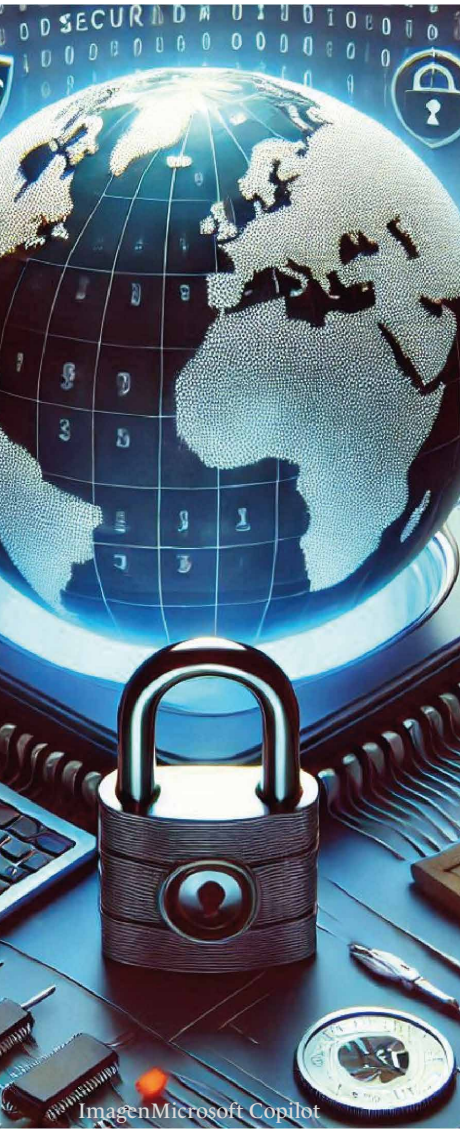
Ciberseguridad para todos:
orígenes, concepto y alcance

Josué Tonathiú Lopez Díaz[1]
Jerjes Izcoatl Aguirre Ochoa[2]
Patricia Navarrete Soriano[3]



ImagenMicrosoft Copilot

ININEE CIENCIA Revista de Divulgación Científica, 2(4) Julio-Diciembre 2024. pp: 39-48.

Resumen

La ciberseguridad es clave en un mundo interconectado por las TIC, donde millones de personas y dispositivos interactúan a diario. Este concepto, derivado de la seguridad de la información, busca proteger la confidencialidad, integridad y disponibilidad de datos ante riesgos y amenazas. Con el 67.5% de la población mundial y 81.4% en México utilizando internet, la ciberseguridad se vuelve esencial para proteger activos informáticos, datos personales y garantizar interacciones seguras en el ciberespacio. Además, abarca esferas clave: protección de datos personales, activos informáticos y seguridad social en contextos globales. Su alcance incluye herramientas, políticas y formación para anticipar amenazas.

Palabras clave: ciberseguridad, México, informática, ciberespacio.

La ciberseguridad se ha manifestado como una idea y/o concepto alienado a la forma de vida moderna, en la que la evolución y la globalización de las Tecnologías de la Información y Comunicaciones (TICs), han revolucionado la forma en la que interactuamos como sociedad. Sin embargo, no muchas personas, en comparación con el colectivo, son capaces de comprender y mucho menos explicar lo que el concepto de ciberseguridad significa, sus orígenes, alcance y sus implicaciones en la vida cotidiana de las personas.

En un mundo interconectado, en el que de acuerdo con Kepios (2024) de los poco más de ocho mil millones de personas en el planeta, el 70.3% cuenta con un teléfono celular, el 67.5% son usuarios de internet y el 63.8% de las redes sociales; y que en México, estas cifras llagan al 81.4% y el 81.2% de la población mayor de seis años que acceden a internet y redes sociales respectivamente (Instituto Nacional de Estadística y Geografía (INEGI), 2024), es decir que 97 millones de personas en México utilizaron intenet durante el año 2023; el concepto de ciberseguridad cobra vital importancia a fin de lograr una navegación segura entre los internautas dentro del ciberespacio y evitar riesgos que los pongan en peligro.

