



Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales

Milena Elizabeth
Realpe Díaz

Giovanni Alberto
Gómez Rodríguez

(Editores)



EDITORIAL ESDEG

Colección Ciberseguridad y Ciberdefensa

Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales



Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales

MILENA ELIZABETH REALPE DÍAZ
GIOVANNI ALBERTO GÓMEZ RODRÍGUEZ
(EDITORES)

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., 2025

Catalogación en la publicación – Escuela Superior de Guerra “General Rafael Reyes Prieto”

Ciberseguridad en la frontera digital : desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales / Editores Milena Elizabeth Realpe Díaz y Giovanni Alberto Gómez Rodríguez -- Bogotá : Editorial ESDEG, 2025.

205 páginas : diagramas y tablas ;24 cm.

Incluye referencias bibliográficas al final de cada capítulo

ISBN impreso: 978-628-7602-99-1

E- ISBN: 978-628-7818-00-2

(Colección Ciberseguridad y Ciberdefensa)

1. Seguridad informática -- Colombia 2. Ciberdefensa -- Colombia. 3. Inteligencia artificial -- Aplicaciones en seguridad informática. 4. Infraestructura crítica -- Protección -- Colombia. 5. Transformación digital -- Aspectos de seguridad. i. Espinosa Torres, León Ernesto, (prefacio) ii. Realpe Díaz, Milena Elizabeth (editor) iii. Gómez Rodríguez, Giovanni Alberto. iv. Suárez Medina, Didier Dubey (autor) v. Giraldo Ríos, Lucas Adolfo (autor) vi. Ospina Navas, Jaider (autor) vii. Carvajal Bernal, Milena (autor) viii. Colombia. Escuela Superior de Guerra “General Rafael Reyes Prieto” (ESDEG).

SCLC QA76.9. A25R43 2025
SCDD 005.8 2 23

Registro Catalográfico SIBFuP 991351642307231



Archivo descargable en formato MARC en: <https://tinyurl.com/esdeg991351642307231>

Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales

Primera edición, 2025

Editores:

Milena Elizabeth Realpe Díaz
Giovanni Alberto Gómez Rodríguez

2025 Escuela Superior de Guerra

“General Rafael Reyes Prieto”

Vicedirección de Investigación

Sello Editorial ESDEG

Carrera 11 N°. 102-50 Bogotá D.C., Colombia

www.esdeglibros.edu.co

Cubierta:

Raquel Arianne Alvarado Candela con base en
imágenes de IA Freepik.com

Libro electrónico publicado a través de la plataforma

Open Monograph Press.

Tiraje de 100 ejemplares

Impreso en Colombia

Colección Ciberseguridad y Ciberdefensa

ISBN impreso: 978-628-7602-99-1

ISBN digital: 978-628-7818-00-2

DOI: <https://doi.org/10.25062/9786287818002>

Libro resultado de investigación de la Escuela Superior de Guerra “General Rafael Reyes Prieto”.

El contenido de este libro corresponde exclusivamente al pensamiento de los autores y es de su absoluta responsabilidad. Las posturas y aseveraciones aquí presentadas son resultado de un ejercicio académico e investigativo que no representa necesariamente la posición oficial ni institucional de las instituciones participantes, la Escuela Superior de Guerra “General Rafael Reyes Prieto”, las Fuerzas Militares de Colombia ni el Ministerio de Defensa Nacional.



Los libros publicados por el Sello Editorial ESDEG son de acceso abierto bajo una licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas.

<https://creativecommons.org/licenses/by-nc-nd/4.0/>



Vicealmirante
León Ernesto Espinosa Torres
DIRECTOR

Brigadier General
Nestor Favian Nieto Rivera
SUBDIRECTOR

Coronel
Aldemar Serrano Cuervo
VICEDIRECTOR DE INVESTIGACIÓN



Coronel
Aldemar Serrano Cuervo
JEFE SELLO EDITORIAL ESDEG

Erika Ramírez Benítez
EDITORA LIBROS ESDEG

Felipe Solano Fitzgerald
Anderson Nicolás Rojas Sierra
Jorge Hernando Aristizabal Gáfaró
Dayan Garzón Martínez
CORRECTORES DE ESTILO

Raquel Arianne Alvarado Candela
DIAGRAMADORA

Contenido

Prefacio VALM. León Ernesto Espinosa Torres	09-10
Introducción Didier Dubey Suárez Medina	11-14
Capítulo 1 Impacto de la ciberseguridad en los modelos de negocio de las organizaciones Lucas Adolfo Giraldo Ríos	15-42
Capítulo 2 Desafíos y tendencias en la identidad digital para la seguridad de las infraestructuras críticas Jaider Ospina Navas	43-78
Capítulo 3 La inteligencia artificial y la transformación digital en el ámbito de la ciberseguridad Lucas Adolfo Giraldo Ríos	79-118
Capítulo 4 Articulación de la ciberseguridad y la ciberdefensa en la planeación estratégica de las organizaciones Lucas Adolfo Giraldo Ríos	119-156
Capítulo 5 Guía para la adopción de una cultura de ciberseguridad en juntas directivas Milena Carvajal Bernal	157-196

Epílogo

Milena Elizabeth Realpe Díaz
Giovanni Alberto Gómez Rodríguez

197-205

Prefacio

Vicealmirante León Ernesto Espinosa Torres

Director Escuela Superior de Guerra "General Rafael Reyes Prieto"

Pocos temas permanecen en la agenda pública por periodos tan prolongados como la revolución tecnológica y su aplicación, la transformación digital. Tras este hecho se oculta una suerte de aporía: no se acaba de implementar, porque las innovaciones no cesan de aparecer. La razón de su relevancia es que nunca una tecnología tuvo un índice de penetración y expansión tan amplio y acelerado. Tampoco la humanidad conoció tecnologías tan disruptivas y a la vez tan peligrosas como la inteligencia artificial (IA) que, ahora, al incursionar en el ciberespacio, tiene el potencial de dominar y controlar activos y sistemas sensibles e infraestructuras críticas cibernéticas que proveen servicios esenciales, de los cuales depende virtualmente la supervivencia humana.

La revolución tecnológica es actualmente una cuestión existencial, como lo expresa Harari (2024) en su más reciente libro *Nexus*: "[...] nos afanamos en la creación de nuevas tecnologías como la IA, que tiene el potencial de escapar de nuestro control y de esclavizarnos o aniquilarnos". La verdad es que la vida social, comercial y financiera de comunidades políticas enteras, corporaciones y empresas tiene lugar en el ciberespacio, en ecosistemas digitales que, no obstante la creciente hiperconectividad, operan atendiendo el principio de segmentación. En este contexto, los contenidos, planteamientos y reflexiones desarrollados en el presente libro se inscriben en un panorama estratégico donde proliferan amenazas sofisticadas capaces de comprometer información personal, encriptar datos para extorsión, sabotear sistemas autónomos y ejecutar ciberataques financieros de alto impacto. En un entorno digital cada vez más interconectado y vulnerable, resulta evidente que ningún sistema es completamente inexpugnable, y todo lo que transita por el ciberespacio enfrenta un riesgo constante de exposición y explotación.

El presente libro, al igual que las publicaciones desarrolladas en el marco de la Maestría en Ciberdefensa y Ciberseguridad, de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG), se fundamenta en un enfoque estratégico orientado a la generación de reflexiones estructurales, normativas e históricas, así

como al análisis de tendencias emergentes y la incorporación de mejores prácticas en el ámbito de la seguridad digital. A través de estudios avanzados y actualizaciones sobre herramientas y tecnologías de vanguardia, estas iniciativas buscan fortalecer la capacidad de respuesta frente a las amenazas cibernéticas, con lo cual se garantiza la protección integral de los activos digitales de individuos, organizaciones e instituciones, al tiempo que se hace más robusta la resiliencia cibernética de la nación.

Los contenidos de esta publicación se centran en los desafíos y las oportunidades que la ciberseguridad y la ciberdefensa presentan en los entornos tecnológicos globales. Partiendo de la premisa de que los requerimientos para garantizar la confidencialidad, integridad y disponibilidad de la información impactan directamente en la adopción de modelos de negocio, así como en la planeación estratégica, se resalta la importancia del liderazgo en ciberseguridad por parte de la alta dirección y los órganos de gobierno corporativo. Su responsabilidad no solo abarca la promoción de una sólida cultura de ciberseguridad, sino también su integración como una decisión estratégica clave para minimizar riesgos y maximizar beneficios. Además, se abordan temas como el uso de tecnologías avanzadas para la identificación digital, orientadas a garantizar el acceso controlado a sistemas críticos. Herramientas basadas en la nube y en IA se perfilan como tendencias clave para enfrentar los retos del futuro en este ámbito.

El compendio de información presentado en este libro constituye un aporte al fortalecimiento de la ciberseguridad y la ciberdefensa en los ámbitos empresarial e institucional. Este esfuerzo refleja el compromiso de la ESDEG con la comunidad académica, los sectores estratégicos y, en última instancia, con la sociedad en general, al ofrecer conocimiento accesible y relevante para enfrentar los desafíos actuales del entorno digital. Más allá de los aspectos técnicos y procedimentales, aspiramos a que estas páginas inspiren reflexiones profundas sobre el papel de la tecnología en nuestra vida cotidiana y en el desarrollo de estrategias sostenibles para proteger nuestros activos digitales. Como señala Kevin Mitnick (2006): "La seguridad no es un producto, es un proceso" (p. 10), un viaje constante hacia la resiliencia y la adaptabilidad en un mundo cambiante.

Referencias

Mitnick, K. (2006). *El arte de la intrusión: La verdadera historia de las hazañas de hackers, intrusos e impostadores*. Ra-Ma.

Introducción

Didier Dubey Suárez Medina

Escuela Superior de Guerra "General Rafael Reyes Prieto"

La ciberseguridad ha surgido como un componente esencial en el entorno empresarial contemporáneo, donde la transformación digital ha reconfigurado la forma en que las organizaciones operan y generan valor. A medida que las empresas adoptan tecnologías avanzadas y se conectan a redes globales, también se enfrentan a un aumento significativo de los riesgos cibernéticos. Este libro, *Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales*, explora cómo la ciberseguridad se ha convertido en un factor determinante para la sostenibilidad y competitividad de las empresas en un mundo cada vez más interconectado.

La creciente interdependencia de los sistemas digitales ha incrementado significativamente la exposición a ciberamenazas, destacando la imperiosa necesidad de implementar estrategias de ciberseguridad robustas y efectivas. No se trata únicamente de proteger los activos digitales, sino también de asegurar la continuidad operativa y reducir el impacto financiero y reputacional de los incidentes cibernéticos, evidenciando que un enfoque proactivo en ciberseguridad es fundamental para que las organizaciones operen con confianza y resiliencia.

Además, el libro subraya la importancia de integrar la ciberseguridad en el modelo de negocio, destacando que esta integración no solo protege a las organizaciones, sino que también puede potenciar su capacidad para innovar y diferenciarse en el mercado. En este sentido, la ciberresiliencia se presenta como un concepto clave, que permite a las empresas prevenir ataques y recuperarse rápidamente de ellos.

El capítulo 1, "Impacto de la ciberseguridad en los modelos de negocio de las organizaciones", examina la creciente interrelación entre la ciberseguridad y los modelos de negocio en un entorno de transformación digital. A medida que las tecnologías disruptivas mejoran la eficiencia empresarial, también exponen a las organizaciones a riesgos cibernéticos significativamente mayores. Esta situación plantea un desafío crítico: muchas organizaciones, especialmente las pequeñas

y medianas empresas, tienden a subestimar la importancia de invertir en ciberseguridad y ciberresiliencia, lo que puede llevar a pérdidas económicas y daños reputacionales severos. La falta de integración de estrategias robustas de ciberseguridad en sus modelos de negocio impide que estas organizaciones operen de manera segura, comprometiendo así su sostenibilidad y competitividad en un mercado cada vez más complejo. La ausencia de conciencia sobre la necesidad de estas inversiones puede resultar en una vulnerabilidad estructural, lo que subraya la urgencia de abordar la ciberseguridad no solo como un gasto, sino como una inversión estratégica fundamental.

