybersecurity-spend

Forbes Centroamérica. (2025). *Para 2030 la demanda de profesionales TI certificados crecerá hasta diez veces en Latinoamérica*. Forbes. https://forbescentroamerica.com/2025/02/10/para-2030-la-demanda-de-profesionales-en-ti-certificados-crecera-hasta-diez-veces-en-latinoamerica

Giraldo, L. (2025). Impacto de la ciberseguridad en los modelos de negocio de las organizaciones. En E. R. Díaz (Ed.). A. G. Rodríguez (Ed.), *Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales*. Sello Editorial ESDEG.

GitLab platform. (2024). *SAST vs. DAST*. https://about.gitlab.com/es/topics/devsecops/sast-vs-dast/

Golombick, C. (2025). *Cyberattack costs in 2025: Statistics, trends, and real examples*. ExpressVPN. https://www.expressvpn.com/blog/the-true-cost-of-cyber-attacks-in-2024-and-beyond/?srsltid=AfmBOoq1KCKwF8e0J8QiUqcmK9BqGOeSurrxzw6acyILNM_JjbG9BrPd

Grupo de investigación y análisis Misión Verdad. (2024). *Ciberataques contra Venezuela: sus alcances y dimensiones técnicas*. misionverdad. https://misionverdad.com/venezuela/ciberataques-contra-venezuela-sus-alcances-y-dimensiones-tecnicas#:%C2%B8~:text=A

International Business Machines. (2025a). *¿Qué es la gestión de identidades y accesos (IAM)?* IBM. https://www.ibm.com/es-es/think/topics/identity-access-management

International Business Machines. (2025b). *¿Qué es un sistema de detección de intrusiones (IDS)?* IBM. https://www.ibm.com/es-es/think/topics/intrusion-detection-system

International Business Machines. (2025c). *Cost of a Data Breach Report 2025*. IBM. https://www.ibm.com/reports/data-breach

International Information System Security Certification Consortium. (2023). *Workforce study: Cybersecurity talent gap*. ISC. https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf

James, N. (2025). *51 Smal Business Cyber Attack Statistics 2025 (And What you can do about them)*. Astra. https://www.getastra.com/blog/security-audit/small-business-cyber-attack-statistics/

Jonker, A., Lindemulder, G., y Kosinski, M. (2025). *What is cybersecurity?* IBM. https://www.ibm.com/think/topics/cybersecurity

Kerner, S. (2022). *Explicación del hackeo del oleodcto Colonial: todo lo que necesitas saber*. TechTarget.com. https://n9.cl/t50jx

Kumar, N. (2025). *59 eCommerce Fraud Statistics (2025) – Latest Trends & Facts*. Demandsage. https://www.demandsage.com/ecommerce-fraud-statistics/

Lee, G. (2025). *Global Cybersecurity Spending Projected to Reach $ 213 Billion in 2025 - Cybersecurity*. Daily Security Review. https://dailysecurityreview.com/cyber-security/global-cybersecurity-spending-projected-to-reach-213-billion-in-2025/

Llanos, A. (2025). *Ciberseguridad como ventaja competitiva: convencer a tu cliente con confianza*. Minery Report. https://mineryreport.com/blog/ciberseguridad-ventaja-competitiva-confianza-cliente/

McCallum, S. (2023). *Meta: Facebook owner fined €1.2bn for mishandling data*. BBC News. https://www.bbc.com/news/technology-65669839

Melero, C. (2025). *El 60 % de las PYMEs cierran tras ataque. Ciberseguridad para Pymes — Protege tu negocio*. Escudopyme. https://escudopyme.com/2025/01/29/el-60-de-las-pymes-cierran-tras-ataque/

Naciones Unidas. (2010). *Module 8: Cybersecurity and Cybercrime Prevention – Strategies, Policies and Programmes*. UNODC. https://www.unodc.org/e4j/en/cybercrime/module-8/key-issues/international-cooperation-on-cybersecurity-matters.html

Naciones Unidas. (2013). *Estudio exhaustivo sobre el delito cibernético*. UNODC. https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime%5C_Study%5C_Spanish.pdf

Niccum, J. (2021). *Cyberattack on Colonial Pipeline affected gas prices far less than initially reported, study finds*. The University of Kansas.

Observatorio de la Ciberseguridad en América Latina y el Caribe. (2016). *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe)*. Banco Interamericano de Desarrollo. https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

Picus Security Validation Platform. (2025). *¿Que es el marco MITRE?* picussecurity. https://n9.cl/s8fll

Raji, A., Olawore, A., Ayodeji, A., y Josepf, J. (2023). Integrating Artificial Intelligence, machine learning, and data analytics in cybersecurity: A holistic approach to advanced threat detection and response. *World Journal of Advanced Research and Reviews*, *20*(3). https://www.researchgate.net/publication/

385695339_Integrating_Artificial_Intelligence_machine_learning_and_data_analytics_in_cybersecurity_A_holistic_approach_to_advanced_threat_detection_and_response

Rego, M., y Pérez, P. (2017). El intercambio de información de ciberamenazas. En U. de la Rioja (Ed.), *El intercambio de información de ciberamenazas* (1.ª ed., pp. 139-169). Universidad de la Rioja. https://dialnet.unirioja.es/descarga/articulo/6115623.pdf

Rifa, H. (2024). *Factor humano: punto clave en la ciberseguridad*. Universitat Oberta de Catalunya. https://blogs.uoc.edu/informatica/es/factor-humano-en-la-ciberseguridad/

Rodriguez, G. (2016). Cibersiguridad realidad y tendencias en Venezuela. *Cuestiones Jurídicas*, *10*(1), 13-39. https://www.redalyc.org/journal/1275/127550463012/html/

Saeed, S. (2022). *Disaster Recovery Planning: Best Practices for Ensuring Operational Continuity*. Mehran University of Engineering y Technology. www.researchgate.net/publication/383360303_Disaster_Recovery_Planning_Best_Practices_for_Ensuring_Operational_Continuity

Sánchez, J., y Montoya, L. (2016). Factores que afectan la confianza de los consumidores por las compras a través de medios electrónicos. *Pensamiento y Gestión*, (40), 159-183.

Santos, J. (2024). *La importancia de priorizar la asignación de recursos financieros para la ciberseguridad de todo negocio*. Worldnetpr. https://www.worldnetpr.com/2024/04/02/la-importancia-de-priorizar-la-asignacion-de-recursos-financieros-para-la-ciberseguridad-de-todo-negocio/

Shivarkar, A. (2025). *Cyber security market size to hit USD 878.48 bn by 2034*. Precedence Research. https://www.precedenceresearch.com/cyber-security-market

Singh, H., Shepherd, L., Nurse, J., Erola, A., Epiphanuou, G., Maple, C., y Bellekens, X. (2021). *Cyber security in the age of COVID-19: A timeline anda analysis of cybercrime and cyber-attacks during the pandemic*. National Center for Biotechnology Information. https://pmc.ncbi.nlm.nih.gov/articles/PMC9755115/

Sood, N. (2024). *Cryptography in Post Quantum Computing Era*. researchgate. https://www.researchgate.net/publication/377696294%5C_Cryptography%5C_in%5C_Post%5C_Quantum%5C_Computing%5C_Era

Sutherland, T. (2016). *Las violaciones de los datos afectan la confianza del consumidor*. Security. https://n9.cl/5aeax

UNESCO. (2025). *Plataforma electrónica internacional de alfabetización mediatica e informacional*. ONU. https://www.unesco.org/mil4teachers/es/module8

Unifiedpost Group. (2023). *El auge de las ayudas a la digitalización en Singapur*. Unifiedpost. https://www.unifiedpostgroup.com/es/news/the-rise-of-singapores-digitalisation-grants

Unión Europea. (2016). *Reglamento General de Protección de Datos (GDPR)*. EU. https://gdpr-info.eu/

Urciuoli, L. (2022). *La ciberseguridad en la cadena de suministro, una tendencia al alza*. Mecalux.es. https://www.mecalux.es/articulos-de-logistica/luca-urciuoli-ciberseguridad-cadena-suministro

World Economic Forum. (2023). *Global Risks Report 2023: 18th Edition (Insight Report)*. WEF. https://www3.weforum.org/docs/WEF%5C_Global%5C_Risks%5C_Report%5C_2023.pdf

World Economic Forum. (2025). *Global Cybersecurity Outlook 2025*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

Consideraciones sobre criptografía cuántica y su futuro en el campo de la Ciberseguridad

Jesús Erazo[1]

Introducción

En el año de 1982, en su visionario seminario titulado *Simulating Physics with Computers*, el físico Richard Feynman contextualizó la dificultad de simular estados cuánticos de sistemas físicos, como átomos y moléculas, con el uso de computadoras clásicas, debido a que los principios intrínsecamente probabilísticos de la mecánica cuántica exigían recursos computacionales exponenciales, presentando un gran desafío. Ante este hecho, Feynman (1982), planteó una pregunta fundamental: *¿Qué tipo de computadora necesitamos para simular la física?*. Su respuesta, futurista y tenaz, sentó las bases para el campo de desarrollo de la computación cuántica, al proponer una computadora que emulara el comportamiento mismo de la naturaleza a nivel atómico.

En este contexto, en 1985, la revolucionaria visión de Feynman comenzó a tomar cuerpo gracias al trabajo del físico David Deutsch. En su artículo clásico *Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer*, introdujo de manera formal un modelo para computador mecano-cuántico, un tipo de extensión cuántica de la máquina de Turing. Aunque comparte con las computadoras clásicas la característica de operar con recursos finitos, sus propiedades computacionales intrínsecamente cuánticas permiten resolver ciertos problemas probabilísticos de manera mucho más eficiente (Deutsch, 1985).

Aproximadamente, una década después del modelo de computador cuántico de Deutsch, Peter Shor en 1994, en su artículo *Algorithms for quantum computation: discrete logarithms and factoring*, presentó los primeros ejemplos de algoritmos cuánticos capaces de resolver problemas de factorización de números enteros y logaritmos discretos, iniciando así el campo del criptoanálisis cuántico (Shor, 1994). Es en este contexto, donde los expertos en criptografía vislumbran el potencial de la computación cuántica para vulnerar los sistemas de cifrado de información.

Si bien es cierto que los computadores cuánticos por ahora no han alcanzado su máximo potencial y no tienen aplicaciones prácticas en la actualidad, su desarrollo promete revolucionar diversos campos. Más allá de los algoritmos cuánticos para factorización de números enteros, se divisa un futuro prometedor en el campo financiero, la gestión de riesgos, la ciencia de los materiales y la optimización logística (Brooks, 2023). De hecho, investigadores, académicos y expertos en el desarrollo de tecnologías cuánticas son optimistas y esperan que en la próxima década se logre aplicar en el mundo real en

[1]Licenciado en Física y MSc. en Física Fundamental (ULA, Venezuela). Investigador en Tecnologías. Se ha desempeñado como responsable de diversas áreas relacionadas con la planificación en la administración publica y en espacios comunales. jerazo@cenditel.gob.ve

el análisis y estudio del metabolismo de fármacos (comprender el procesamiento de los medicamentos por el cuerpo, desde su absorción y distribución hasta su biotransformación y excreción), el secuestro de CO_2 (para reducir su concentración en la atmósfera y mitigar el cambio climático), la fertilización agrícola, el desarrollo de cátodos para baterías más eficientes, la investigación en reacciones de fusión (desarrollar una fuente de energía limpia y abundante), desarrollo de espectómetros superconductores de rayos X y rayos gamma (para aplicaciones que incluyen análisis de materiales y contabilidad de materiales nucleares), la resolución de ecuaciones diferenciales lineales complejas (ecuaciones de Navier-Stokes, teoría de cuerdas) y la búsqueda de patrones ocultos en grandes conjuntos de datos (Genkina, 2024).

Posiblemente, por ser una solución prometedora en ciberseguridad, uno de los campos con mayor probabilidad de materializarse en el corto o mediano plazo es el de la *criptografía cuántica*, la cual es impulsada por la permanente y creciente preocupación por la vulnerabilidad de los sistemas digitales a ciberataques cada vez más sofisticados. En términos generales, la criptografía cuántica engloba diversos métodos de ciberseguridad que buscan cifrar y transmitir datos de forma segura, basándose en las leyes fundamentales e inmutables de la mecánica cuántica. El encriptado cuántico, a diferencia de los algoritmos criptográficos clásicos, ofrece la posibilidad de una seguridad mucho mayor, e incluso se considera teóricamente invulnerable (Schneider y Smalley, 2023c).

En este contexto, resulta esencial comprender a fondo esta tecnología, sus principios físicos subyacentes, sus beneficios y limitaciones, así como sus implicaciones para organizaciones empresariales, financieras, tecnológicas, militares y gubernamentales. Por lo tanto, este ensayo se centra en la computación cuántica y su rama especializada, la criptografía cuántica, con la finalidad de explorar una tecnología con un potencial transformador para el futuro de la ciberseguridad.

Generalidades

La aparición del neologismo ciberseguridad y su importancia está estrechamente relacionada con las consecuencias derivadas de los ciberdelitos a través de ataques realizados por medio de redes de computadoras. Básicamente, un ciberdelito principalmente se refiere a un intento de obtener acceso ilegal a una computadora o sistema informático con el propósito de causar daño o perjuicio (Merriam-Webster Dictionary, 2025). En términos prácticos, un ciberataque es cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital. Se utilizan varias tácticas, como ataques de *malware*, estafas de ingeniería social y robo de contraseñas, para obtener acceso a información no autorizada (International Business Machines Corporation, 2024).

Ahora bien, la protección de los activos digitales frente a los ciberataques es realmente una preocupación, es mas, es un peligro latente, sobre todo por el surgimiento de una sociedad cada vez más digitalizada. Existe una amenaza real de robo de datos operativos, información de identificación personal (PII) o información estratégica, tanto en organizaciones, hogares

y dispositivos personales (Iturbe y Rifà-Pous, 2023).

La historia de los ciberataques, va desde las llamadas telefónicas gratuitas de larga distancia hasta el espionaje virtual (Llinares, 2012). En particular e históricamente, se considera que el primer ciberataque se realizó a través de un sistema de telégrafos, el cual consistió en robo de información del mercado financiero francés en 1834. Ahora bien, con el avance de las tecnologías digitales, se ha ampliado el abanico de estrategias para la arremetida de delitos cometidos por medio de ciberataques que se aprovechan de las vulnerabilidades de los sistemas informáticos, lo que ha provocado un crecimiento exponencial en el número de ciberdelitos (Monroe University, 2025).

En la próxima sección, se presenta un compendio de eventos que han marcado la pauta en la evolución de las diferentes modalidades de ciberataques y ciberdelitos, reflejando el hecho de que a medida que los sistemas informáticos (*hardware* y *software*) mejoran sus capacidades técnicas, a la par se va ampliando el conjunto de estrategias para cometer ciberdelitos. En efecto, a partir de la aparición de la red global de computadoras interconectadas conocida como *Internet*, también inició la era de los crackers, los cuales roban las credenciales de los usuarios a través de técnicas de *phishing* por medio de mensajería instantánea o correo electrónico.

Evolución histórica de los ciberataques y el ciberdelito

A continuación se presenta un conjunto de eventos que permiten tener una perspectiva las modalidades y evolución de los ciberataques. En tal sentido, de acuerdo con Yeshiva University (2025); Monroe University (2024) y Choi et al. (2019), los sucesos que han marcado y caracterizado la evolución de los ciberataques a través del tiempo, son los siguientes:

- En 1962 se realizó el primer ciberataque simulado contra redes informáticas. Consistió en el robo de contraseñas de la base de datos del Massachusetts Institute of Technology a través de tarjetas perforadas.
- En 1971, se creó con fines de investigación el primer virus informático llamado *Creeper Virus* (programa autorreplicante). El *software* malicioso fue detectado por la red de computadoras creada por el Departamento de Defensa de los Estados Unidos (Advanced Research Projects Agency Network, ARPANET).
- A principios de la década de 1980, logran *crackear* con éxito los sistemas internos del holding multinacional estadounidense de telecomunicaciones $AT\&T$.
- A finales de la década de 1980, aparece *ransomware* AIDS Trojan (secuestro de datos) con el uso de disquetes, afectando los soporte de almacenamiento de datos de la conferencia de la Organización Mundial de la Salud sobre el SIDA.
- En el año 1988, se realizó el primer ciberataque a la incipiente *World Wide Web*, afectando los sistemas informáticos de las universidades de Princeton, Stanford, Johns

Hopkins, Berkeley, Lawrence Livermore National Laboratory y la National Aeronautics and Space Administration.

- A mediados de la década de 1990, se utiliza un programa robo de contraseñas para afectar los sistemas informáticos para el robo de datos de investigación Air Force Research Laboratory de los Estados Unidos.

- En el año de 1995, logran *crackear* la red de la institución financiera Citibank, realizando transacciones fraudulentas a varias cuentas bancarias en todo el mundo. También, en este mismo año, a través de un ciberataque acceden a los códigos de acceso a Motorola y Nokia obteniendo así información privilegiada de usuarios.

- A finales de la década de los noventa, *crackean* sitios web del gobierno de los Estados Unidos. Un año después, aparece el *software* malicioso conocido como *Melissa Virus*, su acción consistía en primer lugar, acceder a las aplicaciones de *Microsoft Word* de los usuarios. Posteriormente, establecía un vínculo con *Microsoft Outlook* y de allí se replicaba a través del envío de correo electrónico a varias cuentas.

- A principios del año 2000, se realizó el primer ataque de denegación de servicio distribuido (Distributed Denial-of-Service, DDoS) contra los sitios web de la plataforma multinacional de comercio electrónico Amazon, a la empresa de tecnología Yahoo, al canal de televisión por suscripción CNN y la plataforma de ecommerce eBay. En este mismo año, con el uso del virus *ILOVEYOU* (virus de la carta de amor), se logró un ciberataque de tipo *phishing*, el cual consistió en el acceso a todo el sistema operativo *Windows* de usuarios de *e-mail* que accidentalmente ingresaban a un correo electrónico no deseado.

- A mediados de la primera década del siglo XXI, se llevó a cabo a través de un ciberataque la fuga de datos de 1.4 millones de usuarios de servicios de pago *MasterCard* de la empresa británica de servicios financieros multinacional HSBC.

- En el año 2006, hace aparición el *ransomware Archievus*, que utiliza cifrado avanzado *RSA* o algoritmo criptográfico de clave pública. Dos años más tarde, a través de un ataque cibernético resultado de conjugación de inyección *SQL* (infiltración de código intruso), *sniffer* de contraseñas (*software* de monitoreo de contraseñas) y *malware* (programa diseñado para dañar los sistemas informáticos), afectó al proveedor estadounidense de tecnología y procesamiento de pagos Heartland Payment Systems, vulnerando los datos de 134 millones de usuarios.

- A principios de la década de 2010, el gusano *Stuxnet*, saboteó las instalaciones de enriquecimiento de uranio de Irán. En ese mismo momento, algunas organizaciones de servicios financieros fueron afectadas por el virus troyano *Zeus* que ingresaba a través de correo electrónico. Un año después, la multinacional japonesa de productos electrónicos y entretenimiento Sony, experimentó un ciberataque, el cual consistió en el robo de nombres de usuario y contraseñas, fechas de nacimiento, respuestas a preguntas de seguridad de jugadores de su *PlayStation Network*.

- En los primeros años de la década del 2010, un ataque de *phishing* a través del envío de un correo electrónico con *malware* afectó a más de 100 millones de clientes de la corporación minorista estadounidense *Target*. En el transcurso de este año, también se descubrió que la multinacional Nokia Corporation realizó ataques preventivos *man-in-the-middle* (intercepción y modificación de los datos que se intercambian entre dos partes) a sus usuarios de smartphone a través del envío tráfico HTTP (Protocolo Seguro de Transferencia de Hipertexto) a través de sus servidores para descifrar datos.

- En el 2013, utilizando una red de computadoras y servidores conectados a *Internet* o *botnet* e ingeniería social se propagó a través de e-mail un *ransomware* tipo troyano denominado *CryptoLocker* dirigido a cifrar archivos en los ordenadores infectados. Por otro lado, empresa estadounidense de *software* Adobe Inc., reportó que al acceder a los servicios de *cloud computing* hizo que fuera vulnerable a los ciberataques resultando en la filtración de la información de 38 millones de usuarios, además de la información de tarjetas de crédito de tres millones de ellos.

- En 2014, se *crackean* fotos íntimas y de desnudos de celebridades de cuentas del servicio de almacenamiento en la nube de *Apple iCloud*.

- En el transcurso del 2015, un ataque cibernético del tipo *spear phishing* con el uso de correos electrónicos personalizados filtró datos de 4.000 militares y personal civil del Departamento de Defensa.

- Durante el 2016, aparece el *ransomware* para infectar equipos y cifrar sus archivos llamado *TeleCrypt* dirigido a jugadores en línea. En este mismo año, apareció el *malware Petya* (cifrado de archivos) que tiene la característica de sobrescribir el registro de arranque maestro y cifrar la tabla maestra de archivos dentro de un sistema, bloqueando el acceso a todo el disco duro.

- En el año 2017, el *ransomware WannaCry*, afectó a más de 200.000 computadoras con Windows en 150 países. Como caso especial, los hospitales del Servicio Nacional de Salud del Reino Unido. En el transcurso de este año, aparece *NotPetya* afectando a la empresa danesa de transporte naviero Maersk y a la multinacional alemana de ciencia y tecnología Merck.

- En 2018, plataforma basada en la nube GitHub experimenta un ataque *DDoS* de 1.3 terabytes por segundo, lo cual produjo la paralización de todas sus operaciones en su servidor.

- A finales de la década del 2010, Coinhive (servicio de minería de criptomonedas) fue utilizado por los cibercriminales como un *malware* de *criptojacking*, su código informático se utilizó en sitios web crackeados para obtener ilegalmente capacidad de procesamiento.

- A mediados del año 2022, la agencia que administra la Seguridad Social de Costa Rica fue cerrada por un ataque de *ransomware*.

Ciberseguridad

A partir de la sección precedente es fácil reconocer que, en primer lugar a medida que los sistemas digitales evolucionan, del mismo modo avanzan las prácticas maliciosas del robo de todo tipo de información sensible, comprometiendo de esta manera la integridad de las personas, instituciones no gubernamentales y dependencias de gobiernos. En segundo lugar, los principales riesgos están asociados con: i) *malware* que borra todo el sistema operativo (SO), ii) *cracker* que ingresa a un sistema y modifica archivos, iii) *cracker* que usa red de computadora para atacar a otros y iv) *cracker* que roba información de tarjetas de créditos para realizar.

Es ese sentido que surge la necesidad y motivación de la ciberseguridad. Históricamente, el término ciberseguridad aparece en la palestra pública en 1984 a través de una novela de ciencia ficción escrita por William Gibson titulada *Neuromante* (Valadés, 2022). Técnicamente, la ciberseguridad se puede entender como el conjunto de técnicas, políticas y mecanismos digitales para proteger redes, dispositivos y datos del acceso no autorizado o uso delictivo, y la práctica de garantizar la confidencialidad, integridad y disponibilidad de la información (U.S. Department of Homeland Security, 2024).

Ahora bien, dentro de las amenazas a la ciberseguridad se encuentran: 1) *ransomware*, 2) *malware*, 3) estafas de *phishing*, 4) robo de datos y 5) uso de inteligencia artificial para ciberataques (Jonker et al., 2025). En tal sentido, a la ciberseguridad deben estar asociados los tres principios de la seguridad de la información (confidencialidad, integridad y disponibilidad), los tres estados de los datos (datos en reposo, datos en tránsito y datos en uso) y las tres salvaguardas de la ciberseguridad (prevención, la detección y la respuesta), cuyo objetivo principal es proteger la información y los sistemas digitales en todas sus facetas (D. et al., 2022).

Tipos comunes de amenazas de ciberseguridad

Con fines de conocer con cierta profundidad algunos conceptos o términos asociados al ciberdelito, se presenta una descripción somera, pero oportuna de cada uno de ellos. De acuerdo con Cisco Security (2025), se tienen los siguientes tipos más comunes de amenazas:

- ***Malware***. Es un *software* diseñado para obtener acceso no autorizado o causar daños a un equipo.
- ***Phishing***. Básicamente, consiste en el envío de e-mails que imitan correos electrónicos de fuentes fiables, con la finalidad de obtener datos confidenciales, números de tarjetas de crédito e incluso información de inicio de sesión.
- ***Ransomware***. *Software* diseñado que bloquea el acceso a archivos o al sistema operativo con el objetivo de extorsionar.
- **Ingeniería social**. Táctica utilizada para engañar y conseguir información confidencial. Los atacantes pueden solicitar un pago monetario o acceder a sus datos confidenciales.

- Economía compartida.

Como se mencionó anteriormente, el avance de las tecnologías asociadas a los sistemas informáticos va acompañado con un conjunto de desafíos que emergen con las nuevas tendencias tecnológicas: computación en la nube, entornos multicloud, trabajo distribuido e inteligencia artificial, porque implican más conexiones, aumenta la complejidad de la gestión de la red, ofrecen más puntos de ataque, fragmentan las capacidades de seguridad y aumentan las oportunidades para amenazas (Jonker et al., 2025).

Otro aspecto, que subyace a todo lo anteriormente expuesto y que además representa el núcleo de los ciberataques es el fallo en el software del sistema operativo debido a errores de su programación, sin dejar de lado el *firmware* e incluso el *hardware*. Un *cracker* puede aprovecharse de este hecho para realizar acciones no autorizadas en el sistema como infectar equipos con *malware* o realizar otras actividades maliciosas (U.S. Department of Homeland Security, 2024).

Ahora bien, la National Institute of Standards and Technology (2024) define cinco funciones que debe cumplir un programa de ciberseguridad para que resulte exitoso: 1) Identificar (riesgos de ciberseguridad), 2) Proteger (salvaguardas y controles), 3) Detectar (ocurrencia de incidentes), 4) Responder (contener y mitigar el impacto) y 5) Recuperar (restaurar los servicios y capacidades afectadas). De tal manera que un programa de ciberseguridad debe tener como finalidad gestionar y reducir el riesgo de ciberseguridad de manera efectiva y continua de las organizaciones.

Por otro lado, de acuerdo con Jonker et al. (2025), se identifica varios tipos de ciberseguridad entre los cuales se encuentran: 1) ciberseguridad de la infraestructura crítica (proteger los sistemas y redes), 2) ciberseguridad de la red (protección de la infraestructura de red cableada como inalámbrica), 3) ciberseguridad de las aplicaciones (proteger el *software* y los dispositivos), 4) ciberseguridad de la información (independientemente de su formato digital o físico), 5) ciberseguridad en la nube (protección de los datos alojados en entornos de computación), 6) seguridad de la identidad (gestión de identidad y acceso), 7) seguridad de los endpoints (Protección de dispositivos de usuario final) y 8) seguridad de la IA (protección de los modelos de IA contra ataques).

Para concluir, en términos generales, existe una relación entre ciberseguridad, ingeniería social, contraseñas y actividades intrusivas ilegales a una red o a un sistema informático. Del mismo modo, entre redes, aplicaciones, usuarios finales y dispositivos. Cada elemento representa desafíos en la gestión de la identidad y los dispositivos de los usuarios. En tal sentido, toda esta infraestructura interconectada requiere un enfoque integral.

Computación cuántica

En la actualidad, existe un conjunto de tecnologías emergentes con un potencial transformador en diferentes aspectos de la vida humana. Entre ellas, se encuentran la computación cuántica. En particular, su aplicación en el campo de la criptografía no solo

representa una oportunidad, sino también un desafío para la ciberseguridad.

Ahora bien, la teoría de la mecánica cuántica busca explicar además de predecir el comportamiento de partículas como: electrones, protones, neutrones, núcleos atómicos, átomos, moléculas y fotones (Fitts, 1999). En términos generales, el formalismo de la mecánica cuántica se apoya en tres postulados fundamentales: el principio de superposición, el principio de incertidumbre y el principio de complementariedad.

Por otro lado, la computación cuántica utiliza los principios de la mecánica cuántica para abordar aquellos problemas complejos cuyos métodos matemáticos de resolución resultan inaccesibles con las capacidades actuales de las computadoras clásicas más potentes. La forma de funcionar los computadores cuánticos es aprovechando los fenómenos cuánticos de la superposición, entrelazamiento cuántico, decoherencia e interferencia (Schneider y Smalley, 2023a).

Por tanto, en la base de los algoritmos cuánticos está implícito, de acuerdo con Di Giovanni (2020):

- El principio de superposición, a partir del cual un cúbit puede estar en una combinación de estados de 0 y 1. Bajo estas condiciones, las computadoras cuánticas realizar múltiples cálculos simultáneamente.
- El entrelazamiento, el cual permite a los sistemas cuánticos representar y manipular correlaciones complejas en los datos. Bajo estas circunstancias, los cúbits pueden representar y procesar múltiples valores simultáneamente, lo que aumenta el paralelismo computacional. Además, el entrelazamiento de cúbits se utiliza para detectar y corregir errores en sistemas cuánticos, manteniendo la coherencia durante períodos más largos. También, las puertas cuánticas multi-cúbit CNOT, utilizan entrelazamiento para manipular datos entre cúbits.
- La interferencia cuántica, que permite amplificar las trayectorias correctas y anular las incorrectas, aumentando la probabilidad de obtener la respuesta correcta. En términos prácticos: los cúbits se preparan en la computadora cuántica. Luego, se los pone en un estado de superposición. Usando la interferencia cuántica, el sistema puede ser programado a través de operaciones o puertas. Esto significa que la interferencia aumenta las chances de que los cúbits arrojen la respuesta correcta, mientras que las respuestas equivocadas se vuelven menos probables.

A lo anterior, también se debe adicionar el teorema de no clonación, el cual establece que es imposible crear una copia perfecta de un estado cuántico desconocido.

Por otro lado, según la National Academies of Sciences (2020), una computadora cuántica está conformada básicamente por:

- Cúbits físicos. Opciones de cúbits que se están considerando para las computadoras cuánticas para llevar a cabo las operaciones de lógica cuántica: los cúbits superconductores y trampa de iones.

- Plano de datos cuánticos. Incluye los cúbits físicos y las estructuras necesarias para mantenerlos en su lugar. Además, debe contener una circuitería especial para medir el estado de los cúbits y para ejecutar operaciones de compuerta en estos cúbits físicos dentro de un sistema basado en compuertas.

- Plano de control y medida. Convierte las señales digitales del procesador de control, que indican las operaciones cuánticas que deben realizarse, en las señales de control analógicas necesarias para realizar las operaciones en los cúbits del plano de datos cuánticos. Del mismo modo, convierte la salida analógica de las mediciones de cúbits en el plano de datos en datos binarios clásicos que el procesador de control puede procesar.

- Plano del procesador de control y procesador host. Tiene la tarea de identificar y activar la forma adecuada de energía del sistema o la secuencia de operaciones y mediciones de compuertas cuánticas (que luego son llevadas a cabo por el plano de control y medición en el plano de datos cuánticos). Estas secuencias ejecutan el programa, entregado por el procesador principal, para implementar un algoritmo cuántico.

Con respecto a las puertas y circuitos cuánticos, de acuerdo con Cooper (2024), se encuentran los siguientes:

- Puerta Hadamard: permite colocar un cúbit en un estado de superposición, con la misma probabilidad de ser medido como 0 o 1.

- Puerta Pauli-X: invierte el estado de un cúbit, cambiando de 0 a 1 y viceversa (análoga a la puerta NOT clásica).

- Puerta CNOT (NOT Controlado): crea entrelazamiento entre los cúbits. Dados dos cúbits, invierte el estado de uno (objetivo) solo si el otro (control) está en estado 1.

En la actualidad se conocen dos tipos de *software* cuánticos, según Dilmegani (2025):

- *Software* que ejecuta algoritmos cuánticos. Los kits de desarrollo de *software* cuántico y las plataformas computacionales ofrecen soluciones a los usuarios finales. Estos les ayudan a desarrollar y probar sus algoritmos cuánticos.

- *Software* que permite que las computadoras cuánticas funcionen. Las computadoras cuánticas presentan problemas de rendimiento debido a errores aleatorios, y se ha desarrollado software de corrección de errores para corregirlos. Un *software* o *firmware* de corrección de errores es un programa de bajo nivel que aumenta la estabilidad de las computadoras cuánticas.

En principio, las posibles aplicaciones más inmediatas de la computación cuántica son: el modelado del comportamiento de sistemas físicos e identificar patrones y estructuras en la información (Schneider y Smalley, 2023c). En ese sentido, sus potenciales usos abarcan desde la medicina hasta pronósticos meteorológicos (Allende y Da Silva, 2019). Por la posibilidad identificar patrones y estructuras en la información de una manera

más eficiente, rápida y óptima, la computación cuántica se podría presentar como una posible fuente de oportunidades o peligros para la criptografía como la seguridad informática.

En resumidas cuentas, la computación emergente tiene su marco teórico es la mecánica cuántica. La unidad mínima de información se denomina cúbit (sistema cuántico sensible a la medida), que puede representar el estado 0 o 1, o la superposición de estados 0 y 1. Es una tecnología aún en desarrollo, que busca utilizar propiedades cuánticas como el espín del electrón o la polarización del fotón (para representar el estado 0 o 1, o la superposición o la combinación simultánea de los dos valores 0 y 1. El tratamiento y procesamiento de la información se fundamenta en los fenómenos físicos de la superposición y el entrelazamiento cuántico.

Criptografía cuántica

La criptografía cuántica fue propuesta por el físico Stephen Weisner en la década de 1970. A mediados de los años ochenta, Bennett y Brassard desarrollaron el primer protocolo, conocido como *BB84*. Ahora bien, en el año 2003, se logró la transmisión de fotones entrelazados a través del río Danubio. Un año más tarde, se realizó la primera transferencia de dinero cifrada con claves cuánticas entre dos bancos austriacos. En ese mismo año 2004, se lanzó la *Quantum Net* (Qnet) en Cambridge, Massachusetts, la primera red de computadoras con más de dos nodos que utiliza criptografía cuántica (Russakovsky, 2021).

En esencia, la criptografía cuántica consiste en un conjunto de métodos que aprovecha los fenómenos cuánticos como la superposición (las partículas pueden existir en más de un estado de ser al mismo tiempo), el entrelazamiento (el estado cuántico de dos o más partículas no puede describirse de forma independiente porque están correlacionadas) y la interferencia cuántica (en un estado de superposición probabilística, dos o más partículas entre sí) para cifrar, transmitir y decodificar información. Emplea sensores capaces de detectar fotones individuales, para proteger los datos de ataques adversarios. Por ejemplo, el protocolo criptográfico cuántico denominado Distribución Cuántica de Claves (QKD) se transmite utilizando partículas cuánticas: fotones. Este protocolo utiliza clave de cifrado convencional compartida entre dos partes de confianza para codificar y decodificar datos. La diferencia crucial es que esta clave de cifrado se transmite utilizando partículas cuánticas: fotones (National Institute of Standards and Technology, 2025).