1 Universidad Michoacana de San Nicolás de Hidalgo. ORCID: 0000-0002-1328-5805
2 Universidad Michoacana de San Nicolás de Hidalgo. ORCID: 0000-0001-7858-5166
3 Universidad Michoacana de San Nicolás de Hidalgo. ORCID: 0000-0002-0722-5064

Bajo este panorama en el que millones de personas utilizan a diario las TICs, ya sean dispositivos móviles como celulares (smartphones), tabletas o laptops; e incluso en diversos dispositivos electrónicos domésticos interconectados (IoT) (*internet de las cosas)* por sus siglas en inglés, que hoy día funcionan a partir de los servicios de internet para realizar un sinfín de tareas, el concepto de ciberseguridad se vuelve cada vez más relevante para garantizar la conectividad y funcionalidad de dichos dispositivos, así como de las tareas y servicios que brindan a la humanidad. Por ello que el presente articulo tiene como objetivo realizar una aproximación conceptual del significado de la ciberseguridad, su origen y sus alcances en la vida cotidiana de los cibernautas que navegan por el ciberespacio.

Seguridad de la información como antecedente de la ciberseguridad

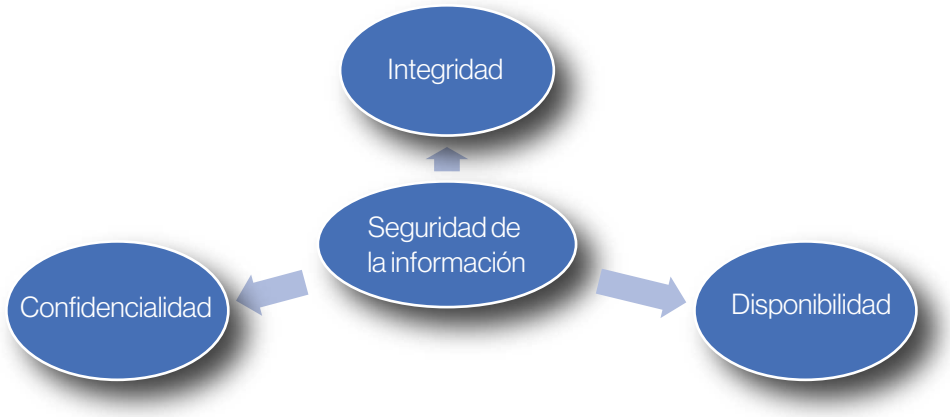
La ciberseguridad surge como una rama de las ciencias computacionales e informáticas y como concepto teórico-práctico desarrollado para proteger los activos informáticos, como lo pueden ser los equipos de cómputo, las redes e infraestructura que los mantienen interconectados, así como los sistemas, aplicativos y bases de datos que en estos se alojan, ante fallas, riesgos y/o amenazas; a esta rama del conocimiento se le denominó seguridad de la información.

De acuerdo con Pallero y Heguiabehere (2023), Vega (2021) e INCIBE (2023); la seguridad de la información consite en el conjunto de actividades destinadas a proteger la confidencialidad, integridad y disponibilidad, dimensiones que son conocidas como la triada de la seguridad de la información. Con la primera se garantiza que la información generada únicamente sea utilizada por las personas autorizadas para su manejo. El segundo elemento consite en garantizar que la información se mantenga sin cambios o modificacones no autorizadas que pudiesen alterar su interpretación y utilidad. Por último, la disponibilidad hace referencia a la capcidad de los sistemas de información para proveer datos de forma oportuna, es decir que de la información sea almacenada de forma tal que se pueda acceder a ella en el momento que sea requerida.

Pero, ¿Por qué es necesario proteger la información? A primera vista la respuesta a esta pregunta parece obvia, esto es porque la información en la actualidad se considera un activo, lo que significa que posee un valor para su propietario.