El capítulo 2, “Desafíos y tendencias en la identidad digital para la seguridad de infraestructuras críticas”, analiza la creciente vulnerabilidad de las infraestructuras críticas cibernéticas (ICC) en un entorno digital interdependiente y complejo. A medida que estas infraestructuras —que son esenciales para el funcionamiento de sistemas vitales como energía, telecomunicaciones y transporte— se vuelven más integradas, también se exponen a ciberataques que pueden comprometer su operatividad. La gestión inadecuada de la identidad digital se presenta como un riesgo significativo, ya que la falta de un enfoque robusto en este aspecto puede resultar en brechas de seguridad que, a su vez, pueden desencadenar efectos en cascada devastadores en las infraestructuras físicas que dependen de las ICC.

El capítulo destaca, además, las diferencias entre las infraestructuras críticas físicas y cibernéticas, subrayando que las ICC requieren una atención especial debido a su papel en el control y la gestión de sistemas físicos. La identificación de diversas vulnerabilidades en las capas de percepción, red y seguridad física revela la necesidad urgente de desarrollar marcos normativos sólidos para proteger estas infraestructuras. En resumen, este capítulo aborda la imperante necesidad de implementar una gestión efectiva de la identidad digital como un pilar esencial para asegurar la resiliencia de las infraestructuras críticas frente a las crecientes amenazas cibernéticas, lo que plantea un desafío significativo tanto a nivel técnico, como normativo.

El capítulo 3, “La inteligencia artificial y la transformación digital en el ámbito de la ciberseguridad”, explora los desafíos y oportunidades asociados con la integración de la inteligencia artificial (IA) en la ciberseguridad, en un contexto de transformación digital. A pesar del gran potencial de la IA para revolucionar la protección de sistemas y datos mediante técnicas avanzadas como el aprendizaje automático, el aprendizaje profundo y las redes neuronales, su implementación efectiva presenta varios retos significativos.

Uno de los principales problemas es la necesidad de una comprensión profunda y continua de las herramientas y técnicas de IA por parte de los profesionales de ciberseguridad, ya que la falta de formación adecuada puede limitar su capacidad para utilizar estas tecnologías de manera efectiva. Además, la rápida evolución de las amenazas cibernéticas exige que las estrategias de ciberseguridad se adapten de manera dinámica, lo que plantea un desafío adicional en términos de personalización y optimización de políticas de seguridad.

De igual manera, la integración de la IA en plataformas de seguridad unificadas implica la superación de barreras técnicas y organizativas, así como la necesidad de establecer protocolos claros para la colaboración entre expertos. La dependencia de la inteligencia artificial también introduce riesgos relacionados con la seguridad de los propios sistemas de IA, lo que podría resultar en vulnerabilidades adicionales si no se gestionan adecuadamente.

En resumen, este capítulo evidencia que, aunque la implementación de IA ofrece la promesa de mejorar la capacidad de respuesta y resiliencia ante amenazas cibernéticas, la problemática radica en la necesidad de abordar las complejidades técnicas, formativas y estratégicas que surgen en este proceso, asegurando que las organizaciones estén preparadas para enfrentar un entorno digital en constante evolución.

El capítulo 4, "Articulación de la ciberseguridad y la ciberdefensa en la planeación estratégica de las organizaciones", destaca una serie de problemáticas clave relacionadas con la integración de la ciberseguridad y la ciberdefensa en la planificación estratégica de las organizaciones. En primer lugar, se evidencia que las amenazas cibernéticas han evolucionado y se han sofisticado considerablemente, lo que plantea un reto significativo para las empresas. Los ataques no solo son más complejos, sino también más variados, lo que obliga a las organizaciones a adoptar enfoques de protección y respuesta más dinámicos. Sin embargo, se observa que, a menudo, la ciberseguridad y la ciberdefensa se tratan de manera separada, lo que genera una falta de coordinación en la estrategia global. Esta fragmentación puede dejar a las organizaciones vulnerables, ya que mientras la ciberseguridad se enfoca en la prevención, la ciberdefensa debe encargarse de mitigar los efectos de un ataque y asegurar la recuperación. Además, la falta de una colaboración efectiva entre los sectores público y privado es otro desafío importante. A pesar de la creciente necesidad de intercambiar información sobre amenazas y mejores prácticas, las organizaciones privadas suelen ser reticentes a compartir datos sensibles, mientras que las entidades públicas carecen, en muchos casos, de los recursos necesarios para gestionar dicha información de

manera eficiente. Finalmente, la integración insuficiente de la ciberseguridad y la ciberdefensa en la planificación estratégica de las organizaciones pone en riesgo la continuidad operativa y la reputación organizacional. La falta de una estrategia coherente y coordinada puede resultar en una respuesta inadecuada ante incidentes cibernéticos, lo que pone en peligro la estabilidad y sostenibilidad de la empresa a largo plazo.

El capítulo 5, "Guía para la adopción de una cultura de ciberseguridad en juntas directivas", pone en evidencia una problemática crítica que muchas organizaciones enfrentan: la falta de conciencia y preparación de las altas esferas directivas respecto de los riesgos cibernéticos. A pesar de la creciente amenaza de ataques cibernéticos, muchas juntas directivas continúan viendo la ciberseguridad como una responsabilidad exclusiva del departamento de tecnología de la información, en lugar de reconocerla como un desafío integral que debe involucrar a todos los niveles de la organización. Esta perspectiva limitada puede llevar a una gestión reactiva y descoordinada de los riesgos, en lugar de una proactiva y estratégica. El capítulo también resalta que la falta de conocimiento y preparación entre los directores sobre ciberseguridad puede resultar en decisiones equivocadas, lo que aumenta la vulnerabilidad organizacional frente a ataques. La ausencia de una estrategia formalizada, que incluya la creación de comités dedicados y la asignación de presupuestos específicos, limita la capacidad de la organización para fortalecer su resiliencia cibernética. En este contexto, la adopción de una cultura de ciberseguridad en la junta directiva se presenta como un paso esencial para garantizar que las decisiones empresariales se alineen con las mejores prácticas de seguridad y gestionen adecuadamente los riesgos cibernéticos, contribuyendo así a la protección de los activos, la continuidad operativa y la reputación organizacional.

En el epílogo, por último, el lector encontrará un resumen de los principales hallazgos de los autores, que abarcan los desafíos y las oportunidades clave en el ámbito de la ciberseguridad dentro de los nuevos ecosistemas tecnológicos empresariales. Se destacan las principales tendencias identificadas a lo largo del libro, así como las recomendaciones estratégicas para enfrentar las amenazas cibernéticas emergentes. Además, se presenta la conclusión central, que subraya la necesidad de una integración integral de la ciberseguridad en la planificación empresarial y la importancia de una cultura organizacional proactiva para garantizar la resiliencia ante los riesgos digitales, con el fin de proteger tanto los activos digitales, como la reputación de las empresas en un entorno cada vez más complejo y vulnerable.

Capítulo 1

Impacto de la ciberseguridad en los modelos de negocio de las organizaciones^{*}

DOI: <https://doi.org/10.25062/9786287818002.01>

Lucas Adolfo Giraldo Ríos

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: La transformación digital ha reconfigurado los modelos de negocio, aumentando la dependencia de las organizaciones en sistemas interconectados y exponiéndolas a riesgos cibernéticos significativos. Este capítulo destaca la ciberseguridad como un componente esencial para la sostenibilidad y competitividad empresarial, definiéndola no solo como la protección de activos digitales, sino también como la implementación de políticas organizacionales que aseguren la continuidad operativa. Se analiza el concepto de ciberresiliencia, que permite a las organizaciones continuar operando a pesar de los ciberataques, enfatizando su importancia en la recuperación rápida y la minimización del impacto financiero y reputacional. Las amenazas cibernéticas actuales, como ataques de denegación de servicio (DDoS) y *ransomware*, son discutidas en el contexto de su impacto en diversas industrias. En conclusión, un modelo de negocio exitoso en la era digital debe integrar estrategias robustas de ciberseguridad y ciberresiliencia para garantizar su operación segura y efectiva en un entorno cada vez más complejo.

Palabras clave: amenazas cibernéticas; ciberresiliencia; ciberseguridad; continuidad operativa; modelos de negocio; transformación digital.

^{*} Capítulo de libro resultado del proyecto de investigación "*Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales*" del grupo de investigación "Ciberespacio Tecnología e Innovación", de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado C por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) y registrado con el código COL0181179. Los puntos de vista y los resultados de este capítulo pertenecen al autor y no reflejan necesariamente los de las instituciones participantes.

Lucas Adolfo Giraldo Ríos

Candidato a doctor en Ingeniería, Industria y Organizaciones, Universidad Nacional de Colombia. Magíster en Administración de Empresas de Base Tecnológica, Universidad Antonio de Nebrija, España. Magíster en Innovación, Universidad EAN, Colombia. Especialista en Gestión Financiera Empresarial, Universidad de Medellín, Colombia. Administrador de Empresas, Universidad de Antioquia, Colombia.

<https://orcid.org/0000-0002-9947-7882> - Contacto: lucas.giraldo@esdeg.edu.co

Citación APA: Giraldo Ríos, L. A. (2025). Impacto de la ciberseguridad en los modelos de negocio de las organizaciones. En M. E. Realpe Díaz & G. A. Gómez Rodríguez (Eds.), *Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales* (pp. 15-42). Sello Editorial ESDEG.
<https://doi.org/10.25062/9786287818002.01>

CIBERSEGURIDAD EN LA FRONTERA DIGITAL: DESAFÍOS Y OPORTUNIDADES EN LOS NUEVOS ECOSISTEMAS TECNOLÓGICOS EMPRESARIALES

ISBN impreso: 978-628-7602-99-1

ISBN digital: 978-628-7818-00-2

DOI: <https://doi.org/10.25062/9786287818002>

Colección Ciberseguridad y Ciberdefensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2025



Introducción

La transformación digital ha reconfigurado la dinámica empresarial al acelerar la integración de tecnologías disruptivas que facilitan la realización de procesos y los hacen más eficientes, flexibles y personalizados. Sin embargo, esta evolución digital también ha incrementado los riesgos asociados a la ciberseguridad, convirtiéndola en un factor decisivo para el éxito o fracaso de los modelos de negocio contemporáneos. En este capítulo se analiza la importancia de la ciberseguridad en las organizaciones y cómo su gestión influye directamente en la sostenibilidad y la competitividad de los modelos de negocio.

Definición y conceptos clave

Definición de modelo de negocio

El concepto de modelo de negocio ha sido ampliamente estudiado y definido desde diversas perspectivas, lo cual refleja su importancia en la comprensión de cómo una organización genera, entrega y captura valor. A continuación, se presentan algunas definiciones

- Osterwalder y Pigneur (2010) lo definen como “la lógica mediante la cual una organización crea, entrega y captura valor”. Para estos autores, el modelo de negocio es un lienzo compuesto por nueve bloques que describen los principales elementos de una organización, como la propuesta de valor, los segmentos de clientes, los canales de distribución y la estructura de costos.

- Para Teece (2010), es “la arquitectura conceptual que define la lógica de cómo una empresa entrega valor a los clientes, atrae clientes y convierte ese valor en beneficios”. Este enfoque enfatiza la importancia que tiene la rentabilidad como resultado del modelo de negocio.
- Por su parte, Chesbrough (2007) considera que es “un marco para crear, entregar y capturar valor, que a su vez permite a la empresa aprovechar nuevas oportunidades de mercado”. Este enfoque destaca la capacidad del modelo de negocio para adaptarse a la innovación y a los cambios tecnológicos.
- Magretta (2002) lo define como “el relato de cómo funciona una empresa”. En esta visión, el modelo de negocio es una narrativa clara y coherente que explica quiénes son los clientes, qué valor se ofrece y cómo se generan ingresos.

De estas definiciones, la de Osterwalder y Pigneur (2010) es particularmente adecuada, dado que su enfoque detallado y estructurado permite a las empresas visualizar claramente todos los componentes esenciales para generar valor. De hecho, el Business Model Canvas propuesto por estos autores es ampliamente utilizado en el ámbito empresarial y académico por su capacidad para integrar aspectos claves como la propuesta de valor, los recursos y las actividades clave, lo cual facilita la planificación y la ejecución de estrategias de negocio.