El cifrado cuántico, funciona de la siguiente manera según la Stanford University (2023):

- Codificación: en el envío de datos digitales, el emisor polariza con ayuda un filtro o polarizador los fotones de cuatro maneras distintas, asignando así valores de bits 0 o 1 a cada polarización.
- Recepción: el receptor posee dos tipos de lectores (corresponden a divisores del haz de fotones) y elige cuál usar para medir la polarización de cada fotón. Es decir, el dispositivo de recepción determina qué divisor utilizar para cada fotón.

- Generación de clave: el receptor informa al emisor qué lector usó para cada fotón. El emisor descarta las lecturas incorrectas al comparar la información con la secuencia de polarizaciones con el divisor incorrecto, y la secuencia de bits resultante se convierte en la clave de cifrado.

- Detección de intrusos: la seguridad clave radica en que si un intruso intenta leer o copiar un fotón, su estado cuántico cambia inevitablemente. Este cambio es detectado por los sistemas, lo que impide que la información sea interceptada sin ser descubierta. Es decir, el cifrado tiene la característica de impedir que un fotón se lea o copie sin ser detectado.

Ahora bien, uno de los principales desafíos de la criptografía cuántica, más allá de los detalles de tipo técnico, es el hecho de que se deben desarrollar sistemas criptográficos seguros tanto contra computadoras cuánticas como clásicas, y que puedan interoperar con los protocolos y redes de comunicación existentes (National Institute of Standards and Technology, 2024).

En cuanto a los tipos de criptografía cuántica que se desarrollan en la actualidad, de acuerdo con Schneider y Smalley (2023b), se tienen los siguientes:

- Distribución de clave cuántica (QKD). Los sistemas QKD operan enviando partículas individuales de luz, o fotones, a través de un cable de fibra óptica. Cada uno de estos fotones viaja en una única dirección y representa un cúbit, de información: ya sea un cero o un uno. En el lado del emisor, unos filtros polarizados alteran la orientación física de cada fotón a una posición predeterminada. Luego, el receptor emplea un par de divisores de haz para interpretar la posición de cada fotón al momento de su llegada. Posteriormente, el emisor y el receptor contrastan las posiciones de los fotones que se enviaron con las posiciones que se decodificaron. La serie de coincidencias se transforma entonces en la clave. Los sistemas QKD no se suelen utilizar para cifrar datos seguros, sino para realizar un intercambio seguro de claves entre dos partes mediante la creación colaborativa de una clave privada compartida, que a su vez puede utilizarse para los métodos tradicionales de cifrado de clave simétrica.

- Lanzamiento cuántico de moneda. Protocolo criptográfico que aprovecha los principios de la física cuántica para garantizar que dos partes, incluso si una de ellas es deshonesta, puedan acordar un resultado verdaderamente aleatorio (como el de un lanzamiento de moneda), y que ninguna de las partes pueda manipular el resultado a su favor sin ser detectada.

- Criptografía cuántica basada en la posición

- Criptografía cuántica independiente del dispositivo

- Protocolo Kek

- Protocolo Y-00

A estas alturas, es importante resaltar las diferencias entre lo que se conoce como criptografía clásica y la criptografía cuántica en lo que se refiere al enfoque y solución al problema del intercambio de claves. La primera, utiliza métodos de cifrado basados exclusivamente en la complejidad matemática de factorizar grandes números. Por ejemplo, la criptografía RSA se basa en un par de claves pública-privada, donde la clave pública consiste en un exponente e y un módulo N = p × q, donde p y q son números primos grandes. La clave privada se deriva utilizando estos primos y aritmética modular. La seguridad de RSA se basa en la dificultad de factorizar N en p y q, un problema que las computadoras clásicas tienen dificultades para resolver eficientemente (Wadhwa, 2025).

Mientras que la segunda, utiliza los principios de la física cuántica como el entrelazamiento, el cual hace imposible medir un estado cuántico sin perturbarlo. Es decir, si un intruso intenta interceptar un mensaje, el acto de medir o interactuar con su contenido lo alterará, de tal manera que revelará así la presencia del agente extraño (M., 2023). Con referente a este aspecto, los protocolos de distribución de claves cuánticas (QKD), como BB84 y Ekert91, basados en la teoría de la información cuántica, de acuerdo con la literatura especializada, han demostrado ser teóricamente indescifrables, lo que proporciona un método seguro para cifrar específicamente las VPN así como cifrar y descifrar mensajes (Delaney, 2024b).

Un elemento importante a destacar es que las computadoras cuánticas, mediante el algoritmo de Shors, pueden factorizar N exponencialmente más rápido, lo que representa una amenaza significativa para la seguridad criptográfica moderna (Wadhwa, 2025).

Algoritmo de Shor

En el año de 1994, Peter Shor, desarrollo el primer algoritmo cuántico creado para factorizar números enteros grandes en sus factores primos de manera exponencialmente, lo cual resulta en una manera más rápida que la llevada a cabo por los algoritmos clásicos, además de representar una amenaza directa para el cifrado RSA. El algoritmo opera en dos fases: 1) Un preprocesamiento; en el cual una computadora clásica reduce el problema de factorización a la búsqueda del período de una función específica. 2) Uso de una computadora cuántica; la cual emplea la transformada cuántica de Fourier (TCF) para hallar el período de dicha función (Delaney, 2024a).

Esquema del algoritmo de Shor:

- Elegir el número N para factorizar, donde N es un número compuesto grande con dos factores primos, p y q.
- Selecionar un número aleatorio a menor que N y relativamente primo con N.
- Aplicar la TCF a un conjunto de n cúbits en una superposición de todos los estados posibles. Este paso genera una superposición igual de todos los valores posibles de la función periódica, $f(x) = a^x$ mód N, donde x es un entero entre 0 y $N - 1$.

- Medir la salida de la TCF (valor aleatorio de la función periódica). Esta medición reduce la superposición de estados a un solo estado.
- Calcular el máximo común divisor (MCD) de N y $(a^{s/2}) + 1$ o $(a^{s/2})$–1. Donde s es el valor aleatorio de la función periódica. Si el MCD no es igual a 1 o N, entonces se ha encontrado un factor no trivial de N. De lo contrario, repetir los pasos 2 a 5 hasta encontrar un factor no trivial.

Oportunidades de la criptografía cuántica

Por su potencial nivel de seguridad resistente a los ataques, la criptografía cuántica ofrece:

- Transmisión de información confidencial y sensible de forma segura en los sectores militar, gubernamental y financiero.
- Uso de una red basada en QKD, para el envío de datos e investigaciones científicas.
- Creación de canales de comunicación seguros para dispositivos IoT: sensores, *software* y conectividad a internet.

Desafíos de la criptografía cuántica

La criptografía cuántica es una herramienta que resulta muy prometedora en el campo de la ciberseguridad. Sin embargo, asociado a su desarrollo se encuentra un conjunto de problemas por resolver. Debido a que se trabajan con sistemas físicos muy sensibles (fotones) que requieren, por un lado, condiciones de funcionamiento muy especiales de refrigeración y blindaje electromagnético. Por el otro lado, el desarrollo de nuevos materiales y el consumo de ingentes cantidades de energía (Erazo y Sulbarán, 2021).

Asimismo, se presenta el desafío de la coherencia necesaria para aumentar el número de cúbits y la decoherencia de los mismos debido a la interacción con su entorno (pérdida de información cuántica) aunado a la transmisión de la información. En tal sentido, el control de los cúbits y su uso en operaciones lógicas de forma eficiente resulta un gran reto por superar en el corto y mediano plazo.

Además, en la actualidad y para los próximos años, se presenta otro conjunto de retos en el desarrollo e implementación de la criptografía cuántica. Por ejemplo, en el ámbito económico, se tiene el desafío de la obtención del financiamiento para la investigación, el desarrollo y el despliegue de soluciones de criptografía cuántica que requieren una inversión multimillonaria en *hardware* e infraestructura especializados.

También, es necesario la experiencia y el talento, por tanto se requiere impulsar y fomentar la investigación avanzada en los campos científicos que sustentan la criptografía cuántica, como la mecánica cuántica, la computación cuántica y los algoritmos post-cuánticos. Por otro lado, en el ámbito jurídico, se precisa establecer regulaciones y la legislación sobre el uso apropiado de la criptografía cuántica en lo que respecta a la

privacidad de los datos y la seguridad nacional. En ese sentido, en el plano político, debe haber un consenso, además tomar decisiones apoyadas por un comité técnico y científico, entre las autoridades gubernamentales e instituciones públicas y privadas, con respecto al desarrollo responsable y estratégico de la criptografía cuántica.

En cuanto a la seguridad de la información, se debe garantizar transiciones seguras de los sistemas clásicos a los sistemas cuánticos. Asimismo, se debe considerar que existe el riesgo de que los avances cuánticos puedan ser explotados por agentes maliciosos. Por tanto, se necesita desarrollar salvaguardias y la cooperación a nivel internacional para prevenir el uso de la criptografía cuántica con fines delictivos o dañinos. Es decir, es necesario establecer e implementar reglas o normas y estándares de calidad muy rigurosos para los dispositivos y protocolos criptográficos cuánticos. Además, se requiere validar y certificar la efectividad y confiabilidad de las soluciones cuánticas en la protección de datos sensibles.

En el área de la defensa militar, podrían surgir amenazas cibernéticas muy sofisticadas a partir del uso de las capacidades de la computación cuántica. Por tanto, obligadamente es necesario investigar e implementar una protección digital robusta para salvaguardar la inteligencia nacional y militar contra el uso indebido de las nuevas tecnologías cuánticas.

Con base a este conjunto de hechos, se listan los desafíos actuales en el campo emergente de la criptografía cuántica:

- Alto costo y complejidad (necesidad de *hardware* especializado: computadoras cuánticas y detectores de fotones).
- Escalabilidad.
- Necesidad de estados cuánticos transmisibles a largas distancias.
- Velocidad, eficiencia y capacidad para proteger los datos.
- Investigación y desarrollo de métodos prácticos de cifrado.
- Modificación de los protocolos existentes para gestionar tamaños de clave más grandes.
- Redes y canales de comunicación para transmitir información cuántica de forma fiable.
- Comprensión del uso de la tecnología.
- Adaptación en el ámbito público.
- La migración cuántica requiere tiempo.
- Resistir ataques de computadoras cuánticas.
- Aumentar la distancia máxima a la cual se puede transmitir información.
- Compatibilidad con los sistemas existentes.

- Viabilidad de utilizar medios de transmisión de información existente como las fibras ópticas para distribuir claves cuánticas a largas distancias.
- Implementación en redes de comunicación industrial.
- Adopción eficiente y oportuna en infraestructuras gubernamentales.
- Consumo energético.

Reflexiones finales

El avance de las computadoras y los dispositivos móviles, *cloud computing*, *Internet* y redes e *internet de las cosas* (IoT), aumentó el valor de los datos intercambiados y al unísono los requerimientos de ciberseguridad.

Ahora bien, las deficiencias de los métodos criptográficos clásicos (métodos de clave pública o secreta) y la propuesta teórica de las computadoras cuánticas con su potencial capacidad para descifrar protocolos criptográficos de vanguardia ha motivado el desarrollo de la criptografía cuántica en el ámbito de la seguridad informática.

Sin embargo, la criptografía cuántica a pesar de ser una prometedora herramienta en el campo de la ciberseguridad, presenta un conjunto de desafíos asociados a su investigación, desarrollo e implementación. Principalmente, se requiere conocimientos especializados en física cuántica y se necesita computadoras cuánticas y detectores de fotones.

No obstante, la tecnología continúa con su evolución y en los próximos años podría alcanzar su pleno desarrollo, por tanto, las organizaciones e instituciones públicas y privadas deben estar preparadas para la transición de sus comunicaciones al paradigma de seguridad cuántica. Por un lado, deben reconocer las vulnerabilidades de los algoritmos criptográficos clásicos frente a la computación cuántica. Por otro lado, deben desarrollar de un plan de transición, crear la infraestructura criptográfica y establecer el marco de regulación.

Referencias

Allende, M., y Da Silva, M. (2019). *Tecnologías cuánticas: Una oportunidad transversal e interdisciplinar para la transformación digital y el impacto social*. BID. https://bit.ly/3vj5PNe

Brooks, M. (2023). Quantum computers: what are they good for? *Nature*, *617*(7962), S1-S3. https://doi.org/10.1038/d41586-023-01692-9

Choi, K., Lee, C., y Louderback, E. (2019). Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime. *Springer eBooks*, 1-17. https://doi.org/10.1007/978-3-319-90307-1_2-1

Cisco Security. (2025). *A better way of doing security*. Cisco. https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html

Cooper, A. (2024). *Understanding Quantum Software: How it operates*. ValueCoders. https://www.valuecoders.com/blog/software-engineering/what-is-quantum-software/

D., N., L., M., y R., F. (2022). *What is Cybersecurity?* Wiley. https://doi.org/10.1002/9781119788317.ch2

Delaney, I. (2024a). *A Brief History Of Shor's Algorithm And Peter Shor, The Quantum Algorithm From 1994 That Threatens The Security Of All Our Data*. Quantum Zeitgeist. https://quantumzeitgeist.com/a-brief-history-of-shors-algorithm-and-peter-shor/

Delaney, I. (2024b). *Quantum Cryptography: the future of secure communications*. Quantum Zeitgeist. https://quantumzeitgeist.com/quantum-cryptography-the-future-of-secure-communications/

Deutsch, D. (1985). Quantum theory, the Church–Turing principle and the universal quantum computer. *Proceedings Of The Royal Society Of London A Mathematical And Physical Sciences*, *400*(1818), 97-117. https://doi.org/10.1098/rspa.1985.0070

Di Giovanni, F. (2020). *Physical Principles Underpinning Quantum Computing*. EE Times Europe. https://www.eetimes.eu/physical-principles-underpinning-quantum-computing/

Dilmegani, C. (2025). *Quantum Software in 2025: What It Is & How It Works*. AIMultiple. https://research.aimultiple.com/quantum-software/

Erazo, J., y Sulbarán, P. (2021). Es posible desarrollar computación cuántica en Venezuela? *Revista CLIC*, (24). https://convite.cenditel.gob.ve/publicaciones/revistaclic/article/view/1093/37

Feynman, R. (1982). Simulating physics with computers. *Int J Theor Phys*, *21*, 467-488. https://doi.org/10.1007/BF02650179

Fitts, D. (1999). *Principles of quantum mechanics: As applied to chemistry and chemical physics*. Cambridge University Press. https://catdir.loc.gov/catdir/samples/cam032/98039486.pdf

Genkina, D. (2024). Here Are 6 Actual Uses for Near-Term Quantum Computers. *IEEE Spectrum*, *10*. https://spectrum.ieee.org/what-are-quantum-computers-used-for

International Business Machines Corporation. (2024). *ciberataque*. IBM-Topics. https://www.ibm.com/es-es/topics/cyber-attack

Iturbe, J., y Rifà-Pous, H. (2023). Anomaly-based cyberattacks detection for smart homes: A systematic literature review. *Internet Of Things*, *22*. https://doi.org/10.1016/j.iot.2023.100792

Jonker, A., Lindemulder, G., y Kosinski, M. (2025). *What is cybersecurity?* IBM. https://www.ibm.com/think/topics/cybersecurity

Llinares, F. (2012). *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons, Ediciones Jurídicas y Sociales. https://dialnet.unirioja.es/servlet/libro?codigo=756351

M., A. (2023). *Classical vs Quantum Cryptography*. Girls in Quantum. https://girlsinquantum.com/classical-vs-quantum-cryptography/

Merriam-Webster Dictionary. (2025). *Definition of cyberattack*. Encyclopædia Britannica, Inc. https://www-merriam--webster-com.translate.goog/dictionary/cyberattack?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Monroe University. (2024). *Cybersecurity history: Hacking & data breaches*. monroeu. https://www.monroeu.edu/news/cybersecurity-history-hacking-data-breaches

Monroe University. (2025). *Cybersecurity history: Hacking & data breaches*. monroeu. https://www.monroeu.edu/news/cybersecurity-history-hacking-data-breaches

National Academies of Sciences. (2020). *Quantum computing*. NAP. https://doi.org/10.17226/25196

National Institute of Standards and Technology. (2024). *The CSF 1.1 Five Functions*. NIST. https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions

National Institute of Standards and Technology. (2025). *What is quantum cryptography?* NIST. https://www.nist.gov/cybersecurity/what-quantum-cryptography

Russakovsky, J. (2021). *Modern Cryptography: Theory and Applications*. Stanford University. https://cs.stanford.edu/people/eroberts/courses/soco/projects/2004-05/cryptography/quantum.html

Schneider, J., y Smalley, I. (2023a). *Quantum Computing*. IBM Research. https://www.ibm.com/think/topics/quantum-computing

Schneider, J., y Smalley, I. (2023b). *Quantum Cryptography*. IBM Research. https://www.ibm.com/think/topics/quantum-cryptography

Schneider, J., y Smalley, I. (2023c). *What is quantum cryptography?* IBM Research. https://www.ibm.com/think/topics/quantum-cryptography

Shor, P. (1994). Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124-134. https://doi.org/10.1109/SFCS.1994.365700

Stanford University. (2023). *Modern Cryptography: Theory and Applications*. monroeu. https://cs.stanford.edu/people/eroberts/courses/soco/projects/2004-05/cryptography/quantum.html

U.S. Department of Homeland Security. (2024). *What is Cybersecurity? Cybersecurity And Infrastructure Security Agency*. https://www.cisa.gov/news-events/news/what-cybersecurity

Valadés, B. (2022). *'Neuromante': el origen del ciberespacio*. CiberiLATAM. https://www.segurilatam.com/actualidad/neuromante-el-origen-del-ciberespacio_20221220.html

Wadhwa, S. (2025). Classical Cryptography to Quantum Cryptography. *International Journal Of Engineering Research & Technology*, *14*(6). https://doi.org/10.17577/IJERTV14IS060235

Yeshiva University. (2025). *The Evolution of Cyber Threats: Past, Present and Future*. monroeu. https://online.yu.edu/katz/blog/the-evolution-of-cyber-threats

Ciberseguridad e Intersección Tecnológica

Ciberseguridad e Inteligencia Artificial: Una mirada desde el Ciberpoder

Santiago Roca[1]

Introducción: Ciberpoder, contexto político de la ciberseguridad

El ciberpoder puede definirse como la capacidad de un Estado para proyectar e imponer sus intereses en el sistema internacional mediante el uso estratégico de los recursos que ofrece el ciberespacio. En este contexto, la ciberseguridad, entendida como el conjunto de estrategias y acciones dirigidas a proteger los sistemas de información y las infraestructuras digitales, proporciona a los Estados mayor capacidad de maniobra en el ámbito digital. Por lo tanto, la ciberseguridad se presenta como un aspecto fundamental en la consolidación del ciberpoder, dado que permite fortalecer las capacidades institucionales y responder ante las amenazas propias de la gestión de activos de información, pero también hacer frente a otros retos en el plano internacional.

En paralelo, en los últimos años, la Inteligencia Artificial (IA) ha irrumpido como una tecnología transformadora con un impacto significativo en la ciberseguridad. Su capacidad para potenciar las herramientas digitales ha generado nuevas oportunidades y amenazas en el campo de la ciberseguridad, y el escenario se complica, entre otros aspectos, debido a la interacción entre actores estatales y no estatales en el contexto global. La IA se aplica, por ejemplo, en la detección de patrones de tráfico de red para prevenir ciberataques, pero también puede ser utilizada por actores hostiles para la creación de mensajes maliciosos. Por lo tanto, la formulación de políticas y la gestión de riesgos de ciberseguridad deben tener en cuenta el potencial de las aplicaciones basadas en IA para la formulación de estrategias y acciones.

Este ensayo tiene como objetivo explorar diferentes modos de convergencia entre el ciberpoder y la ciberseguridad, tomando como referencia la IA como exponente tecnológico relevante en la actualidad. Para ello, se exploran las condiciones que permiten la consolidación del ciberpoder, se examina la importancia de la ciberseguridad y de la IA en el momento actual, y se analizan las implicaciones de la adopción de IA para la ciberseguridad y el ciberpoder. Entre los aportes del ensayo, se plantea una concepción multidimensional del ciberpoder, lo que conduce a fundamentar una enfoque integral de la ciberseguridad y de su importancia para la generación de políticas nacionales.

[1]Politólogo egresado de la Universidad de Los Andes (ULA), Especialista en Sistemología Interpretativa, Magíster en Ciencias Políticas y Doctor en Gestión para la Creación Intelectual. Investigador del Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL). Editor y autor de publicaciones académicas y de divulgación científica, y coordinador de proyectos de conocimiento y tecnologías libres. sroca@cenditel.gob.ve

Ciberpoder y ciberseguridad: Objetivos nacionales y capacidades informáticas

Es necesario revisar diferentes perspectivas sobre el concepto de "ciberpoder", con el fin de aproximarse a una definición operativa que abarca sus atributos fundamentales, dimensiones y criterios de observación. Desde una perspectiva que reúne las dimensiones militar e informacional, el ciberpoder es la "capacidad de usar el ciberespacio para generar ventajas e influir en los acontecimientos en otros entornos operativos y a través de los instrumentos de poder" (Starr, 2009, p. 5). Sin embargo, tal aproximación debe ser ampliada para comprender qué nociones de poder, estrategias, medios técnicos y objetivos pueden abarcarse desde la perspectiva del ciberpoder.

Nye (2011) describe el significado de ciberpoder en los siguientes términos:

> ... el ciberpoder es la capacidad de obtener resultados deseados mediante el uso de los recursos de información interconectados electrónicamente del ciberdominio. El ciberpoder puede utilizarse para producir resultados deseados dentro del ciberespacio o puede utilizar ciberinstrumentos para producir resultados deseados en otros dominios fuera del ciberespacio (p. 123).

En otras palabras, el ciberpoder es el ejercicio del poder mediante los recursos que ofrecen las telecomunicaciones, con el fin de obtener resultados dentro y fuera del ciberespacio. Forma parte del fenómeno más amplio del "poder", por lo que es posible comprenderlo de acuerdo con tres características (Nye, 2011): (a) consiste en la habilidad de influenciar las decisiones de otros actores; (b) involucra la posibilidad de moldear las preferencias de los demás actores y (c) implica la definición de agendas u objetivos. En tal sentido, el ejercicio continuado del poder permite extender la capacidad de agencia de un actor sobre los demás, optimizando sus capacidades para formar agendas, definir preferencias, tomar decisiones y ejecutar acciones que puedan contribuir con sus propios intereses.

El ciberpoder puede comprenderse desde la perspectiva del poder duro (coerción) y del poder blando (influencia) (Nye, 2004). Así mismo, puede separarse en las dimensiones de "intra-ciberespacial" y "extra-ciberespacial" (Nye, 2011). Por ejemplo, algunas acciones informáticas pueden tener como finalidad detener las decisiones de un rival por medio de obstáculos materiales, como la imposición de un bloqueo de Internet, mientras que otras se proponen disuadirlo de tomar sus propias decisiones, como la utilización de los medios web para proyectar una imagen de superioridad estratégica. La Tabla 1 permite observar algunos ejemplos de desenvolvimiento del ciberpoder en términos de poder duro y poder blando.

Tabla 1: Objetivos de ciberpoder e instrumentos de aplicación.

	Objetivos del Ciberpoder	
	Intra-ciberespacio	**Extra-ciberespacio**
Instrumentos de información	Duro: Ataques de denegación de servicio. Blandos: Establecimiento de normas y estándar.	Duro: Ataque a los sistemas SCADA. Blandos: Campañas de diplomacia pública para influir en la opinión.
Instrumentos físicos	Duro: Control gubernamental de las empresas. Blando: Software para ayudar a los activistas de derechos humanos.	Duro: bombardear routers o cortar cables. Blando: protestas para desacreditar a los proveedores de servicios.

Fuente: Nye (2004).

Ahora bien, resulta necesario considerar las características de los actores involucrados en las relaciones de ciberpoder. Nye (2011) los divide en tres categorías: gobiernos importantes, organizaciones con redes altamente estructuradas e individuos/redes poco estructuradas, cada uno con diferentes recursos de poder, como se explica a continuación:

1. Gobiernos importantes: Tienen capacidad de desarrollar infraestructuras tecnológicas, imponer autoridad dentro de sus fronteras, controlar mercados globales, fortalecer capacidades cibernéticas ofensivas y defensivas, proveer bienes públicos digitales y construir una reputación internacional que refuerce su influencia. Enfrentan vulnerabilidades como la dependencia de sistemas complejos, inestabilidad política y riesgos de pérdida de legitimidad. Por ejemplo, Estados Unidos y China tienen un impacto significativo en el ciberespacio debido a su capacidad para influir en las políticas globales.

2. Organizaciones altamente estructuradas: Poseen capacidad de influencia en virtud de diversidad de recursos, flexibilidad transnacional, control tecnológico y reputación. Enfrentan riesgos como persecución legal, robo de propiedad intelectual y pérdida de reputación. Por ejemplo, empresas como Google y Microsoft poseen recursos que les permiten tener influencia en el ciberespacio.

3. Individuos y redes poco estructuradas: Tienen capacidad para operar con bajo costo, así como anonimato y facilidad para migrar de actividades. Enfrentan vulnerabilidades como la coerción legal e ilegal por parte de gobiernos y organizaciones. Por ejemplo, activistas cibernéticos y redes de voluntarios que actúan de forma intermitente en el ciberespacio.

Betz y Stevens (2011) complementan la idea de ciberpoder como forma de influencia directa (poder duro) o indirecta (poder blando) que utiliza los recursos informáticos y materiales del ciberdominio. En sus palabras, el ciberpoder puede entenderse como "la variedad de poderes que circulan en el ciberespacio y que moldean las experiencias de quienes actúan en él" (p. 44). En este sentido, hacen referencia a cuatro dimensiones de ciberpoder:

1. Ciberpoder coercitivo: Uso de coerción directa en el ciberespacio para modificar el comportamiento o las condiciones de otro actor. Este poder puede ser ejercido por Estados, actores no estatales o por interacciones entre ambos. Los ejemplos incluyen activistas, criminales, empresas privadas y alianzas militares. Cualquier actor con acceso y habilidades puede ejercer esta forma de poder, que abarca conflictos cibernéticos como sabotaje, espionaje y subversión.

2. Ciberpoder institucional: Control indirecto de actores del ciberespacio mediante instituciones formales e informales, que no son completamente manejadas por un solo actor estatal. Este poder permite influir en normas, estándares y comportamientos a través de dichas instituciones. Por ejemplo, los Estados pueden usar recursos para establecer reglas que les generen ventajas y creen obstáculos a sus rivales en el ciberdominio.

3. Ciberpoder estructural: Capacidad de moldear las relaciones en las que operan todos los actores, influyendo en sus posiciones y limitando sus acciones. Se enfoca en cómo las tecnologías de información y comunicación determinan las posiciones estructurales, por lo que cobran relevancia conceptos como "dependencia tecnológica".

4. Ciberpoder productivo: Capacidad para transmitir narrativas que orientan o limitan la acción social. Este poder contribuye con la creación y reproducción de discursos, por lo que resulta fundamental para moldear las percepciones y las dinámicas de interacción en el entorno digital.

Esta perspectiva esboza una comprensión integral del ciberpoder, que parte del reconocimiento de la complejidad del poder como fenómeno social. En este plano, el ciberpoder puede manifestarse directamente como forma de coerción, indirectamente a través de la influencia en organizaciones multilaterales, como parte de condiciones estructurales y a través de discursos sobre el dominio del ciberespacio. En tal sentido, abarca un conjunto de relaciones estratégicas e interpretativas que se desenvuelven en el marco de las interacciones y las instituciones que sostienen y engloban al ciberespacio.

En consonancia con lo anterior, es necesario establecer referencias acerca de cómo observar el ciberpoder. Por ejemplo, Van Haaster (2016) compara las aproximaciones de Nye (2011) y Betz y Stevens (2011), entre otros, y elabora un listado de capacidades y cibercapacidades que identifican el alcance de los diferentes actores en el ciberdominio, separado en las categorías de política, informacional, económica y militar. De forma similar, diferentes organizaciones se han ocupado de señalar algunos atributos característicos de las entidades que ejercen eficientemente el ciberpoder, como se explica a continuación.

El *Índice Nacional de Ciberpoder 2022* (Voo et al., 2022) plantea un esquema a partir de ocho objetivos estratégicos que formulan los Estados en el ciberespacio. Partiendo de que "el ciberpoder es el despliegue efectivo de capacidades cibernéticas por parte de un Estado para lograr sus objetivos nacionales" (Voo et al., 2022, p. 7), se evalúa la capacidad de los Estados de alcanzarlos utilizando medios cibernéticos. En palabras de los autores:

"medimos las estrategias gubernamentales, la capacidad para operaciones defensivas y destructivas, la asignación de recursos, las capacidades del sector privado dentro de un país, como las empresas tecnológicas, la fuerza laboral y la innovación" (p. 4). Así, el índice de 2022 ubicó a Estados Unidos, China y Rusia en los primeros lugares; seguidos de Reino Unido, Australia, Países Bajos, Vietnam, República de Corea, Francia e Irán como parte de los primeros 10 puestos.

En este sentido, los autores definieron 29 indicadores distribuidos entre los ocho objetivos para medir las capacidades de los Estados evaluados. Los objetivos considerados se exponen en la Tabla 2.

Tabla 2: Objetivos de ciberpoder según el Índice Nacional de Ciberpoder 2022.

Objetivos	**Referentes**
1. Vigilancia y monitoreo de grupos domésticos	Otorgar permisos legales y capacidades de vigilancia cibernética para monitorear y detectar amenazas internas, incluyendo el seguimiento de ciudadanos y la detección de servicios de inteligencia extranjeros.
2. Fortalecimiento de las defensas cibernéticas nacionales	Mejorar la defensa de activos gubernamentales y nacionales, promover la ciberseguridad y las buenas prácticas en la industria y en la población general.
3. Control y manipulación del entorno de información	Utilizar medios electrónicos para controlar la información y cambiar narrativas dentro y fuera del país, incluyendo propaganda doméstica y desinformación en el extranjero.
4. Recopilación de inteligencia extranjera para la seguridad nacional	Recopilar secretos nacionales de un adversario extranjero mediante medios cibernéticos para informar actividades diplomáticas, planificación militar, etc.
5. Desarrollo de la competencia tecnológica nacional	Fomentar la industria tecnológica doméstica mediante medios legales o ilegales, como el espionaje industrial.
6. Destruir o inhabilitar la infraestructura y capacidades de un adversario	Utilizar técnicas cibernéticas destructivas para erosionar la capacidad de un adversario en el ciberespacio o en el dominio convencional.
7. Definir normas y estándares cibernéticos internacionales	Participar activamente en debates legales, políticos y técnicos sobre normas cibernéticas, incluyendo la firma de tratados cibernéticos.
8. Acumular riqueza o extraer criptomonedas	Realizar operaciones cibernéticas para acumular riqueza, incluyendo el uso de ransomware y ataques a infraestructuras financieras.

Fuente: Adaptado de Voo et al. (2022).

Otro reporte, *Capacidades cibernéticas y poder nacional: una evaluación en red* (International Institute for Strategic Studies, 2021) evalúa a los Estados a partir de criterios similares. En función de estos aspectos, el reporte presenta los casos de Estados Unidos, Reino Unido, Canadá, Australia, Francia, Israel, Japón, China, Rusia, Irán, Corea del Norte, India, Indonesia, Malasia y Vietnam como exponentes de poder cibernético. Así mismo, entre sus conclusiones, considera que Estados Unidos, China y Rusia exceden en capacidades a sus aliados y competidores, aunque observan que el escenario se organiza en bloques contando a los partidarios de esos tres países. Los puntos que considera el informe se resumen en la Tabla 3.

Tabla 3: Capacidades cibernéticas según Capacidades cibernéticas y poder nacional: una evaluación en red.

Capacidades	Definición	Referentes
1. Estrategia y doctrina	Estrategia cibernética nacional coherente que alinee los objetivos políticos y de seguridad con las capacidades cibernéticas.	Definición de roles y responsabilidades, la asignación de recursos y la formulación de políticas para abordar los desafíos y oportunidades en el ciberespacio.
2. Gobernanza, mando y control	Estructura organizativa y los mecanismos de coordinación que un país utiliza para gestionar sus actividades cibernéticas.	Existencia de agencias gubernamentales dedicadas, la cooperación entre los sectores público y privado, y los protocolos para la toma de decisiones y la respuesta a incidentes.
3. Capacidad central de ciberinteligencia	Capacidad de un país para recopilar, analizar y utilizar inteligencia cibernética para comprender las amenazas, identificar vulnerabilidades y apoyar la toma de decisiones.	Capacidades de monitorear redes, rastrear actores maliciosos y anticipar ataques.
4. Investigación y dependencia cibernética	Grado en que un país depende de las tecnologías cibernéticas para su economía, infraestructura crítica y sociedad en general.	Políticas y programas para promover la alfabetización digital, la innovación tecnológica y el desarrollo de una fuerza laboral cibernética capacitada.
5. Ciberseguridad y resiliencia	Capacidad de un país para proteger sus sistemas y redes contra ataques cibernéticos y para recuperarse rápidamente de incidentes.	Medidas de seguridad técnicas y organizativas, realización de ejercicios de simulación y promoción de una cultura de ciberseguridad.
6. Liderazgo global en asuntos del ciberespacio	Participación de un país en foros internacionales y su capacidad para influir en las normas, políticas y estándares relacionados con el ciberespacio.	Incluye la promoción de la cooperación internacional, la defensa de sus intereses y la contribución al desarrollo de un ciberespacio seguro y estable.
7. Capacidad cibernética ofensiva	Capacidad de un país para llevar a cabo operaciones cibernéticas ofensivas con el fin de lograr objetivos estratégicos.	Desarrollo de herramientas y técnicas para penetrar redes, interrumpir sistemas y llevar a cabo espionaje cibernético.

Fuente: Adaptado de International Institute for Strategic Studies (2021).

La comparación entre los distintos referentes expuestos permite respaldar la concepción multidimensional del ciberpoder, observable en las capacidades ofensivas y defensivas de los entes estatales y para-estatales, pero también en objetivos como tener influencia en los órganos multilaterales o en la generación de discursos propagandísticos, entre otros mencionados. Claro está, la ciberseguridad aparece como una categoría relevante desde la

perspectiva del ciberpoder. El potencial informático de un país incluye el desarrollo de opciones de ciberseguridad en diferentes ámbitos, tanto por la garantía de salvaguarda de los activos de información como por la necesidad de contar con estrategias para hacer valer los intereses estatales en el ciberespacio.