Y ¿por qué la información se convierte en algo valioso para sus propietarios? La respuesta es tan amplia como los diferentes tipos de información que se producen, lo que hace dificil de medir su valor, sin embargo se puede hacer la aclaración que hoy día las empresas pueden generar información vital para sostener su actividad económica como lo pueden ser fórmulas químicas y/o recetas de productos; patentes sobre desarrollos tecnológicos y/o procesos productivos; productos y servicios protegidos por leyes de propiedad intelectual como contenido audiovisual de carácter recreativo, obras literarias o científicas; bases de datos con infor-

Triada de la seguridad de la información



Fuente: Elaboración propia con base en Pallero y Heguiabehere (2023), Vega (2021) e INCIBE (2023)

mación confidencial de clientes; entre muchas más, que de verse afectadas, dañadas, robadas o difundidas sin autorización, pudiesen causar graves pérdidas económicas a sus propietarios.

Los ciudadanos también generan y poseen información personal valiosa para cada uno de ellos y que puede tomar diferentes formas como lo pueden ser datos personales como nombre, edad, direcciones de correo electrónicos, números de teléfono, cuetas bancarias, domicilio, fotografías, audios, videos y comunicaciones privadas; las cuales si bien su valor dificilmente se puede cuantificar, si esta información quede expuesta, los hace vulnerables y los pone en riesgo de sufrir afectaciones en sus derechos, en sus bienes o incluso en su propia integrida físisca y psicológica, por lo que se hace necesario mantenerla segura y protegida.

Los gobiernos, de igual forma generan y almacen grandes cantidades de datos e información relacionada con sus actividaes, que si bien es cierto que gran parte de la información que producen se considera pública, tambien almacenan datos de los ciudadanos que, de ser difundidos, podrían resultar en afectaciones graves a la población.

Individuos, organizaciones y gobiernos genran información, sin embargo, esta información para que cumpla su propósito en muchas ocasiones requiere de su transmisión o intercambio con otros agentes manteniendose en constante flujo por diversos canales. Estas interaciónes al ser relativamente permanentes y al reunir una infinidad de sujetos, forman en su conjunto una red global de canales y medios de tranmisión de datos conocida como ciberespacio, en el que la seguridad de la información enfrenta enormes desafiós para poder proteger los activos informáticos. De ello que para comprender el término ciberseguridad, surge otro concepto clave para su definición, siendo este el ciberespacio.

ImagenMicrosoft Copilot

El ciberespacio

De acuerdo con Ardissom de Souza (2018), para comprender el termino ciberespacio es necesario evocar el concepto de red utilizado por las ciencias sociales, el cual permite comprender el conjunto de interacciones humanas dentro de una comunidad y en general en la sociedad, a partir de las comunicaciones que se dan entre los individuos. La red se encuentra

formada por múltiples nodos con funciones y/o tareas específicas que se encuentran interconectados y son capaces de recibir y entregar información al resto.

Es así que las ciencias computacionales retoman el concepto de redes como principio fundamental para resolver los problemas relacionados con la entrega de paquetes de información de un nodo a otro dentro de una misma red. En la actualidad estas redes se encuentran formadas por una infinidad de dispositivos simples que represnetan los nodos como lo pueden ser computadoras, servidores, smartphones, televisores, vehículos y electrodomésticos, hasta las grandes infraestructuras que permiten la interconexion y comunicación entre los distintos dispositivos como lo pueden ser antenas de telecomunicaciones, cables submarinos y satélites que forman parte de las redes globales de comunicación (Ardissom de Souza, 2018).

En su conjuto estos nodos conforman una red permanente en la que las personas y los dispositivos, interactuan de forma constante con infinidad de propósitos y realizan multiples tareas, ofreciendo con ello un espacio o territorio diferente en donde se da la interaccion humana, al que se le ha denomindo ciberespacio.

Por su parte Santana-Soriano y Báez (2022), definen al ciberespacio como un lugar artificial y ficticio, que solo se puede explicar por el conjunto de interacciones entre máquinas (hardware y software), personas y organizaciones. Dichas interacciones complejas entre máquinas y humanos, no solo generan un ciberespacio sino que dan origen al mismo tiempo a los cibersujetos.