Definición de ciberseguridad

La ciberseguridad también ha sido definida desde diferentes perspectivas, lo cual refleja su relevancia en el contexto digital. A continuación, se presentan varias definiciones:

- National Institute of Standards and Technology (NIST, 2018) la define como “la capacidad de proteger o defender el uso de ciberespacio de ataques cibernéticos”. Esta definición se centra en el aspecto técnico y la protección de las infraestructuras digitales.
- Según la International Telecommunication Union (ITU, 2008), es “el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas, directrices, enfoques de gestión, acciones, capacitación, mejores prácticas, garantías y tecnologías que pueden ser utilizados para proteger los activos de información, los usuarios y las organizaciones en el ciberespacio”.
- La European Union Agency for Cybersecurity (ENISA, 2020) la define como “el conjunto de actividades, políticas y procedimientos que una

organización implementa para proteger sus sistemas, redes y datos de accesos no autorizados, interrupciones o ataques".

- ISO/IEC 27032 (ISO, 2012) considera que es "la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio".

De estas definiciones, la proporcionada por ENISA (2020) resulta ser la más completa y adecuada en el contexto empresarial, ya que abarca no solo los aspectos técnicos, sino también las políticas y procedimientos organizacionales necesarios para una protección integral de los activos digitales.

Definición de ciberresiliencia

El concepto de ciberresiliencia ha cobrado relevancia en los últimos años debido al creciente número de ciberataques que enfrentan las organizaciones. A continuación, se presentan algunas definiciones:

- International Organization for Standardization (ISO, 2016) la define como "la capacidad de una organización para continuar operando a pesar de ciberataques, incidentes o interrupciones de sistemas".
- El World Economic Forum (WEF, 2018) sostiene que es "la capacidad de una organización para anticipar, resistir, recuperarse y adaptarse a eventos cibernéticos adversos".
- Por su parte, el National Institute of Standards and Technology (NIST, 2020) argumenta que es "la capacidad de un sistema o red para continuar funcionando adecuadamente en presencia de fallas o ataques maliciosos".

La definición más adecuada en el contexto organizacional es la de ISO (2016), que resalta la importancia de mantener la continuidad operativa a pesar de que ocurran incidentes cibernéticos, lo cual es clave para minimizar el impacto en el negocio y garantizar la sostenibilidad de la organización a largo plazo.

La relación entre modelo de negocio, ciberseguridad y ciberresiliencia es clave para el éxito de las organizaciones en la era digital. Un modelo de negocio, tal como lo definen Osterwalder y Pigneur (2010), describe la lógica mediante la cual una empresa crea, entrega y captura valor. En un contexto digital, esta creación y entrega de valor dependen cada vez más de infraestructuras tecnológicas que requieren protección constante. Es aquí donde la ciberseguridad desempeña un papel fundamental al garantizar que los activos digitales críticos de la empresa estén protegidos frente a amenazas, de tal manera que minimiza las interrupciones en la operación y asegura la capacidad de generar ingresos y satisfacer a los clientes (Teece, 2010).

La ciberseguridad, tal como es definida por ENISA (2020), abarca no solo la protección técnica de sistemas y redes, sino también la implementación de políticas y procedimientos organizacionales que aseguren la integridad y la disponibilidad de la información. Estos elementos son fundamentales para la operación de un modelo de negocio moderno, ya que la mayoría de los procesos empresariales están interconectados a través de redes y sistemas digitales. Sin medidas adecuadas de ciberseguridad, una empresa se expone a ciberataques que pueden comprometer la confidencialidad de la información, dañar su reputación y afectar su capacidad para entregar valor a sus clientes (Gordon & Loeb, 2021).

Por otro lado, el concepto de ciberresiliencia es un complemento esencial para la ciberseguridad, ya que no se trata solo de prevenir ataques, sino de mantener la operación a pesar de ellos. Según la definición de la ISO (2016), la ciberresiliencia es la capacidad de una organización para continuar operando tras sufrir un incidente cibernético, lo cual es crucial para los modelos de negocio, especialmente en sectores donde la interrupción del servicio puede tener consecuencias significativas tanto financieras como en la lealtad de los clientes. Una empresa resiliente puede recuperarse rápidamente de un ataque, restableciendo la confianza de sus clientes y manteniendo su capacidad competitiva (NIST, 2020).

La integración de ciberseguridad y ciberresiliencia dentro del modelo de negocio también fomenta la innovación y la diferenciación competitiva. Al incorporar medidas de seguridad avanzadas, las empresas no solo protegen sus activos, sino que también pueden acceder a nuevos mercados y cumplir con normativas internacionales, lo cual les otorga una ventaja competitiva. Además, la capacidad de una empresa para demostrar que es ciberresiliente puede atraer clientes que valoren la estabilidad y la continuidad operativa, lo que convierte a la ciberseguridad en un diferenciador clave en mercados altamente competitivos y globalizados (Porter & Millar, 2017).

En este sentido, un modelo de negocio sostenible en la era digital debe incorporar estrategias claras de creación de valor, una estructura robusta de ciberseguridad que proteja sus activos críticos y una capacidad de ciberresiliencia que le permita recuperarse de incidentes cibernéticos. La sinergia entre estos tres elementos —modelo de negocio, ciberseguridad y ciberresiliencia— es esencial para que las organizaciones logren operar de manera segura y exitosa en un entorno digital cada vez más complejo y vulnerable a ciberataques (Lewis, 2020).

Impacto de la ciberseguridad en las organizaciones

La transformación digital ha intensificado la dependencia de las organizaciones en sistemas interconectados y plataformas digitales. Esta interconexión, si bien ofrece una mayor eficiencia y nuevas oportunidades de negocio, también aumenta significativamente la exposición de las empresas a ciberataques. Un ataque exitoso puede comprometer activos críticos, detener operaciones y generar daños financieros sustanciales. Según Gordon y Loeb (2021), la interrupción de sistemas debido a ataques cibernéticos puede llevar a pérdidas económicas considerables, dañar la reputación de la empresa y afectar gravemente la continuidad operativa. En este sentido, la ciberseguridad se ha convertido en un elemento central para asegurar la estabilidad de los negocios.

Las empresas, tanto grandes como pequeñas, han comenzado a reconocer que la inversión en ciberseguridad no es un gasto opcional, sino una inversión estratégica. Implementar soluciones de seguridad robustas permite mitigar los riesgos asociados a ciberataques, con lo cual se garantiza la confidencialidad, integridad y disponibilidad de los activos de información, esenciales para la operación diaria. Las normativas internacionales, como la ISO 27001 y la creciente presión regulatoria en materia de protección de datos, como el Reglamento General de Protección de Datos (GDPR), están incentivando a las organizaciones a fortalecer sus mecanismos de defensa cibernética. En este contexto, no cumplir con los estándares de seguridad puede tener implicaciones legales y reputacionales significativas.

Una de las áreas más vulnerables dentro del panorama empresarial son las pequeñas y medianas empresas (pymes). De acuerdo con Berger (2022), las pymes suelen tener presupuestos más ajustados y, a menudo, subestiman el impacto potencial de los ciberataques. Esta percepción errónea las hace menos propensas a invertir en medidas de seguridad adecuadas, lo que las convierte en blancos fáciles para los atacantes. A pesar de su menor tamaño, las pymes manejan datos valiosos y operan en ecosistemas interconectados con proveedores, socios y clientes, lo que las expone a riesgos similares a los de grandes corporaciones. La falta de inversión en ciberseguridad puede generar una cascada de consecuencias negativas, desde interrupciones en los servicios hasta la pérdida de la confianza de los clientes.

Por otra parte, las grandes empresas tampoco están exentas de los riesgos. A medida que las organizaciones crecen y adoptan nuevas tecnologías, como la nube, la inteligencia artificial (IA) y el internet de las cosas (IoT), aumentan las superficies de ataque potenciales. Además, la complejidad de las infraestructuras

tecnológicas y la mayor cantidad de puntos de entrada para los atacantes hacen que las empresas tengan que actualizar constantemente sus sistemas de seguridad. Como se observa, las brechas de seguridad en grandes corporaciones pueden impactar no solo en el negocio afectado, sino también en sus socios y clientes, de tal manera que se amplifica el daño.

El impacto de la ciberseguridad en las organizaciones también está relacionado con la capacidad de respuesta y recuperación ante incidentes, es decir, la ciberresiliencia. En este sentido, como se ha indicado, las organizaciones deben estar preparadas para prevenir ataques, recuperarse de ellos rápidamente y mantener la operación en marcha para minimizar el daño financiero y reputacional. Al respecto, cabe enfatizar que, según la ISO (2016), una organización resiliente puede continuar operando pese a los ataques, recuperándose con rapidez y adaptándose a nuevos entornos de amenaza, una capacidad clave para la competitividad de las empresas en un mercado globalizado.

Además de los marcos normativos internacionales, en América Latina se han desarrollado iniciativas que buscan fortalecer la ciberseguridad regional como un componente estratégico para proteger infraestructuras críticas y modelos de negocio. Países como México, Chile, Brasil, Argentina y Colombia han adoptado estrategias nacionales de ciberseguridad que establecen principios de protección de datos, continuidad operativa y cooperación público-privada. En el caso colombiano, se destacan la Ley 1581 de 2012, que regula la protección de datos personales, y su Decreto Reglamentario 1377 de 2013, que establece las condiciones para el tratamiento de datos por parte de organizaciones públicas y privadas. Adicionalmente, la Ley 1266 de 2008 regula el *habeas data* financiero, y la Ley 1273 de 2009 tipifica los delitos informáticos, lo cual brinda herramientas legales para sancionar las conductas cibernéticas que afectan los activos digitales empresariales.

A nivel estratégico, el país cuenta con el CONPES 3995 de 2020, que establece la Política Nacional de Seguridad Digital, y la Estrategia de Ciberseguridad 2020-2025, liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTic), que reconoce a la ciberseguridad como un habilitador de la transformación digital y prioriza la protección de los sectores económico, financiero, salud, energía y defensa. Estas normativas y políticas no solo buscan reducir la vulnerabilidad digital, sino también generar condiciones de confianza para el desarrollo empresarial y la inversión en tecnologías emergentes. Su adecuada implementación por parte de las organizaciones fortalece su cumplimiento normativo, su reputación corporativa y su resiliencia frente a amenazas cibernéticas avanzadas.

Amenazas y riesgos en la era digital

En la era digital las organizaciones están expuestas a un espectro cada vez más amplio de amenazas cibernéticas que afectan su funcionamiento y seguridad. La evolución de estas amenazas, tanto en complejidad como en frecuencia, pone en riesgo la infraestructura tecnológica, la confidencialidad de la información y, en última instancia, la viabilidad financiera y la reputación de las empresas. En particular, uno de los mayores desafíos que enfrentan las organizaciones es que los atacantes utilizan herramientas cada vez más sofisticadas, lo cual les permite vulnerar sistemas, acceder a datos confidenciales o interrumpir servicios críticos sin ser detectados inicialmente (Lewis, 2020).

Entre las amenazas más comunes se encuentran los ataques de denegación de servicio distribuido (DDoS), el *ransomware*, el *phishing* y el *malware*. Los ataques DDoS, por ejemplo, tienen como objetivo abrumar la infraestructura de una organización con tráfico masivo, bloqueando el acceso a los usuarios legítimos. En tanto, el *ransomware* secuestra datos o sistemas y exige un rescate a cambio de devolver el acceso. El *phishing* es otro tipo de ataque que engaña a los empleados para que proporcionen credenciales o información confidencial a través de correos electrónicos fraudulentos. El *malware*, por su parte, puede instalarse silenciosamente en un sistema, comprometer la seguridad de la red y permitir el acceso no autorizado a los ciberdelincuentes (Porter & Millar, 2017).

El impacto de estos ataques varía según el sector. Por ejemplo, las industrias financieras son especialmente vulnerables debido a la naturaleza sensible de los datos que manejan, como información bancaria y personal de clientes, de manera que un ataque en este sector puede tener consecuencias devastadoras, tanto financieras como reputacionales. De hecho, según un informe reciente, el 71 % de las empresas financieras han sufrido ciberataques en los últimos cinco años, lo cual resalta la gravedad del problema (Gordon & Loeb, 2021). Además, las brechas de seguridad en este sector también pueden desencadenar sanciones regulatorias, como las impuestas por el Reglamento General de Protección de Datos (GDPR) en Europa, lo que agrava aún más las pérdidas.