Así, el concepto de ciberpoder ofrece un contexto de sentido a la ciberseguridad como parte de la presencia de los Estados en el ciberespacio. Por ejemplo, Nye (2011) menciona cuatro ciberamenazas a la seguridad nacional: espionaje económico, cibercrimen, ciberterrorismo y ciberguerra, que plantean diferentes exigencias a las capacidades de respuesta de los Estados y de cooperación internacional. Cada una de esas amenazas involucra componentes de seguridad que abarcan lo informático, pero que también traspasan los límites del ciberdominio. Por lo tanto, la ciberseguridad cobra importancia en el marco del ciberpoder como parte de las estrategias de consolidación de los intereses de los Estados, sustentada en las capacidades institucionales e informáticas de una sociedad nacional.

Resulta previsible que la IA juegue un papel importante en el desarrollo de otras capacidades de ciberseguridad y, en consecuencia, en las relaciones de poder en el escenario internacional. Si bien la IA parece orientada a reforzar tendencias existentes, también representa un elemento que puede cambiar las relaciones entre actores estatales y no estatales, como por ejemplo al modificar los medios tecnológicos que canalizan las rivalidades operativas entre los Estados "importantes", pero también al traer otros temas de agenda a la política internacional. Para abordar esta materia, resulta necesario partir de una aproximación a ciberseguridad y a la manera en que la IA se integra en el repertorio de sus opciones tecnológicas.

Ciberseguridad e IA: Escalamiento de las capacidades informáticas

Como ocurre con diferentes temas organizacionales, la ciberseguridad puede comprenderse en varios niveles. Por ejemplo, las políticas y agendas de ciberseguridad abarcan las acciones orientadas a la planificación (detección de necesidades, definición de prioridades, formulación de planes, etc.), mientras que los protocolos técnicos incluyen las acciones de respuesta ante amenazas informáticas concretas. En este trabajo se apoya una perspectiva amplia de ciberseguridad, que reconoce la pertinencia de sus diferentes dimensiones estratégicas. En tal sentido, la ciberseguridad puede entenderse como:

> El conjunto de políticas y acciones que se utilizan para proteger las redes conectadas (incluidos los ordenadores, los dispositivos, el hardware, la información almacenada y la información en tránsito) del acceso y la modificación no autorizados, el robo, la interrupción u otras amenazas (Unión Internacional de Telecomunicaciones, 2008, p. 7).

En consonancia, el papel de la ciberseguridad es proteger al conjunto de usuarios, información, dispositivos, servicios, aplicaciones e infraestructuras conectados a través de Internet. Se utilizan políticas, estrategias y técnicas de ciberseguridad para garantizar las

condiciones de salvaguarda de los activos de información y aspectos fundamentales como la privacidad de los usuarios. Por lo tanto, en un sentido restringido, la ciberseguridad puede entenderse como el conjunto de conceptos, directrices, métodos, prácticas, acciones y tecnologías dirigidas a proteger a los activos informáticos y a los usuarios en el ciberespacio (Unión Internacional de Telecomunicaciones, 2008). Entre los activos pueden incluirse los dispositivos informáticos, los servicios y aplicaciones, los sistemas de comunicaciones y la información almacenada y transmitida a través de medios informáticos.

En esta materia, es necesario conocer las amenazas que encuentran las organizaciones en el ciberentorno y las acciones pertinentes para la gestión de riesgos (Unión Internacional de Telecomunicaciones, 2008). Las amenazas del ciberentorno son variadas e incluyen ataques de interrupción de servicio, utilización fraudulenta de infraestructura, robo de activos de información, suplantación de identidad con fines maliciosos, entre muchas otras. Pueden clasificarse en accidentales o intencionales, según su origen, así como también en activas y pasivas, dependiendo de si causan cambios en los sistemas de información. Entre las medidas de gestión de riesgo, se puede contar con estrategias de prevención, defensa, detección, respuesta y recuperación para hacer frente a los ataques informáticos. Convencionalmente, se considera que algunas de las condiciones que permiten garantizar la seguridad de los activos de información son las siguientes:

- Disponibilidad: Los sistemas y datos deben estar accesibles cuando se necesiten.
- Integridad: La información no debe ser alterada de forma no autorizada.
- Autenticidad: La información o la identidad de un usuario son genuinas.
- No repudio: Una parte no pueda negar haber realizado una acción o transacción.
- Confidencialidad: Solo las personas autorizadas puedan acceder a la información.

La ciberseguridad es un tema de interés global que exige la construcción de capacidades conjuntas entre diferentes sectores. El *Global Cybersecurity Index* (International Telecommunication Union, 2024) clasifica a los países de acuerdo con cinco áreas: Legal, Técnica, Organizacional, Desarrollo de Capacidades y Cooperación. Esto significa que alcanzar altos niveles de desempeño en materia de ciberseguridad implica desarrollar facultades en diferentes instancias, tales como regulaciones en materia de cibercrimen, incremento de competencias técnicas, formulación de estrategias institucionales, ejecución de campañas públicas y apoyo entre distintos organismos. La construcción de aptitudes de ciberseguridad es resultado de esfuerzos organizacionales de distinto tenor, que integran la formulación de acciones estratégicas con el contenido de disciplinas asociadas a la informática, lo que refuerza su carácter vinculante con el ciberpoder.

En tal sentido, es posible observar que los países con mayores avances institucionales y técnicos son también quienes tienen mejor desempeño en materia de ciberseguridad. Si se comparan los países ubicados en los primeros lugares del índice de ciberpoder con el índice de ciberseguridad, se encuentran coincidencias en los siguientes casos: Estados Unidos,

China, Rusia, Reino Unido, Australia, Países Bajos, Vietnam, Corea del Sur, Francia e Irán. Así mismo, al comparar la lista de países punteros en cibercapacidades con el índice de ciberseguridad, se encuentran las siguientes coincidencias: Estados Unidos, Reino Unido, Canadá, Australia, Francia, Japón, China, Rusia, Irán, India, Indonesia, Malasia, Vietnam y Corea del Sur. Los países que aparecen en las tres listas son: Estados Unidos, China, Rusia, Reino Unido, Australia, Vietnam, Corea del Sur, Francia, e Irán. Por lo tanto, es factible fundamentar una correlación entre el ciberpoder y las fortalezas en ciberseguridad.

Ahora bien, la relación entre la ciberseguridad y la IA ha evolucionado en las últimas décadas. En los inicios (décadas de 1960 y 1970), la IA se centraba en diferentes áreas, mientras que la ciberseguridad era incipiente debido a la escasa interconexión de sistemas. En los 80 surgieron herramientas basadas en firmas (predecesoras del aprendizaje automático), mientras que los 90 marcaron las primeras aplicaciones de IA en detección de intrusiones y *malware*. En los 2000, el Big Data permitió usar IA para analizar patrones de amenazas, y en los 2010 el aprendizaje profundo incorporó la detección proactiva de *malware* y la respuesta automatizada, aunque también aparecieron los "ataques adversarios". Hoy se considera que la IA es clave para la detección, predicción y respuesta ante las ciberamenazas de última generación (Centro Criptológico Nacional, 2023).

Existen tres dimensiones de la relación entre IA y ciberseguridad: el uso de IA para apoyar la ciberseguridad, el uso de IA con propósitos maliciosos y la seguridad de los sistemas de IA (Car y Marcelin, 2024). En cuanto a la IA como herramienta de ciberseguridad, se han planteado aplicaciones en materias como detección, predicción, análisis y mitigación de amenazas. Así mismo, como herramienta de ataque a la ciberseguridad, la IA puede utilizarse para tareas como la codificación de *malware* y la ejecución de acciones de ingeniería social. En este sentido, la IA puede ser adoptada tanto por atacantes como por defensores de los sistemas informáticos, lo que contribuye a hacer más complejo el escenario de vulnerabilidades y amenazas en el ciberespacio. Como resultado, las organizaciones se están adaptando para incluir la IA en acciones de predicción, detección y respuesta a las ciberamenazas (Capgemini Research Institute, 2019).

Las alternativas tradicionales de ciberseguridad dependen de analistas humanos para examinar incidencias y responder a posibles ataques, pero considerando que varias actividades pueden automatizarse con la ayuda de la IA, también es posible actuar de forma más precisa en la identificación y respuesta ante amenazas. No obstante, el campo de las aplicaciones de IA en la ciberseguridad es muy amplio (Nour y Said, 2024; Roshanaei et al., 2024; Temara, 2024). Actualmente, la IA permite analizar grandes bases de datos, aprender sobre los patrones hallados y optimizar su propio funcionamiento, por lo tanto, "la integración de la IA en la ciberseguridad ha transformado la manera en que las organizaciones abordan la seguridad digital" (Folorunso et al., 2024, p. 169), dado que permite potenciar la prevención, detección y respuesta ante las amenazas.

En términos informáticos, las técnicas tradicionales de detección de amenazas incluyen: firmas, anomalías, comportamientos, redes, *endpoints*; detección de intrusiones, sistemas

basados en reglas, software antivirus, análisis de registros y escaneo de vulnerabilidades. Sin embargo, esas técnicas se centran en patrones conocidos, reglas predefinidas y monitoreo reactivo del entorno. En comparación, "la IA agrega un nuevo nivel de sofisticación a la detección y respuesta ante amenazas debido a su capacidad de procesar volúmenes masivos de datos y aprender de patrones y anomalías" (Nour y Said, 2024, p. 2). Esto permite pasar de una posición reactiva, basada en el análisis de datos convencional, una posición proactiva, orientada hacia la prospección, que genera un abanico de alternativas de respuesta ante las amenazas en el ciberentorno. En tal sentido, la Tabla 4 resume las aplicaciones de algunos algoritmos de IA en materia de ciberseguridad.

Tabla 4: Aplicación de algunos algoritmos de IA en ciberseguridad con líneas divisorias

Algoritmo de IA	**Aplicación en Ciberseguridad**
1. Redes Neuronales	Detección de patrones complejos en tráfico de red y malware.
2. Árboles de Decisión	Clasificación de tráfico de red y decisiones de bloqueo.
3. Random Forest	Detección de intrusiones con mayor precisión (combina múltiples árboles).
4. Máquinas de Soporte Vectorial (SVM)	Clasificación de ataques y filtrado de spam.
5. Redes Neuronales Profundas (DNN)	Análisis de malware avanzado (polimórfico) y detección de amenazas.
6. Redes Bayesianas	Modelado probabilístico de riesgos de ciberataques.
7. Naive Bayes	Filtrado de spam y detección básica de malware.

Fuente: Adaptado de Nour y Said (2024).

Una revisión de las posibilidades de la IA en ciberseguridad ofrece diversos resultados (Folorunso et al., 2024). En cuanto a la detección de amenazas, la IA permite el análisis de grandes volúmenes de datos en tiempo real y el aprendizaje continuo mediante algoritmos de *machine learning* y *deep learning*. En cuanto a la respuesta ante ciberataques, permite la automatización de acciones como el bloqueo de accesos sospechosos, identificación de brechas de seguridad, reconstrucción de ataques y detección de amenazas residuales, incluyendo la reducción de tiempos de respuesta y de errores humanos. La IA también permite la utilización de un enfoque predictivo mediante la identificación de patrones en los datos históricos con el fin de anticiparse a los ataques, la evaluación de vulnerabilidades y la evaluación de riesgos, a partir de la combinación de datos históricos y actuales. En otras palabras, la IA combina las capacidades de análisis de datos y aprendizaje automático, con las potencialidades del análisis de comportamiento y la detección de patrones para facilitar la generación de respuestas automatizadas.

La IA tiene el potencial de impactar en las opciones de ciberseguridad gracias a sus capacidades de análisis, automatización y adaptación, que le permiten facilitar tareas

como la detección avanzada de amenazas (procesamiento de grandes volúmenes de datos y aprendizaje automático), automatización (bloqueos de IP´s maliciosas, etc.) y reducción del tiempo de reacción. Con respecto a los entornos específicos del ciberdominio, la IA permite implementar técnicas como *machine learning* para predecir ataques basándose en datos históricos; procesamiento de lenguaje natural para analizar correos electrónicos, salas de chats y redes sociales con el fin de detectar actividades de *phishing* o de ingeniería social; análisis de comportamiento para identificar acciones anómalas de usuarios o dispositivos, y analítica predictiva para anticiparse a las amenazas antes de que ocurran (Nour y Said, 2024). La Tabla 5 ofrece un resumen de las aplicaciones de IA en materia de ciberseguridad.

Tabla 5: Aplicación de la IA en materia de ciberseguridad

Aplicación	**Tecnologías IA/ML Utilizadas**	**Beneficios Clave**
1. Detección de amenazas.	- Redes Neuronales - Random Forest	Identifica patrones anómalos en tiempo real, superando métodos basados en firmas.
2. Detección de malware.	- Deep Learning - SVM	Detecta malware desconocido analizando comportamiento (no solo firmas).
3. Análisis de comportamiento (UEBA).	- Redes Neuronales - Árboles de Decisión	Identifica amenazas internas y comportamientos sospechosos de usuarios.
4. Seguridad de redes.	- Random Forest - Redes Bayesianas	Detecta tráfico anómalo y protocolos no autorizados.
5. Inteligencia de amenazas.	- NLP - Deep Learning	Predice tendencias de ataques analizando fuentes globales.
6. Detección de fraude.	- Redes Neuronales - Naive Bayes	Identifica fraudes financieros y suplantación de identidad.
7. Automatización de respuesta.	- Árboles de Decisión - Random Forest	Bloquea automáticamente amenazas (ej: aislamiento de endpoints).

Fuente: Adaptado de Nour y Said (2024).

Como se comentó anteriormente, la IA también es útil para reforzar las facultades de los atacantes en ciberseguridad, que pueden utilizarla para tomar ventaja de las vulnerabilidades de los activos de información (Mahfuri et al., 2024; Zambrano, 2024). Por una parte, la automatización permite lanzar ataques masivos en tiempo real, como *phishing* personalizado o propagación de *malware*. Así mismo, los algoritmos de IA pueden analizar sistemas de seguridad y modificar sus ataques para evitar la detección (ataques adversarios). Además, los sistemas maliciosos pueden aprender de las defensas existentes y desarrollar nuevas amenazas (como el *malware* generativo). En otros casos, la IA puede analizar grandes volúmenes de datos para seleccionar víctimas específicas (*spear-phishing* con mensajes similares a comunicaciones legítimas). Finalmente, puede generar ataques

más escalables, capaces de infiltrarse en múltiples sistemas simultáneamente, como el *ransomware*. También existen diversas aplicaciones de IA para la ingeniería social, como la utilización de generadores de texto e imágenes para el envío de mensajes maliciosos y la suplantación de identidad (Tang et al., 2024).

La IA también presenta nuevos retos para la gestión de riesgos de ciberseguridad. Por ejemplo, la adopción de IA impone ciertos cuestionamientos, como el uso de datos sensibles o la invasión de la privacidad de los usuarios (Folorunso et al., 2024). En términos técnicos, existen obstáculos como la calidad de los datos, ya que los algoritmos requieren información consistente para realizar predicciones confiables. Además, la falta de interpretabilidad de los modelos avanzados de IA (como *deep learning*) dificulta que los expertos comprendan las decisiones del sistema, afectando la posibilidad de ofrecer respuestas adecuadas a las amenazas. Por otra parte, la ausencia de estándares globales complica la comparación y la evaluación de las soluciones de IA (Nour y Said, 2024). Finalmente, un estudio en materia de ciberseguridad e IA identificó tres categorías de riesgo que transcienden el ámbito informático: uso malicioso de la IA (contenido falso, manipulación), consecuencia de mal funcionamiento (confiabilidad, sesgos) y riesgos sistémicos (empleo, mercado, ambiente, derechos de autor, etc.) (Yohsua et al., 2024).

Como herramienta tecnológica, la IA tiene un impacto significativo en los campos de la ciberseguridad y del ciberpoder, dado que no solo apunta a transformar las condiciones de confrontación técnica entre diferentes actores, sino que también tiende a influenciar las relaciones entre los Estados. Por lo tanto, es claro que: "las implicaciones más plausibles de la IA para el ciberpoder en el futuro cercano implican cambios evolutivos en la escala y velocidad potenciales de los ciberataques, así como en su identificación y remediación" (Devanny, 2024, p. 25), por lo que actores estatales y no estatales se verán confrontados con nuevos retos informáticos y geopolíticos.

Resulta pertinente observar la importancia de la ciberseguridad y de la IA como factores con impacto potencial en diferentes escenarios de la geopolítica global. En tal sentido, es necesario retomar el lente del ciberpoder para examinar el papel de tecnologías como la IA en las relaciones internacionales.

Discusión: La ciberseguridad y la IA en el contexto del ciberpoder

Como se ha explicado previamente, el ciberpoder puede comprenderse como la capacidad de los actores (Estados, organizaciones o individuos) para utilizar recursos tecnológicos, informáticos y estratégicos del ciberespacio con el fin de influenciar, coaccionar o lograr resultados tanto dentro como fuera de este dominio. Combina instrumentos de poder duro (coerción directa) y poder blando (influencia indirecta) y genera facultades para definir preferencias, establecer agendas, controlar estructuras y elaborar discursos para moldear dinámicas sociales, económicas y políticas en entornos digitales y físicos. Desde esta perspectiva, pueden resumirse las dimensiones de ciberpoder de la siguiente manera:

1. Operativa (ofensiva y defensiva): Capacidad para realizar acciones directas en el

ciberespacio, como ataques ofensivos (sabotaje, espionaje) o defensivas (protección de infraestructuras críticas). Ejemplos: Operaciones cibernéticas destructivas, vigilancia doméstica, políticas de ciberseguridad.

2. Institucional-Normativa: Influencia en la creación y control de normas, estándares internacionales y estructuras de gobernanza del ciberespacio. Ejemplos: Participación en tratados normativos, definición de protocolos técnicos, promoción de agendas multilaterales.

3. Estructural-Tecnológica: Control sobre la infraestructura tecnológica global y capacidad para moldear las condiciones que determinan las relaciones en el ciberespacio. Ejemplos: Desarrollo de tecnologías críticas (IA, 5G), autonomía de los sistemas técnicos.

4. Discursiva-Informacional: Capacidad de crear y difundir narrativas, controlar flujos de información y manipular la percepción general mediante herramientas digitales. Ejemplos: Propaganda digital, desinformación, control de redes sociales.

La ciberseguridad es un elemento de ciberpoder en varios sentidos. En la dimensión operativa, se identifica como un proceso estratégico que permite crear condiciones de salvaguarda de los activos informáticos desde una perspectiva defensiva, y actuar en contra de los rivales geopolíticos desde una perspectiva ofensiva. En esta dimensión se encuentran las capacidades informáticas y las actividades organizacionales que permiten ofrecer alternativas para la prevención, detección y respuesta ante amenazas. En otras palabras, las capacidades informáticas son interdependientes con respecto al desarrollo político, legal, administrativo y organizativo del Estado en materia de ciberseguridad. Por lo tanto, se requiere de un núcleo político consciente de las condiciones de ciberpoder que genere requerimientos para la expansión de capacidades en esta materia.

La ciberseguridad también es un elemento en las otras dimensiones del ciberpoder, dentro y fuera del ciberespacio. En tal sentido, es tema de interés en las dimensiones Institucional-Normativa, Estructural-Tecnológica y Discursiva-Informacional. Por ejemplo, un país importante puede esforzarse por tener influencia en la definición de normas en ciberseguridad a través de su participación en organismos multilaterales, promover condiciones estructurales favorables a través de la definición de estándares técnicos y difundir un discurso propicio a sus intereses en el ciberespacio. Este tipo de interacciones definen la ciberseguridad como un proceso estratégico en el contexto de una concepción integral de ciberpoder. En la Tabla 6 se presentan algunos ejemplos de iniciativas de ciberseguridad alineadas con las dimensiones del ciberpoder.

Tabla 6: Casos de iniciativas de Ciberseguridad en el marco del Ciberpoder

Dimensiones	**Casos en Ciberseguridad**
Operativa (Ofensiva y Defensiva)	Protección de infraestructuras críticas nacionales (redes eléctricas, plantas de agua) contra amenazas persistentes avanzadas (APTs).
	Acciones internacionales como operaciones contra espionaje, desactivación de servidores en otros países, defensa de infraestructuras compartidas (cables submarinos, redes energéticas).
	Operaciones contra delitos financieros, sistemas de detección de intrusos en infraestructuras críticas, neutralización de amenazas mediante alianzas defensivas.
Institucional-Normativa	Marcos regulatorios nacionales (leyes de protección de datos, estándares para operadores críticos) con requisitos para entidades públicas y privadas.
	Marcos de gobernanza de Internet, negociación de tratados sobre ciberseguridad, armonización de estándares técnicos en la Unión Internacional de Telecomunicaciones.
	Mecanismos de cooperación internacional, acuerdos de cooperación cibernética, creación de entidades especializadas en ciberseguridad.
Estructural-Tecnológica	Protección de infraestructura crítica, centros de datos autónomos, criptografía para comunicaciones gubernamentales.
	Control en cadenas de suministro, intervención en los mercados de tecnologías, consultoría y certificación internacional de hardware y software.
	Medidas de vigilancia del ciberespacio, intercambio de datos con centros de ciberseguridad, desarrollo de protocolos de seguridad.
Discursiva-Informacional	Campañas públicas para influenciar el espacio mediático, verificación de noticias importantes, capacitación digital en centros educativos.
	Coaliciones mediáticas contra desinformación, contrarrestar operaciones de influencia extranjera, mecanismos de verificación de noticias.
	Construcción de narrativas institucionales, promoción de cultura ciudadana de ciberseguridad, incorporación de los sectores públicos y privados.

Fuente: Elaboración propia (2025).

La ciberseguridad resulta entonces un componente del balance de poder en el plano internacional. Esto puede observarse al examinar la competencia que existe entre países como Estados Unidos, Rusia y China, conflicto que posee una dimensión operativa (ofensiva y defensiva), pero que también se desenvuelve en las arenas de los organismos multilaterales, los estándares técnicos y las narrativas difundidas globalmente. Una comparación de las iniciativas nacionales de IA de Estados Unidos y China (Spratt, 2024) deja en evidencia

la importancia de la tecnología para los países industrialmente avanzados, en particular para la formulación de estrategias globales. En tal sentido, "la definición de prioridades de desarrollo tecnológico está subordinada a los intereses nacionales y a las condiciones del entorno global" (Roca, 2022, p. 40), en el contexto de la interacción entre las relaciones geopolíticas y los intereses nacionales con los factores de innovación y la implementación de avances tecnológicos.

Este año, Estados Unidos y China anunciaron políticas nacionales para fomentar el desarrollo de IA en el marco de sus propios intereses de seguridad. El Plan de Acción de EEUU plantea el abandono de políticas de regulación para fortalecer la infraestructura estadounidense y ganar espacio en el mercado mundial. El mismo posee tres pilares: (1) acelerar la innovación en IA; (2) construir la infraestructura estadounidense de IA; y (3) liderar la diplomacia y la seguridad internacionales en materia de IA. En contraste, el Gobierno chino propuso la creación de una organización internacional para la generación de políticas de IA que apunten a fortalecer la industria y la ciberseguridad. De esta manera, se confrontan dos iniciativas, una basada en la desregulación de los mercados internos y la utilización de la influencia en los organismos internacionales, y otra que propone la creación de un ente multilateral que genere un balance de poder frente al unilateralismo económico estadounidense (Abott, 2025).

La rivalidad entre las dos potencias tiene lugar también en los mercados tecnológicos. En materia de IA, China cuenta con mayores capacidades de gestión de talento y muchos más consumidores. Además, las aplicaciones desarrolladas en China son competitivas y su industria posee menos reservas en temas polémicos como la privacidad de los usuarios, lo que ha permitido que la industria china gane espacio a la estadounidense (Allison et al., 2021). Esto no ha pasado desapercibido para el gobierno de EEUU, que ha impuesto controles para la exportación de materiales tecnológicos al país asiático, como semiconductores y microprocesadores, al tiempo que busca la adhesión de países como Japón a este tipo de medidas. Ahora las políticas chinas buscan mitigar el efecto de las decisiones estadounidenses a través de la prohibición la importación de componentes extranjeros, el desarrollo y fabricación de tecnología china y vinculación entre los sectores público y privado (González, 2025; Triolo, 2024).

La infraestructura de ciberseguridad es otro espacio de rivalidad entre ambas potencias, como puede ejemplificar la relación con América Latina y el Caribe. EEUU ha hecho énfasis en apoyar alianzas internacionales y mecanismos de cooperación, fortalecer las infraestructuras esenciales y resguardar las cadenas de suministro contra los ciberdelincuentes. En contraste, China ha ampliado sus inversiones en la región, especialmente en materia de infraestructura, con las redes 4G y 5G, así como también en capacitación de personal técnico (Pestana, 2025). Paralelamente, China y EEUU han intercambiado acusaciones de ataques cibernéticos con los objetivos de sabotear infraestructuras claves o sustraer información (Deutsche Welle, 2025), por lo que la confrontación directa en el ciberespacio continúa siendo un tema fundamental entre ambas potencias.

En síntesis, la IA y la ciberseguridad pueden tomar parte de diferentes dimensiones del ciberpoder, al contribuir para modificar las relaciones institucionales entre los Estados, las condiciones de dependencia alrededor de la infraestructura y los discursos que respaldan la superioridad de cada país. El ciberpoder y la ciberseguridad son factores interdependientes, no solo en virtud de la capacidad de la tecnología de modificar la relación entre operaciones ofensivas y defensivas, sino también por su impacto en la carrera tecnológica y las relaciones entre los Estados.

Así mismo, la IA tiene un papel que cumplir en cada una de las dimensiones de integración entre la ciberseguridad y el ciberpoder. Por una parte, contribuye a ampliar las capacidades ofensivas-defensivas de las organizaciones capaces de implementarla. Como se señaló anteriormente, ofrece posibilidades de automatización informática, por lo que se convierte en un potenciador de las capacidades estratégicas y tácticas en el ciberespacio (Folorunso et al., 2024). De este modo, es más probable que "quienes combinen un propósito estratégico (...) y la potencia computacional necesarias para la investigación de vanguardia en IA obtengan los beneficios" en el escenario geopolítico (Devanny, 2024, p. 11). Precisamente, la formulación de objetivos estratégicos abarca el fomento de capacidades de ciberpoder y la implementación de iniciativas informáticas de ciberseguridad.

Paralelamente, los países más avanzados pueden lograr mayores niveles de automatización a través de la implementación de IA, mientras que los países rezagados observan cómo se amplía la brecha con respecto a aquellos, al tiempo que enfrentan nuevas amenazas en el ciberespacio. En este sentido: "la complejidad y la intensidad de los recursos necesarios para mantenerse a la vanguardia de la investigación, el desarrollo y la explotación de la IA probablemente reforzarán las asimetrías de poder existentes entre los países en el ciberespacio" (Devanny, 2024, p. 9). Este aspecto hace énfasis en las diferencias entre las oportunidades disponibles para la implementación eficiente de tecnologías, pero así mismo permite llamar la atención sobre la importancia de las relaciones de cooperación en el fomento de mejores condiciones de ciberseguridad. No se trata solo de reconocer las asimetrías existentes, sino también de observar estrategias que permitan mitigarlas a través de la colaboración entre actores estatales, con miras a la incorporación de actores no estatales y entes multilaterales.

El proceso de adopción de IA ha sido gradual pero consistente, de manera que "en el corto plazo, es probable que la IA siga teniendo un impacto evolutivo, más que revolucionario, en la competencia entre defensores y atacantes en el ciberespacio" (Devanny, 2024, p. 11). Esto significa que los ámbitos en los cuales resulta relevante la adopción de inteligencia artificial continuará ampliándose, particularmente en el campo de la ciberseguridad, con el consecuente incremento de casos de uso y organizaciones adoptando aplicaciones de IA en esta materia. Así mismo, es previsible que se incremente la demanda de actividades conexas, como talento especializado; productos de investigación y desarrollo; suministro de recursos manufacturados como componentes electrónicos; y disponibilidad de recursos naturales como agua y energía eléctrica, todo lo cual genera otras fuentes de presión en el

sistema internacional.

En el contexto del ciberpoder, la ciberseguridad representa una categoría significativa para el logro de los objetivos de política exterior de un Estado en el ciberespacio. En la dimensión operativa tiene lugar el campo de batalla en torno a amenazas como el ciberterrorismo y el espionaje industrial. Pero también intervienen otros planos de política, como la definición de agendas globales y la proyección de superioridad estratégica. Así mismo, la IA es un factor tecnológico que contribuye a potenciar las capacidades de los Estados y tiene consecuencias en el balance ofensivo-defensivo en el ciberespacio. Pero además, es un elemento a tener en cuenta en las diferentes dimensiones organizativas de la ciberseguridad, tales como la definición de aspectos legales y la formación de alianzas. El estudio de la IA como herramienta de ciberseguridad representa un escenario de la vinculación entre los avances tecnológicos y las relaciones geopolíticas a nivel global.

Conclusiones: Informática avanzada y política internacional

La incorporación de la IA en el campo de la ciberseguridad deja en evidencia el peso de los avances tecnológicos en escenarios donde se confrontan las capacidades ofensivas y defensivas de diferentes actores. La IA tiene el potencial de ofrecer un abanico de opciones de respuesta ante las amenazas, pero también puede contribuir a crear nuevos riesgos en el ciberdominio. Así mismo, el desarrollo de capacidades de ciberseguridad puede influir en las asimetrías entre actores estatales y no estatales, como por ejemplo en el caso del balance entre ataque y respuesta. La informática y la ciberseguridad son herramientas propicias para garantizar la salvaguarda de los activos de información y, consideradas de modo estratégico, juegan un papel fundamental en el conjunto de las relaciones de poder en el sistema internacional.

El concepto de ciberpoder ofrece un contexto de análisis para valorar cómo los países más avanzados, en términos estratégicos e informáticos, son aquellos que poseen marcos institucionales y capacidades de adaptación más propicios para hacer frente a diferentes amenazas. La selección de objetivos de política externa, utilizando los recursos que ofrece el ciberespacio, abre un repertorio de estrategias, desde las más operativas a las más mediáticas, pasando por el trabajo diplomático y la definición de estándares y capacidades técnicas. La ciberseguridad representa un aspecto esencial de la presencia de los Estados en el ciberespacio, no solo por la necesidad de resguardo de los activos de información, sino también como parte de su imagen de poder en el entorno global. Por lo tanto, todos los países pueden explorar sus capacidades en materia de ciberseguridad para ganar un lugar en espacios de deliberación, normalización y ejecución de operaciones cibernéticas.

El estudio del ciberpoder y la ciberseguridad abre la posibilidad de examinar los factores constantes y las variables de cambio dentro y fuera del ciberespacio. Los países tecnológicamente más avanzados han sido capaces de incrementar sus condiciones de respuestas ante las amenazas, pero también se han abierto oportunidades para que otros países desarrollen competencias en ciberseguridad y sean capaces de fortalecer su posición en

términos de ciberpoder. Esto permitiría incrementar su participación en un contexto donde las capacidades políticas y tecnológicas, y no solo la magnitud de los arsenales, pueden definir la importancia de cada actor en un entorno de conflicto global.

Referencias

Abott, A. (2025). *La competencia entre Estados Unidos y China en IA en el punto de mira*. Forbes. https://forbes.es/tecnologia/774352/la-competencia-entre-estados-unidos-y-china-en-ia-en-el-punto-de-mira/

Allison, G., Klyman, K., Barbesino, K., y Yen, H. (2021). *The great tech rivalry: China vs. US*. Harvard Kennedy School. Belfer Center for Science; International Affairs. https://www.belfercenter.org/sites/default/files/pantheon_files/GreatTechRivalry_ChinavsUS_211207.pdf

Betz, D., y Stevens, T. (2011). *Cyberspace and the State: Toward a Strategy for Cyber-Power*. Routledge.

Capgemini Research Institute. (2019). *Reinventing Cybersecurity with Artificial Intelligence: The new frontier in digital security*. https://www.capgemini.com/gb-en/wp-content/uploads/sites/5/2022/05/AI-in-Cybersecurity_Report_20190710_V05.pdf

Car, P., y Marcelin, T. (2024). *Artificial intelligence and cybersecurity*. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/762292/EPRS_ATA(2024)762292_EN.pdf

Centro Criptológico Nacional. (2023). *Nuevo informe de Buenas Prácticas BP/30 sobre aproximación a la Inteligencia Artificial y la ciberseguridad*. CCN-CERT. https://www.ccn-cert.cni.es/es/seguridad-al-dia/novedades-ccn-cert/12852-nuevo-informe-de-buenas-practicas-bp-30-sobre-aproximacion-a-la-inteligencia-artificial-y-la-ciberseguridad.html

Deutsche Welle. (2025). *China acusa a la NSA de EE. UU. de ciberataques*. DW. https://www.dw.com/es/china-acusa-a-la-nsa-de-ee-uu-de-ciberataques/a-72247876

Devanny, J. (2024). *Artificial intelligence and cyber power*. Research Publications, Florida International University. https://digitalcommons.fiu.edu/jgi_research/63/

Folorunso, A., Adewumi, T., Adewa, A., Okonkwo, R., y Olawumi, T. (2024). Impact of AI on cybersecurity and security compliance. *Global Journal of Engineering and Technology Advances*, *21*(1), 167-184. https://doi.org/10.30574/gjeta.2024.21.1.0193

González, F. (2025). *China vs. Estados Unidos: estos son todos los frentes de su batalla tecnológica*. Wired. https://es.wired.com/articulos/china-vs-estados-unidos-estos-son-todos-los-frentes-de-su-batalla-tecnologica

International Institute for Strategic Studies. (2021). *Cyber capabilities and national power: A net assessment*. iiss. https://www.iiss.org/research-paper/2021/06/cyber-capabilities-national-power/

International Telecommunication Union. (2024). *Global Cybersecurity Index 2024: 5th Edition*. ITU. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

Mahfuri, M., Ghwanmeh, S., Almajed, R., Alhasan, W., Salahat, M., Lee, J., y Ghazal, T. (2024). Transforming Cybersecurity in the Digital Era: The Power of AI. *2nd International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates*, 1-8. https://doi.org/10.1109/ICCR61006.2024.10533072

Nour, S., y Said, S. (2024). Harnessing the Power of AI for Effective Cybersecurity Defense. *6th International Conference on Computing and Informatics (ICCI), New Cairo - Cairo, Egypt*, 98-102. https://doi.org/10.1109/ICCI61671.2024.10485059

Nye, J. (2004). *Soft power: The means to success in world politics*. PublicAffairs.