A partir de estas definiciones se puede comprender al ciber espacio como un territorio ficticio creado por el hombre mediente la conexión de multiples dispositivos (hardware y software) en el cual las personas, ahora cibersujetos, interactúan creando relaciones y experiencias humanas, humano-máquinas y máquina-humano.

En el ciberespacio, al igual que cualquier otro espacio de interaccion social, ofrece un territorio en el que la distancia, el anonimato y la falta de vigilancia formal, se convierte en un campo fértil, no solo para el detrimento de activos informáticos, sino para el surgimiento desorden, conflictos, caos, violencia, delitos y afecciones a los derechos de las personas e incluso de su integridad y salud física y psicológica, surgiendo con ello la necesidad encontrar un mecanismo que pueda proteger estas interaciones dentro del ciberespacio, siendo este, a groso modo la ciberseguridad.

Ciberseguridad: conceptos

Una primera aproximación conceptual de la ciberseguridad se puede intuir a partir de la descomposición de los vocablos que la conforman, ciber y seguridad, correspondiendo el primero a la palabra cibernética, que a su vez proviene del griego kybernetes, utilizado para definir el arte de manejar un navío; y el segundo seguridad que implica encontrarse libre de peligro, daño o riesgos, en conjunto, la palabra ciberseguridad se utiliza para identificar esta característica de encontrarse libre de riesgos y peligro al navegar por el ciberespacio.

Para Pallero y Heguiabehere (2023) la ciberseguridad implica la protección física de los servicios digitales y la infraestructura que los soporta, la seguridad de la información que por estos se transmite y de las personas que los utilizan.

Rodríguez (2024), afirma que la ciberseguridad abarca la protección de infraestructuras críticas como lo pueden ser redes eléctricas, sistemas de transporte y de salud que se encuentran conectados y soportados en servicios digitales, así como la protección de la privacidad y seguridad de las personas ante incidentes que pongan en riesgo sus activos financieros.

Para Aldeco, Gallegos y Rodríguez (2020), la ciberseguridad abarca una amplia gama de técnicas y herramientas destinadas a proteger el ciberespacio y sus componentes.

Kaspersky (2025) señala que la ciberseguridad consiste en "*defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos*."

Para la Unión Internacional de Telecomunicaciones (2010), *"La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber-entorno"*.

Para la Unión Europea (2020), la ciberseguridad comprende el conjunto de actividades fundamentales para la protección de la información y los canales por los que esta transita, así como las personas encargadas de su gestión y del resto de la población que puede ser afectada por ciberamenazas. Su función es anticiparse a las amenazas a fin de detectarlas, contrarrestarlas y/o recuperarse de ellas, sin importar si sus consecuencias fueron resultado de una actividad intencionada o no.

Alcance y esferas de la ciberseguridad

En un mundo en el que gran parte de la población se ha convertido en un cibersujeto, cibernauta o ciudadano virtual, la sociedad mundial enfrenta retos y amenazas que son capaces de afectar distintas esferas de la convivencia humana, de esto que la ciberseguridad se vuelve fundamental para proteger la interacción y desarrollo de la vida humana. Estas esferas de desarrollo y convivencia se pueden resumir de la siguiente manera:

1. De la información y protección de datos personales de los individuos. Esta esfera

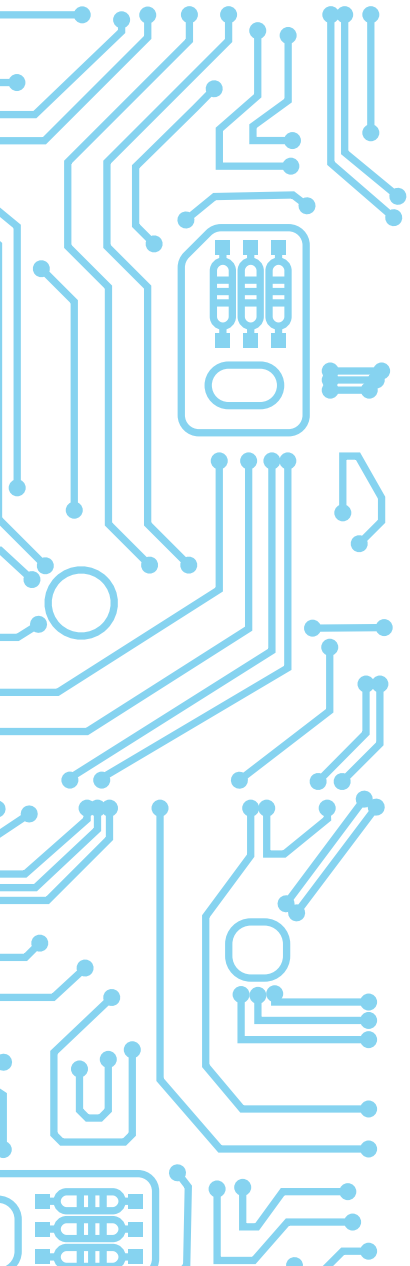
Imagem Microsoft Copilot

de la ciberseguridad consiste en la aplicación de técnicas, procedimientos, prácticas y protocolos por medio de los cuales los cibernautas, evitan compartir datos personales e información que ponga en riesgo el ejercicio de sus derechos, libertades e integridad física y psicológica.

2. De la protección de activos informáticos: La cual se encarga de proteger los recursos físicos como infraestructuras, equipos, hardware y software, ante cualquier amenaza que ponga en riesgo su confidencialidad, integridad y disponibilidad, para personas, organizaciones y Estados.

3. De la interacción social dentro de los límites geopolíticos: a pesar de que los cibernautas ejercen libertades y comunicación dentro de una comunidad global, cada Estado mantiene vigente la autodeterminación de lo que considera una amenaza a su forma de vida y organización política, así como de la protección de sus ciudadanos, ante riesgos y amenazas globales que puedan afectar a su población de forma masiva a tal grado que se convierta en un problema público e incluso que pueda afectar la soberanía dentro de su territorio o su desarrollo y bienestar social.

Estas tres esferas o ámbitos de aplicación representan las mayores preocupaciones de la ciberseguridad en un contexto global , a fin de garantizar la seguridad de los ciudadanos en nuevo espacio libre de fronteras, restricciones y discriminación a lo que los ciudadanos del mundo llaman ciberespacio.



Conclusiones

La ciberseguridad surge como una rama de las ciencias computacionales destinada a proteger los activos informáticos de los individuos, organizaciones y gobiernos, a la cual se le denominó seguridad de la información y que se basa en tres principios fundamentales conocidos como la triada de la información que son la confidencialidad, integridad y disponibilidad.

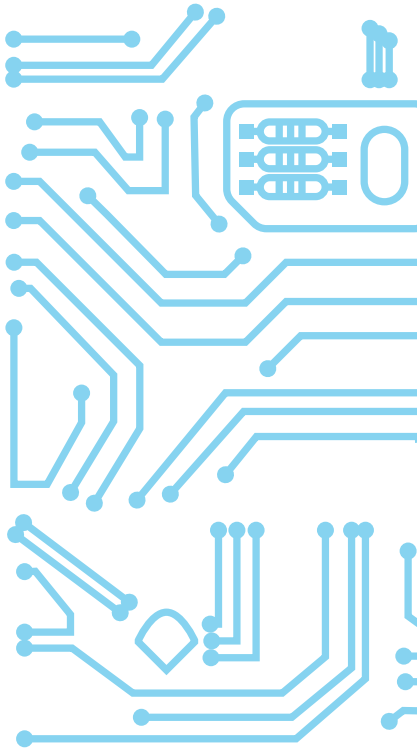
De igual forma la seguridad de la información surge como un enfoque organizacional dirigido a la protección de activos informáticos desde un punto de vista individual, es decir, su uso parte de la voluntad de cada ciudadano, empresa o gobierno por proteger su propia información.