El sector salud es otro objetivo atractivo para los atacantes. Dado que las organizaciones de salud manejan grandes volúmenes de datos personales y clínicos, son un blanco ideal para el robo de información. Los ciberataques en este sector no solo exponen la información privada de los pacientes, sino que también pueden comprometer la seguridad física de las personas, especialmente cuando los sistemas hospitalarios que controlan equipos médicos son vulnerados. Al

respecto, cabe recordar que el ataque de *ransomware* a los hospitales de National Health Service (NHS) en el Reino Unido en 2017 mostró el potencial catastrófico de estos incidentes al interrumpir servicios críticos (Lewis, 2020).

Con la adopción de nuevas tecnologías como el IoT y la IA, las organizaciones han expandido considerablemente sus superficies de ataque. Los dispositivos IoT, que incluyen desde cámaras de seguridad hasta termostatos conectados, son particularmente vulnerables debido a la falta de estandarización en sus medidas de seguridad. Muchos de estos dispositivos no cuentan con características de seguridad básicas, lo cual los convierte en puertas de entrada fáciles para los atacantes. La IA, por otro lado, aunque ofrece grandes beneficios en términos de automatización y análisis predictivo, también puede ser explotada para lanzar ataques más precisos y efectivos (Gordon & Loeb, 2021).

En este escenario, a medida que las organizaciones siguen digitalizándose, también enfrentan el reto de mantenerse al día con las regulaciones y los estándares de ciberseguridad que exigen cada vez más medidas preventivas. Normativas como la ISO 27001 y el GDPR están diseñadas para proteger los datos personales y asegurar que las organizaciones implementen medidas de seguridad adecuadas. El incumplimiento de estas normativas no solo expone a las empresas a ataques, sino que también puede resultar en multas significativas, como se vio en los casos de Facebook y British Airways, que enfrentaron sanciones millonarias por incumplimiento del GDPR (ISO, 2013).

Sintetizando, en la era digital las organizaciones enfrentan una amplia gama de amenazas cibernéticas que varían en complejidad y en su capacidad de interrumpir las operaciones críticas. Esto puede comprometer la seguridad de los datos, dañar la infraestructura tecnológica y tener un impacto significativo en la reputación y las finanzas de las empresas. La tabla 1 resume las principales amenazas en la era digital y proporciona una descripción general de cada amenaza, su probabilidad de impacto en las organizaciones y las fuentes bibliográficas que respaldan esta información.

Tabla 1. Amenazas y riesgos en la era digital en 2024

Amenaza	Descripción	Probabilidad de impacto	Fuente
Denegación de Servicio Distribuido (DDoS)	Ataques que sobrecargan los servidores y las redes de la organización con una cantidad masiva de tráfico, de tal forma que bloquea el acceso a usuarios legítimos.	Alta	Lewis (2020); Porter y Millar (2017).

Amenaza	Descripción	Probabilidad de impacto	Fuente
Ransomware	Secuestro de datos o sistemas informáticos para solicitar un rescate a cambio de devolver el acceso.	Alta	Lewis (2020); Gordon y Loeb (2021).
Phishing	Correos electrónicos fraudulentos que engañan a los empleados para que proporcionen credenciales o información confidencial.	Media	Porter y Millar (2017).
Malware	Software malicioso que se instala en un sistema para comprometer la seguridad de la red o permitir acceso no autorizado.	Alta	Lewis (2020); ISO (2013).
Ataques al Internet de las Cosas (IoT)	Ataques a dispositivos IoT debido a la falta de estandarización en las medidas de seguridad, lo cual los convierte en un blanco fácil para atacantes.	Media	Gordon y Loeb (2021).

Fuente: Elaboración propia.

La tabla 1 destaca, por una parte, que el *ransomware* y los ataques DdoS y a dispositivos IoT han crecido en frecuencia y sofisticación, y, por otra, que su impacto potencial puede variar según la preparación y las defensas de cada organización. Dado que estas amenazas afectan tanto a grandes corporaciones como a pequeñas y medianas empresas, es necesario que estas adopten medidas de ciberseguridad robustas para mitigar los riesgos asociados.

Si bien es común analizar las amenazas cibernéticas desde una perspectiva técnica, es igualmente importante evaluar su impacto económico para comprender la magnitud del riesgo que representan para las organizaciones, pues los ciberataques no solo afectan la integridad de los sistemas, sino que generan pérdidas millonarias relacionadas con la interrupción operativa, la pérdida de datos, el deterioro reputacional y los costos legales asociados. Precisamente, con base en estudios recientes y reportes de instituciones reconocidas, la tabla 2 relaciona algunas de las amenazas más comunes en el entorno digital con su impacto económico estimado. Esta información resalta la urgencia de incorporar la ciberseguridad como una inversión estratégica clave para la sostenibilidad y la competitividad empresarial.

Tabla 2. Impacto económico estimado de las principales amenazas cibernéticas en las organizaciones

Amenaza cibernética	Impacto económico estimado (USD)	Fuente
Ransomware	4.44 millones por incidente (promedio).	IBM Security (2023) – Cost of a Data Breach Report.

Ataques DDoS	20 000 – 100 000 por hora de inactividad.	Kaspersky (2022).
Phishing	17 700 por minuto (pérdida promedio).	FBI Internet Crime Report (2021).
Ataques a IoT	1 millón por incidente (estimado).	Ponemon Institute (2022).
Violación de datos personales	3.86 millones por incidente.	IBM Security (2020).
Suplantación de identidad (deepfake)	250 mil – 1 millón por fraude dirigido.	Deloitte (2021) ; Chesney (2019).
Ataques de cadena de suministro	4.29 millones por incidente.	IBM Security (2023).
Malware (troyanos, spyware, etc.)	2.6 millones promedio en costos de remediación.	Accenture Cyber Threatscape (2022).

Fuente: Elaboración propia.

La ciberseguridad como prioridad estratégica

Como se indicó en los apartados anteriores, en la era digital la ciberseguridad ha dejado de ser un mero componente técnico para convertirse en una prioridad estratégica clave para la continuidad operativa de las empresas. Con el crecimiento de las amenazas cibernéticas y el aumento de la dependencia de las organizaciones en infraestructuras tecnológicas, las empresas están comprendiendo que la ciberseguridad es un factor fundamental no solo para proteger sus activos, sino también para mantener su competitividad en un entorno global altamente digitalizado. A continuación, se exploran tres aspectos esenciales: la importancia de la ciberseguridad en la continuidad operativa, su relación con la competitividad empresarial y algunos estudios de caso de empresas que han convertido la ciberseguridad en un diferenciador clave.

Importancia de la ciberseguridad en la continuidad operativa

La continuidad operativa, un principio fundamental en la gestión empresarial, se refiere a la capacidad de una organización para mantener sus funciones críticas durante o después de un incidente. En este contexto, la ciberseguridad tiene un papel crucial para que los sistemas de información, que son el núcleo de muchas operaciones empresariales, estén protegidos frente a interrupciones causadas por ataques cibernéticos. Incidentes como los ataques de *ransomware* o las brechas de datos pueden paralizar completamente una empresa y provocar no solo pérdidas económicas, sino también daños reputacionales a largo plazo (Gordon & Loeb, 2021).

Para mitigar estos riesgos, las empresas están implementando planes de continuidad del negocio que incluyen medidas de ciberseguridad robustas. Estos planes integran estrategias para la recuperación de datos, la protección de infraestructuras críticas, y la resiliencia cibernética, lo cual permite a las organizaciones responder rápidamente a incidentes y minimizar las interrupciones. Por ejemplo, las organizaciones que han implementado la norma ISO 22301, la cual establece un marco para gestionar la continuidad del negocio, han fortalecido su capacidad para resistir ciberataques y seguir operando (ISO, 2016). Esto subraya la importancia de la ciberseguridad como un pilar esencial para la continuidad operativa, especialmente en industrias que dependen de la disponibilidad constante de sus sistemas.

Relación entre la ciberseguridad y la competitividad

La ciberseguridad no solo protege los activos de una organización, sino que también puede actuar como un diferenciador competitivo en el mercado. Las empresas que demuestran un compromiso con la seguridad de los datos pueden generar mayor confianza entre los clientes, los socios comerciales y las otras partes interesadas. Esta confianza es especialmente valiosa en sectores como las finanzas y la salud, donde los consumidores son cada vez más conscientes de la importancia de la privacidad y la protección de la información personal (Porter & Millar, 2017).

Además, la implementación de normativas de ciberseguridad como la ISO 27001 y el cumplimiento de regulaciones como el Reglamento General de Protección de Datos (GDPR) no solo ayudan a proteger los sistemas, sino que también abren oportunidades para acceder a nuevos mercados. En la Unión Europea, por ejemplo, las empresas que cumplen con el GDPR pueden participar en licitaciones y proyectos públicos que exigen altos estándares de seguridad. De esta forma, la ciberseguridad no solo actúa como una medida preventiva, sino que también se convierte en una herramienta estratégica que impulsa la innovación y mejora la competitividad (ISO, 2013).

Estudio de caso de empresas que han convertido la ciberseguridad en un diferenciador clave

Un claro ejemplo de una empresa que ha convertido la ciberseguridad en un diferenciador clave es Apple Inc. A lo largo de los años, Apple se ha destacado por su enfoque riguroso en la protección de los datos de sus usuarios, para lo cual ha integrado medidas de encriptación y protección de la privacidad en todos sus dispositivos y servicios, lo cual le ha permitido diferenciarse en un mercado tecnológico altamente competitivo, donde los consumidores valoran cada vez más la

privacidad y la seguridad de sus datos. En otras palabras, Apple ha convertido la seguridad en un pilar de su propuesta de valor, y esto se ha reflejado en la lealtad de sus clientes y en el crecimiento de sus ingresos (Smith, 2018).

Otro estudio de caso interesante es Aetna, una empresa de seguros de salud que ha implementado un enfoque proactivo en ciberseguridad. Aetna ha desarrollado un sistema avanzado de inspección del tráfico y detección de amenazas en tiempo real, lo cual le ha permitido ofrecer un nivel de protección superior a sus clientes. Esta capacidad para garantizar la seguridad de la información personal y de salud ha mejorado la reputación de la empresa en un sector donde la confianza y la confidencialidad son esenciales. La inversión en ciberseguridad no solo ha protegido a Aetna de posibles brechas de datos, sino que también le ha permitido posicionarse como un líder en seguridad dentro del sector asegurador (Porter & Millar, 2017).

Por su parte, Verizon, una de las principales empresas de telecomunicaciones del mundo, ha integrado la ciberseguridad en su estrategia global como un factor diferenciador. Específicamente, su enfoque en la seguridad no solo se centra en proteger su infraestructura, sino también en ofrecer soluciones de seguridad avanzadas a sus clientes. Además se ha destacado por su capacidad de respuesta ante incidentes y por su inversión en tecnologías de seguridad de vanguardia, lo cual le ha permitido fortalecer su posición en el mercado y ganar la confianza de los consumidores y las empresas que dependen de sus servicios (Gordon & Loeb, 2021).

El papel del Estado y las Fuerzas Armadas en la protección de modelos de negocio estratégicos

En el contexto de las amenazas híbridas y el ciberterrorismo, si bien las capacidades en ciberdefensa, inteligencia y respuesta ante incidentes que tienen el Estado y las Fuerzas Armadas son cruciales para proteger las infraestructuras críticas y los modelos de negocio estratégicos, estas deben ser complementarias a las acciones del sector privado. En países como Colombia, la Política Nacional de Seguridad Digital (CONPES 3995 de 2020) y la Estrategia de Ciberseguridad 2020-2025, lideradas por el MinTic y la Presidencia de la República, establecen lineamientos para fortalecer la ciberresiliencia nacional. Por su parte, las Fuerzas Armadas, a través de unidades especializadas en ciberdefensa, también cumplen un papel fundamental en la protección de activos estratégicos ante amenazas de origen estatal o criminal. Esta colaboración público-privada es esencial para garantizar un entorno digital seguro para el desarrollo empresarial.