Nye, J. (2011). *The future of power*. PublicAffairs.

Pestana, R. (2025). *Ciberseguridad: la próxima frontera de la competencia entre Estados Unidos y China en las Américas*. Americas Quarterly. https://www.americasquarterly.org/article/ciberseguridad-la-proxima-frontera-de-la-competencia-entre-estados-unidos-y-china-en-las-americas/

Roca, S. (2022). Las estrategias nacionales de inteligencia artificial de China y EEUU. En Y. Rondón (Ed.), *La Inteligencia artificial. Reflexiones sobre los desafíos de una tecnología divergente* (1.ª ed., pp. 23-44). CENDITEL. https://convite.cenditel.gob.ve/files/2022/11/Libro_Inteligencia_Artificial_2022.pdf

Roshanaei, M., Khan, M., y Sylvester, N. (2024). Enhancing cybersecurity through AI and ML: Strategies, challenges, and future directions. *Journal of Information Security*, (15), 320-339. https://doi.org/10.4236/jis.2024.153019

Spratt, F. (2024). *El ciberpoder: La carrera invisible entre China y Estados Unidos*. Centro de Estudios Estratégicos de Relaciones Internacionales. https://www.ceeriglobal.org/wp-content/uploads/2024/03/Informe-GI-PDF.pdf

Starr, S. (2009). The Virtual Battlefield: Perspectives on Cyber Warfare. En Center for Technology and National Security Policy (CTNSP) (Ed.), *Towards an evolving theory of cyberpower* (1.ª ed., pp. 18-52). National Defense University (NDU). https://doi.org/https://doi.org/10.3233/978-1-60750-060-5-18

Tang, J., Saade, T., y Kelly, S. (2024). *The implications of artificial intelligence in cybersecurity: Shifting the offense-defense balance*. Institute for Security y Technology. https://securityandtechnology.org/virtual-library/reports/the-implications-of-artificial-intelligence-in-cybersecurity/

Temara, S. (2024). Harnessing the power of artificial intelligence to enhance next-generation cybersecurity. *World Journal of Advanced Research and Reviews*, *23*(2), 797-811. https://doi.org/10.30574/wjarr.2024.23.2.2428

Triolo, P. (2024). A new era for the Chinese semiconductor industry: Beijing responds to export controls. *American Affairs Journal*, *1*(8), 797-811. https://americanaffairsjournal.org/2024/02/a-new-era-for-the-chinese-semiconductor-industry-beijing-responds-to-export-controls/

Unión Internacional de Telecomunicaciones. (2008). *Seguridad en el ciberespacio – Ciberseguridad: Aspectos generales de la ciberseguridad (Recomendación UIT-T X.1205). Sector de Normalización de las Telecomunicaciones de la UIT*. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-S&type=items

Van Haaster, J. (2016). Assessing Cyber Power. En N. Pissanidis, R. H. y V. M. (Eds.), *Cyber Power: Proceedings of the 8th International Conference on Cyber Conflict* (pp. 7-21). NATO CCD COE Publications. https://ccdcoe.org/uploads/2018/10/CyCon_2016_book.pdf

Voo, J., Hemani, I., y Cassidy, D. (2022). *National Cyber Power Index 2022*. Belfer Center for Science; International Affairs, Harvard Kennedy School. https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf

Yohsua, B., Daniel, P., Tamay, B., Rishi, B., Stephen, C., Yejin, C., Danielle, G., Hoda, H., Leila, K., Shayne, L., Vasilios, M., Mantas, M., Yee, N., Deborah, R., Theodora, S., Florian, T., y Soren, M. (2024). *International Scientific Report on the Safety of Advanced AI*. UK Government. https://hal.science/hal-04612963

Zambrano, A. (2024). Impacto de la inteligencia artificial en los ciberataques. *Revista Sinapsis*, *24*(1). https://revistas.itsup.edu.ec/index.php/sinapsis/article/view/895/2080

Ciberseguridad aplicada a los sistemas de control industrial: Caracterización, vulnerabilidades, estrategias y expectativas

Pablo Sulbarán [1]

Introducción

La Ciberseguridad, en primera instancia, es una disciplina cuyo ámbito se circunscribe a los activos digitales, los cuales incluyen datos, información, aplicaciones y sistemas operativos. No obstante, en el contexto del Control y Automatización de Procesos, los sistemas presentan una mayor interconexión de sus elementos debido a la incorporación de nuevas tecnologías, lo cual incrementa significativamente el procesamiento digital de las señales generadas en todas las etapas del proceso, siendo, por ende, susceptibles a amenazas provenientes del Ciberespacio. En este sentido, es importante comprender que los sistemas de control inicialmente fueron diseñados para operar en entornos aislados, con poca o ninguna interconexión, lo cual deriva en vulnerabilidades inherentes a las limitaciones de medidas de seguridad.

En este orden de ideas, los Sistemas de Control Automáticos (SCA) son infraestructuras basadas en procesos físicos que incorporan dos tipos de tecnologías a saber: Tecnologías de Información (TI) y Tecnologías de Operación (TO). Las TI involucran las plataformas de hardware, software, redes y bases de datos destinadas a la monitorización del sistema, enfocándose en la supervisión y toma de decisiones, mientras que las TO se refieren a los dispositivos a nivel de campo, es decir, transductores, controladores y los componentes asociados a los procesos físicos de la planta. Con el auge de la Cuarta Revolución Industrial, existe cada vez mayor convergencia entre las TI y TO dentro de los sistemas de control automáticos, dando lugar al enfoque de la Industria 4.0, cuyo basamento en tecnologías emergentes tales como el Internet de las Cosas (IoT), Internet Industrial de las Cosas (IIoT), Computación en la Nube (*Cloud Computing*) y la Inteligencia Artificial (IA) genera altísimos niveles de conectividad, conllevando a la introducción de sistemas más abiertos y de propósito general, y por ende, mayor exposición ante potenciales amenazas (Instituto Nacional de Ciberseguridad, 2015).

Los SCA de infraestructura crítica (o Sistemas de Control Industrial, SCI) son el blanco de ataque de ciberdelincuentes. Esta categoría abarca sectores de vital importancia, como la industria petrolera, la generación y distribución de energía eléctrica, el tratamiento de agua potable, la industria petroquímica, generación de energía nuclear telecomunicaciones, entre otros. Dichos ataques tienen objetivos malintencionados y ya se tienen precedentes

[1]Ingeniero de Sistemas egresado de la Universidad de Los Andes (ULA). Actualmente se desempeña como analista de desarrollo en el Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL). psulbaran@cenditel.gob.ve

de los mismos, por ejemplo en 2010 el ataque del gusano Stuxnet a centrales nucleares de Irán, el ciberataque a la red eléctrica de Ucrania en 2015, el ciberataque a los oleoductos de Colonial Pipeline, entre otros, constituyendo un desafío de gran magnitud en materia de Ciberseguridad.

El presente ensayo se enfoca en una revisión del estado del arte de la Ciberseguridad en los SCI, dividiéndose en dos grandes partes: la primera es una revisión de la literatura acerca de los fundamentos teóricos relacionados con SCA, seguido de una descripción de la arquitectura de los SCI, con el objeto de comprender su funcionamiento y así poder identificar los aspectos vulnerables inherentes al mismo; la segunda parte del ensayo es concerniente al tema de Ciberseguridad, donde se categoriza los vectores de ataque y los componentes del sistema de control afectados por los mismos, así mismo se enuncian las estrategias de protección adoptadas por la industria actual y reflexionar acerca de las expectativas a futuro de la Ciberseguridad en los SCI.

Sistemas de control

Un sistema de control es una interconexión de componentes físicos de diversa naturaleza (eléctricos, electrónicos, mecánicos, térmicos, etc.), cuyo propósito es generar una respuesta requerida (Dorf y Bishop, 2005). En tal sentido, se trata de una unidad funcional conformada por elementos o subsistemas de que ejecutan acciones para alcanzar un objetivo determinado, donde a su vez existen mecanismos de compensación que se encargan de ajustar las variables propias del proceso para obtener el resultado esperado; en otras palabras, aplica la noción de control. Por otra parte, los sistemas de control automáticos se caracterizan por funcionar con poca o ninguna intervención humana.

Partiendo de las ideas generales enunciadas en el apartado anterior, se muestran a continuación algunas definiciones fundamentales planteadas por Ogata (2003) para comprender el desempeño de un sistema de control automático:

- **Planta:** Es el equipo, dispositivo, maquinaria o sistema que se desea regular.
- **Variables:** Existen dos tipos de variables: variable controlada y variable manipulada. La primera se refiere a la magnitud que se quiere controlar, es la salida del sistema; y la segunda hace referencia al resto de elementos que se modifican para el alcance de los resultados deseados.
- **Proceso:** Es un conjunto de operaciones que conducen a un resultado, se rige de acuerdo a principios físicos o químicos, según sea el caso.
- **Control realimentado (lazo cerrado):** Es la operación que consiste en el ajuste de las variables del sistema para que el mismo logre su propósito, teniendo en cuenta un valor de referencia para la salida.
- **Control en lazo abierto:** A diferencia del anterior, los sistemas operan sin comparar la salida con una referencia.

- **Perturbaciones:** Son las señales de entrada no deseadas del sistema que perjudican el normal desenvolvimiento del mismo

En cuanto a su estructura, un sistema de control automático se conforma de la siguiente manera:

- **Planta:** Es el sistema en cuestión que se va a controlar. En este sentido también se puede hacer referencia al proceso cuya respuesta se quiere ajustar a un valor determinado.
- **Actuadores:** Es un tipo de transductor que recibe una señal proveniente del elemento de control y la transforma en una acción mecánica de forma directa sobre la planta. Su principio se basa en la conversión de energía, es por ello que existen varios tipos según su fuente: eléctricos, neumáticos, térmicos, hidráulicos, electromecánicos, entre otros.
- **Sensores:** Es el dispositivo que mide una magnitud física del proceso y luego la convierte en una señal eléctrica que será recibida por el elemento de control y así completar el lazo de realimentación. En el ámbito de la industria, las magnitudes o variables físicas medidas por los sensores son nivel, presión, flujo y temperatura.
- **Controladores:** Es el "cerebro" del sistema de control. Es el dispositivo que compara el valor de la respuesta del sistema con el valor de referencia o consigna. Un controlador obtiene a cada instante una señal de error, que consiste en la diferencia entre el valor de la variable de salida del sistema y la referencia; el cual se debe minimizar mediante el envío de una señal llamada acción de control. Controlar significa medir el valor de la variable controlada del sistema y ajustar la variable manipulada al sistema para compensar la desviación del valor medido respecto del valor deseado (Ogata, 2003), como lo muestra el diagrama de bloques de la Figura 1.

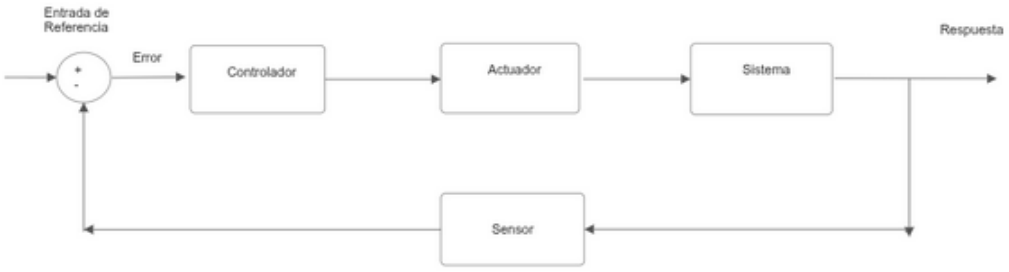

Figura 1: Diagrama de bloques de un sistema de control automático con realimentación.
Fuente: Elaboración propia (2025).

La función de un controlador en un sistema de control automático es emitir una señal a los actuadores de acuerdo al valor del error obtenido. En los sistemas de control se tienen dos tipos de controladores, clasificados en función del tipo de señal que manejan: controladores analógicos y controladores digitales. Los controladores analógicos son aquellos que manejan señales continuas y las mismas fluctúan en rango de valores determinado (Monilithic

Power Systems, 2025); su composición se basa en elementos eléctricos y electrónicos como resistencias, condensadores, potenciómetros y amplificadores operacionales; el uso de este tipo de componentes es cada vez más reducido debido al evidente avance de la tecnología digital asociada a la automatización. Por su parte, los controladores digitales se basan en la conversión analógico-digital de las señales, el procesamiento se realiza a través de un microprocesador, cuya base de funcionamiento son algoritmos que convierten las señales analógicas en valores numéricos que están en sintonización con los parámetros asociados a las variables del proceso a regular.

En virtud de la anterior definición de controlador digital, la implementación de estos han potenciado los sistemas modernos con una serie de ventajas tales como la disposición de múltiples controladores conectados en redes, el acoplamiento de sensores, transductores, actuadores y otros dispositivos de planta a dichos controladores mediante el sistema de buses de campo, en conjunto con la instalación de plataformas de hardware y software, garantizando altos niveles de optimización y seguridad del control del proceso.

SCI

Los Sistemas de Control Industrial (SCI) comprenden una gama de tecnologías asociadas al control automático de procesos, a menudo encontradas en todos los sectores industriales y de infraestructura crítica (Cossio, 2020). Este tipo de sistemas engloban las infraestructuras críticas y constituyen la base de los procesos industriales de alta complejidad, como generación y distribución de energía, refinerías, siderúrgicas, columnas de destilación, manufacturas a gran escala, entre otros, caracterizándose por la alta cantidad de subsistemas que se deben regular con el fin de garantizar el resultado final de manera óptima. En este sentido, las variables físicas que se controlan en los SCI con mayor frecuencia son: nivel, presión, temperatura y flujo. Los SCI están conformados por sensores, hardware y software cuya interacción se basa en la ejecución de bucles de control, diagnósticos remotos, herramientas de mantenimiento e interfaces humanas basadas en arquitecturas de red dispuestas en capas siguiendo diversos protocolos (Nankya et al., 2023). Estos dispositivos se conectan mediante redes, bien sea de forma cableada o inalámbrica según la tecnología que se esté implementando.

En la Figura 2 se observa un diagrama de bloques del bucle de control de un SCI, el cual representa los elementos fundamentales que intervienen en un sistema físico determinado y la interacción entre ellos a través de la transmisión de señales emitidas desde los sensores de la planta y las interfaces hombre-máquina hasta el controlador, el cual a su vez genera señales hacia los actuadores que finalmente intervienen en el proceso en cuestión. En el diagrama se muestra también un conjunto de señales adicionales denominadas perturbaciones, las cuales afectan el normal desempeño del sistema a controlar.

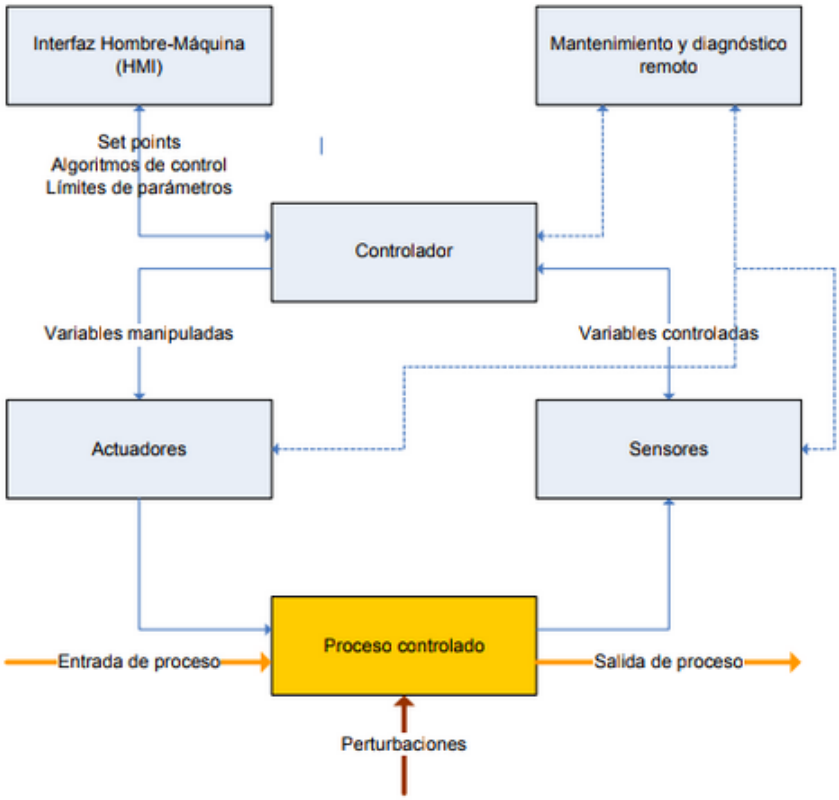

Figura 2: Lazo de control de un SCI.
Fuente: Cossio (2020).

Los SCI están estructurados de la siguiente manera:

- Controlador Lógico Programable (*Programmable Logic Controller*, PLC).
- Control Supervisor y Adquisición de Datos (*Supervisory Control And Data Acquisition*, SCADA).
- Unidades de Terminal Remota (*Remote Terminal Unit*, RTU).
- Interfaces Humano-Máquina (*Human-Machine Interface*, HMI).
- Sistemas de Control Distribuidos (SCD).
- Buses de campo.

PLC

Un PLC es un dispositivo utilizado en la industria para controlar y automatizar procesos. Está diseñado para gestionar operaciones en tiempo real y puede programarse para realizar tareas específicas, como encender y apagar motores, monitorear sensores y automatizar líneas de producción (Siemens PLC Guides, 2025). Es un computador caracterizado por su robustez para funcionar en condiciones difíciles en planta tales como impactos y vibraciones,

además que tiene la capacidad de operar en un amplio rango de temperatura, de allí que su instalación se hace directamente a nivel de campo. Además, destaca su flexibilidad para adaptarse ante cualquier proceso que implique su control automático, programándose según sean los requerimientos de la planta en el momento, con la ventaja adicional de acoplarse a cualquier otra plataforma destinada al control automático de procesos. La programación de los PLC se rigen por el estándar IEC 61131.

La arquitectura de un PLC es la siguiente:

- Unidad Central de Procesamiento (CPU): Es el encargado de ejecutar las instrucciones almacenadas en memoria mediante operaciones aritméticas y lógicas. Se relaciona con los módulos de entrada y salida.
- Módulos de entrada: Recibe las señales del entorno físico, las mismas provienen de sensores y se convierten en señales digitales para ser dirigidas al CPU.
- Módulos de salida: Reciben señales de control digitales provenientes del CPU para luego ser emitidas a los actuadores que intervienen en la planta.
- Fuente de alimentación: Distribuye energía a todos los componentes del PLC.
- Interfaces de comunicación: Son puertos a través de los cuales el PLC se comunica con otros plataformas de control como interfaces hombre-máquina (HMI), sistemas SCADA, computadoras para su programación u otros PLC, siguiendo protocolos de comunicación.

El funcionamiento de un PLC se basa en un bucle de monitorización de señales, denominado también escaneo, que inicia con la lectura del estado de los dispositivos de entrada, seguidamente se ejecuta la ley de control programada para el proceso en cuestión y culmina con la emisión de la señal de control que es recibida por los elementos de salida. El ciclo se ejecuta en forma permanente e instantánea con el objeto de mantener los valores deseados de las variables controladas del proceso. Evidentemente, durante todo el proceso de operación de un PLC existe un intercambio de datos con el resto de elementos del sistema de control, por ende se establecen protocolos de comunicación cuya función es determinar tipo de conexiones, formatos de datos, velocidad de transmisión y manejo general de errores. En la Figura 3 se muestra un modelo de PLC presente en el mercado:

Figura 3: PLC modelo SIMATIC S7-1200 de Siemens.
Fuente: Siemens (2025).

RTU

Son dispositivos de control basados en microprocesadores, operan a nivel de planta. Se conectan de manera directa a los elementos de campo tales como sensores, actuadores e interruptores. Se diferencian de los PLC por el hecho de que son diseñados para operar a grandes distancias, de allí que se basan en el principio de la telemetría. Otra diferencia respecto a los PLC, es que éstos últimos requieren el conocimiento de la programación basada en lógica de escalera, en cambio las RTU se pueden programar a través de una interfaz de navegador web simple. Las RTU están diseñadas para funcionar en entornos industriales bastante exigentes, por ejemplo altos niveles de humedad, polvo y rangos de temperatura muy elevados. Son compatibles con protocolos de comunicación industrial comunes como Modbus, Profibus y DNP3. Además, pueden utilizar tecnologías de comunicación Ethernet, serie (como RS-232 y RS-485) e inalámbricas (Mikrodev, 2025).

La arquitectura de una RTU está estructurada de la siguiente manera: módulo de entrada, encargado de recibir datos de los elementos de campo; módulo de control, cuya función es el registro, recepción y transmisión de los comandos de control recibido desde la unidad maestra o sistema supervisorio; módulo de procesamiento de información (CPU), el cual contiene una serie de registros asociados a los datos adquiridos en campo o emitidos desde la unidad maestra; y finalmente el módulo de comunicaciones, que se encarga de codificar, decodificar y transmitir la información procesada en el control. La RTU realiza un monitoreo constante de las variables controladas y, a través de un módulo de comunicación permite el intercambio de la información capturada con la sala de control central, utilizando diversos medios de comunicación: línea telefónica, UHF / VHF, microondas, satélite, fibra óptica u otro medio, a través de puertos auxiliares con otras unidades remotas. A continuación, en la Figura 4 se tiene una RTU de uso frecuente en la industria:

Figura 4: RTU.
Fuente: Mikrodev (2025).

SCADA

Durante el Comité de 5 de Mayo del 2017, señala Nasby (2019, p. 10), que la International Society of Automation, definió SCADA como un sistema definido como una combinación de hardware y software utilizado para enviar comandos y adquirir datos con el fin de supervisar y controlar sistemas.

Se trata de una arquitectura de hardware y software que se encarga de monitorear procesos con el fin de aplicar el control automático del mismo mediante la adquisición de datos en tiempo real. Generalmente los sistemas SCADA se instalan en una sala de control donde se supervisa el proceso industrial de manera remota, donde cada uno de los componentes del sistema a controlar están ubicados a grandes distancias. Es importante resaltar que los SCADA se encuentran en un nivel superior en la pirámide de automatización, por encima de los PLC y las RTU, debido a que estos se encuentran directamente en campo conectados a los actuadores y sensores de la planta.

La arquitectura de un sistema SCADA viene dada por capas, las cuales se describen a continuación:

- En la primera capa se tienen los dispositivos de campo, tales como sensores y actuadores. Los sensores monitorizan variables a controlar como la temperatura, la presión o el caudal, mientras que los actuadores ajustan equipos como válvulas, bombas o servomotores, los cuales intervienen en las variables manipuladas. Estos dispositivos proporcionan datos en tiempo real y ejecutan acciones directas en los elementos de la planta para mantener los procesos operativos.
- En la siguiente capa se tienen los PLC (ya definidos en el apartado anterior) y las RTU; estos dispositivos obtienen datos de los sensores, los procesan y aplican el control según

las instrucciones programadas, por ejemplo, si un sensor de presión detecta un aumento de presión, el PLC puede activar una válvula disminuir el valor.

- Seguidamente se tiene la capa de comunicación; los datos son transmitidos entre los PLC/RTU y el computador SCADA; dichas redes pueden ser cableadas (en serie o basadas en Ethernet) o inalámbricas (como radio o satélite), dependiendo de la distancia y la ubicación de los dispositivos.

- Finalmente, en la capa superior se encuentra el servidor o estación maestra SCADA, base del sistema. Este computador recopila datos de campo, los almacena y los presenta a través de la HMI. Los operadores utilizan la HMI para supervisar el rendimiento del sistema controlado, realizar ajustes en la configuración o responder a las alertas. Este diseño en capas mantiene las tareas críticas (como detener una bomba ante picos de presión) bajo control de los PLC y las RTU, mientras que el servidor SCADA se centra en la monitorización y el análisis de datos de todo el sistema controlado. Esta estructura ha demostrado un desempeño eficiente en sistemas de control automáticos de cualquier escala y complejidad. La Figura 5 ilustra la arquitectura de un sistema SCADA:

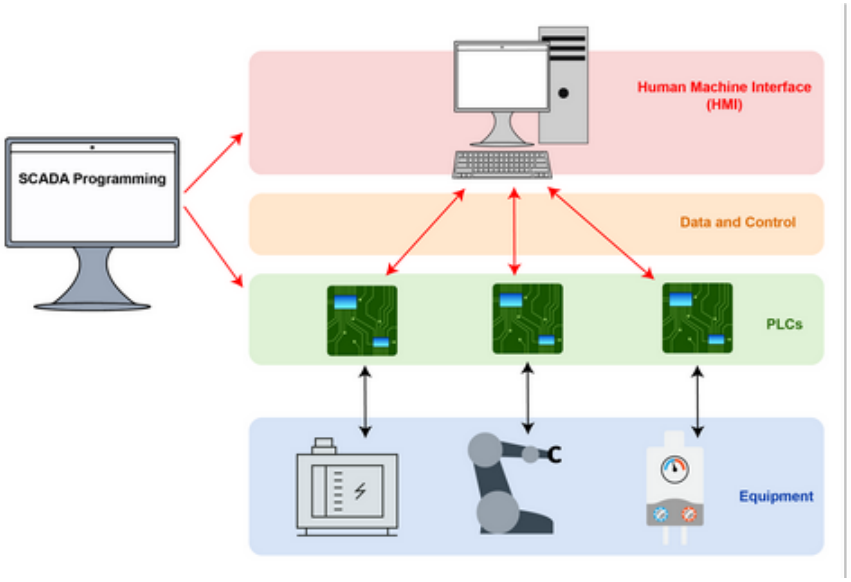

Figura 5: Esquema de un sistema SCADA.
Fuente: Digital Prototype Systems Inc. (2022).

HMI

Una interfaz hombre-máquina (IHM) es una plataforma de hardware y software que conecta a un usuario con una dispositivo, planta o sistema. El término engloba ampliamente cualquier dispositivo que permita a un usuario interactuar con un SCI (Pro-face, 2025). La Interfaz Hombre-Máquina (HMI) actúa como el centro de operaciones entre el operador y sistema de control automático, utilizando diversas formas de interacción para la supervisión y el control. La HMI facilita la interacción humana a través de tres sentidos principales:

- Control Táctil: Permite al operador ingresar datos e instrucciones utilizando elementos físicos tales como botones, teclados pantallas táctiles y paneles numéricos.
- Visualización (Visión): Se muestra la información sobre el estado actual del proceso mediante el monitoreo por pantalla, el uso de gráficos y el uso de indicadores externos como torres de iluminación.
- Alertas sonoras (Audición): Consiste en la emisión de sonidos como alarmas para informar al operador sobre eventos, fallos o condiciones de planta que requieren atención inmediata.

El dispositivo HMI industrial permite el monitoreo y control directo del sistema, mediante la interconexión de un controlador como PLC o una RTU, permitiendo funciones cruciales como:

- Ajuste de parámetros: Permite ajustar la configuración y puntos de operación del sistema.
- Control y mando: Facilita la ejecución de comandos para operar los equipos (iniciar, pausar, detener, entre otros).
- Supervisión continua: Muestra el estado actual del proceso en tiempo real.
- Registro histórico: Almacena datos recopilados en el tiempo para la realización de análisis pertinente para la optimización de planta.
- Puerta de enlace inteligente (*Gateway*): Actúa como un punto de acceso para la gestión e intercambio de datos entre los equipos de campo y los sistemas de nivel superior.

DCS

Un sistema de control distribuido (DCS) es un SCI digital y automatizado que utiliza lazos de control distribuidos geográficamente en una máquina, industria o área de control (Gillis, 2025). Básicamente, su arquitectura consiste en una capa de control supervisorio general y una capa compuesta de subsistemas de control de procesos ubicados en un entorno espacial específico. El nivel superior funciona aplicando un lazo de control general que regula cada uno de los bucles específicos asociados a cada subsistema, aplicando un esquema modular que produce la ventaja de minimizar el impacto de las fallas a nivel macro. En tal sentido, el controlador centralizado participa activamente en el lazo maestro de control, realizando tareas de corrección automática y manteniendo los puntos de funcionamiento de los lazos de menor jerarquía a través de un ajuste de una variable de error (Cossio, 2020).

Un DCS opera basándose en el estado del proceso, es decir que monitorea y registra continuamente todas las variables críticas del proceso en tiempo real, permitiendo mantener un modelo virtual o una abstracción digital que refleja con precisión el estado físico actual del proceso en todo momento. Por otra parte, un DCS puede estar estructurado por lazos de control intermedios entre el bucle supervisorio y los subsistemas que componen el sistema de

control general, manteniendo el criterio de funcionamiento en un espacio limitado. La Figura 6 representa la estructura de un DCS:

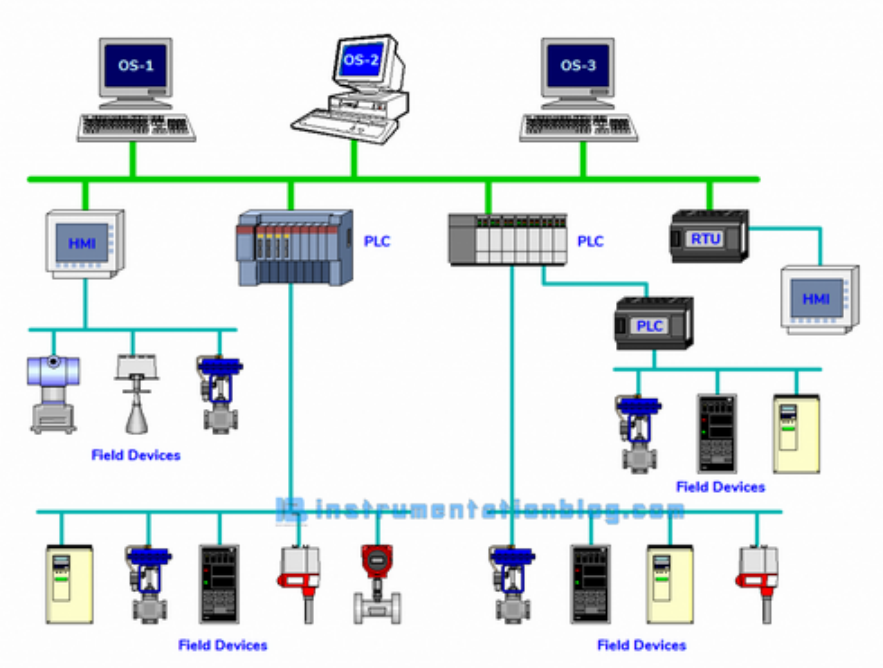

Figura 6: Esquema de un DCS.
Fuente: InstrumentationBlog (2025).

Bus de datos

Son sistemas de comunicación digital que permiten la comunicación entre los dispositivos de control en campo con los dispositivos de monitoreo y supervisión de un sistema de control automático. Se caracterizan por transmitir paquetes de datos en forma de mensajes digitales siguiendo una estructura definida mediante una única línea de comunicación, derivando en la bidireccionalidad de los datos; por su arquitectura descentralizada se garantiza un diagnóstico completo de los elementos de planta y su gestión de manera remota. Los buses de campo se rigen por protocolos de comunicación y presentan las siguientes ventajas:

- Reducción de cableado debido al carácter bidireccional
- Velocidad en el diagnóstico del estado del sistema
- Flexibilidad y escalabilidad
- Comunicación en tiempo real
- Estandarización mediante protocolos siguiendo las normas establecidas en el ámbito del control y automatización industrial.

Protocolos de comunicación de los SCI

Los protocolos de comunicación de los SCI son un conjunto de estándares que permiten establecer el intercambio de datos con el resto de elementos del sistema a controlar, garantizando la interacción eficaz con los mismos en tiempo real. A continuación, se muestran los protocolos de SCI más utilizados en la industria:

Modbus

Desarrollado a finales de la década de 1970 por la empresa Modicon, ahora Schneider Electric, es uno de los protocolos más utilizados en el contexto de los sistemas de control automáticos. Es una forma de comunicación de solicitud-respuesta basado en el esquema de relación maestro-esclavo. Una relación maestro-esclavo consiste en un tipo de comunicación basado en pares: un dispositivo debe iniciar una solicitud y esperar una respuesta, y el dispositivo iniciador (el maestro) es responsable de iniciar cada interacción (National Instruments, 2025). Es un estándar abierto, no propietario, lo cual hace que sea de amplia implementación en la industria.

En términos de capa física, Modbus opera de dos formas diferenciadas: Modbus RTU y Modbus TPC/IP. Modbus RTU es un protocolo basado en conexiones en serie, lo cual permite una integración eficaz con el resto de dispositivos involucrados en el control de la planta tales como los sensores y actuadores; en cuanto a la estructura de la trama[2] se compone de un campo de dirección, código de función, campo de datos y suma de comprobación (Sharma, 2025). Por su parte, Modbus TPC/IP se fundamenta en el Protocolo de Control y Transmisión (*Transmission Control Protocol*, TPC) y el Protocolo de Internet (*Internet Protocol*, IP), lo cual implica la transmisión de los datos a través de redes Ethernet; su esquema de comunicación consiste en una arquitectura cliente-servidor; su trama consta de dos partes: el encabezado del Protocolo de Aplicación Modbus (MBAP) y la Unidad de Datos del Protocolo (Waseem, 2025); su principal ventaja es la capacidad de operación en entornos complejos, mayor velocidad y escalabilidad.

PROFINET

PROFINET (*Process Field Network*) es un estándar de comunicación basado en Ethernet industrial, a diferencia de Modbus TCP/IP que consiste en Ethernet convencional. PROFINET funciona en un entorno determinístico y con un amplio espectro de aplicación. El bus de campo utiliza estándares TCP/IP e IT, funciona en tiempo real y permite la integración de sistemas de bus de campo (Burkert, 2025). Desarrollado por Siemens y PROFIBUS, PROFINET se ha convertido en un sistema de comunicación en la industria debido a su cumplimiento con el estándar IEEE 802 con la implementación de las normas IEC 61158 e IEC 61784. La naturaleza abierta de la plataforma PROFINET posibilita la incorporación eficiente de soluciones de bus de campo heredadas mediante el empleo de dispositivos *proxy* y *gateway*. Asimismo, PROFINET incorpora funcionalidades de

[2]Trama: En el ámbito de los protocolos, una trama es un paquete estructurado de datos que constituye un mensaje a ser transmitido.

diagnóstico exhaustivas para redes industriales. Específicamente, la transmisión de datos acíclicos suministra inteligencia crucial sobre la condición de los componentes y las comunicaciones PROFINET, permitiendo una representación topológica de la red que resulta altamente comprensible.