Al encontrarnos en un mundo interconectado en el que estos tres agentes (individuos, organizaciones y gobiernos) interactúan de forma masiva y constante, el ciberespacio representa un nuevo territorio de interacción social en el cual las amenazas y riesgos asociados, han causado graves afectaciones económicas, vulneraciones de derechos e incluso facilitado la comisión de múltiples delitos, convirtiéndose en un problema público de naturaleza global, ante el cual se acuñó el concepto de ciberseguridad.

La ciberseguridad se considera un enfoque transversal para la protección, no solo de la información que circula en el ciberespacio, sino como una herramienta fundamental que, mediante la concientización y difusión de prácticas, políticas y reglas de convivencia en el ciberespacio, ayuda a proteger los derechos fundamentales de los cibernautas, su patrimonio e incluso la integridad física y salud mental.

Por lo anterior, se puede definir a la ciberseguridad como:

> "Proceso que mediante el uso herramientas tecnológicas, políticas, conceptos de seguridad de la información, métodos de gestión, prevención y concientización de riesgos asociados a las TICs, establece mecanismos para proteger, almacenar y manejar los activos informáticos; así como para la protección de bienes económicos o jurídicos de las personas, como la privacidad, derecho de la información y comunicación, ante cualquier daño o amenaza en el ciberespacio o de aquellas que trascienden al plano material, incluyendo la salud física y/o psicológica de individuos, organizaciones, familias y sociedad en general."



La ciberseguridad no solo consiste en proteger los activos informáticos de individuos, organizaciones y gobiernos, sino que trasciende al ámbito social y estatal en el que estos agentes, encuentran los mecanismos para el libre ejercicio de sus derechos y libertades, más aún, el conjunto social globalizado se auxilia de la ciberseguridad para mantener un espacio de convivencia libre de riesgo y amenazas en el cual se pueda extender la vida misma en un entorno armónico, pacífico y capaz de reproducir los vínculos humanos para alcanzar una sociedad global más avanzada.

Referencias

Aldeco, R., Gallegos, G., & Rodríguez , L. (2020). *Introducción a la Ciberseguridad y sus aplicaciones en México.* ACADEMIA MEXICANA DE COMPUTACIÓN, A. C.

AO Kaspersky Lab. (14 de 01 de 2025). *Kaspersky*. Obtenido de https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security?srsltid=AfmBOooWfp59O9862OrieiEpCA-9MuyO79e887E2PstwvrEZW2ALn4hvH

Ardissom de Souza, R. (2018). De las redes al ciberespacio. *Revista Digital Universitaria (RDU), 19*(2). doi:http://doi.org/10.22201/codeic.16076079e.2018.v19n1.a2

INCIBE Instituto Nacional de Ciberseguridad. (01 de 02 de 2023). *Protección de la Información.* Obtenido de INCIBE: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

Instituto Nacional de Estadística y Geografía (INEGI). (13 de 06 de 2024). *INEGI.* Obtenido de https://www.inegi.org.mx/programas/endutih/2023/#documentacion

Kepios Pte. Ltd. (Octubre de 2024). *KEPIOS.* Recuperado el 03 de 01 de 2025, de https://datareportal.com/reports/digital-2024-october-global-statshot

Pallero, M., & Heguiabehere, J. (2023). *Seguridad de la información y ciberseguridad.* Fundación Sadosky.

Rodríguez , H. (2024). Seguridad de la información y ciberseguridad: su importancia para los Estados, empresas y las personas, una revisión sistemática. *Estudios y perspectivas. Revista científica y académica, 4*(1). doi:https://doi.org/10.61384/r.c.a.v4i1.90

Santana-Soriano, E., & Báez, K. (2022). Ciberespacio y Cibermundo: delimitaciones conceptuales desde el materialismo sistémico. *Ciencia y Sociedad, 47*(1). doi:https://doi.org/10.22206/cys.2022.v47i1.pp45-57

Unión Europea. (2020). *La ciberseguridad en la UE y sus Estados miembros.*

Vega, E. (2021). *Seguridad de la información.* Editorial Área de Innovación y Desarrollo,S.L. doi:https://doi.org/10.17993/tics.2021.4