Impacto en grandes corporaciones y tecnologías emergentes

En la actualidad, las grandes corporaciones están adoptando rápidamente nuevas tecnologías, como el IoT, la IA y los servicios en la nube para mejorar la eficiencia operativa, optimizar la toma de decisiones y generar nuevas oportunidades de negocio. Estas tecnologías emergentes ofrecen una gran cantidad de beneficios, pero también aumentan significativamente la exposición de las empresas a ciberataques debido a la expansión de la superficie de ataque. No obstante, a medida que estas tecnologías se integran en los procesos críticos de las organizaciones, las amenazas cibernéticas evolucionan y se diversifican, lo cual exige una atención especial en la gestión de los riesgos cibernéticos.

Cómo las grandes empresas están adoptando nuevas tecnologías y cómo esto aumenta su exposición a ataques

El IoT ha transformado la forma en que las empresas recopilan y gestionan datos, conectando dispositivos y sensores en red para monitorizar, controlar y automatizar procesos en tiempo real. Particularmente, en sectores como la manufactura y la logística, el IoT ha permitido avances significativos en la gestión de cadenas de suministro y en la eficiencia operativa (Gordon & Loeb, 2021). Sin embargo, cada dispositivo conectado a la red representa un potencial punto de entrada para los ciberdelincuentes, pues la falta de estándares de seguridad en muchos dispositivos IoT y la creciente conectividad entre ellos crea vulnerabilidades explotables. Por ejemplo, en 2016, el ataque de Mirai Botnet aprovechó dispositivos IoT vulnerables para llevar a cabo un DDoS masivo que interrumpió grandes porciones de internet, lo cual afectó a empresas como Twitter, Netflix y Amazon (Lewis, 2020).

De igual forma, aunque la adopción de IA también ha revolucionado áreas como la analítica predictiva, la automatización de procesos y la detección de fraudes, esta tecnología también puede ser explotada por atacantes que utilicen técnicas avanzadas para manipular sistemas de toma de decisiones automatizados. Por ejemplo, pueden entrenar modelos de IA con datos manipulados para que tomen decisiones erróneas, lo que se conoce como un ataque adversarial (Porter & Millar, 2017). Además, los sistemas de IA que manejan grandes cantidades de datos personales o financieros son objetivos prioritarios para los ciberdelincuentes que buscan acceder a esta información sensible.

Por su parte, la nube ha proporcionado a las grandes corporaciones flexibilidad y escalabilidad en sus infraestructuras tecnológicas, lo cual les ha permitido almacenar y gestionar grandes volúmenes de datos a bajo costo. Sin embargo, el uso de la nube también presenta riesgos de seguridad, ya que los datos almacenados

en servidores de terceros pueden ser objeto de acceso no autorizado o de ataques a gran escala. De hecho, los incidentes de violación de datos en servicios en la nube, como el ataque a Equifax en 2017, que expuso los datos personales de 147 millones de personas, subrayan la vulnerabilidad inherente de las infraestructuras en la nube cuando no se implementan adecuadas medidas de seguridad (Gordon & Loeb, 2021).

Brechas de seguridad en infraestructuras tecnológicas complejas

Las infraestructuras tecnológicas complejas que gestionan grandes corporaciones a menudo combinan diversas tecnologías y plataformas, lo cual incrementa el riesgo de brechas de seguridad. En una infraestructura compleja, un solo punto débil puede comprometer toda la red y crear, por tanto, oportunidades para que los atacantes exploten vulnerabilidades. Además, se debe tener en cuenta que los sistemas de tecnología de la información (TI) de las grandes corporaciones suelen ser el resultado de integraciones y migraciones de tecnologías antiguas a nuevas, lo cual resulta a menudo en incompatibilidades y malas configuraciones que pueden ser explotadas por los ciberdelincuentes (Lewis, 2020).

Por ejemplo, las organizaciones que migran sus datos y aplicaciones a la nube, pero conservan sistemas *on-premise*, pueden no implementar adecuadamente las políticas de seguridad entre entornos híbridos, lo cual crea brechas que los atacantes pueden explotar. Las malas configuraciones en la nube también son un problema recurrente. Según un informe de Gartner (2020), hasta el 99 % de los fallos de seguridad en la nube para 2025 serán responsabilidad del cliente, lo cual implica que las configuraciones inadecuadas, los permisos excesivos y la falta de control sobre los datos almacenados pueden abrir la puerta a ataques devastadores (Porter & Millar, 2017).

Un caso reciente que evidencia estas brechas es el que sufrió Capital One en 2019, donde una mala configuración en un servidor en la nube permitió que un ciberdelincuente accediera a los datos personales de más de cien millones de clientes. Este tipo de incidentes demuestra que, aunque las nuevas tecnologías ofrecen ventajas significativas, las empresas deben estar preparadas para gestionar de manera adecuada los riesgos asociados a las infraestructuras tecnológicas complejas (Gordon & Loeb, 2021).

Además, las redes de grandes corporaciones usualmente incluyen numerosos proveedores externos, lo cual aumenta las superficies de ataque. En este sentido, dado que cada proveedor puede introducir vulnerabilidades adicionales, es necesario que las grandes corporaciones implementen controles estrictos para

asegurar que todos los componentes de su infraestructura cumplan con los más altos estándares de ciberseguridad. La complejidad de las redes y la integración de proveedores externos significa que un ataque exitoso en un eslabón más débil puede comprometer toda la cadena de suministro, como ocurrió con el ataque a Target en 2013, donde los ciberdelincuentes accedieron a la red a través de un proveedor de servicios de climatización (ISO, 2013).

En síntesis, si bien adoptar tecnologías emergentes en grandes corporaciones puede mejorar considerablemente su eficiencia operativa, también es cierto que incrementa su exposición a riesgos cibernéticos. En otras palabras, las infraestructuras tecnológicas complejas introducen nuevos puntos de vulnerabilidad que requieren medidas de seguridad avanzadas y una gestión de riesgos proactiva para proteger a las empresas de ciberataques cada vez más sofisticados.

Beneficios de invertir en ciberseguridad

En un mundo cada vez más digitalizado, invertir en ciberseguridad no es solo una necesidad operativa, sino una estrategia clave que ofrece múltiples beneficios en términos de protección, confianza del cliente y desarrollo empresarial. Actualmente, la transformación digital ha impulsado a las organizaciones a depender cada vez más de sistemas conectados y del intercambio de datos a nivel global, lo que hace que la ciberseguridad sea esencial para la continuidad del negocio y el desarrollo de operaciones. En este contexto, la ciberseguridad no solo protege los sistemas de la organización, sino que también refuerza su reputación y mejora su posición competitiva en el mercado. Las organizaciones que destinan recursos a implementar medidas sólidas de ciberseguridad están mejor preparadas para enfrentar las amenazas emergentes, al tiempo que apoyan su transformación digital de manera segura.

Una de las principales razones por las cuales la ciberseguridad es crucial para las organizaciones modernas es su impacto directo en la continuidad del negocio. La disponibilidad de los sistemas y la protección de los datos son fundamentales para garantizar que las operaciones críticas no se vean interrumpidas por un ciberataque. Un incidente de seguridad que paralice los sistemas operativos o comprometa datos clave puede resultar en graves pérdidas financieras, daños a la reputación y, en algunos casos, el cese total de las operaciones (ISO, 2016). Por lo tanto, implementar un sólido plan de continuidad del negocio que incluya medidas de ciberseguridad permite a las empresas mantenerse operativas incluso frente a incidentes inesperados, de tal forma que pueden minimizar el tiempo de

inactividad y las pérdidas asociadas. En este sentido, la ciberseguridad no solo es una barrera contra los ciberataques, sino también un componente vital para asegurar la resiliencia operativa de la organización.

El desarrollo de operaciones también se ve beneficiado por la inversión en ciberseguridad. En la medida en que las organizaciones integran tecnologías emergentes como la IA, el IoT y los servicios en la nube, la seguridad de los datos y la protección de los sistemas interconectados se vuelven imprescindibles. Si bien es cierto que estas tecnologías permiten la optimización de procesos, la automatización de tareas y la toma de decisiones más rápidas y basadas en datos, lo cual mejora significativamente la eficiencia operativa, también es importante tener presente que crean nuevas superficies de ataque. Teniendo en cuenta lo anterior, se puede afirmar que una empresa que invierte en ciberseguridad desde el inicio de su transformación digital garantiza que sus operaciones sean ágiles, escalables y seguras, lo cual le permite adaptarse rápidamente a los cambios del entorno y a las exigencias del mercado global, sin exponer sus sistemas a vulnerabilidades críticas (Lewis, 2020).

En este contexto, la transformación digital no puede considerarse completa sin una sólida estrategia de ciberseguridad. Las empresas que se embarcan en la digitalización de sus procesos deben asegurar que cada paso esté respaldado por medidas de seguridad que protejan tanto sus activos como los datos de sus clientes. Esto resulta relevante en un contexto en el que la confianza digital se ha convertido en uno de los factores determinantes en la adopción de nuevas tecnologías y servicios, de manera que los clientes y los socios comerciales exigen que las empresas que adoptan la digitalización garanticen altos niveles de protección de datos y privacidad (Gordon & Loeb, 2021). Por tanto, una transformación digital segura permite a las organizaciones no solo mejorar su eficiencia y competitividad, sino también consolidar la confianza de sus clientes, quienes estarán más dispuestos a compartir sus datos y participar en ecosistemas digitales interconectados.

Además, el cumplimiento de normativas y estándares internacionales de ciberseguridad tiene un papel vital en el éxito de la transformación digital de una organización. La adopción de estándares como la ISO/IEC 27001 y el Reglamento General de Protección de Datos (GDPR) no solo asegura que las empresas cumplan con las regulaciones más estrictas en términos de seguridad, sino que también les permiten acceder a nuevos mercados y establecer relaciones comerciales con empresas que valoran la ciberseguridad como un componente esencial de la cooperación. Así, el cumplimiento de estas normativas demuestra que las empresas están

comprometidas con la protección de datos y la seguridad de sus operaciones, lo cual les otorga una ventaja competitiva en un entorno globalizado donde la confianza digital es fundamental para el crecimiento y la expansión (ISO, 2013).

Desde otra perspectiva, cabe señalar que el retorno de inversión en ciberseguridad va más allá de la mera protección contra amenazas, pues las empresas que invierten en ciberseguridad logran mejorar su capacidad de innovación al garantizar que sus infraestructuras digitales sean seguras y estén preparadas para el futuro. Es decir, al reducir el riesgo de ciberataques, las empresas pueden centrarse en el desarrollo de nuevos productos, servicios y estrategias que impulsen el crecimiento, sin temor a que sus avances sean comprometidos por brechas de seguridad. En resumen, la ciberseguridad no solo es una necesidad operativa en la era digital, sino también un impulsor clave de la continuidad, el desarrollo y la transformación empresarial.

Cómo la ciberseguridad impulsa la confianza de los clientes y mejora la reputación corporativa

Uno de los beneficios más inmediatos de invertir en ciberseguridad es la mejora de la confianza de los clientes. En un entorno digital cada vez más complejo, donde los consumidores están profundamente preocupados por la seguridad de sus datos personales y financieros, la ciberseguridad se ha convertido en un factor decisivo para la construcción de relaciones de confianza a largo plazo. En este sentido, las empresas que demuestran un fuerte compromiso con la protección de la información pueden diferenciarse en un mercado saturado y ganar la lealtad de los clientes. Esta lealtad no solo se traduce en ventas repetidas, sino también en la disposición de los clientes a recomendar la marca, lo cual refuerza la reputación de la empresa de manera positiva (Porter & Millar, 2017).

El hecho de que los consumidores estén dispuestos a cambiar de proveedor si sienten que su información no está suficientemente protegida resalta la importancia de la ciberseguridad en la toma de decisiones de compra. De hecho, un estudio de PricewaterhouseCoopers (PwC, 2020) encontró que el 87 % de los consumidores afirmaron que cambiarían de proveedor si perciben que una empresa no tiene medidas adecuadas para proteger su información; sin duda, este dato revela que la confianza no solo es un beneficio secundario, sino también un factor crítico para la sostenibilidad empresarial. Por otro lado, una encuesta realizada por Deloitte (2021) mostró que las empresas que implementan medidas de ciberseguridad y transparencia en el manejo de los datos experimentan un crecimiento de la satisfacción del cliente y una mayor retención de estos. Como se puede evidenciar, estos

resultados refuerzan la idea de que la inversión en seguridad no es un gasto, sino un activo valioso que protege a la empresa de daños financieros y reputacionales.