Una de las fortalezas de PROFINET es su escalabilidad en tiempo real, destacando su capacidad de transmisión de datos a velocidades extremadamente rápidas en comparación con otros estándares, de hasta 1 µs (Sokacheske, 2025). Además, consta de una única infraestructura de cableado para conectar dispositivos, permitiendo el intercambio de datos con servidores y la nube de forma eficiente, facilitando así su integración en los entornos de la Industria 4.0. A nivel de topologías de red es flexible, incorporando configuraciones tales como anillo y/o estrella. Por otra parte, este protocolo puede ser adaptable a diversas aplicaciones e inclusive acoplarse a tecnologías inalámbricas y Bluetooth. PROFINET también se caracteriza por una mayor disponibilidad del sistema mediante recursos de respuesta automática redundantes, donde se pueden programar acciones según el diagnóstico de los dispositivos de campo (Sokacheske, 2025).

DeviceNet

Es un protocolo que se implementa a nivel de campo en la planta, es decir interconecta PLC con actuadores y sensores a través de una capa de medios CAN (*Controller Area Network*). Las principales aplicaciones del protocolo DeviceNet incluyen dispositivos de seguridad, intercambio de datos y grandes redes de control de Entrada/Salida (ElProCus, 2025). Su arquitectura consiste en la conexión directamente numerosos dispositivos industriales tales como sensores, interruptores, luces y controladores de motor en red. Al eliminar el cableado punto a punto, se reduce la complejidad y el costo. Esta conectividad directa no solo mejora la comunicación, sino que también permite realizar diagnósticos detallados a nivel de cada dispositivo, algo imposible con interfaces de E/S cableadas tradicionales. Es un sistema que puede ser configurado para operar tanto en una arquitectura maestro-esclavo cuanto en una arquitectura distribuida punto a punto. Además de eso, define dos tipos de mensajes, I/O (datos de proceso) y explicit (configuración y parametrización). Posee también mecanismos de detección de dirección dobles y aislamiento de los nudos en caso de fallas críticas.

Ethernet/IP

Es un protocolo de comunicación abierto desarrollado con base al Protocolo Industrial Común (CIP). EtherNet/IP se basa en el estándar TCP/IP y se rige por los estándares IEEE Ethernet y ofrece a los usuarios un conjunto de velocidades de interfaces de red que van desde 10, 100 Mbps y 1 Gbps (Sokacheske, 2025). Este protocolo utiliza estándares Ethernet tradicionales, incluidos el Protocolo de Control de Transporte (TCP), el Protocolo de Internet (IP) y las tecnologías de señalización y acceso a medios que se encuentran en todas las interfaces de red Ethernet, por ende, es compatible y funciona adecuadamente con los demás dispositivos Ethernet estándar existentes en el mercado. En este sentido, es

un tipo de red adaptable a cualquier aplicación y también se puede utilizar en tecnologías inalámbricas y Bluetooth.

La ciberseguridad

La Ciberseguridad se refiere al conjunto de métodos, procedimientos y tecnologías que tienen por objeto la protección de los datos de los sistemas digitales, garantizando la integridad, confidencialidad y disponibilidad; se busca el resguardo de los datos y en general de la infraestructura del sistema en cuestión. A continuación, se citan algunas definiciones realizadas por empresas especializadas en este campo de estudio:

- La Ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Estos ciberataques suelen tener como objetivo acceder, modificar o destruir información confidencial; extorsionar a los usuarios mediante ransomware; o interrumpir los procesos comerciales normales (Cisco Systems, Inc., 2025).
- Por su parte, AO Kaspersky Lab. (2025) define la Ciberseguridad como la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos.
- Huawei Technologies Co., Ltd. (2023) enuncia que el objetivo principal de la Ciberseguridad es proteger activos como redes, computadoras, dispositivos móviles, aplicaciones y datos contra ciberataques para prevenir problemas de seguridad como fugas de datos e interrupciones del servicio.

En primera instancia, la Ciberseguridad es aplicada exclusivamente a las Tecnologías de Información (TI), en el ámbito netamente informático. No obstante, los SCI también son susceptibles a amenazas provenientes del Ciberespacio debido su carácter digitalizado e interconectado de su infraestructura, a pesar que, en principio, no fueron diseñados para enfrentar ese tipo de peligros, sus medidas de seguridad definidas fueron limitadas. El riesgo en los entornos de SCI implica amenazas que afectan la seguridad operativa (seguridad física de bienes, equipos y personas, impacto medioambiental) y la integridad física de las herramientas de producción (Cisco Systems, Inc., 2025). En tal sentido es de crucial importancia establecer un enfoque de Ciberseguridad Industrial que priorice la integridad del sistema de control con criterios de confidencialidad, ya que la interrupción o manipulación de un proceso en un SCI automatizado puede tener consecuencias directas en la infraestructura física y, a diferencia de las pérdidas principalmente de datos en el ámbito tradicional de TI.

Antecedentes de ciberataques a SCI

Los ataques a las infraestructuras críticas se han llevado a cabo a partir de la segunda década del siglo XXI. A continuación, Dreamlab Technologies (2025) realiza un esbozo de algunos ciberataques realizados a SCI:

Stuxnet (Natanz, Irán, 2010)

El gusano Stuxnet de 2010 marcó un punto de inflexión en la ciberseguridad industrial, siendo el primer vector de ataque capaz de causar daños físicos directos al infiltrarse en la planta de enriquecimiento de uranio de Natanz. Ese malware incursiona a través de la HMI y se propaga mediante dispositivos USB, dirigiéndose directamente a los PLC de Siemens, forzando a las centrifugadoras a operar a velocidades anormales hasta su destrucción, logrando así retrasar significativamente el programa nuclear iraní y demostrando el poder destructivo de un ataque enfocado en la TO.

BlackEnergy (Ucrania, 2015)

El ataque BlackEnergy en 2015 evidenció la vulnerabilidad de los servicios públicos básicos al dejar a más de 230.000 ucranianos sin electricidad durante el invierno. El asalto se ejecutó luego de una campaña de phishing dirigida a operadores, quienes instalaron el malware al abrir documentos adjuntos, lo que otorgó a los atacantes control remoto sobre los sistemas de distribución de energía; este incidente determinó que la falta de segmentación de red y la obsolescencia de los sistemas SCI eran fallas críticas que permitieron el desastre físico.

NotPetya (Ucrania y resto del mundo, 2017)

En 2017, el malware NotPetya demostró la magnitud de un ataque para saltar de un enfoque destructivo a nivel local a uno con consecuencias globales, actuando inicialmente como ransomware. Su rápida propagación se debió a la explotación de la vulnerabilidad EternalBlue en Windows, activada a través de una actualización maliciosa del software contable ucraniano MeDoc, lo cual permitió al código cifrar y, en esencia, destruir datos en redes corporativas fuera de Ucrania, forzando a empresas en diversos sectores a asumir pérdidas millonarias y destacando la urgencia de aplicar parches de seguridad de forma inmediata.

Colonial Pipeline (Estados Unidos, 2021)

El incidente de Colonial Pipeline en 2021 evidenció la fragilidad de la infraestructura crítica estadounidense ante el ransomware, al paralizar una de las redes de distribución de combustible del país y provocar escasez en la costa este. La seguridad se vulneró cuando el grupo de ramsonware DarkSide utilizó credenciales robadas de una cuenta VPN sin protección de autenticación para acceder a la red de TI de la empresa, obligándola a detener las operaciones del oleoducto para contener el cifrado. Este evento resaltó la prioridad de blindar los accesos remotos y segmentar las redes operacionales.

Ciber Kill Chain

Es un concepto que caracteriza la estructura de un intento de intrusión complejo, muy frecuente en los nuevos tipos de ciberataques en SCI (Cisco Systems, Inc., 2025). En este

contexto, se presupone que el ciberdelincuente ha logrado establecer una presencia en la red, superando con éxito las etapas iniciales de la cadena de ataque, que incluyen:

- **Reconocimiento:** Recolección de información técnica y operacional de la organización objetivo. Esto abarca la investigación de publicaciones, licitaciones y el análisis de la presencia humana a través de redes sociales para obtener datos de utilidad para el ataque.
- **Militarización**[3] **y entrega:** Creación y distribución del malware específico. Esto se logra mediante la entrega del código malicioso (por ejemplo, archivos PDF o MS Office infectados, o malware oculto en sitios web comprometidos [water hole]) a través de la web o correo electrónico.
- **Instalación:** Fase en la que el malware se establece en la red, ya sea a través de un movimiento lateral desde la red corporativa hasta el punto de interconexión con la red industrial, o mediante la inserción directa en la red de control, afectando especialmente a las estaciones de ingeniería del proceso.

Por ende, el foco del análisis se sitúa en los siguientes pasos de la intrusión: operaciones, mando y control, y acciones sobre objetivos. Se asume que el atacante ya está çonectado.[a] la red de control industrial, ya sea a través de un programa malicioso activo en una estación industrial o por un acceso físico exitoso.

Vulnerabilidades de los SCI

Los ataques remotos son el punto de partida de los ciberdelincuentes para realizar la intrusión al SCI. Los atacantes aprovechan vulnerabilidades conocidas en implementaciones de protocolos específicos, utilizando *scripts* (programas) ya predefinidos, lo que simplifica el proceso de ataque. En este contexto, cuando detectan flujo de información no cifrado, los atacantes pueden capturan información valiosa sobre la planta, lo que les permite intensificar el ataque y, finalmente, obtener el control del dispositivo de control objetivo. De hecho, los atacantes que se dirigen a sistemas de control industrial se basan en la explotación de una o más vulnerabilidades existentes (Nankya et al., 2023). Los componentes de infraestructura de SCI que pueden ser atacados son especificados por Nankya et al. (2023) en los siguientes apartados:

Vulnerabilidades de arquitectura y diseño

Las deficiencias en la arquitectura y el diseño general del sistema son aprovechadas por factores maliciosos para lograr el acceso no autorizado a la plataforma y así poder alterar los procesos de control a su voluntad. La seguridad en los SCI debe ser una prioridad desde las fases iniciales de la arquitectura y el diseño, integrándose como un componente fundamental en la estructura de la planta. Es importante señalar que la

[3]Militarización es el proceso en el que el ciberatacante combina los hallazgos de la fase de reconocimiento con herramientas de ataque para crear un empaquetado con fines maliciosos.

infraestructura de red de los SCI ha evolucionado adaptándose a las nuevos enfoques operativos y de producción, no obstante el diseño original de su arquitectura carecía de las consideraciones de seguridad adecuadas, al menos en el contexto de las tecnologías actuales y emergentes. Este enfoque de diseño realizado sin evaluar exhaustivamente ciertos elementos de seguridad, ha generado un conjunto de vulnerabilidades no previstas en la infraestructura.

Por otra parte, la ausencia de un perímetro de seguridad (o delimitación) claramente definido que separe los dispositivos críticos del SCI (como PLCs, RTU, SCADA y HMI) del entorno exterior, incluyendo la red corporativa de TI, compromete las medidas de protección básicas, por ende aumenta el riesgo de intrusiones a los sistemas y datos. Esta vulnerabilidad se complica con la recopilación inadecuada del historial de eventos de la planta, lo cual es crucial para cualquier análisis posterior. Sin una recolección de datos exhaustiva y precisa, resulta difícil o incluso imposible detectar la causa raíz de un evento de seguridad, permitiendo que las intrusiones o ataques pasen desapercibidos y causen daños irreversibles.

Vulnerabilidades de configuración y mantenimiento

Una vulnerabilidad crítica en las plataformas es el uso de sistemas operativos y software de aplicación privativos y obsoletos, debido a que ya no reciben soporte técnico ni actualizaciones de seguridad por parte de las empresas desarrolladoras de los mismos, en consecuencia los sistemas quedan expuestos a amenazas recientes e incluso desconocidas. Aunque existan parches de seguridad, su desempeño para entornos de SCI suele ser insuficiente debido a la necesidad de realizar pruebas de regresión exhaustivas y costosas al momento de su implementación.

En cuanto al aspecto de la seguridad, la misma se ve afectada por una gestión deficiente de las credenciales y el acceso al SCI. Por ejemplo, si las contraseñas de acceso para alguna interfaz no se generan, utilizan o protegen de forma coherente con las medidas de seguridad pertinentes, aumentan los riesgos de manera exponencial. De igual forma, los controles de acceso insuficientes o erróneos pueden otorgar privilegios excesivos o restringidos inadecuadamente al personal, produciéndose un desajuste en los roles. Un riesgo adicional lo constituye la información confidencial (contraseñas, por ejemplo) almacenada sin cifrar en dispositivos externos (móviles, unidades USB, etc), lo cual pone constituye un peligro para el sistema en caso que estos dispositivos sean robados o estén en poder de personas con propósito de perjudicar. Finalmente, el acceso remoto, necesario para mantenimiento o soporte técnico, debe someterse a un control estricto para prevenir el acceso no autorizado a los componentes del SCI.

El hardware de los SCI enfrenta un doble riesgo: amenazas físicas directas y peligros ambientales. Por un lado, el acceso físico no autorizado al equipo puede derivar en el robo o la destrucción de datos y componentes, la desconexión de enlaces de datos críticos y alteraciones malintencionadas del entorno operativo, incluyendo la adición de recursos no autorizados o la intercepción de información mediante el registro de pulsaciones de teclas. Existe un tipo de vulnerabilidad del hardware relacionada con factores ambientales, esto

se debe a fenómenos como la interferencia por radiofrecuencia, el pulso electromagnético (PEM), las descargas estáticas, y las fluctuaciones de energía (caídas o picos de tensión). Estos eventos pueden causar desde interrupciones temporales en el mando y control hasta daños irreversibles en las placas de circuitos.

Vulnerabilidades en el desarrollo de software

Los SCI presentan importantes fallos de seguridad derivados de un desarrollo de software deficiente, destacando principalmente la validación de datos inadecuada. Cuando el software del SCI no verifica eficazmente los datos de entrada o del usuario, se abren puertas a serias vulnerabilidades como desbordamientos de búfer, inyecciones de comandos, secuencias de comandos entre sitios (XSS) y recorridos de directorios. Paralelamente, la seguridad se ve comprometida cuando las funciones de seguridad que vienen instaladas con el producto permanecen inactivas en su configuración predeterminada. Estas características protectoras son completamente ineficaces a menos que los usuarios o administradores las activen de forma intencional o, por lo menos, reconozcan y manejen activamente su estado de desactivación.

Vulnerabilidades de comunicación y red en SCI

La seguridad de las redes de los SCI está comprometida por la falta de controles esenciales y visibilidad. Existe una debilidad crítica en la gestión del flujo de datos, ya que la ausencia de controles impide regular la transferencia de información según sus atributos. Esta situación se agrava por los registros inadecuados de firewalls y enrutadores, lo que hace casi imposible la identificación forense de la causa de ciberataque. En la primera línea de defensa, los cortafuegos a menudo están ausentes o mal configurados, permitiendo el flujo libre de datos entre las redes de control y las corporativas, lo que se convierte en un vector de propagación de malware y acceso no autorizado. Además, en los entornos inalámbricos, la insuficiente autenticación mutua entre clientes y puntos de acceso crea un riesgo latente de conexión a redes o dispositivos maliciosos.

El segundo grupo de vulnerabilidades se centra en las deficiencias de autenticación y cifrado en los protocolos. El riesgo más grave proviene de la utilización de protocolos estándar que transmiten datos en texto plano sin cifrado (como Telnet), lo que permite a los adversarios interceptar credenciales y comandos para ejecutar ataques de intermediario o secuestro de sesiones. Complementando esta falla, la autenticación de usuarios, datos o dispositivos es inadecuada o inexistente en muchos protocolos SCI, permitiendo la suplantación de identidad y ataques de repetición. Finalmente, la mayoría de los protocolos carecen de verificación de la integridad de las comunicaciones, lo que permite la manipulación de datos sin ser detectado; una debilidad que solo puede mitigarse implementando protocolos de capa inferior como IPsec para garantizar la protección criptográfica.

Vulnerabilidades cibernéticas en los protocolos de comunicación de los SCI

Una vulnerabilidad determinante en entornos SCI radica en el uso de protocolos fundamentales que carecen de mecanismos de seguridad integrados. Por ejemplo, el

protocolo IEC 60870-5-104 es un estándar de comunicación esencial entre sistemas SCADA y subestaciones, se caracteriza por ser no cifrado. Esto implica que transmite la Unidad de Datos de Servicio de Aplicación (ASDU) en texto plano sobre TCP/IP sin ninguna forma de autenticación. Esta exposición directa permite a un atacante con acceso a la red interceptar y leer datos sensibles fácilmente. Por otra parte, el estándar OPC (*Open Platform Communications*, Plataforma de Comunicaciones abierta) si bien facilita la interoperabilidad en la Industria 4.0, sus especificaciones más antiguas también eran vulnerables a la interceptación de datos y ataques de Denegación de Servicio (DoS), aún cuando la versión OPC UA aborda estas debilidades con cifrado y autenticación robustos.

Otros protocolos también presentan vulnerabilidades relacionadas con su diseño. MQTT (*Message Queuing Telemetry Transport*, Transporte de Telemetría por Cola de Mensajes) es un protocolo ligero de publicación/suscripción, ideal para redes IoT con recursos limitados, no obstante, su propia naturaleza ligera lo hace vulnerable a la interceptación de comunicaciones, ataques de intermediario y accesos no autorizados si no se implementan medidas de seguridad en la capa de aplicación, como TLS/SSL para el cifrado. Por el contrario, los protocolos usados para la sincronización y la transmisión de datos en subestaciones, como IEEE C37.118, aseguran que los mensajes (datos, encabezado, configuración y comando) que transmiten las PMU se manejen de manera segura para evitar la manipulación o la interrupción de la sincronización.

Ciertos protocolos de gran alcance, como el conjunto de normas IEC 61850 (para la automatización de subestaciones) y su extensión, IEC 61400-25 (para parques eólicos), si bien establecen directrices para el modelado y la comunicación en sistemas de energía, también presentan sus falencias. Su función es estructurar la comunicación en múltiples capas (proceso, intervalo, estación) y son cruciales para la comunicación de alta velocidad. Cualquier vulnerabilidad o configuración errónea en estas capas, especialmente en las interfaces que utilizan MMS y servicios web (como lo hace IEC 61400-25), puede ser aprovechada por un atacante para comprometer la protección, el control y la monitorización de la subestación o el parque eólico.

Vectores de ataque de ciberseguridad en los ISC

En la medida que los SCI se encuentren cada vez más interconectados, los riesgos en materia de Ciberseguridad aumentan drásticamente, generándose más vulnerabilidades tanto a nivel de TI y de TO. Básicamente, las vulnerabilidades radican en sistemas de hardware y software heredados, tecnologías obsoletas, protocolos de comunicación inseguros y la carencia de parches de seguridad en las plataformas de hardware y software en general. En tal sentido, en los intentos de intrusión se identifican estas debilidades utilizando vectores de ataque para violar la integridad, confidencialidad y capacidad operativa de los sistemas de control. Los vectores de ataque identificados en los SCI son: *malware*, *ramsonware*, *phishing*, ataques de denegación de servicio (DoS), ataques de fuerza bruta, entre otros.

Malware

Es un tipo de programa malicioso diseñado para infiltrarse en los SCI. El malware tienen como objetivo el robo de información confidencial, la alteración de la operatividad de los sistemas o la provocación de daños físicos a la infraestructura crítica. Un malware puede insertarse a través de internet, la red interna de la empresa o localmente por los usuarios con acceso a la HMI; por ejemplo, insertando una memoria USB infectada en una HMI, servidor o PC que se encuentre en la red PLC-BS. El malware puede espiar y dañar sistemas industriales, ralentizar o bloquear redes, e incluso incluir rootkits para PLC (Serhane et al., 2019).

El *malware* actúa como un vector de ataque principal, capaz de ingresar a través de la red corporativa mediante Phishing o dispositivos USB infectados, para luego propagarse a la red OT. Una vez dentro, este código malicioso tiene la capacidad de manipular los procesos en cada nivel: en las capas de supervisión, puede corromper la información mostrada en las HMI y los sistemas SCADA para cegar a los operadores; en el nivel de control, puede alterar la lógica de los PLC y RTU para forzar un funcionamiento inseguro que cause daños físicos; y todo esto se facilita por la violación de protocolos de comunicación industrial (como Modbus o PROFINET) que, al carecer de cifrado y autenticación robusta, permiten la inyección de comandos no autorizados para el sabotaje.

Ramsonware

Es una variante del malware. Los vectores de infección iniciales a través de los cuales el *ransomware* accede a una red CPS objetivo proporcionan información sobre las tácticas del adversario y las vulnerabilidades que se explotan (Benmalek, 2024).

Los atacantes utilizan tanto la explotación de vulnerabilidades técnicas como la manipulación psicológica para infiltrarse en los entornos de Sistemas Ciberfísicos (CPS). Una táctica principal es el acceso remoto, donde los ciberdelincuentes explotan servicios de interfaz de administración obsoletos y sin parches expuestos a internet, como las puertas de enlace VPN o el Protocolo de Escritorio Remoto (RDP). Paralelamente, las campañas de phishing altamente elaboradas siguen siendo un método frecuente, en el que los atacantes investigan a fondo a la víctima para suplantar identidades de confianza. Mediante esta ingeniería social y manipulación psicológica, logran engañar a los usuarios finales para que desactiven las seguridades e instalen malware o ransomware contenido en enlaces o documentos adjuntos.

Las defensas de los CPS se ven comprometidas a través de canales indirectos y amenazas internas. El compromiso de terceros de confianza, como contratistas y proveedores de servicios gestionados (MSP), permite a los atacantes eludir las barreras de ciberseguridad convencionales al utilizar las credenciales robadas y las redes ya comprometidas de estos intermediarios. Asimismo, las amenazas internas, ya sean empleados descontentos o contratistas malintencionados, utilizan su acceso privilegiado para infectar intencionalmente las redes, haciendo crucial la estricta monitorización del personal. Adicionalmente, las

infecciones físicas mediante dispositivos infectados (como unidades USB o tarjetas SD) introducidos directamente en las instalaciones son un vector de propagación efectivo que permite que el malware entre a redes seguras que están físicamente aisladas de redes no confiables.

Ataques de denegación de servicio (Denial of Service, DoS)

Los ataques de denegación de servicio (DoS) y de denegación de servicio distribuida (*Distributed Denial of service*, DDoS) funcionan sobrecargando las redes SCI con tráfico malicioso, causando interrupciones o un cierre total. Los ataques DoS suelen provenir de una sola fuente, mientras que los ataques DDoS utilizan múltiples sistemas comprometidos. Ambos tipos son disruptivos y pueden provocar interrupciones en entornos que dependen de un funcionamiento continuo, como las empresas de energía o de agua (Paloalto Networks, 2025).

En los entornos de TO, estos ataques buscan agotar los recursos de los controladores y servidores HMI, poniendo en riesgo la disponibilidad y la integridad de los procesos críticos. Para contrarrestarlos, es vital implementar sistemas de detección de anomalías de red, utilizar tasas limitadas de paquetes en la configuración de *firewalls*, y segmentar rigurosamente la red para que los floods de tráfico queden contenidos y no afecten la continuidad operativa de la planta o subestación.

Ataques de fuerza bruta

Los ataques de fuerza bruta son intrusiones en las que los ciberdelincuentes intentan acceder a los sistemas probando automáticamente diversas combinaciones de credenciales de inicio de sesión y contraseñas (Dal Molin, 2024). En el contexto de los SCI, esta técnica busca explotar las vulnerabilidades de los dispositivos y sistemas de control a nivel de acceso, que suelen utilizar credenciales predeterminadas o contraseñas débiles. Por lo tanto, la creciente interconexión y la automatización industrial han convertido este tipo de ataque en una amenaza cada vez más común.

Una vez que tienen éxito, los atacantes pueden escalar privilegios, manipular la configuración de equipos críticos como PLCs o RTUs, e incluso tomar control total del proceso industrial. Para mitigar esta amenaza, es preciso adoptar políticas de contraseñas robustas y únicas, deshabilitar o cambiar todas las credenciales predeterminadas, e implementar mecanismos de bloqueo de cuentas o retardos de tiempo tras múltiples intentos fallidos, además de utilizar autenticación de múltiples factores y varias capas de acceso.

Estrategias de ciberseguridad para la protección de los SCI

En virtud de las vulnerabilidades y vectores de ataque descritos en las secciones anteriores, se va a caracterizar el estado del arte de las estrategias o tecnologías aplicadas para mitigar las amenazas a los entornos de SCI. En este contexto, Nankya et al. (2023) analizan

detalladamente las herramientas existentes en Ciberseguridad para SCI, tal y como se muestra en los siguientes apartados.

Gestión de riesgos y gerencia de la ciberseguridad

Una base sólida de ciberseguridad comienza con una gestión de riesgos efectiva:

- **Identificación de amenazas:** El proceso inicial implica identificar las amenazas específicas para la organización. Para ello se requiere la definición de métricas precisas para cuantificar el nivel de riesgo y la búsqueda exhaustiva de posibles vectores de ataque.
- **Inventario de activos de los SCI:** Es crucial mantener una lista actualizada de todo el hardware, software y tecnologías de infraestructura de soporte. Este inventario permite clasificar los activos y procesos críticos, facilitando el análisis de impacto y evaluando las consecuencias de un fallo en la disponibilidad, integridad y confidencialidad de los datos.
- **Desarrollo de políticas y capacitación:** Las gerencias de los sistemas en cuestión deben crear y difundir políticas, procedimientos y materiales educativos de ciberseguridad aplicables a los SCI.
- **Políticas adaptativas:** Es prioritario que las organizaciones que gestionan infraestructura crítica adopten medidas de seguridad enmarcadas con las tecnologías de vanguardia.
- **Procedimientos de respuesta a incidentes:** Poner en práctica procedimientos de respuesta que se sincronicen los procesos de actuación de las áreas de TI y de TO.

Arquitectura de red SCI

El diseño de la red SCI debe construirse priorizando la seguridad para reducir la superficie de ataque y garantizar el aislamiento:

- **Segmentación de la red:** Es una de las estrategias clave en cuanto a protección de red en SCI. Los sistemas deben dividirse en zonas de red basadas en criterios como su función, perfil de riesgo o importancia crítica en el proceso en cuestión. Para el control del tráfico entre zonas, se requiere el uso de dispositivos de filtrado (como firewalls de inspección con estado) en el punto de entrada de cada segmento. Cada zona debe adherirse a una línea base de seguridad consistente y definida. Un principio clave es que cada zona de red debe tener un punto de entrada único.
- **Topología multicapa:** Se debe diseñar una topología que incorpore múltiples capas de seguridad, asignando las comunicaciones más críticas a la capa más confiable y protegida del diseño.

- **Zonas desmilitarizadas (*Demilitarized Zone*, DMZ):** Se deben establecer para crear una subred lógica y física intermedia. Las DMZ actúan como un buffer o mediador para los dispositivos de seguridad, asegurando que estos no estén directamente expuestos ni a la red externa ni a la red de control crítica. Seguridad perimetral de la red SCI. La seguridad del perímetro es la primera línea de defensa, enfocándose en el control del tráfico y el acceso:

- **Configuración de cortafuegos (Firewalls):** Son esenciales para controlar el tráfico que fluye entre las redes de TI corporativas y las redes SCI. Los firewalls supervisan e inspeccionan el tráfico de red, aplicando un conjunto de reglas para permitir o denegar paquetes específicos.

- **Bloqueo geográfico de IP:** El filtrado geográfico es una herramienta de seguridad que bloquea las conexiones entrantes y salientes basándose en la ubicación geográfica de la dirección IP. Esto se utiliza para mitigar riesgos provenientes de regiones geográficas específicas consideradas de alto riesgo.

- **Servidores de salto (*Jump Servers*):** Se utilizan como una ubicación de autorización central entre las diferentes zonas de seguridad de la red SCI. Estos servidores ayudan a aislar segmentos con diferentes niveles de seguridad y a menudo se combinan con otras herramientas, como los sistemas de detección de intrusiones (IDS), para implementar el concepto de defensa en profundidad.

- **Restricción de acceso remoto:** Es crucial prohibir el acceso remoto y continuo de proveedores o empleados a la red de control. Esto incluye eliminar el uso de cuentas de mantenimiento o contraseñas de puerta trasera que puedan ser conocidas por los fabricantes o terceros. La documentación debe revelar la existencia de tales cuentas.

- **Monitorización de conexiones remotas:** Se deben catalogar y monitorizar todas las conexiones que accedan remotamente a la red. Dado que dispositivos como los PLC y las RTU carecen de mecanismos de seguridad robustos frente a vulnerabilidades como los *buffer overflows* o ataques *man-in-the-middle*, se ha propuesto el uso de una Unidad de Seguridad en la Sombra (SSU). Este dispositivo actúa como una "caja negra", conectándose en paralelo a los dispositivos de control para capturar y decodificar el flujo de datos del protocolo SCADA. La SSU verifica si el comportamiento de los dispositivos monitoreados se alinea con el estado de los módulos de E/S físicos, estableciendo un mecanismo de verificación de seguridad redundante.

Monitoreo de seguridad

La detección temprana de anomalías es clave en entornos donde la continuidad es crítica:

- **Medición de la línea base:** Para identificar comportamientos anómalos, los investigadores sugieren un método que combina el aprendizaje automático con el monitoreo pasivo (para no interferir con las operaciones) y el conocimiento de los protocolos SCI. El objetivo es medir la línea base de las operaciones y del tráfico de red normales.

- **Sistemas de detección de intrusiones (IDS):** Deben configurarse específicamente para generar alarmas ante cualquier tráfico de red que se desvíe del funcionamiento normal o que sea atípico para el entorno SCI.
- **Gestión de registros de auditoría y SIEM:** Es fundamental realizar un seguimiento y análisis de los registros de auditoría en áreas críticas. Un Sistema de Gestión de Información y Eventos de Seguridad (SIEM) debe configurarse para centralizar la recopilación de datos de diversos orígenes, detectar variaciones en las normas operativas y ejecutar las respuestas adecuadas ante posibles intrusiones.

Seguridad del *host*

Las medidas aplicadas directamente a los dispositivos dentro de la red son primordiales para la defensa en profundidad:

- **Cultura de gestión de parches:** Se debe fomentar una cultura proactiva de aplicación de parches y gestión de vulnerabilidades para reducir los riesgos de ciberseguridad y proteger la disponibilidad de la producción. La priorización inteligente es un método avanzado que secuencia la aplicación de parches en redes complejas, combinando el modelado de sistemas, la evaluación de riesgos y la teoría de juegos para una estrategia de defensa eficaz.
- **Prueba de parches:** Todos los parches deben ser probados rigurosamente en entornos de prueba offline (fuera de la red de producción) antes de cualquier implementación en los sistemas SCI.
- **Listas blancas de aplicaciones (*Application Whitelisting*):** Se recomienda su implementación, especialmente en las interfaces hombre-máquina (HMI). Esta técnica de seguridad eleva la protección al permitir que los sistemas ejecuten únicamente las aplicaciones explícitamente aprobadas y enumeradas en una lista blanca.
- **Refuerzo de dispositivos de campo:** Es necesario reforzar la seguridad de todos los dispositivos de campo, incluyendo los teléfonos inteligentes y tabletas utilizados por el personal operativo.
- **Reemplazo de hardware obsoleto:** Se debe llevar a cabo el reemplazo del software y dispositivos de hardware obsoletos, ya que a menudo carecen de soporte de seguridad.
- **Deshabilitación de puertos y servicios:** Tras realizar pruebas exhaustivas para asegurar que no se afectarán las operaciones, se deben deshabilitar todos los puertos y servicios no utilizados en los dispositivos SCI.

Expectativas a futuro de la Ciberseguridad en SCI

En el marco de las tecnologías emergentes, la Industria 4.0 está acelerando la convergencia entre las redes de TI y OT, introduciendo nuevos riesgos por la expansión del IIoT. Ante

esto, la ciberseguridad en los SCI se orienta hacia la adaptación y el aislamiento estricto.

Las futuras estrategias de gestión de riesgos se basarán en la IA y el *Machine Learning* para establecer modelos de tráfico de red base, permitiendo la detección de anomalías en tiempo real con mayor eficacia que los Sistemas de Detección de Intrusiones (IDS) convencionales.

En la arquitectura de red, la principal tendencia es migrar hacia el modelo *Zero Trust* (nunca confiar, siempre verificar la identidad y el acceso de todos los usuarios y dispositivos). Esto se combina con la segmentación física reforzada, empleando diodos de datos para asegurar que el flujo de información sea estrictamente unidireccional y proteger los procesos más críticos.

A nivel perimetral y de host, la seguridad se centrará en la monitorización pasiva y continua a través de sistemas como las Unidades de Seguridad en la Sombra (SSU). Además, se exigirá la eliminación total de cuentas *backdoor* (claves ocultas de acceso) de los fabricantes. Estas medidas buscan asegurar que la disponibilidad y la integridad operativa se mantengan como prioridades máximas en este entorno de creciente interconexión.

Las expectativas a futuro indican una estandarización de la seguridad del host mediante la implementación obligatoria de listas blancas de aplicaciones en HMI y una gestión de vulnerabilidades regida por la priorización inteligente de parches, donde la IA determinará la secuencia de aplicación para minimizar el impacto en la producción. Dado que la expansión del IoT/IIoT incrementa el número de dispositivos de campo (como sensores y actuadores inteligentes) con escasa seguridad inherente, será crucial reforzar su protección y la de los dispositivos móviles que los gestionan. El SIEM evolucionará para correlacionar grandes volúmenes de datos OT/IT y registros de auditoría de forma predictiva.

Reflexiones finales

La vulnerabilidad de los SCI reside en su propia arquitectura (RTU, PLC, SCADA, HMI), históricamente optimizada para la disponibilidad y fiabilidad en entornos aislados, no para la defensa moderna. Esta prioridad se traduce en vulnerabilidades explotadas directamente: los ciberdelincuentes obtienen control de campo (RTU/PLC) mediante ataques de fuerza bruta aprovechando credenciales débiles o predeterminadas, mientras que los ataques DoS/DDoS buscan paralizar los servidores SCADA y HMI, esenciales para la supervisión. Por otra parte, la militarización se centra en crear malware específico para estas plataformas, siendo así el punto de partida esencial para el ataque.

Para contrarrestar esta cadena de ataque exige que la Ciberseguridad se eleve a una prioridad de gestión. La defensa debe ser adaptativa, comenzando por una rigurosa gestión de riesgos y la creación de un inventario exhaustivo de activos. A nivel de red, la segmentación y la seguridad perimetral son vitales: el uso de servidores de salto aísla el acceso de terceros, y la configuración de *firewalls* con bloqueo geográfico de IP reduce

la superficie de exposición. En ese sentido, para proteger los dispositivos de control más vulnerables (PLC/RTU), la estrategia avanza hacia controles de host como las listas blancas de aplicaciones en las HMI, complementados con soluciones de monitorización pasiva (SSU) que detectan anomalías sin riesgo de interferir con las operaciones críticas.