Como se señaló en otro apartado, empresas como Apple han convertido la seguridad y la privacidad en pilares de su propuesta de valor, lo cual ha fortalecido su posición en el mercado como una marca confiable. Desde la introducción de funciones avanzadas, como el encriptado de extremo a extremo y la implementación de políticas de privacidad estrictas, Apple ha construido una reputación sólida en torno a la protección de los datos de sus clientes y, por este camino, además de destacarse frente a sus competidores, se ha ganado la lealtad de sus usuarios. Para Apple, la ciberseguridad no es solo una respuesta a los riesgos, sino un elemento esencial de su estrategia de diferenciación. Como resultado, la empresa ha logrado mantener y mejorar su reputación corporativa y posicionarse como líder en la seguridad de la información en la industria tecnológica (Smith, 2018).

Por el contrario, las organizaciones que no logran proteger adecuadamente los datos de sus clientes corren el riesgo de perder no solo la confianza de los consumidores, sino también su posición en el mercado, como sucedió con Equifax y Target en los últimos años. En el caso de Equifax, la brecha de seguridad en 2017 expuso los datos personales de más de 147 millones de personas, incluyendo números de seguridad social, lo cual resultó en una pérdida masiva de confianza por parte de los clientes, una caída significativa en el valor de las acciones de la empresa y una larga batalla legal. Del mismo modo, en 2013 Target sufrió un ataque que comprometió los datos de pago de aproximadamente 40 millones de clientes, lo que también afectó gravemente su reputación y le costó millones en multas y compensaciones (Gordon & Loeb, 2021).

Estas situaciones ilustran que la falta de inversión en ciberseguridad puede tener consecuencias a largo plazo y afectar no solo las operaciones internas de la empresa, sino también la relación con los clientes y la percepción pública de la marca. En este punto es importante recalcar que una vez la confianza se ve comprometida, resulta extremadamente difícil restaurarla, de manera que las empresas pueden necesitar años para recuperarse completamente de los efectos de un ciberataque. Además, la pérdida de reputación no solo afecta a la relación con los clientes actuales, sino que también puede desalentar a posibles clientes o socios comerciales de involucrarse con la organización. Por lo tanto, es fundamental que las empresas vean la ciberseguridad como un elemento estratégico y no solo como una medida de protección (ISO, 2013).

En conclusión, se puede afirmar que la confianza digital es un activo valioso en la economía moderna, por cuanto las empresas que invierten en ciberseguridad pueden cosechar sus beneficios en términos de lealtad del cliente y reputación corporativa. En este sentido, las organizaciones que priorizan la seguridad de los datos no solo protegen su negocio de los riesgos cibernéticos, sino que también fortalecen su marca y su capacidad para competir en un mercado cada vez más exigente.

La ciberseguridad como ventaja competitiva y diferenciador en el mercado

En un entorno empresarial altamente digitalizado y con un creciente número de amenazas cibernéticas, la ciberseguridad no solo es una medida de protección, sino que también puede convertirse en un diferenciador competitivo clave en el mercado. Las organizaciones que priorizan la seguridad de sus datos y sistemas tienen la capacidad de utilizar esta inversión como un argumento de venta para atraer a clientes y socios comerciales que valoran la protección de su información. Así, a medida que la confianza en la seguridad digital se convierte en un factor decisivo para los consumidores, las empresas que demuestran un compromiso firme con la ciberseguridad son percibidas como más confiables y atractivas. Esta percepción no solo refuerza la lealtad del cliente, sino que también mejora el posicionamiento de la marca en el mercado (ISO, 2013).

En sectores altamente regulados como la salud, las finanzas y el comercio electrónico, la ciberseguridad no es solo una cuestión de confianza, sino una exigencia estratégica. En estas industrias, las normativas regulatorias y la sensibilidad de los datos manejados obligan a las organizaciones a cumplir con altos estándares de protección de la información. Por ejemplo, en el sector financiero, los datos sensibles relacionados con transacciones bancarias y activos de clientes exigen estrictos mecanismos de protección de datos, lo cual hace que la seguridad sea un diferenciador crucial en la relación con los clientes. Las empresas que pueden garantizar un nivel superior de ciberseguridad no solo cumplen con las regulaciones, sino que también se posicionan como las opciones más seguras y confiables para los consumidores (Gordon & Loeb, 2021).

Un ejemplo notable de cómo la ciberseguridad puede actuar como una ventaja competitiva es el caso de los proveedores de servicios en la nube como Amazon Web Services (AWS) y Microsoft Azure. Estas empresas han construido una sólida reputación al demostrar su capacidad para manejar datos sensibles de manera segura, cumpliendo con regulaciones estrictas como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. AWS y Azure no solo

proporcionan servicios avanzados de computación en la nube, sino que también ofrecen garantías de seguridad, lo cual les ha permitido atraer a clientes de industrias altamente reguladas, como los sectores financiero y gubernamental. Es decir, al utilizar la seguridad de los datos como un elemento diferenciador, estas empresas no solo satisfacen las necesidades operativas de sus clientes, sino que también se posicionan como líderes en un mercado donde la confianza digital es un requisito fundamental (Porter & Millar, 2017).

Además, la ciberseguridad ofrece un claro retorno de inversión a largo plazo porque reduce los costos asociados con brechas de seguridad y ciberataques, de manera que invertir en medidas preventivas de ciberseguridad permite a las organizaciones minimizar el riesgo de sufrir incidentes que puedan resultar en costos financieros significativos. Además, como se ha enfatizado, las empresas que no priorizan la seguridad enfrentan el riesgo de demandas legales, multas regulatorias y pérdida de clientes en caso de una brecha de seguridad. De hecho, según un estudio realizado por IBM Security (2020), el costo promedio de una brecha de datos en 2020 fue de 3.86 millones de dólares. Este estudio también mostró que las organizaciones que habían implementado medidas de seguridad avanzadas, como la automatización de la ciberseguridad y la encriptación de datos, lograron reducir estos costos en 30 % en comparación con aquellas que no lo hicieron.

En este contexto también conviene tener presente que la prevención es clave, pues las organizaciones que invierten en seguridad avanzada no solo protegen sus operaciones diarias, sino que también previenen futuros gastos relacionados con la remediación de brechas. Además, no solo está el hecho de que el costo de implementar soluciones robustas de ciberseguridad es significativamente menor al que tiene gestionar las consecuencias de un ataque, sino que además las empresas que gestionan adecuadamente su ciberseguridad también pueden beneficiarse de descuentos en seguros cibernéticos, ya que demuestran un perfil de riesgo más bajo. Por lo tanto, la inversión en ciberseguridad no solo proporciona una ventaja competitiva, sino que también asegura la viabilidad financiera de la organización a largo plazo (IBM Security, 2020).

En resumen, dado que la ciberseguridad se ha convertido en un activo estratégico, las empresas que pueden demostrar una mayor ciberresiliencia frente a los ataques no solo mejoran su propia seguridad, sino que también se vuelven más atractivas para los consumidores y los socios comerciales. Por esta razón, la capacidad de mitigar los riesgos y de operar de manera confiable y segura en un entorno digital constituye actualmente un diferenciador clave que puede mejorar

la imagen corporativa y proporcionar una ventaja sostenida en el mercado. Así, al integrar la ciberseguridad como parte central de su estrategia empresarial, las organizaciones no solo están protegiendo sus activos, sino también construyendo una base sólida para el crecimiento a largo plazo.

Evolución de las amenazas cibernéticas

En la última década, el panorama de amenazas cibernéticas ha evolucionado significativamente debido a la rápida adopción de tecnologías emergentes como la nube, el IoT y la IA. Aunque estas tecnologías han traído beneficios incuestionables en términos de eficiencia y capacidad operativa, también han creado nuevas vulnerabilidades que los ciberdelincuentes han aprovechado para lanzar ataques más sofisticados y a gran escala. Como se ha enfatizado, este aumento en la superficie de ataque ha incrementado el riesgo de ciberataques para organizaciones de todos los sectores y tamaños (Lewis, 2020).

La nube, por ejemplo, ha transformado la forma en que las empresas almacenan y gestionan sus datos, ofreciendo flexibilidad y escalabilidad sin precedentes. Sin embargo, el uso generalizado de servicios en la nube también ha generado riesgos significativos en términos de control de acceso, configuración incorrecta y violaciones de datos. Los atacantes pueden aprovechar estos puntos débiles para comprometer grandes cantidades de datos sensibles, como se vio en los ciberataques a Equifax y Capital One en los últimos años, donde millones de registros fueron expuestos debido a fallos en la seguridad de la nube (Gordon & Loeb, 2021).

Por su parte, el IoT ha ampliado enormemente el número de dispositivos conectados a las redes empresariales y domésticas, desde cámaras de seguridad hasta termostatos inteligentes. Si bien estos dispositivos facilitan la automatización y optimización de procesos, a menudo carecen de medidas de seguridad robustas, lo que los convierte en blancos fáciles para los atacantes. Por ejemplo, los cibercriminales pueden utilizar dispositivos IoT comprometidos para formar *botnets* que lanzan ataques DDoS, como ocurrió con el ataque Mirai en 2016, que afectó a gran parte de internet al aprovechar dispositivos IoT mal protegidos (Lewis, 2020).

En este contexto, la adopción de la IA también ha traído consigo nuevos desafíos en ciberseguridad. Si bien esta tecnología se utiliza para detectar y prevenir amenazas de manera proactiva, los ciberdelincuentes también pueden utilizarla para desarrollar ataques más efectivos, como en el caso de la suplantación de

identidad mediante el uso de técnicas avanzadas de *deepfake*. Específicamente, estas técnicas permiten falsificar credenciales o crear identidades digitales falsas, lo cual puede tener consecuencias devastadoras en contextos donde la autenticación segura es crucial (Chesney, 2019). Además, la manipulación de sistemas de IA para que tomen decisiones erróneas o sesgadas, lo que se conoce como ataques adversariales, representa una nueva frontera en el panorama de amenazas. Finalmente, con la idea de sintetizar este panorama, a continuación la tabla 3 presenta la evolución de las amenazas cibernéticas.

Tabla 3. Evolución de las amenazas cibernéticas

Período	Principales amenazas	Tecnologías afectadas	Nuevas vulnerabilidades
2000-2004	<i>Spyware</i> , <i>phishing</i> , DDoS y gusanos. Aparecen troyanos más avanzados.	Servidores web, correos electrónicos y redes más avanzadas.	Uso masivo del correo electrónico y poca educación en <i>phishing</i> .
2005-2009	<i>Ransomware</i> temprano, violaciones de datos masivas y <i>malware</i> móvil.	Plataformas móviles, servidores empresariales y datos masivos.	Uso masivo de dispositivos móviles y falta de protección adecuada en almacenamiento masivo.
2010-2014	Crecimiento de <i>ransomware</i> , violaciones a gran escala de datos y ataques en la nube.	Nube, plataformas móviles y redes empresariales.	Almacenamiento en la nube y adopción masiva de la movilidad en las empresas.
2015-2019	<i>Ransomware</i> sofisticado, ataques dirigidos (APT), ataques a IoT y violaciones de datos.	Dispositivos IoT, redes críticas e infraestructura en la nube.	IoT sin protección adecuada y ataques APT a objetivos críticos.
2020-2024	<i>Ransomware</i> avanzado, suplantación de identidad con IA (<i>deepfake</i>), ataques a IA y IoT, así como ataques de cadena de suministro.	Infraestructura crítica, IA, IoT y dispositivos personales.	Falta de estandarización en IoT, explotación de vulnerabilidades en IA y <i>deepfakes</i> .

Fuente: Elaboración propia con base en Gordon y Loeb (2021), Lewis (2020), Porter y Millar (2017), Chesney (2019) e IBM Security (2020).

Tipos de ciberataques comunes

La evolución del panorama de amenazas ha llevado a un aumento de varios tipos de ciberataques que buscan comprometer la confidencialidad, la integridad y la disponibilidad de los sistemas y datos:

1. *Ataques a la confidencialidad*: tienen como objetivo comprometer la privacidad de la información. Ejemplos comunes incluyen el robo de credenciales de acceso, números de tarjeta de crédito o información personal de los usuarios. Específicamente, en los ataques de *phishing*, una de las tácticas más utilizadas para obtener acceso a esta información confidencial, los ciberdelincuentes engañan a los usuarios para que proporcionen información sensible a través de correos electrónicos o sitios web fraudulentos (Porter & Millar, 2017).
2. *Ataques a la integridad*: implican la alteración o la manipulación de datos, lo cual puede tener consecuencias graves para las organizaciones. Un ejemplo claro de un ataque a la integridad es el *ransomware*, donde los atacantes cifran los datos de la víctima y exigen un pago a cambio de la clave de descryptación. Además, los ciberdelincuentes pueden modificar registros financieros o médicos, lo cual podría comprometer la toma de decisiones en contextos críticos (Gordon & Loeb, 2021).
3. *Ataques a la disponibilidad*: los DDoS son un ejemplo de este tipo de ataque, en el cual los ciberdelincuentes sobrecargan los servidores o redes con tráfico masivo para que se vuelvan inaccesibles para los usuarios legítimos y, de este modo, interrumpir las operaciones de una empresa, con lo cual causan pérdidas financieras y dañan la reputación de la organización. El ataque DDoS masivo que afectó a varias empresas importantes en 2016 es un recordatorio de los devastadores que pueden ser estos incidentes (Lewis, 2020).
4. *Suplantación de identidad*: la falsificación de credenciales digitales o la suplantación de identidad es otro riesgo creciente, especialmente con el auge de las tecnologías de *deepfake*. Los atacantes pueden utilizar técnicas avanzadas para suplantar a individuos de manera convincente, lo cual les permite acceder a sistemas restringidos o ejecutar transacciones fraudulentas. Cabe agregar que este tipo de ataques puede ser difícil de detectar debido a la sofisticación de las técnicas empleadas (Chesney, 2019).

En síntesis, la evolución del panorama de amenazas cibernéticas ha estado impulsada por el crecimiento de tecnologías emergentes como la nube, el IoT y la IA. Si bien estas tecnologías han traído avances significativos, también han creado nuevas vulnerabilidades que los atacantes pueden explotar. Por lo tanto, a medida que las amenazas continúan evolucionando, las organizaciones deben estar preparadas para implementar medidas de ciberseguridad robustas y proactivas que aborden los riesgos asociados con estas nuevas tecnologías.

Conclusiones

En la era digital, la ciberseguridad se ha convertido en un componente esencial para el éxito y la sostenibilidad de los modelos de negocio de las organizaciones. La creciente digitalización y el uso masivo de tecnologías emergentes, como la nube, el IoT y la IA han creado nuevas vulnerabilidades que los atacantes cibernéticos pueden explotar, lo cual ha incrementado la exposición de las organizaciones a riesgos cibernéticos que pueden afectar gravemente su capacidad para operar y generar valor.

En este escenario, un modelo de negocio bien estructurado, como el propuesto por Osterwalder y Pigneur (2010), depende en gran medida de la protección de los activos digitales, lo cual convierte a la ciberseguridad en un elemento clave para garantizar la continuidad operativa y la satisfacción de los clientes. Por lo tanto, integrar medidas robustas de ciberseguridad no solo mitiga los riesgos de ciberataques, sino que también impulsa la confianza de los clientes y mejora la reputación corporativa. Así, las organizaciones que demuestran un fuerte compromiso con la protección de la información ganan la lealtad de los consumidores y se posicionan de manera más competitiva en el mercado.

Además, la ciberresiliencia, definida como la capacidad de una organización para continuar operando a pesar de los ataques cibernéticos (ISO, 2016), es fundamental para minimizar el impacto de los incidentes y mantener la operación del negocio. En particular, esta capacidad de recuperación es crucial para sectores que dependen de la continuidad de sus operaciones, como las finanzas, la salud y la manufactura.

Por último, la inversión en ciberseguridad no solo protege los activos de una organización, sino que también facilita el cumplimiento de normativas internacionales, como la ISO 27001 y el GDPR. Estas certificaciones no solo ayudan a las empresas a cumplir con los requisitos legales, sino que también les permiten acceder a nuevos mercados y proyectos de gran envergadura, lo cual les otorga una ventaja competitiva.

La sinergia entre modelo de negocio, ciberseguridad y ciberresiliencia es esencial para el éxito en un entorno digital cada vez más vulnerable a ciberataques. Las organizaciones que invierten en estas áreas no solo protegen sus operaciones, sino que también construyen una base sólida para el crecimiento y la innovación.

Referencias

- Aldasoro, I. (2020). *Ciberseguridad en las organizaciones: retos y estrategias*. Editorial Tecnológica.
- Anderson, R., & Moore, T. (2018). *The economics of information security*. The MIT Press.
- Berger, A. (2022). *Small business cybersecurity: Protecting your business from digital threats*. Cybertech Publications.
- Chesbrough, H. (2007). *Open business models: How to thrive in the new innovation landscape*. Harvard Business School Press.
- Chesney, R. (2019). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
- European Union Agency for Cybersecurity (ENISA). (2020). *ENISA threat landscape report*. ENISA. <https://tinyurl.com/4fxctppp>
- Gartner. (2020). *Magic quadrant for security information and event management*. Gartner. <https://tinyurl.com/4v8czak2>
- Gordon, L. A., & Loeb, M. P. (2021). *Managing cybersecurity risk: Why investing in cybersecurity matters*. Business Insights.
- Howard, P., & Prince, A. (2019). *Cybersecurity: Managing systems and data in the information age*. Wiley.
- IBM Security. (2023a). Cost of a data breach report. IBM. <https://www.ibm.com/reports/data-breach>
- International Organization for Standardization (ISO). (2012). *ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity*. <https://www.iso.org/standard/76070.html>
- International Organization for Standardization (ISO). (2013). *ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements*. <https://tinyurl.com/ktkufp2u>
- International Organization for Standardization (ISO). (2016). *ISO 22301:2016 Security and resilience – Business continuity management systems – Requirements*.
- International Telecommunication Union (ITU). (2008). *ITU-T X.1205 - Overview of cybersecurity*. <https://www.itu.int/rec/t-rec-x.1205-200804-i>
- Lewis, J. (2020). *The future of cybersecurity: Emerging technologies and evolving threats*. Routledge.
- Magretta, J. (2002). Why business models matter. *Harvard Business Review*, 80(5), 86-92. <https://tinyurl.com/yc3svm5d>
- National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity*. U.S. Department of Commerce.

- National Institute of Standards and Technology (NIST). (2020). *Cyber resilience engineering*. U.S. Department of Commerce.
- Osterwalder, A., & Pigneur, Y. (2010). *Business model generation: A handbook for visionaries, game changers, and challengers*. John Wiley & Sons.
- Porter, M. E., & Millar, V. E. (2017). How information gives you competitive advantage. *Harvard Business Review*. <https://tinyurl.com/3jxv7amf>
- PricewaterhouseCoopers (PwC). (2020). *Global consumer insights survey 2020*. <https://www.pwc.com/gx/en.html>
- Smith, J. (2018). Apple's privacy strategy: Security as a differentiator in the tech market. *Technology Review*. <https://tinyurl.com/ypj9by3m>
- Teece, D. J. (2010). Business models, business strategy and innovation. *Long Range Planning*, 43(2), 172-194. <https://doi.org/10.1016/j.lrp.2009.07.003>
- World Economic Forum (WEF). (2018). *Cyber resilience: Playbook for public-private collaboration*. WFC. https://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf

Capítulo 2

Desafíos y tendencias en la identidad digital para la seguridad de las infraestructuras críticas*

DOI: <https://doi.org/10.25062/9786287818002.02>

Jaider Ospina Navas

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: En un contexto global marcado por la creciente digitalización, las infraestructuras críticas cibernéticas (ICC) enfrentan importantes desafíos en materia de protección, impulsados por la convergencia entre las tecnologías operativas (TO) y las tecnologías de la información (TI). Este capítulo analiza el papel fundamental de la gestión de la identidad digital en la seguridad de estas infraestructuras, abordando su evolución, vulnerabilidades y tendencias emergentes. Se examinan las ciberamenazas asociadas a la autenticación, la autorización y la suplantación de identidad, así como la interdependencia crítica entre los sistemas físicos y digitales. Asimismo, se presentan soluciones innovadoras basadas en inteligencia artificial, *blockchain*, biometría y autenticación multifactor adaptativa, que fortalecen la resiliencia de las ICC frente a los ciberataques. Por último, se abordan los retos normativos y técnicos que dificultan la adopción de tecnologías avanzadas, destacando la necesidad de marcos abiertos y estrategias integrales que garanticen la continuidad y la seguridad de los servicios esenciales.

Palabras clave: cibernética; ciberriesgos; infraestructura crítica; internet de las cosas; SCADA; tecnologías de la información.

* Capítulo de libro resultado del proyecto de investigación "Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales" del grupo de investigación "Ciberespacio Tecnología e Innovación", de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado C por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) y registrado con el código COL0181179. Los puntos de vista y los resultados de este capítulo pertenecen al autor y no reflejan necesariamente los de las instituciones participantes.

Jaider Ospina Navas

Doctorando en Sistemas de Información. Magíster en Ciencias de la Información y las Comunicaciones e ingeniero electrónico, Universidad Distrital Francisco José de Caldas, Colombia. Consultor en ciberseguridad y arquitecto en soluciones en la nube.

<https://orcid.org/0000-3251-3017> - Contacto: jaider.ospina@esdeg.edu.co

Citación APA: Ospina Navas, J. (2025). Desafíos y tendencias en la identidad digital para la seguridad de las infraestructuras críticas. En M. E. Realpe Díaz & G. A. Gómez Rodríguez (Eds.), *Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales* (pp. 43-78). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818002.02>

CIBERSEGURIDAD EN LA FRONTERA DIGITAL: DESAFÍOS Y OPORTUNIDADES EN LOS NUEVOS ECOSISTEMAS TECNOLÓGICOS EMPRESARIALES

ISBN impreso: 978-628-7602-99-1

ISBN digital: 978-628-7818-00-2

DOI: <https://doi.org/10.25062/9786287818002>

Colección Ciberseguridad y Ciberdefensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2025



Introducción

En la era de la digitalización, las IC, como las redes de energía, las telecomunicaciones, el transporte y el suministro de agua, se han convertido en sistemas altamente interconectados y automatizados.

Esta creciente dependencia de la tecnología digital, si bien mejora la eficiencia operativa, también incrementa su vulnerabilidad ante amenazas cibernéticas. En este contexto, la gestión de la identidad digital de los actores que interactúan con estas infraestructuras adquiere un papel fundamental en su protección y seguridad.

El propósito de este artículo es analizar el rol de la identidad digital en la protección de las ICC, examinando los desafíos que enfrenta, así como las tendencias emergentes en ciberseguridad y ciberdefensa, orientadas a fortalecer la resiliencia de estos sistemas frente a posibles ciberataques.

Identidad digital y su importancia de ciberseguridad para las infraestructuras críticas cibernéticas

Infraestructuras críticas cibernéticas vs. infraestructuras críticas

Este documento centra su análisis en las ICC, entendidas como los componentes digitales que controlan o gestionan las IC, por lo que resulta pertinente identificar sus diferencias y similitudes.

Infraestructuras críticas

Las IC son sistemas físicos y virtuales esenciales para el funcionamiento de una sociedad, como las redes eléctricas, el suministro de agua, el transporte y las telecomunicaciones (Rinaldi et al., 2001).

Estos sistemas son vitales para el bienestar económico, la seguridad y la salud pública de una nación. Por esta razón, su interrupción o destrucción podría tener un impacto significativo en la seguridad nacional, la estabilidad económica y el tejido social.