La expansión de la Industria 4.0 y el IIoT obliga a la arquitectura SCI a abandonar la obsoleta confianza en el aislamiento lógico. En este contexto, los diodos de datos son cruciales: al forzar un flujo de datos unidireccional mediante hardware, establecen una separación física absoluta entre la red OT de proceso y la red TI más expuesta. Esta estrategia neutraliza la posibilidad de inyección de comandos maliciosos o *malware* desde el exterior. Esta medida de aislamiento extremo se robustece con la adopción del marco Zero Trust (nunca confiar, siempre verificar), que se consolida como el estándar para gestionar el riesgo de la interconexión garantizando la operatividad.

Las expectativas a futuro se centran en el blindaje con tecnologías emergentes y disruptivas inclusive. La IA y el *Machine Learning* pueden convertir en el núcleo de la detección de intrusiones, creando modelos altamente precisos integrados con sistemas SIEM avanzados. En cuanto a la gestión de vulnerabilidades, la tendencia es la priorización inteligente de parches, donde la IA juega un papel crucial para la protección de SCADA/PLC. Finalmente, la seguridad se convertirá en una prioridad de los SCI futuros, mediante una integración cada vez más fuerte con el IIoT, englobando las nuevas tecnologías.

Referencias

AO Kaspersky Lab. (2025). *¿Qué es la ciberseguridad?* AO Kaspersky Lab. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security?srsltid=AfmBOoo9eartUNb9rv269k3picGOqXE4_HeMEJQGCaqZHW9UhkQyUdxI

Benmalek, M. (2024). Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. *Internet of Things and Cyber-Physical Systems*, *4*, 186-202. https://doi.org/10.1016/j.iotcps.2023.12.001

Burkert. (2025). *PROFINET: el estándar de comunicación seguro para las redes industriales.* Burkert Fluid Control Systems. https://www.burkert.es/es/servicio-asistencia/centro-de-documentacion/glosario/PROFINET-el-estandar-de-comunicacion-seguro-para-las-redes-industriales

Cisco Systems, Inc. (2025). *¿Qué es la Ciberseguridad?* Cisco Systems, Inc. https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html

Cossio, O. (2020). *Vulnerabilidades de ciberseguridad en sistemas de control industrial y accesibilidad a través de redes públicas* [Tesis de Maestría]. Universidad Nacional del Nordeste, Argentina. https://repositorio.unne.edu.ar/bitstream/handle/123456789/28453/RIUNNE_FACENA_TM_Cossio%20Cisneros_OA.pdf?sequence=1&isAllowed=y

Dal Molin, P. (2024). *Cyberattack on industrial systems: A growing threat.* Lumiun Blog. https://www.lumiun.com/blog/en/cyberattack-on-industrial-systems-is-a-growing-threat/

Digital Prototype Systems Inc. (2022). *Learn SCADA Software Programming For Remote Monitoring*. Digital Prototype Systems Inc. https://www.dpstele.com/scada/programming-concepts.php

Dorf, R., y Bishop, R. (2005). *Sistemas de control moderno*. Pearson Prestince Hall. ISBN: 84-205-4401-9.

Dreamlab Technologies. (2025). *Ciberseguridad en la infraestructura crítica: protegiendo los pilares de la sociedad moderna*. Dreamlab Technologies AG. https://dreamlab.net/es/blog/entrada/ciberseguridad-en-la-infraestructura-critica-protegiendo-los-pilares-de-la-sociedad-moderna/

ElProCus. (2025). *DeviceNet : Architecture, Message Format, Error Codes, Working & Its Applications*. ElProCus: Electronic — Projects — Focus. https://www.elprocus.com/devicenet-architecture/

Gillis, A. (2025). *Distributed Control System (DCS)*. TechTarget. https://www.techtarget.com/whatis/definition/distributed-control-system

Huawei Technologies Co., Ltd. (2023). *¿Qué es la ciberseguridad?* Huawei Technologies Co., Ltd. https://info.support.huawei.com/info-finder/encyclopedia/en/Cybersecurity.html

Instituto Nacional de Ciberseguridad. (2015). *La Ciberseguridad en la Industria 4.0*. Instituto Nacional de Ciberseguridad. https://www.incibe.es/incibe-cert/blog/ciberseguridad-industria-4-0

InstrumentationBlog. (2025). *Distributed Control Systems (DCS)*. InstrumentationBlog. https://instrumentationblog.com/distributed-control-system-dcs-system/

Mikrodev. (2025). *What Is RTU Device?* Mikrodev. https://www.mikrodev.com/what-is-rtu-device/

Monilithic Power Systems. (2025). *Principles of Analog Control*. Monilithic Power Systems. https://www.monolithicpower.com/en/learning/mpscholar/analog-vs-digital-control/fundamentals-of-analog-control/principles?srsltid=AfmBOoo7qQhhuxjVkU7H1-HN7zbLwJ0mPMLp7IB5KKIWRoDjW3S8mcCB

Nankya, M., Chataut, R., y Akl, R. (2023). Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies. *Sensors*, *23*(21), 8840. 10.3390/s23218840

Nasby, G. (2019). *Introduction to ISA112 SCADA Systems Standard*. ISA112 committee co-chair. https://www.grahamnasby.com/files_publications/NasbyG_2019_Intro-to-ISA112_Halton-SCADA-Workshop_jun26-2019_slides.pdf

National Instruments. (2025). *Modbus Protocol in Depth*. National Instruments. https://www.ni.com/en/shop/seamlessly-connect-to-third-party-devices-and-supervisory-system/the-modbus-protocol-in-depth.html

Ogata, K. (2003). *Ingeniería de Control Moderna*. Pearson Prestince Hall.

Paloalto Networks. (2025). *What Is SCI Security? — Industrial Control Systems Security*. Paloalto Networks. https://www.paloaltonetworks.ca/cyberpedia/what-is-ics-security

Pro-face. (2025). *Simple definition of HMI*. Schneider Electric Japan Holdings Ltd. https://www.proface.com/en/what_is_HMI

Serhane, A., Raad, M., Raad, R., y Susilo, W. (2019). Programmable logic controllers based systems (PLC-BS): vulnerabilities and threats. SN Applied. *Science*, *1*(924). https://doi.org/10.1007/s42452-019-0860-2

Sharma, S. (2025). *Modbus RTU: A comprehensive guide to undestanding and implementig the protocol*. Wevolver. https://www.wevolver.com/article/modbus-rtu-a-comprehensive-guide-to-understanding-and-implementing-the-protocol

Siemens. (2025). *SIMATIC S7-1200*. Siemens. https://www.siemens.com/mx/es/productos/automatizacion/systems/industrial/plc/s7-1200.html

Siemens PLC Guides. (2025). *Home*. Siemens Guide. https://www.siemensguides.com/Hardware

Sokacheske, M. (2025). *PROFINET and Ethernet/IP: Key protocols for Industry 4.0 and IoT*. Blog ISA Interchange. https://blog.isa.org/profinet-and-ethernet-ip-key-protocols-industry-4.0-iot

Waseem, U. (2025). *Modbus TCP: A Comprehensive Guide to the Protocol and its use*. Wevolver. https://www.wevolver.com/article/modbus-tcp

Ciberseguridad en Educación y Formación

Formando ciudadanos digitales críticos: El papel de la Ciberseguridad en la Educación

Yazmary Rondón[1]

Introducción

Con el auge de las Tecnologías de la Información y Comunicación (TIC) y más recientemente de la Inteligencia Artificial (IA) en todos los ámbitos de la vida, se recopila, procesa y difunde a diario una gran masa de datos e información a través de distintos canales (correos, redes sociales, entre otros), sin menoscabo de los riesgos y vulnerabilidades asociadas a ella.

Entre las áreas críticas en materia de ciberseguridad, debido a la gran cantidad de información que procesan, se halla la Educación. Por tal razón, este ensayo busca exponer un desarrollo teórico de la situación actual, por medio de experiencias en esta área, en los niveles de educación primaria, secundaria y universitaria. Además, de un análisis de las competencias digitales necesarias, ventajas, desventajas, políticas y recomendaciones, tanto en la formación dirigida hacia los niños y jóvenes como usuarios vulnerables, como hacia las instituciones para el manejo eficiente y seguro de la información derivada de sus procesos académicos y administrativos. Además, la importancia del uso y desarrollo de Tecnologías Libres para incorporar elementos de seguridad en los sistemas de las instituciones.

Ciberseguridad y áreas críticas

La ciberseguridad se concibe como un área que se dedica al estudio de mecanismos para resguardar todo aquello que pueda almacenarse de manera personal o institucional en la web, cuyo objetivo principal es proteger la información e infraestructura (Arreola, 2019).

Actualmente, el ámbito de la ciberseguridad cuenta con mecanismos de *blockchain*, Inteligencia Artificial (IA), Aprendizaje Automático y Profundo o Incremental. Mediante ellos procesan y analizan grandes volúmenes de datos, permitiendo a los expertos en esta área, detectar patrones y posibles amenazas en tiempo real (Arias y Vargas, 2025). De esta manera, logran anticipar los mecanismos de defensa y tomar las decisiones más pertinentes para la organización.

Aunque los estándares de ciberseguridad protegen desde algoritmos de cifrado, hasta seguridad de aplicaciones de navegadores web y seguridad de la información, es fundamental que las normas de ciberseguridad (de la información y de su gobernanza) a adoptar sean

[1]Licenciada en Educación mención Matemática egresada de la Universidad de Los Andes (ULA), MSc. en Educación mención informática y Diseño Instruccional, Doctora en Educación. Actualmente se desempeña como docente en la ULA, y como investigadora en el Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL). yrondon@cenditel.gob.ve

prácticas y económicas para que puedan adaptarse a las limitaciones técnicas y de recursos de los diversos usuarios (Torres, 2025).

Sin embargo, en algunos países latinoamericanos debido a los altos costos para la adquisición de hardware y software de este tipo, aunado a la alta inversión para capacitación de personal especializado, se incrementan las debilidades en el conocimiento de estas nuevas tecnologías para el manejo, procesamiento y resguardo de la información; cuestiones que desencadenan en un uso limitado y más vulnerable a ataques cibernéticos, que pueden provenir de fuentes internas o externas, debido a factores técnicos, naturales o humanos.

En este sentido, según Altamirano y Oré (2008) la gran cantidad de información que manejan algunas instituciones públicas y privadas, las convierten en áreas críticas para ataques cibernéticos:

1. Bancos y organizaciones financieras
2. Instituciones de salud públicas y privadas
3. Empresas de servicios profesionales e industriales (aseguradoras, inmobiliarias, bufetes, constructoras, entre otras)
4. Administración pública
5. Educación
6. Telecomunicaciones, suministro energético

Particularmente, la educación requiere de sistemas informáticos para gestionar y desarrollar las actividades académicas y administrativas relacionadas a datos de estudiantes, representantes y personal (fichas de inscripción, gestión de contenidos, registros de calificaciones año tras año, entre otras), por ello recurren al uso de diferentes plataformas donde alojan una gran cantidad de información con escasas medidas de ciberseguridad, situación que la convierte en una de las áreas criticas en esta materia.

En este campo, se han realizado investigaciones que proporcionan evidencias respecto a los profundos efectos que la situación económica, social y cultural tiene sobre las competencias digitales de los docentes, estudiantes, representantes y demás actores educativos. Los resultados muestran que el nivel de formación de los representantes es un factor relevante para explicar el rendimiento de los estudiantes en la competencia digital, reflejando la existencia de una segunda brecha en el campo de la educación, debido a que la experiencia TIC en la escuela es indisociable de la del hogar.

En consecuencia, es necesario abordar un nuevo esquema de competencias digitales que deben desarrollar las personas en los distintos niveles educativos, para insertarse satisfactoriamente en la sociedad actual, donde el uso de las TIC es cotidiano en: lo laboral, social y económico. Tales competencias no solo atañen al uso de la tecnología desde el

punto de vista práctico, sino también crítico, es decir, la formación que derive en un uso responsable, ético y seguro de la información.

Por lo tanto, la escuela, familia y comunidad juegan un papel fundamental en el desarrollo de estas competencias digitales desde temprana edad, para evitar riesgos y amenazas; debido a la exposición excesiva e incauta de información en las redes.

Ciberseguridad y educación

En este apartado se abordan dos enfoques de atención en ciberseguridad en el ámbito educativo, el primero dirigido hacia los niños y jóvenes como usuarios vulnerables y el segundo centrado en la institución, como consecuencia de la gran cantidad de datos académicos y administrativos, recopilados y procesados por distintos actores de la institución, año tras año, relacionados a padres, madres, representantes, estudiantes, docentes, empleados y obreros.

En el primer caso, los hallazgos de numerosos estudios en el área de la ciberseguridad resaltan la importancia de la formación del estudiante en el desarrollo de las competencias digitales, puesto que el acceso a equipos inteligentes desde edades cada vez más tempranas, debe llamar la atención sobre lo inaplazable de educar a los niños en materia de ciberseguridad. Con el fin de evitar riesgos (acoso, robo de datos e identidad, entre otros) en las redes, por medio de una formación que les permita detectar comportamientos inapropiados en Internet, los peligros de comunicarse con extraños y navegar en sitios inseguros.

Aunque, existen legislaciones que protegen a los niños en la red, mediante controles parentales o eliminación de contenido perjudicial en las plataformas, todavía en algunos países los delitos informáticos no se encuentran debidamente tipificados y exponen a los usuarios más pequeños a muchos riesgos. En promedio desde los 8 años los niños acceden a través de dispositivos móviles a Internet sin supervisión, con el fin de distraerse y jugar, descargando aplicaciones inocentemente, sin percatarse de lo vulnerables que resultan ante los ciberdelincuentes. Estos se aprovechan de su inmadurez para ofrecer enlaces que descargan *malware* o los desvían de su búsqueda original, con malas intenciones, entre ellas el robo de datos de integrantes de su familia (Herrera et al., 2025).

Ante tal realidad, como medida preventiva para evitar *Ciberbullying*, *Grooming*, entre otros; en las redes es fundamental promover en la familia, escuela y comunidad la educación en ciberseguridad, dirigida a la familia y con especial atención hacia los niños y adolescentes (entre los 5 y 16 años), resultan ser los más vulnerables. Tal formación debe empezar desde la toma de medidas simples como usar contraseñas fuertes y disminuir la exposición de información personal en línea, hasta formación y adiestramiento en el uso de herramientas que permitan verificar la autenticidad de los sitios; y a los padres tener un mayor control sobre los lugares a los que pueden acceder sus hijos, Así como también, monitorear las actividades que realizan en línea, a fin de evitar la exposición a contenidos inapropiados que producen daños emocionales y materiales, y además pueden conducir a aislamiento social,

bajo rendimiento académico, depresión y hasta el suicidio en los casos más graves.

Entonces, la educación en ciberseguridad es un contenido apremiante en el currículo, porque además de proteger a los niños de todos los riesgos anteriores, los va formando como seres responsables y conscientes del buen uso de la tecnología, críticos ante los contenidos que se les pueden presentar en distintos formatos, y cautos con la información que ceden en Internet, puesto que conocen la importancia para sí mismos y su familia de navegar de manera segura y con limites de tiempo firmes.

Aunado a lo anterior, también es fundamental la capacitación y formación permanente sobre medidas y prácticas de ciberserguridad de los profesores y demás personal que labora en las instituciones educativas, para que además de formar a los estudiantes en esta área los apliquen ellos mismos y eviten riesgos personales e institucionales. Debido a la exposición incauta y excesiva de datos en los diversos sistemas en los que procesan la información y en las redes sociales, por ejemplo evitar caer en engaños a través del uso del teléfono móvil (*Phishing*), cediendo contraseñas, datos bancarios, personales o de otros contactos muy relevantes. Poniendo en riesgo de esta forma tanto su información personal, como la de la institución en la que labora.

En este sentido, se recomienda la implementación de aplicaciones de seguridad basados en Inteligencia Artificial (IA) por medio del análisis de comportamiento y la detección de patrones, que ayuden a detectar y bloquear posibles intentos de robo de datos provenientes de mensajes de textos, correos, aplicaciones falsas y redes sociales; a través del uso de algoritmos prevenir y descubrir posibles amenazas, al establecer múltiples factores para el acceso y autenticación (*Google Authenticator*, *Duo Security*, entre otras), uso de navegadores más seguros, descarga de aplicaciones en sitios oficiales, comprobar las URL antes de abrirlas y la instalación de antivirus para móviles (Chilquina y Garcés, 2025). Con el objeto de ahondar más en este tema, a continuación se presentan varias experiencias en los diversos niveles educativos.

Experiencias sobre ciberseguridad en educación

Educación primaria y secundaria

A. García et al. (2019), realizaron una evaluación de las competencias digitales de niños que estaban finalizando el sexto grado de Primaria, junto a otros que iniciaban el primer año de Secundaria en algunas instituciones educativas de España. Seleccionaron aleatoriamente y aplicaron una prueba objetiva a 600 niños, con edades comprendidas entre 12 y 14 años. La prueba medía los conocimientos, capacidades y actitudes de los estudiantes en las 4 competencias del área de seguridad señaladas en el modelo DigComp (protección de los dispositivos, de los datos personales, de la salud y del medio ambiente). Los resultados muestran en general que los niños usan más las TIC para esparcimiento que para las tareas académicas, juegan con los amigos *online* de forma positiva, manteniendo buenas relaciones, pero no son conscientes del impacto medioambiental de la fabricación de los dispositivos que utilizan. Tienen mayores conocimientos y capacidades en primer lugar en lo referente

a la protección de la salud, en segundo lugar, en la protección de dispositivos, seguido de la protección de datos personales y, finalmente, en la protección del entorno. Por lo tanto, determinaron la importancia de la adquisición de este tipo de competencias por parte de los estudiantes, para algunas conductas que tienen que ver con la salud, no comunicarse con personas desconocidas, jugar *online* en periodos breves para prevenir adicciones, mantener posturas adecuadas o no perder el tiempo al navegar por Internet. También, encontraron que se requiere mayor formación en cuanto a usar los dispositivos de manera más amigable con el medio ambiente, siendo conscientes del impacto positivo al utilizar opciones para ahorrar energía, entre otros.

De forma similar, Torres (2025) desarrolló un marco de ciberseguridad para una Unidad Educativa en Ecuador, mediante un enfoque experimental y cuantitativo. Los participantes fueron estudiantes de secundaria, docentes y personal administrativo. Diseñó un sistema para detectar intromisiones usando IA en simulación de ataques cibernéticos, análisis de tráfico y evaluación de posibles aspectos de vulnerabilidad. El marco inició con un análisis de la infraestructura tecnológica de la institución, después a través del uso de herramientas como: Snort, Nmap y *Machine Learning*, se logró una detección temprana de posibles amenazas hasta en un 95 %, tomando a partir de estas prácticas los correctivos y la elaboración de un esquema de medidas mínimas que se deben adoptar por parte de todos los actores educativos involucrados en el uso del sistema. Demostrando que es posible mitigar riesgos en los sistemas educativos, robusteciendo esos entornos virtuales, monitoreando constantemente el sistema, y formando a los estudiantes, docentes, representantes y resto de personal, en el desarrollo y uso de buenas prácticas de ciberseguridad para garantizar la confidencialidad, integridad y disponibilidad de la información.

Asimismo, Jimenez (2025) diseñó un curso en línea interactivo (*Massive Open Online Course: MOOC*) sobre ciberseguridad, dirigido a estudiantes de secundaria de una institución educativa en Ecuador. Participaron 39 estudiantes con edades comprendidas entre 15 y 16 años, cuyo objetivo principal fue fortalecer la conciencia y protección digital a través de materiales educativos en línea. La metodología utilizada fue mixta (cualitativa y cuantitativa) para explorar las experiencias y percepciones de los estudiantes en cuanto a la ciberseguridad. Los datos se recolectaron en varias etapas, a través de entrevistas, cuestionarios y debates aplicados pre y post curso a los integrantes del grupo piloto. Los resultados obtenidos muestran que este MOOC fue efectivo, con mejoras del 25 % al 85 % en reconocimiento de amenazas y aplicación de medidas de seguridad por parte de los estudiantes.

Educación universitaria

J. García et al. (2019) desarrollaron un estudio en un Instituto Tecnológico de Educación Superior de México, sobre la educación en ciberseguridad, cuyo objetivo fue indagar sobre la integración de las tecnologías en la educación y su relación con la formación de ingenieros en informática, como profesionales resilientes ante los ciberataques. Los datos fueron recolectados mediante una encuesta, como instrumento se usó un cuestionario compuesto

por 20 ítems, distribuidos en tres secciones: datos sociodemográficos, conocimientos sobre ciberseguridad, y percepción y prácticas sobre ciberseguridad. La muestra se tomó de forma probabilística y estuvo conformada por 37 estudiantes de la carrera de Ingeniería en Informática. Entre los resultados más destacados están: más del 70 % considera que las pruebas de seguridad deberían realizarse al menos trimestralmente, más del 60 % no sabe cómo reportar un incidente de seguridad, evidenciando una brecha en la formación práctica en esta área, casi un 70 % utiliza un antivirus actualizado como principal medida de seguridad. Sin embargo, el uso de herramientas adicionales como: gestores de contraseñas y VPN sigue siendo bajo, lo cual refleja la necesidad de fomentar mejores prácticas de seguridad digital, más del 65 % están dispuestos a participar en programas de concienciación en ciberseguridad organizados por loa universidad. Finalmente, el 100 % indicó que no conocen las posibles consecuencias legales de los ciberataques y violaciones de ciberseguridad en el ámbito universitario. En general, los resultados muestran una correlación negativa entre la valoración de la educación en ciberseguridad y las habilidades prácticas para reportar incidentes en tiempo real. Por lo tanto, la integración de la tecnología educativa debe considerar los aspectos técnicos, prácticos, legales y éticos.

En este mismo orden de ideas, Morales-Sáenz et al. (2025), realizaron una investigación cuyo objetivo fue analizar los factores que influyen en el comportamiento de seguridad cibernética de los empleados en instituciones de educación superior en México. Como fundamento teórico usaron la Teoría de la motivación, y aplicaron encuestas a 159 empleados. Los resultados muestran que: la conciencia de ciberseguridad influye positivamente en la autoeficacia y la eficacia de respuesta, es decir, cuando los empleados están más informados y alertas sobre los riesgos cibernéticos que enfrenta su institución se sienten más capaces de tomar medidas preventivas y reactivas. Por lo tanto, los programas de educación y concientización sobre ciberseguridad son fundamentales para mejorar la confianza de los empleados en sus habilidades y en la efectividad de las medidas de seguridad institucionales. También, arrojaron la necesidad de considerar un enfoque holístico de ciberseguridad que tome en cuenta tanto los factores individuales como los organizacionales, para promover prácticas de seguridad efectivas en el contexto educativo, es decir, además de que los empleados desarrollen rutinas de seguridad: uso de contraseñas robustas, actualización de software y protección de datos; estas prácticas deben estar acompañadas de esquemas de seguridad institucionales, para que pueden percibirse como generadoras de un impacto integral, más allá de lo individual.

También, Campos et al. (2024) realizaron un análisis sobre el uso de sistemas de Inteligencia Artificial (IA) para generar resiliencia cibernética como medida de detección de intrusos en los entornos digitales académicos. La investigación fue documental, seleccionaron 15 artículos de acuerdo a criterios de relevancia del contenido y calidad metodológica. Para el análisis de los resultados elaboraron una matriz con aspectos fundamentales de la implementación de sistemas de IA en entornos de educación superior. Entre los resultados más importantes de este estudio están: el uso de sistemas de IA es crucial para la detección de intrusiones; sobre los desafíos técnicos y conceptuales de implementar sistemas de IA destacan la necesidad de considerar la complejidad de los sistemas modernos y las

posibles vulnerabilidades en su diseño, y la criptografía como herramienta fundamental para proteger la integridad de los datos en entornos de educación superior. Además, se plantean preocupaciones sobre la ética y la privacidad en el uso de la IA para la detección de intrusiones, advirtiendo sobre el riesgo de una vigilancia excesiva y la limitación de la privacidad individual. Finalmente, agregan la importancia de la conformación de alianzas internacionales para responder a las ciberamenazas.

Herramientas de ciberseguridad en el área educativa

En cuanto al camino más idóneo y natural para enseñar a los niños y jóvenes sobre ciberseguridad se recomiendan los juegos, como estrategias para identificar situaciones de riesgos y amenazas. A tal efecto, existen algunas plataformas (Google Interland, Sekukid, Space, Shelter, Cyber Scouts, entre otras) que han desarrollado juegos para aprender los conceptos básicos de la ciberseguridad, plantean situaciones de riesgos, guían en la detección de amenazas y enseñan a establecer contraseñas robustas.

De este modo, el uso de estos juegos como recursos educativos en la familia, escuela y comunidad, pueden resultar de gran ayuda en la formación de ciudadanos digitales con mayor conciencia sobre el uso responsable y crítico de la tecnología, al enfrentar mediante simulaciones situaciones similares a la que se le pueden presentar en la red.

De forma similar, respecto al personal que labora en las instituciones educativas, la formación puede llevarse a cabo mediante sistemas que generen simulaciones se puede entrenar para: detectar intromisiones y elaborar esquemas de medidas que se deben adoptar por parte de todos los actores educativos involucrados en el uso del sistema, para disminuir riesgos y desarrollar buenas prácticas de ciberseguridad para garantizar la confidencialidad, integridad y disponibilidad de la información.

Estas estrategias traen como beneficios:

1. A nivel personal y familiar: se ha visto que formar desde temprana edad en ciberseguridad es de suma importancia, para el desarrollo de competencias digitales en identificación de riesgos, tomar decisiones informadas relacionadas a identidad, privacidad y seguridad en las redes (Herrera et al., 2025) y pueden manifestarse como:

   a) Formas de navegación más segura en Internet.

   b) Establecimiento de límites (tiempo, lugares de la red, entre otros) en el uso de la tecnología.

   c) Conciencia y responsabilidad digital.

   d) Desarrollo de habilidades digital para su desempeño en la vida adulta.

   e) Fomento de la autonomía.

   f) Mejoras en la autoestima, confianza y comunicación asertiva ante cualquier inconveniente.

g) Desarrollo de comunidades virtuales respetuosas y cooperativas.

h) Alianzas y colaboraciones entre instituciones educativas y organismos nacionales e internacionales en materia de ciberseguridad.

2. A nivel institucional: según Benavides y Blandón (2018) la implementación de sistemas de gestión de seguridad de la información (SGSI) puede contribuir a:

a) Identificar y priorizar amenazas.

b) Actualizar y mejorar continuamente el sistema, según la experiencia de los usuarios.

c) Mantener disponibles los servicios educativos.

d) Reducción de costos por incidentes informáticos.

e) Cumplir con las legislaciones respectivas.

f) Aumentar la confianza y seguridad de todos los involucrados en la comunidad educativa (Padres, madres, representantes, estudiantes, personal administrativo, docente y obrero).

g) Mejorar la imagen institucional.

h) Distribución e identificación de los roles y responsabilidades de cada actor educativo en materia de ciberseguridad.

Políticas de ciberseguridad

Tal como se ha expresado en las secciones anteriores, en el ámbito educativo además de formar a los estudiantes desde temprana edad en materia de ciberseguridad, es fundamental capacitar al los profesores y demás personal administrativo que labora en las instituciones, para evitar la exposición innecesaria de datos y los riesgos que esto desencadena.

En tal sentido, diversos autores continúan realizado análisis de teorías y técnicas para determinar las violaciones a las políticas de seguridad de los sistemas de información, que se originan por la conducta humana. Aunque las organizaciones implementan políticas de seguridad para protección de su información, se producen vulnerabilidades debido a los diferentes roles que desempeñan las personas: usuario final, administrador de equipos de seguridad, administrador de la información, supervisor de las políticas de seguridad, atacante a los sistemas de información, entre otros. Sin embargo, cada uno tendrá un efecto y consecuencia diferente dependiendo del rol y funciones que ejecuta, puesto que las técnicas de ingeniería social realizadas por hackers, se basan en tres elementos principales: los factores humanos, los aspectos organizativos y los controles tecnológicos (Ifinedo, 2014, citado en Altamirano y Oré (2017)):

1. La Teoría del Comportamiento Planificado: explica que el comportamiento individual está influenciado por la actitud, las normas subjetivas y el control de comportamiento percibido.

2. La Teoría de Protección de Motivación: amplia la visión desde la comunicación persuasiva, con énfasis en los procesos cognitivos que median en el cambio de comportamiento. Propone que la intención de protegerse a uno mismo depende de: (1) la percepción de la gravedad de la amenaza, (2) la probabilidad percibida de la vulnerabilidad, (3) la eficacia de la conducta preventiva, y (4) el nivel de confianza en la propia capacidad para llevar a cabo el comportamiento preventivo recomendado.

3. La Teoría del Enlace Social: describe que los vínculos que las personas tienen con su grupo u organización (apego, compromiso, participación y normas personales) reduce la posibilidad de entrar en comportamientos antisociales o que conduzcan a vulneraciones.

4. La Teoría de la Acción Razonada: permite la predicción de comportamiento, sugiere que cuanto más fuerte sea la intención de involucrarse en un comportamiento, mayor será la probabilidad de que se lleve a cabo.

5. La Teoría Social Cognitiva: explica el comportamiento humano y la interacción simultánea y dinámica entre factores sociales y personales, postula que los individuos están activamente comprometidos en su propio desarrollo y obtener los resultados deseados cuando creen que sus acciones están bajo su propio control.

6. La Teoría de la Evaluación Cognitiva: sirve para predecir los efectos perjudiciales de las recompensas sobre la motivación intrínseca, cuando se interpretan como una herramienta para controlar el comportamiento, en contraposición con los efectos positivos de las recompensas verbales.

Dada la naturaleza de las instituciones educativas y los actores que se desenvuelven en ellas (profesores, directivos, personal administrativo), las teorías que parecieran ajustarse y aprovecharse más para el diseño de un plan de ciberseguridad son: la b) Teoría de Protección de Motivación y la c) Teoría del Enlace Social.

En cuanto a la Teoría de Protección de Motivación:

1. La percepción de la gravedad de la amenaza: puede abordarse en jornadas de formación a través de casos de estudio sobre situaciones de robos de datos que han ocurrido en algunas instituciones educativas, con sus correspondientes causas y consecuencias.

2. La probabilidad percibida de la vulnerabilidad: con base en la discusión anterior, realizar un diagnóstico desde el espacio de cada uno de los actores, sobre las condiciones en que se encuentra la institución en materia de ciberseguridad (Conocimiento de los principios y normas básicas; recolección, uso y procesamiento de los datos; entre otros).

3. La eficacia de la conducta preventiva: una vez realizado el diagnóstico, se deben categorizar y sistematizar los resultados, a fin de establecer las condiciones de vulnerabilidad y riesgo presentes en la institución educativa, y tomar las medidas correctivas (formación teórica, práctica, técnica) en cada caso a corto, mediano y largo plazo.

4. El nivel de confianza en la propia capacidad para llevar a cabo el comportamiento preventivo recomendado: sin duda a partir del establecimiento de la medidas anteriores el desenvolvimiento de las labores individuales y colectivas contribuirán a un clima de confianza y seguridad personal y académica.

Como consecuencia de lo anterior, respecto a la Teoría del Enlace Social se incrementarán los vínculos de comunicación de los profesores, directivos y demás personal administrativo, entre ellos mismos y con su institución. Generando apego, compromiso y corresponsabilidad entre el comportamiento personal y colectivo, para reducir los riesgos y vulneraciones de la información personal y académica procesada.

En este mismo orden de ideas, una vez sensibilizado el personal para el diseño del Plan de ciberseguridad de la institución educativa bajo la asesoría de especialistas en sistemas informáticos, podrían seguirse los pasos que señala Altamirano y Oré (2008) para desarrollar una política de seguridad:

1. Análisis y valoración de riesgos, mediante una fase de diagnóstico inicial. El objetivo de esta fase es determinar el grado de cumplimiento de las normas mínimas de ciberseguiridad recomendadas por los especialistas según principios internacionales.

2. Construcción de la política: se realiza el análisis de riesgos y se determina la aplicabilidad, de acuerdo a los resultados obtenidos y se define la documentación necesaria para dar cumplimiento a los requisitos normativos según las características particulares, con el fin de cubrir el 100 % de las vulnerabilidades institucionales, asociadas a temas de mejoramiento y sostenibilidad de su infraestructura.

3. Implementación de la política: en esta fase se ponen en práctica todas las recomendaciones de los especialistas en ciberseguridad, gestionando la operación del plan de tratamiento de riesgos y la aplicación de los controles establecidos. Acompañado de un proceso de reflexión y socialización de los riesgos a los cuales se encuentra expuesta la institución con todo el personal en términos de la vulnerabilidad de la información sensible de todos los actores involucrados.

4. Mantenimiento de la política: se realizan supervisiones internas y revisiones por parte de los especialistas y directivos para verificar el desempeño y mejora de las políticas de seguridad en la institución.

5. Implicación del componente humano: finalmente se revisan los resultados de la fase anterior, permitiendo el análisis de las dificultades, causas para las desviaciones o no conformidades encontradas, de tal manera que los planes de mejoramiento se conviertan en acciones contundentes que impidan la repetición de acciones que conduzcan a riesgos en materia de ciberseguridad.

Desafíos y oportunidades de la educación en ciberseguridad

Según Tiglla (2024) los principales desafíos que enfrenta la educación en varios países de América Latina en términos de ciberseguridad están relacionados con aspectos que abren nuevas brechas:

1. Económicos: escasos recursos financieros que dificultan la adquisición Hardware: y software, que permitan robustecer las infraestructuras y sistemas de seguridad de la institución, para blindar la información que recopilan y procesan.

2. Humanos: dificultad para contratar personal especializado (administradores de sistemas) para la gestión (permisos de acceso, disponibilidad, mantenimiento y solución de problemas técnicos).

3. Servicios: de electricidad e interconectividad baja (con constantes interrupciones, y ancho de banda insuficiente).

Sin embargo, tal como se ha descrito en las secciones anteriores, en el ámbito educativo a la par de estas dificultades, se pueden ir desarrollando habilidades en: formación de competencias digitales (Integración curricular en cuanto al manejo y uso seguro de la información); formación técnica (actualización periódica de al menos una parte del personal con conocimientos en el área de informática); investigación y desarrollo (de planes y políticas de ciberseguridad que permitan un manejo más ético, eficiente y seguro de los datos académicos); establecimiento de alianzas estratégicas (para generar y optimizar los recursos, trabajar colaborativamente, y adaptarse con mayor facilidad a los constantes cambios tecnológicos y sociales).

En este último aspecto, es crucial considerar el uso y desarrollo de Tecnologías Libres, pues permiten incorporar elementos de seguridad en los sistemas de las instituciones, tal como lo señalan Mora et al. (2014, p.38), entre estas potencialidades se incluyen:

1. La capacidad de analizar y estudiar las tecnologías subyacentes a las aplicaciones.

2. La posibilidad de auditar los programas fuentes (código escrito en un lenguaje de programación).

3. La frecuente corrección de errores y publicación de software gracias al apoyo de comunidades de usuarios y desarrolladores alrededor de las aplicaciones y herramientas.

4. El rompimiento del paradigma de la seguridad por obscuridad el cual determina que el funcionamiento de procedimientos de seguridad (criptográficos) deben ser secretos y por lo tanto la seguridad solo reside en la capacidad de ocultar su funcionamiento y no las claves.

Reflexiones finales

Ciertamente, los altos costos para la adquisición de hardware y software especializado y la baja capacitación del personal en las instituciones educativas, incrementan las debilidades en el conocimiento de estas nuevas tecnologías para el manejo, procesamiento y resguardo de la información; cuestiones que desencadenan en un uso limitado y más vulnerable a ataques cibernéticos que pueden provenir de fuentes internas o externas, debido a factores técnicos, naturales o humanos. Justamente este tipo de situaciones de orden económica hacen mucho

más necesario el uso y desarrollo de Tecnologías Libres, que permitan incorporar elementos de seguridad en los sistemas de las instituciones, y aprovechar al máximo sus recursos humanos al analizar y estudiar las tecnologías subyacentes a las aplicaciones, corregir y adaptar los software gracias al apoyo de comunidades de usuarios y desarrolladores, estableciendo alianzas estratégicas.

Por tales razones, la educación en ciberseguridad es primordial, porque además de proteger a los niños desde temprana edad de distintos riesgos en las redes sociales, los va formando como seres responsables y conscientes del buen uso de la tecnología, críticos ante los contenidos que se les pueden presentar y cautos con la información que ceden en Internet. Así, la escuela, familia y comunidad juegan un papel fundamental en el desarrollo de competencias digitales.

Adicionalmente, es fundamental la capacitación y formación permanente sobre medidas y prácticas de ciberserguridad, de los profesores y demás personal que labora en las instituciones educativas, para que además de formar a los estudiantes los apliquen ellos mismos y eviten riesgos personales e institucionales, debido a la exposición incauta y excesiva de datos en los diversos sistemas en los que procesan la información y en las redes sociales.

En suma, se recomienda en la medida de lo posible la implementación de aplicaciones de seguridad basados en Inteligencia Artificial (IA) por medio del análisis de comportamiento y la detección de patrones de comportamiento, que ayuden a detectar y bloquear posibles intentos de robo de datos provenientes de mensajes de textos, correos, aplicaciones falsas y redes sociales. Fomentando buenas prácticas como: establecer múltiples factores para el acceso y autenticación, uso de navegadores más seguros, descarga de aplicaciones en sitios oficiales, entre otras.

Finalmente, considerando que aunque las organizaciones implementan políticas de seguridad para la protección de su información, se producen vulnerabilidades debido a los diferentes roles que desempeña su personal, cada uno tendrá un efecto y consecuencia diferente dependiendo del rol y funciones que ejecuta. En el caso de la educación, dada su naturaleza, los actores que se desenvuelven en ellas, y los procesos académicos y administrativos que desarrollan, las teorías que parecieran ajustarse y aprovecharse más para el diseño de un plan de ciberseguridad son: la b) Teoría de Protección de Motivación y la c) Teoría del Enlace Social.

Referencias

Altamirano, J., y Oré, S. (2008). *Seguridad de la información. Redes, informática y sistemas de información*. Ediciones Paraninfo. ISBN:978-84-9732-502-8.

Altamirano, J., y Oré, S. (2017). Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento. *Revista Ibérica de Sistemas E Tecnologias de Informação*, *25*, 112-134. https://doi.org/10.17013/risti.25.112-134

Arias, A., y Vargas, M. (2025). Introducción a la Inteligencia Artificial y el Aprendizaje Automático en Ciberseguridad. *Revista Colón Ciencias, Tecnología y Negocios*, *12*(1), 32-48. https://revistas.up.ac.pa/index.php/revista_colon_ctn/article/view/6824/5264

Arreola, M. (2019). *Ciber-Seguridad ¿Por qué es importante para todos?* Siglo XXI Editores. ISBN:978-607-03-1041-6.

Benavides, A., y Blandón, C. (2018). Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico. *Scientia Et Technica*, *23*(1), 85-92. https://www.redalyc.org/articulo.oa?id=84956661012

Campos, V., Bastidas, K., Bastidas, D., y Alvarado, S. (2024). Fortalecimiento de la seguridad cibernética en universidad mediante inteligencia artificial para la detección de amenazas. *Revista Social Fronteriza*, *5*(1). https://doi.org/10.59814/resofro.2025.5(1)607

Chilquina, B., y Garcés, E. (2025). Propuesta de seguridad para protección contra amenazas de phishing en usuarios de dispositivos móviles android. *Journal Scientific*, *9*(1), 1-13. https://www.investigarmqr.com/2025/index.php/mqr/article/view/156/6607

García, A., Salvador, L., Casillas, S., y Gómez, V. (2019). Evaluación de las competencias digitales sobre seguridad de los estudiantes de Educación Básica. *Revista de Educación a Distancia*, *5*(61). https://revistas.um.es/red/article/view/398031/273721

García, J., Huicab, Y., Landeros, K., y Vargas, T. (2019). Transformando la educación en ciberseguridad: integrando tecnología educativa para formar profesionales resilientes en la universidad. *Ava Cient*, *5*(1), 22-32. http://avacient.chetumal.tecnm.mx/index.php/revista/article/view/49/50

Herrera, D., Mendoza, T., León, L., Zambrano, M., y Nuñez, A. (2025). La importancia de la educación en ciberseguridad para niños. *Digital Publisher*, *1*(2), 5-19. https://www.593dp.com/index.php/593_Digital_Publisher/article/view/2952/2422

Jimenez, k. (2025). Escudo Digital - un curso interactivo de ciberseguridad para la Unidad Educativa Isaac Jesús Barrera. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades*, *6*(1), 554-560. https://doi.org/10.56712/latam.v6i1.3358

Mora, E., Araujo, A., Bravo, V., Sumoza, R., Contreras, J., y Quintero, D. (2014). *Seguridad informática y la identidad digital. Fundamentos y Aportes*. CENDITEL. https://convite.cenditel.gob.ve/libros/

Morales-Sáenz, F., Medina-Quintero, J., y Abrego-Almazán, D. (2025). Ciberseguridad en instituciones de educación superior: un análisis desde la perspectiva de la teoría de la motivación de protección. *Revista de Investigación Educativa de la REDIECH*, *16*(e2271). https://doi.org/10.33010/ie_rie_rediech.v16i0.2271

Tiglla, B. (2024). Ciberseguridad en educación y política: Desafíos éticos y tecnológicos. *Horizon International Journal*, *2*(1). https://editorialsphaera.com/index.php/hor/article/view/44/111

Torres, D. (2025). *Desarrollo de un marco de ciberseguridad para Unidad Educativa Virtual Zúrich Science* [Tesis de Maestría]. Universidad Estatal Península de Santa Elena. Ecuador. https://repositorio.upse.edu.ec/bitstream/46000/13094/1/UPSE-MCI-2025-0018.pdf

Drones y Ciberseguridad en la enseñanza de la Ingeniería Civil

María Eugenia Acosta[1]

Introducción

En tiempos recientes, la ingeniería civil ha experimentado una transformación notable, motivada por la incorporación progresiva de tecnologías emergentes que permiten optimizar procesos, reducir riesgos y ampliar las posibilidades de análisis y ejecución de obras. Entre estas innovaciones, el uso de vehículos aéreos no tripulados, comúnmente conocidos como drones, ha adquirido una relevancia sin precedentes. Su diversa aplicabilidad en la industria de la construcción ha convertido a esta herramienta en un recurso indispensable para empresas y profesionales del sector.

Lo que en un principio fue visto como un equipo de uso militar, una curiosidad tecnológica o un accesorio de elevado costo, hoy se considera un instrumento eficiente y accesible, útil para recolectar información crítica con una rapidez, precisión y nivel de detalle impensables en métodos tradicionales y que anteriormente requerían largas jornadas de trabajo en campo. Además, gracias a la combinación de cámaras RGB, térmicas, multiespectrales y sensores LiDAR, los drones hacen posible obtener capas de información que pueden ser procesadas para diagnosticar fallas estructurales, detectar filtraciones o modelar escorrentías pluviales con alto nivel de predicción.

Aun así, este panorama optimista trae consigo una serie de retos poco discutidos en el ámbito de la ingeniería tradicional. Uno de ellos, quizá el más subestimado, es el que concierne a la ciberseguridad. La mayoría de las operaciones con drones implican la captura de datos, su almacenamiento en dispositivos móviles, servidores locales o plataformas en la nube; su procesamiento mediante software especializado (frecuentemente con conexión a internet); y, finalmente, su interpretación para la toma de decisiones técnicas. Todo este flujo de información, que abarca desde el vuelo inicial hasta los resultados, representa un sistema vulnerable a múltiples tipos de amenazas digitales.

Los datos generados por drones no son neutros ni inocuos. Constituyen activos de alto valor que pueden revelar el estado estructural de una obra, la planificación urbana de un territorio, la ubicación exacta de recursos estratégicos o incluso el cronograma de actividades de una empresa constructora. En manos equivocadas, esta información puede ser utilizada con fines maliciosos, desde sabotajes industriales hasta espionaje corporativo. De allí que la ciberseguridad en la operación de drones no deba ser un tema

[1]Ingeniero Civil egresada del Instituto Universitario Politécnico Santiago Mariño (IUPSM), MSc. en Educación Superior mención Docencia Universitaria, Doctora en Ciencias de la Educación. Actualmente se desempeña como docente en la UPTM Kléber Ramírez, y como investigadora en el Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL). macosta@cenditel.gob.ve

marginal ni delegado exclusivamente al área tecnológica de una empresa: debe ser parte integral de la cultura profesional de quien diseña, planifica o ejecuta obras de infraestructura.

Desde esta posición, resulta preocupante constatar que la mayoría de los planes de estudio de la carrera profesional de ingeniería civil en Latinoamérica y otras regiones aún mantienen un enfoque clásico, centrado en el cálculo estructural, la hidráulica, la vialidad y la planificación de obras; pero sin incorporar de forma sistemática contenidos relacionados con la gestión de datos, la ética digital o la protección de la información técnica. Es decir, se forman ingenieros capaces de operar tecnología avanzada, sin la preparación adecuada para manejar los riesgos asociados a la exposición digital que esto significa.

La creciente dependencia de la tecnología sin una preparación adecuada en ciberseguridad crea una brecha de conocimiento crítica. No se trata simplemente de añadir una materia optativa o realizar un curso aislado sobre seguridad informática o de la información; el objetivo es promover una cultura de ciberseguridad en la formación del Ingeniero Civil, fomentando una conciencia permanente de que toda tecnología requiere responsabilidades, y que la integridad de los datos no es un asunto ajeno a la práctica profesional, debe entenderse como un componente esencial del ejercicio ético y competente de la ingeniería.

La urgencia de abordar esta temática trasciende lo teórico. Ya existen antecedentes documentados de filtración de datos en plataformas de mapeo digital, manipulación de modelos 3D generados por drones, ataques a redes de transmisión de datos en obras públicas, y errores graves por uso de software no actualizado o mal protegido. Estos eventos generan pérdidas económicas considerables y pueden comprometer la seguridad física de las personas si se manipulan o distorsionan datos sobre el estado de una obra de construcción.

Ahora bien, el auge de la inteligencia artificial y la automatización en los sistemas de análisis topográfico, inspección automatizada o mantenimiento predictivo de estructuras conlleva a nuevos niveles de exposición. Si los algoritmos que procesan la información captada por drones son susceptibles de ser intervenidos, sesgados o replicados maliciosamente, los riesgos se multiplican. La ingeniería civil, entonces, deja de ser únicamente una disciplina técnica orientada al diseño y la construcción de obras físicas para convertirse en una profesión inmersa en entornos híbridos físico-digitales, donde la gestión segura de la información adquiere la misma relevancia que la resistencia de un material o la estabilidad de un terreno.

Este artículo se propone justamente abrir esa discusión: ¿Cómo formar ingenieros civiles conscientes del valor y los riesgos de los datos que utilizan en sus prácticas profesionales? ¿Qué competencias deben incorporarse en los programas de formación para cerrar esta brecha? ¿Cómo se construye una cultura de ciberseguridad desde la universidad, en diálogo con la práctica laboral y las exigencias normativas? ¿Qué principios éticos deben guiar la captura, el procesamiento y el almacenamiento de información sensible mediante tecnologías como los drones?

Desde esta perspectiva, se plantea que uno de los grandes desafíos para las próximas generaciones de profesionales es dominar las herramientas tecnológicas emergentes y comprender los marcos legales, técnicos y culturales que rodean la producción de datos en contextos complejos. La formación del Ingeniero Civil debe orientarse hacia un perfil más integral, que combine la capacidad técnica con una alfabetización digital crítica, una ética profesional sólida y una sensibilidad ante los impactos ambientales y sociales de sus decisiones.

El uso de drones en la ingeniería civil no solo representa una innovación eficiente o un avance tecnológico, además, es una oportunidad para revisar los marcos conceptuales de la enseñanza de esta disciplina. Es vital formar a profesionales que comprendan que los datos además de recopilarse deben protegerse; asimismo, entender que las herramientas automatizadas no disminuyen la responsabilidad humana, más bien la redefinen. En efecto, la seguridad de una obra debe ser evaluada tanto en términos de resistencia mecánica como de su integridad digital.

Esta reflexión adquiere aún más relevancia si se considera el crecimiento acelerado de proyectos de infraestructura en zonas urbanas vulnerables, donde las condiciones de seguridad física, social y tecnológica se entrelazan de forma crítica. En estos contextos, el mal uso o la filtración de datos puede generar conflictos, desinformación o incluso retrasos en la ejecución de obras prioritarias. El diseño de políticas públicas de infraestructura también se ve afectado por la calidad y veracidad de la información técnica disponible. Por lo tanto, asegurar los datos desde su origen, es decir, desde el momento en que un dron sobrevuela una zona para capturar imágenes, es una responsabilidad profesional ineludible.

Este conjunto de antecedentes —históricos, técnicos y normativos— proporciona el marco conceptual para comprender el impacto transformador que los drones han tenido en la ingeniería civil contemporánea. A partir de esta base, el artículo se adentra en un recorrido que comienza explorando al dron como una fuente estratégica de datos críticos, detallando el tipo de información que produce, las herramientas empleadas para su procesamiento y las implicaciones técnicas de su uso en obras de distinta envergadura. Posteriormente, se analizan las vulnerabilidades relacionadas a la gestión de estos datos, tanto desde una perspectiva tecnológica como desde la óptica de la protección de la privacidad y la integridad de la información.

Este análisis se complementa con la presentación del marco normativo venezolano que regula el manejo y resguardo de la información digital, estableciendo las responsabilidades y obligaciones que deben cumplir los profesionales e instituciones que trabajan con este tipo de tecnologías. Finalmente, se aborda la dimensión educativa, subrayando la urgencia de integrar la ciberseguridad como eje transversal en el perfil del Ingeniero Civil. Se plantea que el conocimiento técnico debe ir de la mano con competencias éticas, legales y digitales, de manera que los futuros profesionales dominen el uso de drones y las plataformas asociadas, y también estén preparados para garantizar la seguridad y el uso responsable de los datos en un entorno cada vez más interconectado. De esta forma, el capítulo ofrece una visión

integral que vincula innovación, responsabilidad y cultura de ciberseguridad como pilares para el ejercicio profesional en el siglo XXI.

Los drones como agentes de transformación tecnológica en la ingeniería civil

Recientemente, la industria de la construcción y la ingeniería civil ha sido testigo de un proceso acelerado de evolución digital, impulsado por la incorporación de tecnologías emergentes que redefinen la forma en que se conciben, planifican y ejecutan los proyectos de infraestructura. Entre estas tecnologías, los drones —también conocidos como vehículos aéreos no tripulados (UAV, por sus siglas en inglés)— han irrumpido como herramientas de vanguardia que permiten abordar con mayor precisión, eficiencia y seguridad los retos técnicos y logísticos del sector.

Acerca de ello, Acosta (2023) afirmó que "la adopción de drones en la industria de la construcción ha desencadenado una transformación significativa en la forma en que se concibe, planifica y ejecutan proyectos de construcción y mantenimiento de infraestructuras" (p. 142). Esta aserción señala un cambio técnico y cultural, que abarca desde la captura de datos hasta la toma de decisiones operativas, dado que los drones se han convertido en aliados estratégicos para la ingeniería civil, ofreciendo una visión integral de las obras en tiempo real. Aparte de la simple captura de imágenes aéreas, aportan información capaz de alimentar modelos digitales, respaldar la verificación de la calidad constructiva y anticipar posibles riesgos ambientales o estructurales. Su mayor fortaleza radica en transformar observaciones rápidas en datos técnicos confiables que facilitan decisiones precisas y oportunas en los proyectos.

El desarrollo histórico de los drones hace posible comprender cómo pasaron de ser artefactos de uso militar a convertirse en herramientas especializadas para múltiples industrias. Según Gross (2023), los primeros aviones sin piloto datan de principios del siglo XX, pero su desarrollo se aceleró durante la Segunda Guerra Mundial con fines de reconocimiento aéreo. No fue sino hasta finales del siglo XX y comienzos del XXI, con los avances en electrónica, GPS y telecomunicaciones, que comenzaron a diversificarse y ser incorporados en sectores como la agricultura, el cine, la vigilancia y, especialmente, la ingeniería y la construcción.

La construcción, área tradicionalmente centrada en técnicas manuales y trabajo de campo, encontró en los drones una oportunidad para facilitar tareas críticas. En palabras de Acosta (2023), "estos dispositivos han demostrado ser una herramienta invaluable para agilizar los procesos y mejorar la toma de decisiones en el sector de la construcción" (p. 146). Esta afirmación se sostiene al observar la creciente demanda de los drones con cámaras de alta resolución, sensores multiespectrales, térmicos, LiDAR y softwares especializados que ofrecen la posibilidad de levantar mapas tridimensionales, detectar fallas estructurales, supervisar obras y evaluar el impacto ambiental de grandes proyectos.

En términos técnicos, los drones empleados en ingeniería civil pueden clasificarse, según Negrín (2018), por su configuración (ala fija o multirrotor) y tamaño. Los de ala fija son ideales para el levantamiento de grandes extensiones de terreno, gracias a su autonomía y capacidad de cobertura. Los multirrotores, en cambio, ofrecen mayor estabilidad en vuelo estacionario y maniobrabilidad en espacios confinados, características que los hace útiles en la inspección de estructuras como puentes, túneles o fachadas.

El desarrollo de baterías más eficientes, la mejora en la estabilidad de vuelo y el incremento en la capacidad de carga han sido factores determinantes para ampliar las aplicaciones de los drones. Hoy día, estos dispositivos pueden incorporar sensores que captan datos en diferentes formatos, una idea que refuerza esto es la de Reuter y Pedenovi (2019), quienes destacan que esta diversidad de sensores es capaz de obtener desde imágenes visuales hasta modelos 3D y mapas de calor, todos ellos fundamentales en la toma de decisiones en obras civiles.

Asimismo, la industria ha adoptado herramientas de software especializadas para procesar la información captada por drones. Knisely (2020) explica que, dependiendo de los sensores y del software que se elija se pueden generar productos, como por ejemplo en topografía: ortomosaicos, nubes de puntos, modelos digitales del terreno (MDT), modelos digitales de superficie (MDS), curvas de nivel y mapas multiespectrales. Esta variedad de datos hace viable a los equipos técnicos optimizar la planificación, ejecución y control de obras con un grado de detalle y precisión inédito en la historia de la ingeniería.

En particular, entre los principales usos de drones en la construcción destacan la inspección de estructuras, el monitoreo de obras, la evaluación del impacto ambiental, la optimización logística, la supervisión de seguridad y la integración con sistemas de realidad aumentada y virtual. Estas funciones mejoran la calidad del trabajo técnico, reducen riesgos laborales, ahorran tiempo y disminuyen costos operativos. Como señala Acosta (2023), los drones “pueden detectar peligros inminentes y alertar a los trabajadores para evitar lesiones. Igualmente, monitorizan el cumplimiento de normas de seguridad y protocolos en el lugar de trabajo” (p. 123).

Conviene destacar que la adopción de drones en todo el proceso que implica la construcción de una obra marca una era de innovación sin precedentes. Al transformar la captura de datos en información accionable, estas herramientas optimizan la eficiencia, los costos de los proyectos, elevan los estándares de seguridad y precisión en cada fase. De este modo, se consolidan como pilares en la digitalización del sector, redefiniendo la manera en que se construyen y mantienen las infraestructuras para un futuro más inteligente y seguro.

El dron como fuente de datos críticos

La evolución y transformación tecnológica consecuencia del uso de los drones en el sector de la construcción, ha hecho posible que los profesionales del área cuenten con información de alta precisión, obtenida con rapidez y en condiciones que serían riesgosas o muy costosas

si se emplearan métodos tradicionales. No obstante, la masificación de esta tecnología también ha traído nuevos desafíos relacionados con el manejo, resguardo y protección de los datos que se generan.

Tal como expone Sardanyés (s.f), "los drones pueden representar una amenaza significativa para la ciberseguridad, no solo por su capacidad para recolectar datos de manera no autorizada, sino también por su potencial para ser utilizados como herramientas para comprometer la seguridad de redes y sistemas". En este contexto, resulta esencial comprender qué tipo de datos recolectan los drones, cómo se procesan y almacenan, y cuáles son los riesgos asociados a su uso en obras civiles, a continuación se describen:

Tipos de datos recolectados por drones en ingeniería civil

Los drones utilizados en proyectos de ingeniería civil no son simples dispositivos voladores con una cámara; son plataformas que integran una variedad de sensores capaces de captar diferentes tipos de información según los objetivos del proyecto. Los datos más comunes recolectados incluyen:

- **Imágenes RGB de alta resolución** Las imágenes captadas desde el aire hacen posible documentar el estado actual de un terreno, estructura o zona de construcción. Su calidad y detalle son suficientes para crear modelos 3D, ortofotos y modelos fotogramétricos.
- **Modelos 3D y nubes de puntos:** Mediante técnicas de fotogrametría o escáneres LiDAR (Light Detection and Ranging), los drones pueden crear representaciones tridimensionales precisas de terrenos, edificaciones, túneles o cualquier infraestructura, facilitando la compresión y análisis del proyecto. Tales modelos se usan para calcular volúmenes de corte y relleno, planificar excavaciones y evaluar el avance de obras.
- **Imágenes multiespectrales:** Las imágenes multiespectrales capturan información en diferentes longitudes de onda, más allá del espectro visible, útiles para evaluar la salud de la vegetación, la presencia de humedad, la calidad del agua, el deterioro de materiales y otros aspectos ambientales. Son especialmente eficaces en evaluaciones de impacto ambiental, estudio de cuencas y en el mantenimiento preventivo de infraestructuras.
- **Mapas térmicos:** Gracias a sensores infrarrojos, los drones pueden detectar diferencias de temperatura en superficies, lo cual facilita la identificación de problemas como fugas de calor, filtraciones de agua, zonas de pérdida de energía o fallos estructurales indetectables a simple vista.
- **Datos georreferenciados:** Todos estos datos están vinculados a coordenadas espaciales, gracias al uso de sistemas GNSS de alta precisión. Con ello se puede integrar la información en Sistemas de Información Geográfica (SIG) y desarrollar mapas precisos, lo que resulta fundamental para la toma de decisiones en proyectos a gran escala.

- **Videos en tiempo real:** En operaciones de supervisión o inspección, los drones pueden transmitir video en vivo para monitorear el sitio de construcción e identificar riesgos potenciales, y en consecuencia mejorar la seguridad laboral. A su vez, el equipo técnico tiene la opción de tomar decisiones de manera remota e inmediata.

Herramientas de procesamiento y almacenamiento

La etapa posterior al vuelo es tan crucial como la recolección de datos. Tras su obtención, deben ser procesados, analizados y almacenados. La calidad del análisis final dependerá en gran medida de la integridad de los datos y de la plataforma utilizada para su interpretación.

- **Software de fotogrametría y modelado 3D:** Aplicaciones como Pix4D, Metashape (anteriormente Agisoft), DroneDeploy o RealityCapture, transforman el producto captado en modelos tridimensionales, ortomosaicos, curvas de nivel o mapas de calor. Tales programas emplean algoritmos avanzados que correlacionan miles de puntos comunes entre fotos para construir representaciones realistas.
- **Sistemas de Información Geográfica (SIG):** Los datos georreferenciados pueden ser integrados en plataformas como ArcGIS, QGIS o Bentley ContextCapture, para realizar análisis espaciales, diseñar trazados de obras o superponer diferentes capas de información.
- **Plataformas de Inteligencia Artificial (IA):** En etapas más avanzadas, algunos proyectos integran algoritmos de aprendizaje automático para detectar patrones o anomalías en los datos recolectados, como fisuras en estructuras o deformaciones en el terreno.
- **Almacenamiento en la nube:** Muchos sistemas procesan los datos en plataformas remotas como Amazon Web Services (AWS), Microsoft Azure, Google Cloud y servicios de almacenamiento en la nube de proveedores de software de drones. Dichas nubes hacen posible trabajar de manera colaborativa y escalar el procesamiento, aun cuando introducen riesgos de seguridad si no se gestionan apropiadamente.
- **Aplicaciones móviles y web:** Herramientas como DroneDeploy o DJI Terra ofrecen interfaces intuitivas para planificar vuelos, revisar mapas y compartir resultados desde dispositivos móviles. Aunque cómodas, estas aplicaciones requieren estrictos protocolos de autenticación y cifrado.
- **Bases de datos locales y copias de seguridad:** En algunos entornos, especialmente donde la conectividad es limitada, se opta por el almacenamiento en servidores locales o discos duros externos, lo que conduce a otras prácticas de seguridad digital, como el cifrado y la redundancia de datos.

Aspectos complementarios

- **Integración con sistemas existentes:** Es conveniente elegir herramientas que se integren fácilmente con los sistemas existentes en la organización, como sistemas

de gestión de activos, sistemas de información geográfica y software de gestión de proyectos.

- **Capacidad de procesamiento:** Seleccionar herramientas con la capacidad de procesamiento necesaria para manejar el volumen y la complejidad de los datos generados por los drones, especialmente cuando se trabaja con grandes conjuntos de datos o se requieren análisis complejos.
- **Facilidad de uso:** Optar por herramientas con interfaces intuitivas que sean sencillas de usar para el personal, reduciendo la necesidad de capacitación extensa y adopción rápida.
- **Seguridad:** Considerar la seguridad de los datos almacenados, especialmente cuando se trata de información confidencial, eligiendo herramientas con protocolos de seguridad robustos y opciones de almacenamiento seguro.

Con base en lo descrito, se evidencia que el uso de drones en la ingeniería civil no puede desligarse del concepto de ciberseguridad. La información generada es tan valiosa como los diseños estructurales o los presupuestos, y por lo tanto debe estar protegida mediante prácticas adecuadas de administración de datos, control de accesos, cifrado, auditorías digitales y formación del personal involucrado. Para ello, Cornejo y Clavel (2024) señalan que "se requieren comunicaciones seguras y confiables, así como una sofisticada gestión de identidad y acceso para máquinas, dispositivos y usuarios" (p. 67).

A medida que se expanda el uso de drones en el sector, también lo hará el volumen y la complejidad de los datos generados. Por eso, se requiere que los profesionales del área comprendan que el dominio de esta tecnología no se limita a saber pilotar un dron o procesar un modelo en el software adecuado, implica formación académica para desarrollar una conciencia crítica sobre la seguridad, la confidencialidad y la trazabilidad de la información digital que hoy forma parte esencial del quehacer de la industria. Se deben utilizar sistemas avanzados de gestión de identidad y acceso para garantizar canales de comunicación protegidos y confiables e implementar soluciones preventivas y sistemas de defensa contra los efectos perjudiciales de los ataques a los sistemas de información (Cornejo y Clavel, 2024, p. 67).

Vulnerabilidades asociadas a los datos generados por drones

La progresiva integración de drones en proyectos de construcción ha ampliado las capacidades técnicas del sector y en consecuencia su exposición a riesgos digitales. En la medida en que estos dispositivos capturan, almacenan y transmiten grandes volúmenes de información crítica, se convierten en puntos débiles dentro del ecosistema digital de una obra. Comprender estas vulnerabilidades es relevante desde la perspectiva técnica y esencial desde la formativa, por ello los futuros ingenieros deben estar preparados para prevenir, detectar y mitigar estos riesgos con criterio profesional y ético.

Una primera vulnerabilidad se encuentra en el momento mismo de la captura de datos, es fundamental que el acceso a los sistemas de control del dron requiera autenticación multifactor (MFA), esto garantiza que solo el personal debidamente autorizado pueda operarlo o interactuar con él (Sardanyés, s.f).

Otra importante debilidad, es que muchos drones comerciales emplean sistemas de transmisión de imágenes en tiempo real, utilizando protocolos de comunicación inalámbrica que, si no están adecuadamente cifrados, pueden ser interceptados por terceros. Para proteger la comunicación del dron, es indispensable que todos los datos (comandos de control, información de vuelo, video e imágenes) se transmitan con cifrado de extremo a extremo. Asimismo, las conexiones Wi-Fi deben limitarse a redes seguras que utilicen estándares como WPA3, descartando cualquier protocolo inseguro (Sardanyés, s.f). En contextos de obras públicas, infraestructura crítica o instalaciones estratégicas, esta exposición puede traducirse en riesgos de seguridad nacional o espionaje industrial.

Por otra parte, en el proceso de almacenamiento y procesamiento, los datos son comúnmente trasladados desde el dron hacia dispositivos móviles, computadoras o servidores remotos. Para evitar riesgos asociados a la integridad y confidencialidad de la información, se debe incorporar sistemas de detección de intrusiones (IDS) diseñados para identificar alguna actividad inusual o intentos de acceso no autorizados. Adicionalmente, es obligatorio el uso de herramientas de monitoreo en tiempo real para vigilar el comportamiento del dron y detectar rápidamente acciones sospechosas, como intentos de interferencia o secuestro (Sardanyés, s.f).

Por ejemplo, si un modelo digital de terreno es manipulado sin autorización, las decisiones constructivas derivadas podrían tener consecuencias estructurales o legales graves. Más aún, si la plataforma utilizada para procesar los datos en la nube no cuenta con políticas sólidas de ciberseguridad, los archivos pueden quedar expuestos a ataques externos.

Un riesgo adicional, es el relacionado con la suplantación de identidad digital. Las plataformas de planificación de vuelo y análisis de datos suelen operar mediante cuentas personales o institucionales. Si estas cuentas no utilizan métodos robustos de autenticación (como la verificación en dos pasos), pueden ser objeto de un acceso no autorizado, permitiendo a actores maliciosos obtener información e incluso alterar rutas de vuelo, acceder a datos sensibles o sabotear las operaciones.

Otra vulnerabilidad crítica radica en la dependencia de software de terceros, cuyas actualizaciones, licencias o condiciones de uso pueden cambiar repentinamente. Algunos programas gratuitos o de bajo costo empleados para procesamiento de imágenes, modelado 3D o planificación de vuelo, no cuentan con auditorías externas ni garantizan el resguardo de los datos del usuario. De esta manera, se introduce un riesgo indirecto que compromete la trazabilidad y legalidad de la información generada en entornos de ingeniería. Por ello, la seguridad de los drones depende en gran medida de tener su firmware y software actualizados con regularidad, lo que cierra posibles brechas de seguridad. Asimismo, un paso

fundamental antes de cualquier actualización es comprobar que los archivos descargados no hayan sido manipulados, asegurando así su integridad (Sardanyés, s.f).

Un punto adicional clave es resguardar físicamente los drones cuando no estén en uso, para prevenir el robo o la manipulación no autorizada, lo que implica guardarlos en lugares seguros y limitar el acceso a ellos. Sumado a ello, es recomendable deshabilitar los puertos que no se utilicen y proteger las conexiones físicas para evitar la inserción de algún dispositivo malicioso.

Igualmente, es importante considerar el riesgo de fugas internas de información. En obras donde participan múltiples contratistas, técnicos y operadores, los datos captados por drones pueden pasar por varias manos sin que existan protocolos claros de gestión, clasificación o resguardo. La falta de políticas de administración de datos puede dar lugar a filtraciones accidentales, pérdidas de archivos o usos indebidos, especialmente si no se cuenta con mecanismos de control de acceso o trazabilidad de modificaciones. Sobre el particular, Sardanyés (s.f) especifica la necesidad de implementar políticas estrictas para su manejo y operación, abarcando directrices de ciberseguridad y privacidad de datos, conjuntamente, con un plan de acción ante incidentes, para manejar cualquier vulneración de seguridad, buscando reducir los daños y restablecer el control lo antes posible, en caso de una eventualidad.

Según se ha detallado, todos estos riesgos exigen una respuesta que combine herramientas técnicas y una cultura profesional dirigida a la protección de los datos. No basta con implementar sistemas de cifrado, respaldo o contraseñas complejas; urge que los equipos de trabajo estén formados en buenas prácticas de ciberseguridad, que comprendan la importancia de resguardar la integridad de los datos y que reconozcan los posibles escenarios de ataque.

Por ello, desde el enfoque educativo de los profesionales de la construcción, resulta fundamental señalar que muchos de estos riesgos pueden ser prevenidos si se incorporan tempranamente en la formación del Ingeniero Civil contenidos sobre protección de datos, gestión ética de la información y seguridad digital. La alfabetización en ciberseguridad no debe estar restringida a los especialistas en informática, por el contrario, es indispensable transversalizarse en la enseñanza de todas las disciplinas que hacen uso intensivo de tecnologías digitales, como es el caso de la ingeniería civil actual.

Perspectiva legal en Venezuela

Además de los riesgos técnicos ya descritos con anterioridad, es prioridad considerar las consecuencias legales y éticas que pueden derivarse de la interceptación, alteración o mala gestión de los datos originados por drones en obras civiles. Por ejemplo, si los datos de una obra pública son manipulados o filtrados sin autorización, puede producirse una afectación directa al principio de transparencia en la contratación pública, comprometiendo licitaciones, presupuestos y cronogramas.

Desde la perspectiva legal, el uso indebido de esta información puede derivar en sanciones administrativas, demandas civiles o incluso responsabilidades penales. La legislación sobre protección de datos, aunque todavía incipiente en muchos países de América Latina, ya reconoce como delitos el acceso no autorizado a información sensible, la alteración dolosa de archivos digitales y la distribución sin consentimiento de contenido captado por medios tecnológicos. En este sentido, los ingenieros que operan drones deben tener una comprensión mínima de la normativa vigente relacionada con privacidad, propiedad intelectual y responsabilidad civil.

Concretamente, la ciberseguridad asociada al uso de drones en el área de la construcción está respaldada en Venezuela por un conjunto de normas legales que regulan el uso de tecnologías digitales, el tratamiento de datos y la protección de la privacidad. El siguiente marco jurídico ofrece un contexto esencial para comprender las obligaciones y límites que deben respetarse al capturar, procesar y almacenar información técnica mediante dispositivos aéreos no tripulados.

Constitución de la República Bolivariana de Venezuela (1999)

Nuestra Constitución consagra principios fundamentales sobre el derecho a la privacidad, el acceso a la información y la protección de los datos personales. El artículo 28 garantiza a toda persona el derecho de acceder a la información que sobre ella posean terceros, así como a conocer su uso y exigir su corrección. A su vez, el artículo 60 protege la vida privada, la honra y la confidencialidad de las comunicaciones, lo cual incluye el resguardo frente al uso indebido de tecnologías como los drones, especialmente cuando captan imágenes o datos en entornos privados o sensibles.

Ley Orgánica de Ciencia, Tecnología e Innovación (2010)

Promueve el uso ético y responsable de las tecnologías, además de proteger los desarrollos científicos y técnicos nacionales. Si bien no regula directamente el uso de drones, sí establece principios aplicables al tratamiento de datos generados por medios tecnológicos, con énfasis en la soberanía tecnológica y la protección de infraestructuras críticas.

Ley de Infogobierno (2013)

Esta ley regula los principios para el uso de las Tecnologías de la Información y la Comunicación (TIC) en el sector público. Aun cuando su enfoque está centrado en la administración pública, introduce conceptos clave como la soberanía tecnológica, la interoperabilidad de sistemas y la obligación de resguardar la integridad y confidencialidad de la información manejada electrónicamente. El uso de drones en obras públicas, por ejemplo, debería adecuarse a los estándares de seguridad digital promovidos por esta ley.

Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos (2004)

Contiene disposiciones sobre el uso responsable de medios digitales y protección de la ciudadanía ante contenidos sensibles. Cuando los drones son utilizados para captar imágenes que puedan ser difundidas en medios electrónicos o plataformas públicas, se deben considerar las implicaciones legales derivadas de esta ley, especialmente si las imágenes afectan la privacidad de individuos o colectivos.

Ley de Protección de Datos Personales (en discusión)

Aunque aún no ha sido promulgada, su desarrollo representa un avance hacia un marco específico para el resguardo de la información personal en Venezuela. En caso de aprobación, establecerá obligaciones claras sobre el manejo de datos obtenidos por drones, tanto en contextos privados como institucionales, e impondrá sanciones ante usos indebidos o no autorizados.

Regulaciones específicas y normas técnicas

- Normas del Centro Nacional de Tecnologías de Información (CNTI): incluyen lineamientos sobre la seguridad informática, el uso de software libre, el control de acceso a plataformas y la protección de información sensible.
- Planes y políticas públicas como el Ley Constituyente del Plan de la Patria (2019) hacen mención expresa a la necesidad de proteger las infraestructuras críticas del país y fortalecer una cultura nacional de soberanía tecnológica, que abarca también el uso estratégico de tecnologías como los drones.
- El INAC (Instituto Nacional de Aeronáutica Civil) es la autoridad encargada de regular los drones y han implementado normativas para garantizar la seguridad pública. Para operar un dron legalmente, se exige obtener la certificación y licencia de piloto emitidas por el INAC. Además, todos los drones deben cumplir con ciertos estándares de seguridad, rendimiento y estar en el Registro Nacional de Aviación (RAN), así como lograr un Certificado de Aeronavegabilidad de la CAA (Autoridad de Aviación Civil), antes de ser utilizados en el espacio aéreo venezolano. Es decisivo saber que, únicamente las empresas certificadas y que cuenten con un ROC (RPAS Operator Certificate) pueden realizar operaciones aéreas con drones en Venezuela. En específico y citando a Gross (2022), es obligatorio mantener en todo momento los drones a 9 kilómetros de los aeropuertos, así como a 1,8 kilómetros de los recintos gubernamentales y de las fuerzas de defensa, como instalaciones militares, bases, campamentos, estaciones policiales, instituciones correccionales o centros de detención. Adicionalmente, todas las operaciones deben realizarse durante el día y, en función del tipo de drone, se aplican restricciones en cuanto a la altura de ascenso, siendo necesario permanecer por debajo de los 400 pies de altitud. Para llevar a cabo registros, hay que mantener distancia de propiedades de carácter privado y de zonas pobladas, a menos que se cuente con el permiso correspondiente (Acosta, 2023, p. 153). El cumplimiento de estas normativas

asegura que los vuelos sean legales y seguros, para proteger a la población de posibles riesgos asociados con el uso indebido.

En el plano ético, surgen interrogantes complejas. ¿Es legítimo que una empresa privada utilice drones para captar imágenes detalladas de comunidades donde va a ejecutar una obra sin consultar previamente a sus habitantes? ¿Qué obligaciones tiene un ingeniero si descubre que los datos captados por su equipo han sido utilizados de forma indebida por un tercero? Estas preguntas deben ser parte de la reflexión profesional que acompaña el uso de tecnologías emergentes.

Por tanto, la formación de los futuros Ingenieros Civiles no puede seguir ajena a estas dimensiones. Es urgente incluir en el currículo espacios donde se discutan casos reales, dilemas éticos y responsabilidades legales asociadas al manejo de datos digitales. De este modo, el reconocimiento de estas vulnerabilidades mejora los protocolos técnicos actuales e incluso abre la puerta a una revisión crítica de los programas de estudio, con miras a formar profesionales capaces de operar con eficacia y seguridad en un entorno de creciente complejidad digital.

Cultura de ciberseguridad: Un reto en la formación del Ingeniero Civil

Hacer referencia a la cultura de ciberseguridad supone mucho más que implementar medidas técnicas para proteger los sistemas digitales. Se vincula, ante todo, a la internalización de valores, actitudes y conocimientos que orienten el comportamiento profesional frente al uso, gestión y resguardo de la información.

En esencia, afirma Da Veiga (2016) la cultura de la ciberseguridad promueve la seguridad, la protección, la privacidad y las libertades civiles en el ámbito digital. Demanda comprender los riesgos y las amenazas asociados al ciberespacio y emprender acciones adecuadas para proteger los activos de información, la infraestructura crítica y los datos personales. De todas formas, explica Medina (2022) es común que muchas personas subestimen la posibilidad de ser objeto de un ataque cibernético, lo que conduce a la negligencia en la implementación de medidas de seguridad y en la protección de datos personales y empresariales.

Si bien la cultura de la ciberseguridad es fundamental para la protección, su éxito depende del factor humano, pues desestimar el riesgo por parte de individuos y organizaciones crea una brecha entre la teoría y la práctica. Para que las medidas de ciberseguridad sean verdaderamente efectivas, es necesario superar la complacencia y las negligencias frecuentes que impiden aplicar las acciones adecuadas para hacer frente a las amenazas.

Cabe agregar que, en el ámbito de la ingeniería civil, esta cultura debe ir más allá de saber cómo usar una contraseña robusta o cifrar archivos. Debe fundamentarse en la comprensión ética y estratégica del valor de los datos obtenidos, la responsabilidad asociada a su tratamiento y las consecuencias de su exposición. Por lo tanto, la cultura

de ciberseguridad supone trascender el manejo instrumental de programas y dispositivos, significa formar una actitud consciente frente al ciclo completo de la información. Pese a que las soluciones tecnológicas son esenciales para la ciberseguridad, hay que reconocer que el elemento humano sigue siendo una preocupación central. La cultura de ciberseguridad se moldea significativamente por las actitudes, suposiciones, creencias, valores y conocimientos de quienes la utilizan.

Ciertamente, supone entender que toda acción vinculada a la información — desde capturarla hasta almacenarla o compartirla — tiene implicaciones técnicas, legales y éticas por lo que exige profesionales capaces de evaluar riesgos y actuar de manera preventiva. Fomentar una cultura de ciberseguridad que impulse la eficiencia, innovación y prosperidad económica, al mismo tiempo que protege la seguridad, privacidad, calidad y libertades civiles, exige la participación activa y el comportamiento responsable de individuos, organizaciones y gobiernos. Por esta razón, no surge espontáneamente: debe ser promovida activamente desde la formación universitaria, pues la educación y la concienciación son fundamentales para empoderar a la sociedad en la lucha contra las amenazas cibernéticas (García, 2020).

Ciertamente, en los últimos años ha cobrado relevancia la necesidad de incluir contenidos sobre ciberseguridad en los planes educativos, desde las etapas formativas iniciales y la educación universitaria hasta el nivel de postgrado (Salminen et al., 2023), en realidad, se resalta la responsabilidad de formar en competencias ciudadanas en ciberseguridad a toda la población, independientemente de su edad o formación académica.

En cuanto al diagnóstico actual, los programas del plan de estudios de ingeniería civil en muchas universidades de América Latina aún se enfocan fuertemente en competencias técnicas tradicionales: cálculo estructural, hidráulica, geotecnia, vías, planificación y ejecución de obras. Pese a que algunos han comenzado a incorporar nociones sobre Sistemas de Información Geográfica (SIG) o modelado BIM, el componente de seguridad digital sigue siendo escaso o, en casos, inexistente. Son pocos los currículos que incluyen materias específicas relacionadas con protección de datos, legislación digital o gestión ética de la información, incluso cuando los estudiantes emplean softwares avanzados, la formación se centra en el uso funcional, sin considerar los riesgos o protocolos asociados a la información que estos sistemas procesan.

Esta omisión genera una brecha crítica entre el uso intensivo de tecnología y la conciencia de seguridad digital. Los futuros Ingenieros Civiles se familiarizan con drones, escáneres láser, estaciones Global Navigation Satellite System (GNSS) plataformas en la nube, pero no desarrollan las competencias necesarias para proteger los datos generados por esas mismas tecnologías. El resultado es una fuerza laboral técnicamente competente, aunque vulnerable frente a los desafíos del entorno digital.

Además, existe una falsa percepción de que la ciberseguridad es responsabilidad exclusiva de áreas como la informática o las telecomunicaciones. Este enfoque compartimentalizado

ignora que hoy, cualquier profesional que trabaje con datos — especialmente en sectores sensibles como la infraestructura — debe tener un mínimo de alfabetización digital crítica. La ingeniería civil ya no se limita al diseño y construcción de obras que deben resistir en el tiempo; hoy también se construyen entornos de datos, modelos digitales y sistemas interconectados que requieren protección. Incluso se toman decisiones que afectan a comunidades enteras y actualmente, esas decisiones están mediadas por datos, por lo tanto, manejarlos con responsabilidad y conciencia crítica es una extensión natural de la ética profesional.

Formar una cultura de ciberseguridad en ingeniería civil supone también revisar el papel de la universidad y de los docentes, quienes son los principales mediadores entre los avances tecnológicos y los saberes profesionales. Para conseguirlo, es necesario que el personal docente sea competente en el manejo técnico de herramientas digitales y en específico de los riesgos asociados a su uso. La actualización continua del cuerpo docente y su compromiso activo en estos temas se torna en una condición necesaria para la transformación curricular.

A la vez, las metodologías de enseñanza pueden jugar un papel fundamental. El uso de simulaciones, estudios de caso, proyectos interdisciplinares y prácticas en entornos reales o virtuales hace posible que los estudiantes enfrenten problemas concretos vinculados a la gestión segura de la información. A modo de ejemplo, una práctica en la que los estudiantes procesan datos de drones en una nube pública sin medidas de protección adecuadas puede servir como detonante para discutir las consecuencias de una brecha de seguridad en un proyecto de infraestructura real.

Las universidades, por su parte, tienen que priorizar la ciberseguridad, no solo por la importancia de su misión educativa, sino también por la compleja interacción de elementos en su entorno digital. Con ese fin, es preciso que impulsen una visión estratégica que abarque la planificación, organización, control y promoción, estableciendo políticas institucionales claras sobre el manejo de datos, el uso de plataformas, la protección de la propiedad intelectual y la concientización de toda la comunidad. Por consiguiente, se consolida una sólida cultura de ciberseguridad tanto en las aulas, como en todo el ecosistema donde se forman los futuros profesionales.

Al respecto, la transformación digital es un aspecto clave para la ciberseguridad, ya que busca alcanzar altos niveles de eficiencia y eficacia en los servicios digitales, garantizar la seguridad de los procesos internos, facilitar la toma de decisiones basadas en datos, empoderar a la ciudadanía y capacitar a los funcionarios de las entidades públicas responsables de ejecutar acciones en esta materia (Molina, 2020). Tal integración es decisiva para enmarcar las actividades que se llevan a cabo en las instituciones públicas de educación superior.

Resulta incuestionable que, la función esencial de las universidades es educar y desarrollar conocimiento multidisciplinario, pero también es su deber gestionar eficazmente la información digital que poseen y por ende crear lineamientos para combatir las posibles

amenazas cibernéticas. Estas acciones resultan de gran valor ante la necesidad imperante de manejar la información como un activo fundamental de conocimiento (Pulido y Nájar, 2015). Tales lineamientos deben contar con una visión estratégica clara, junto con un conocimiento profundo de los procesos y actividades específicas de la universidad. Así mismo, son elementos clave una estructura organizacional eficiente, el fomento de una cultura y ética sólida, el desarrollo de las capacidades del talento humano y el uso apropiado de la infraestructura y aplicaciones de tecnologías de la información.

Del mismo modo, es indispensable reflexionar y avanzar en la construcción e implementación de un modelo de ciberseguridad que proteja la información crítica y asegure una gobernanza digital efectiva, que contribuya significativamente al fortalecimiento de los sistemas de información en el ciberespacio universitario. Para que esta idea sea posible, se requiere una alineación coherente y constante entre las autoridades universitarias y el gobierno, en función de una gestión adecuada de la información para beneficio de toda la comunidad universitaria.

A ello se suma, todos quienes hacen vida en el recinto universitario deben involucrarse para evitar posibles ataques, al respecto es necesario que la cultura de ciberseguridad se conecte con la dimensión ética de las carreras universitarias que se dictan en la institución. En términos generales, formar profesionales con cultura de ciberseguridad es preparar ciudadanos digitales responsables, capaces de operar con eficiencia en entornos tecnológicos sin comprometer la integridad de los datos ni la seguridad de las personas.

Esta es una tarea urgente para las instituciones educativas que buscan preparar profesionales para un mundo cada vez más interconectado y expuesto a riesgos complejos e invisibles. Aunque no se trata de una labor sencilla, es vital establecer un proceso de gestión de incidentes para mitigar los efectos de cualquier brecha de seguridad. Dicho plan de respuesta debe incluir la notificación de las brechas y la articulación con las autoridades competentes.

Integración de la ciberseguridad en la formación del Ingeniero Civil

De acuerdo con lo expuesto en el apartado anterior, la transformación digital en la ingeniería civil ha puesto de manifiesto la urgente necesidad de integrar la ciberseguridad en la formación universitaria. Frente a otras disciplinas, la ingeniería civil interviene directamente en el diseño, planificación, ejecución y mantenimiento de obras que afectan a miles de personas, como puentes, edificios, represas, vías, sistemas de drenaje, entre otros. El uso de drones ha potenciado estas capacidades, posibilitando la captura, procesamiento y análisis de datos geoespaciales con gran detalle. Sin embargo, esa misma ventaja tecnológica expone al sector a nuevos riesgos vinculados con la seguridad de la información.

Los datos generados por drones — como modelos tridimensionales del terreno, imágenes multiespectrales o registros térmicos — son esenciales para la toma de decisiones técnicas, económicas y sociales. En consecuencia, comprometer su integridad puede traducirse en

fallas estructurales, errores en la ejecución de obras o incluso daños a la población. A esto se suma la posibilidad de que los datos sean robados, manipulados o usados sin consentimiento, afectando licitaciones, contratos, reputaciones o intereses nacionales. Frente a este contexto, integrar la ciberseguridad en la formación de los Ingenieros Civiles no es una opción, es una necesidad impostergable. Explica Acosta (2023) que "la capacitación y formación adecuadas son imperativas para garantizar un uso seguro y efectivo de esta tecnología" (p. 154).

El Ingeniero Civil contemporáneo ya no puede limitarse al dominio de la matemática aplicada o a la selección de materiales constructivos. Su desempeño exige integrarse en ecosistemas digitales donde se modelan proyectos, se comparten datos en la nube y se gestionan infraestructuras inteligentes. En este escenario, la capacidad para comprender y proteger los entornos de información es tan determinante como el cálculo estructural o la planificación de una obra. Esto conlleva a formar al estudiante para que entienda cómo se generan los datos en campo (por ejemplo, con drones), cómo se procesan (en software y plataformas de análisis), cómo se almacenan (en nubes o servidores institucionales) y, sobre todo, cómo se protegen.

Para lograrlo, se debe incluir en los programas de formación una serie de contenidos básicos de ciberseguridad aplicada, pues "los profesionales deben demostrar competencia tanto en la operación técnica como en la interpretación y aplicación de los datos generados por estos dispositivos" (Acosta, 2023, p. 154). En este marco, se deben abordar aspectos como:

- Introducción a la ciberseguridad y su relación con la infraestructura civil.
- Tipología de amenazas digitales comunes en entornos de construcción.
- Protocolos de seguridad en el manejo de drones y sus plataformas asociadas.
- Normativas legales sobre privacidad, uso de imágenes, almacenamiento de datos y gestión de evidencia digital.
- Ética profesional en el uso de tecnologías de recolección de datos.
- Riesgos asociados a plataformas de nube, redes colaborativas y software no autorizado.

No obstante, estos contenidos deben ser complementados con el desarrollo de competencias prácticas y actitudinales que faciliten que los futuros ingenieros puedan actuar con criterio en entornos digitales, en particular:

- Capacidad de reconocer y mitigar riesgos digitales en proyectos reales.
- Habilidad para implementar buenas prácticas en la captura y almacenamiento seguro de datos obtenidos mediante drones.
- Conocimiento del ciclo de vida de la información técnica desde su generación hasta su archivado o destrucción segura.

- Comprensión de los impactos sociales de una brecha de seguridad, especialmente en obras de alto valor público.
- Desarrollo de una conciencia ética respecto a la manipulación de datos, la confidencialidad de los proyectos y el uso justo de la información.

Asimismo, es importante que la capacitación no se limite a un curso aislado o a un módulo optativo, sino que se integre transversalmente en la formación del Ingeniero Civil. Esto puede lograrse incluyendo casos reales en las asignaturas de planificación, topografía, construcción, mantenimiento y proyectos, donde se analicen incidentes relacionados con la pérdida o filtración de datos. También, mediante talleres interdisciplinarios con estudiantes de informática, derecho y comunicación, que promueva espacios para discutir dilemas éticos y normativos desde diversas perspectivas.

Las universidades deben asumir este reto con visión estratégica, motivando a "la colaboración y cooperación entre instituciones educativas, la industria tecnológica y de la construcción, los profesionales y los reguladores, para establecer estándares de capacitación y garantizar un uso responsable de los drones" (Acosta, 2023, p. 154). Pues en efecto, se trata de anticipar un escenario más que de responder a una moda tecnológica donde la seguridad digital será tan importante como la resistencia de un puente o la eficiencia de un sistema de drenaje. La ingeniería civil trabaja con estructuras físicas, pero cada vez más, con entornos digitales que, si son vulnerables, comprometen la seguridad de las personas y la sostenibilidad de los territorios.

En definitiva, integrar la ciberseguridad en la formación del Ingeniero Civil es formar profesionales completos, capaces de tomar decisiones en entornos híbridos donde lo físico y lo digital se entrelazan. Es preparar a los futuros responsables de la infraestructura del país para que entiendan que los datos son parte del diseño, que la información es un activo que se debe proteger, y que la ética digital es hoy un elemento clave del código profesional.

Conclusiones

El uso de drones en la ingeniería civil ha marcado un hito en la forma en que se recolectan, procesan y analizan los datos para la toma de decisiones técnicas. Estos dispositivos han dejado de ser herramientas complementarias para convertirse en plataformas productoras de datos críticos, con aplicaciones que abarcan desde estudios preliminares hasta la inspección de infraestructuras y el monitoreo del avance de obras. Ahora bien, esta innovación tecnológica trae consigo un conjunto de riesgos y responsabilidades que deben ser abordados bajo una perspectiva integral.

A lo largo de este capítulo, se ha evidenciado que los registros captados por drones son valiosos tanto por su utilidad técnica, como por su potencial impacto si son mal gestionados, manipulados o expuestos. Las vulnerabilidades digitales asociadas al uso de drones plantean un desafío creciente en el contexto de la ingeniería, y exigen medidas preventivas, técnicas y éticas que garanticen la integridad, confidencialidad y disponibilidad de la información.

Bajo este enfoque, se demuestra que la ciberseguridad no es una tarea exclusiva de los especialistas informáticos, sino que constituye un eje transversal que debe ser comprendido y asumido por todos los actores involucrados en el diseño y ejecución de proyectos de infraestructura. Por su parte, la ingeniería civil, al ser una disciplina que articula tecnología, territorio y sociedad, debe responder a estos nuevos desafíos desde la formación de sus profesionales.

Además, se constata que Venezuela cuenta con un marco normativo que, aunque aún en proceso de consolidación, ofrece fundamentos legales suficientes para avanzar en la protección de los datos captados por medios tecnológicos. Desde la Constitución hasta las políticas públicas más recientes, se reconocen principios de soberanía tecnológica, privacidad y uso ético de la información, que deben ser conocidos y aplicados por quienes operan con tecnologías como los drones.

Por otra parte, transversalizar la protección de datos en la formación del Ingeniero Civil no es una posibilidad, es una necesidad que demanda acciones inmediatas. Esta integración debe garantizar que los futuros profesionales dominen tanto el manejo de drones y sus plataformas como las competencias técnicas, éticas y legales para proteger la información en entornos híbridos. Formar ingenieros conscientes de la responsabilidad que implica gestionar datos es, en última instancia, proteger a las comunidades y a los territorios que dependen de su trabajo.

De cara al futuro, la incorporación de tecnologías emergentes como la inteligencia artificial, el blockchain o la computación cuántica transformará aún más el modo de recolectar y preservar datos. Este escenario exigirá marcos normativos dinámicos y un aprendizaje continuo por parte de los profesionales, con el fin de anticipar y mitigar nuevos riesgos, lo que abre una línea de investigación inaplazable para los próximos años. Garantizar la seguridad digital de la información es una exigencia técnica, para mantener la confianza pública, fortalecer la transparencia y asegurar que las obras de infraestructura respondan de manera sostenible a las necesidades de la sociedad. Preparar ingenieros responsables y capaces de preservar los datos que sustentan sus decisiones es, en definitiva, una forma de resguardar también a las comunidades y territorios sobre los cuales actúan.

Referencias

Acosta, M. (2023). La Inteligencia Artificial en la ingeniería civil. *Conocimiento Libre y Licenciamiento (CLIC)*, (27), 113-126. https://convite.cenditel.gob.ve/revistaclic/index.php/revistaclic/article/view/1184

Constitución de la República Bolivariana de Venezuela. (1999). *Gaceta Oficial de la República Bolivariana de Venezuela N° 36.860*. Servicio Autónomo de Imprenta Nacional y Gaceta Oficial (SAINGO). http://crespial.org/wp-content/uploads/2018/10/A%C3%B1o-1999-Constituci%C3%B3n-de-la-Rep%C3%BAblica-Bolivariana-de-Venezuela-Gaceta-Oficial-36.860.pdf

Cornejo, E., y Clavel, M. (2024). *La Ciberseguridad en la Adopción de la Industria 4.0*. Consejo Editorial de la Universidad Autónoma del Estado de Hidalgo. https://repository.uaeh.edu.mx/books/197/cc.pdf

Da Veiga, A. (2016). *Una filosofía y un enfoque de investigación sobre la cultura de la ciberseguridad para desarrollar un instrumento de medición válido y confiable* [13-15 de julio de 2016]. Conferencia de Computación SAI. Londres, Reino Unido. https://doi.org/10.1109/SAI.2016.7556102

García, L. (2020). *La Ciberseguridad en la Adopción de la Industria 4.0*. Universidad Piloto de Colombia. https://repository.unipiloto.edu.co/handle/20.500.12277/9478

Gross, R. (2022). *Nuevas leyes sobre drones en Venezuela (2023 Actualizado)*. Propel RC. https://www.propelrc.com/es/drone-laws-in-venezuela/

Gross, R. (2023). *Evolución completa e historia de los drones: De 1800 a 2022*. Propel RC. https://www.propelrc.com/es/historia-de-los-drones/

Knisely, T. (2020). *Todo lo que necesitas saber sobre topografía con drones*. DJIEnterprise. https://enterprise-insights.dji.com/es/blog/todo-lo-que-necesitas-saber-sobre-topografia-con-drones

Ley Constituyente del Plan de la Patria. (2019). *Gaceta Oficial de la República Bolivariana de Venezuela Nº 6.442 Extraordinaria*. Servicio Autónomo de Imprenta Nacional y Gaceta Oficial (SAINGO). http://spgoin.imprentanacional.gob.ve/cgi-win/be_alex.cgi?Acceso=T028700028441/0&Nombrebd=spgoin&Sesion=225597721&SFmt=Movil

Ley de Infogobierno. (2013). *Gaceta Oficial de la República Bolivariana de Venezuela N.º 40.274*. Servicio Autónomo de Imprenta Nacional y Gaceta Oficial (SAINGO). https://www.mpppst.gob.ve/mpppstweb/wp-content/uploads/2015/02/LEY_DE_INFOGOBIERNO.pdf

Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos. (2004). *Gaceta Oficial de la República Bolivariana de Venezuela Nº 38.095*. Servicio Autónomo de Imprenta Nacional y Gaceta Oficial (SAINGO).

Ley Orgánica de Ciencia, Tecnología e Innovación. (2010). *Gaceta Oficial de la República Bolivariana de Venezuela N.º 39.569, Decreto Nº 7.266*. Servicio Autónomo de Imprenta Nacional y Gaceta Oficial (SAINGO).

Medina, G. (2022). *La seguridad en el ciberespacio: un desafío para Colombia*. 2a ed. Escuela Superior de Guerra.

Molina, A. (2020). *Modelo de gobierno y gestión de riesgos TI para las universidades públicas de Colombia: Caso de estudio Universidad Popular del Cesar* [tesis de Maestría]. Universidad del Norte, Barranquilla. http://hdl.handle.net/10584/10394

Negrín, A. (2018). *Control y monitorización de un prototipo de dron con NI myRIO y LabVIEW* [Trabajo Fin de Grado en Ingeniería Eléctrica]. Universidad Politécnica de Valencia. http://hdl.handle.net/10251/115401

Pulido, D., y Nájar, O. (2015). Gestión del conocimiento en educación con TIC en la transformación de la escuela. *Revista Vínculos*, *12*(1). https://revistas.udistrital.edu.co/index.php/vinculos/article/view/10520/11482

Reuter, F., y Pedenovi, A. (2019). *Los Drones y sus Aplicaciones a la Ingeniería*. Universidad Nacional de Santiago del Estero. https://fcf.unse.edu.ar/wp-content/uploads/2014/07/SD-43-Drones-y-su-aplicacion-a-la-ingenieria-REUTERr.pdf

Salminen, M., Candelin, N., Cullen, K., Latvanen, S., Lindroth, M., y Matilainen, T. (2023). *Educación en ciberseguridad en las instituciones de educación superior europeas* [19 -22 de junio de 2023]. IX Conferencia Internacional sobre Avances en la Educación Superior. Valencia. España. http://ocs.editorial.upv.es/index.php/HEAD/HEAd23/paper/view/16336

Sardanyés, E. (s.f). *Drones: ¿son una amenaza para la ciberseguridad?* Cyber Security & IT Solutions. https://www.esedsl.com/blog/drones-son-una-amenaza-para-la-ciberseguridad

Autores

Autores

Daniel Quintero

Historiador y abogado egresado de la Universidad de Los Andes (ULA). Actualmente se desempeña como docente en la ULA, y como investigador en el Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL). Autor y director de publicaciones académicas y de divulgación científica.

ORCID: https://orcid.org/0000-0001-5330-5690
Correo electrónico: dquintero@cenditel.gob.ve

María Alejandra Rujano

Ingeniero Industrial egresada de la Universidad Yacambú, Magister en Modelado en Simulación de Sistemas y Doctora en Gestión para la Creación Intelectual. Actualmente se desempeña como Investigadora en el Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL). Autora y editora de publicaciones académicas y de divulgación científica.

ORCID: https://orcid.org/0000-0003-3853-4182
Correo Electrónico: mrujano@cenditel.gob.ve

Carlos González

Licenciado en Administración egresado de la Universidad de Los Andes (ULA), MSc. en Educación mención Informática y Diseño Instruccional. Actualmente se desempeña como investigador en el Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL). Autor de publicaciones académicas y de divulgación científica.

ORCID: https://orcid.org/0000-0002-1856-1434
Correo Electrónico: cgonzalez@cenditel.gob.ve

Aida Andrade

Economista y Licenciada en Educación egresada de la Universidad de Los Andes. Actualmente se desempeña como Investigadora en el Centro de Desarrollo e Investigación en Tecnologías Libres (CENDITEL). Autora de publicaciones académicas y de divulgación científica.

ORCID: https://orcid.org/0009-0006-9358-5467
Correo Electrónico: aandrade@cenditel.gob.ve

Jesús Erazo

Licenciado en Física egresado de la Universidad de Los Andes (ULA), Magíster en física fundamental. Actualmente se desempeña como docente en la ULA y como investigador en el Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL). Autor y editor de publicaciones académicas y de divulgación científica.

ORCID: https://orcid.org/0000-0003-3719-6783
Correo Electrónico: jerazo@cenditel.gob.ve

Santiago Roca

Politólogo egresado de la Universidad de Los Andes (ULA), Especialista en Sistemología Interpretativa, Magíster en Ciencias Políticas y Doctor en Gestión para la Creación Intelectual. Investigador del Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL). Editor y autor de publicaciones académicas y de divulgación científica, y coordinador de proyectos de conocimiento y tecnologías libres.

ORCID: https://orcid.org/0000-0002-3701-3409
Correo Electrónico: sroca@cenditel.gob.ve

Pablo Sulbarán

Ingeniero de Sistemas egresado de la Universidad de Los Andes (ULA). Actualmente se desempeña como Analista de Desarrollo en el Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL). Autor de publicaciones académicas y de divulgación científica.

ORCID: https://orcid.org/0000-0002-8422-1024
Correo Electrónico: psulbaran@cenditel.gob.ve

Yazmary Rondón

Licenciada en Educación mención Matemática egresada de la Universidad de Los Andes (ULA), MSc. en Educación mención Informática y Diseño Instruccional y Doctora en Educación. Actualmente se desempeña como docente en la ULA y como investigadora en el Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL). Autora y editora de publicaciones académicas y de divulgación científica.

ORCID: https://orcid.org/0000-0002-5156-221X
Correo Electrónico: yrondon@cenditel.gob.ve

María Eugenia Acosta

Ingeniero Civil egresada del Instituto Universitario Politécnico Santiago Mariño (IUPSM), MSc. en Educación Superior mención Docencia Universitaria, Doctora en Ciencias de la Educación y Postdoctora en Investigación Educativa. Actualmente se desempeña como docente en la Universidad Politécnica Territorial del Estado Mérida Kléber Ramírez (UPTM Kléber Ramírez), y como investigadora en el Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL). Autora y editora de publicaciones académicas y de divulgación científica.

ORCID: https://orcid.org/0000-0002-4226-0666
Correo Electrónico: macosta@cenditel.gob.ve

Otros Títulos de la Colección

Otros títulos de la colección

Los desafíos de la COVID-19

Perspectivas, retos y alternativas tecnológicas desde una mirada latinoamericana

Año: 2021

Depósito Legal: ME2021000382

ISBN: 978-980-7154-20-8

Autores: María Rujano, Julie Vera, Luz Chourio, María Acosta, Yazmary Rondón, Isabel Cassino, Arelis Guzmán, Oscar González, Santiago Roca, Jesús Erazo, Daniel Quintero.

Sitio oficial: https://convite.cenditel.gob.ve/files/2022/01/Libro_2021_CENDITEL.pdf

La Inteligencia Artificial

Reflexiones sobre los desafíos de una tecnología divergente

Año: 2022

Depósito Legal: ME2022000201

ISBN: 978-980-7154-21-5

Autores: Daniel Quintero, Santiago Roca, Gloria Rondón, María Alejandra Rujano, Yazmary Rondón, María Eugenia Acosta, Carlos González, Jesús Erazo y Pablo Sulbarán.

Sitio oficial: https://convite.cenditel.gob.ve/files/2022/12/Libro2022.pdf

Conocimiento Libre Ante la Dominación Tecnológica

Desentrañando el Capitalismo Cognitivo

Año: 2023

Depósito Legal: ME2023000256

ISBN: 978-980-7154-22-2

Autores: Daniel Quintero, Jesús Erazo, Pablo Sulbarán, Santiago Roca, María Alejandra Rujano, Oscar González, Lisbeth Rengifo, Yazmary Rondón, y María Eugenia Acosta.

Sitio oficial: https://convite.cenditel.gob.ve/files/2023/11/Libro2023.pdf

Robótica: promesas, utopía o futuro distópico

Año: 2024

Depósito Legal: ME2024000252

ISBN: 978-980-18-4963-62

Autores: María Eugenia Acosta, Pablo Sulbarán, Yazmary Rondón, Carlos González, Jimena Pérez, María Alejandra Rujano, Santiago Roca y Jesús Erazo.

Sitio oficial: https://convite.cenditel.gob.ve/files/2024/11/Libro2024.pdf

Ciberseguridad en la era de la convergencia tecnológica

NUEVOS RETOS Y OPORTUNIDADES PARA SALVAGUARDAR LA INFORMACIÓN DIGITAL

COLECCIÓN: Oscar Varsavsky
SERIE: Pensamiento crítico sobre la contemporaneidad tecnológica

ISBN: 978-980-18-4963-6

REPÚBLICA BOLIVARIANA DE VENEZUELA | Ministerio del Poder Popular para CIENCIA Y TECNOLOGÍA

CONVITE CENDITEL

CENDITEL