Según la Directiva 2008/114/CE, las IC son elementos vitales para el mantenimiento de las funciones sociales, así como para la salud, la seguridad y el bienestar económico. La USA PATRIOT Act las define de la siguiente manera:

Sistemas y activos, ya sean físicos o virtuales, tan vitales para los Estados Unidos que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitante en la seguridad, la seguridad económica nacional, la salud o seguridad pública nacional, o cualquier combinación de estas. (Moteff & Parfomak, 2004)

El Proyecto de Ley 245 de 2019 define las IC de la siguiente manera:

Aquellas instalaciones, redes, servicios esenciales, y equipos físicos y de tecnología de la información, en los sectores público y privado, cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las instituciones del Estado, en todos sus niveles de administración pública.

En Colombia, al igual que en otros países, la importancia de definir y proteger estas infraestructuras ha sido ampliamente reconocida. Diversos estudios destacan la necesidad de contar con una legislación clara que garantice su protección y conservación (Alirio et al., 2016).

Infraestructuras críticas cibernéticas

Las ICC son los sistemas y activos digitales que controlan, gestionan y soportan el funcionamiento de las IC a través de medios digitales, como las redes de comunicación y los sistemas informáticos interconectados.

Según *la Guía para la identificación de infraestructura crítica cibernética (ICC) de Colombia*, las ICC son:

[...] las infraestructuras estratégicas soportadas por tecnologías de la información y las comunicaciones (TIC) o tecnologías de operación (TO), cuyo funcionamiento es indispensable, por lo que su suspensión, afectación, o destrucción tendría un grave impacto o efecto perturbador sobre los servicios esenciales del Estado. (Comando Conjunto Cibernético [CCOC], 2015)

En esencia, las ICC son los componentes digitales que hacen posible el funcionamiento eficiente y seguro de las infraestructuras físicas. Por ejemplo, una red eléctrica moderna es controlada y gestionada por sistemas cibernéticos que monitorean el flujo de la electricidad y garantizan un suministro continuo y seguro mediante acciones de gobernanza y mecanismos de aseguramiento.

Una característica relevante de las ICC es su capacidad para generar un efecto en *cascada*, con repercusiones significativas en otras IC. Por ejemplo, una falla en el sistema de semaforización podría incrementar considerablemente la cantidad de accidentes de tránsito, lo que, a su vez, saturaría el sistema hospitalario de emergencias y provocaría un uso excesivo de la red celular, comprometiendo su funcionamiento o incluso llevándola al colapso.

Diferencias entre las infraestructuras críticas y las infraestructuras críticas cibernéticas

Las IC suelen ser tangibles, como una planta de tratamiento de agua, una central hidroeléctrica o un reactor nuclear. En cambio, las ICC son intangibles y están compuestas por un *software*, un flujo de datos y redes de comunicación.

Para comprender los elementos que conforman el ecosistema de las IC, es pertinente considerar la siguiente definición de infraestructura estratégica (IE): “Las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre los cuales se soporta el funcionamiento de los servicios esenciales” (CCOC, 2015).

La figura 1 permite visualizar la relación entre las definiciones previamente mencionadas. Se observa que las infraestructuras se dividen en dos categorías: físicas y cibernéticas. Estas últimas, para efectos del presente estudio, se clasifican en críticas y no críticas.

Figura 1. Diagrama de conceptos



Fuente: Tomado de la CCOC (2015).

Finalmente, es importante destacar la interrelación entre las infraestructuras previamente mencionadas, la cual se establece mediante un acoplamiento derivado de las funciones de gobernanza, monitoreo y comunicación provistas por las ICC. Esto da lugar a la conformación de sistemas físico-cibernéticos (CPS) altamente interdependientes (Palleti et al., 2021).

Los resultados expuestos revelan una correlación directa entre la disrupción de las IC y las consecuencias adversas en los sistemas físicos. En este contexto, un ataque cibernético dirigido contra una red de control industrial puede desencadenar interrupciones significativas en procesos críticos, como la generación de energía o el transporte, lo que evidencia la intrincada interdependencia entre ambos dominios (Lewis, 2010). Esta vulnerabilidad subraya la imperiosa necesidad de comprender dicha correlación y de fortalecer la resiliencia de las IC ante amenazas cibernéticas (Vesić & Bjelajac, 2023).

Protección de las infraestructuras críticas

La protección de las ICC es fundamental debido a su estrecha relación con las IE y los servicios esenciales. Las ICC, sustentadas en las TIC y las TO, desempeñan un papel crucial en el mantenimiento de dichos servicios. Su interrupción, daño o destrucción puede tener un impacto significativo y altamente disruptivo, comprometiendo la estabilidad social y económica.

Las IE comprenden las instalaciones, redes, sistemas y equipos, tanto físicos como tecnológicos, que son necesarios para el funcionamiento continuo de los servicios esenciales. Estos servicios, vitales para el desarrollo de actividades sociales y económicas, dependen de las TIC y las TO.

Un fallo en su infraestructura podría paralizar actividades clave, lo que subraya la necesidad de una protección integral y coordinada de las IC y las IE, a fin de garantizar la continuidad y resiliencia de los servicios esenciales del país (Ashibani & Mahmoud, 2017; Chen & Abu-Nimeh, 2011; Humayed et al., 2017).

La función del Estado y las Fuerzas Armadas en la protección de las infraestructuras críticas

En términos generales, la protección de las IC se considera una responsabilidad del Estado, dado que son esenciales para garantizar el bienestar de la sociedad y el funcionamiento de la economía.

El Estado, a través de sus políticas y regulaciones, establece los marcos legales y operativos necesarios para identificar, evaluar y mitigar los riesgos que puedan afectar a estas infraestructuras. Además, coordina esfuerzos entre diversas entidades gubernamentales y privadas, a fin de implementar medidas de seguridad efectivas.

Según Juárez (2024), la seguridad humana y la protección de las IC requieren un enfoque integral que combine la promoción del desarrollo humano con la capacidad operativa de las instituciones estatales.

Por su parte, las Fuerzas Armadas desempeñan un papel crucial en la protección de las IC, especialmente en situaciones de emergencia o conflicto. Su capacidad para movilizar recursos y personal especializado garantiza una respuesta rápida y efectiva ante amenazas que puedan comprometer la seguridad nacional. Asimismo, su vasta experiencia en planificación estratégica y operaciones tácticas es fundamental para la implementación de medidas preventivas y correctivas.

De este modo, las Fuerzas Armadas amplían su misión tradicional hacia el quinto dominio y la defensa híbrida, lo que les permite intervenir en la protección de las IC de tres maneras:

1. Ciberdefensa nacional
 - Los comandos militares son responsables de proteger las redes críticas del Estado, como las de defensa e inteligencia. Además, colaboran con entidades civiles cuando se enfrentan a amenazas complejas.

- Realización de operaciones ofensivas y defensivas para desarticular actores hostiles.
- 2. Respuesta ante emergencias
 - En caso de sabotaje, ataques físicos o digitales, las Fuerzas Armadas pueden:
 - o Asegurar las instalaciones críticas.
 - o Proteger al personal técnico.
 - o Apoyar la restauración de servicios básicos.
- 3. Disuasión estratégica
 - El despliegue de capacidades militares en ciberdefensa y protección física tiene un efecto disuasorio sobre grupos terroristas, cibercriminales o Estados hostiles.

Características de las infraestructuras críticas cibernéticas

Las ICC constituyen un entramado complejo y heterogéneo de sistemas que integran las TI y las TO, como las redes industriales, el internet de las cosas (IoT), el internet industrial de las cosas (IIoT), los sistemas de control industrial (SCI) y los sistemas SCADA.

Esta convergencia tecnológica plantea una serie de desafíos únicos en términos de seguridad debido a la diversidad de protocolos, interfaces y niveles de criticidad de los componentes que las conforman (Kebande & Awad, 2024).

Algunos de sus focos de vulnerabilidad son:

- Vulnerabilidades de la seguridad en la capa de percepción: esta capa, responsable de recopilar datos del entorno físico a través de sensores y actuadores, es susceptible a diversos ataques, incluyendo:
 - o Manipulación y bloqueo que interrumpen la transmisión de datos entre los nodos.
 - o Los adversarios capturan los nodos y, en consecuencia, obtienen control sobre los dispositivos.
 - o Mediante la inyección de datos falsos, los adversarios buscan manipular las lecturas de los sensores.
 - o Clonación de etiquetas para crear dispositivos falsos.
 - o Acceso no autorizado a sistemas con el fin de obtener información sensible (Farooq et al., 2015).

- Vulnerabilidades de la seguridad en la capa de red: esta capa, encargada de la comunicación entre los diferentes componentes del sistema, es susceptible a amenazas en los protocolos de comunicación, transporte y *routing* (Aydin & Sertbaş, 2022; Farooq et al., 2015). Estas amenazas incluyen:
 - o Inseguridad en los protocolos que permite a los atacantes explotar las debilidades de los protocolos de comunicación, como la falta de autenticidad.
 - o El *spoofing* de RFID consiste en la suplantación de nodos RFID legítimos.
 - o Ataques de *sinkholing* (sumideros de DNS) que redirigen el tráfico hacia un nodo malicioso.
 - o Cuellos de botella en la comunicación entre los nodos, lo que provoca retrasos o interrupciones en la transmisión de los datos, afectando así la disponibilidad y degradando el servicio.
 - o Ataques de tipo *hombre en el medio* (MITM) que interceptan y manipulan la comunicación entre dos nodos, comprometiendo la disponibilidad, la integridad y la confidencialidad.
- Vulnerabilidades de la seguridad cibernética: la integración de los entornos de las TI y las TO amplía la superficie de ataque, aumentando la vulnerabilidad de las redes, los SCI, las aplicaciones y los servidores basados en sistemas industriales, así como de los recursos en entornos como Cloud, Edge y Fog Computing (Maglaras et al., 2022.) Esta expansión incrementa la probabilidad de puntos de ataque mediante:
 - o Ataques de suplantación de identidad.
 - o Ataques de *phishing*.
 - o Inyección de *malware*.
 - o Secuestro de sesión.
 - o Denegación de servicio (DoS).
 - o Fallos en el SCI.
 - o Robo de datos.
- Vulnerabilidades de la seguridad física: las características del IoT y de los dispositivos inteligentes empleados en las IC incluyen, *a priori*, elementos físicos con restricciones de energía y potencia. La seguridad de los sensores, los actuadores, los SCI y los SCADA es fundamental, ya que procesan datos en tiempo real que afectan tanto la infraestructura física como a los usuarios. Sin embargo, la implementación de medidas de seguridad y

monitoreo se ve limitada por estas restricciones, lo que exacerba las vulnerabilidades existentes y tiene un impacto directo sobre aspectos como lo mencionados a continuación:

- o La manipulación de los dispositivos puede modificar las lecturas de los sensores o alterar el comportamiento de los actuadores.
- o El bloqueo del servicio tiene el potencial de paralizar el funcionamiento normal del sistema.
- o El robo de información puede poner en riesgo datos confidenciales.
- o El compromiso de un dispositivo otorga a los atacantes la capacidad de controlar dispositivos críticos.
- o La alteración del sistema de control puede tener consecuencias devastadoras, incluyendo la pérdida de vidas humanas.
- o El compromiso del *firmware* puede alterar el funcionamiento del dispositivo.
- o La falta de disponibilidad del servicio tiene el potencial de interrumpir operaciones críticas.

Normatividad aplicable al aseguramiento de las infraestructuras críticas

A nivel mundial y nacional, se han desarrollado diversas iniciativas, a fin de garantizar la protección de las IC (tabla 1).

Tabla 1. Normatividad aplicable al aseguramiento de las infraestructuras críticas

Ámbito	Normativa	Enfoque principal	Detalles adicionales
Internacional	Marco de Ciberseguridad del NIST (CFS) 2.0	Estándares, directrices y mejores prácticas, a fin de gestionar los riesgos de ciberseguridad aplicables a IC.	• Proporciona un enfoque flexible y basado en riesgos para que las organizaciones adapten las medidas de seguridad a sus necesidades. • Consta de seis funciones principales: identificar, proteger, detectar, responder, recuperar y gobernar. • Es una referencia internacional utilizada para la gestión de la ciberseguridad en las IC.
Internacional	Presidential Policy Directive 21	IC nacionales.	• Fortalecer la seguridad y la resiliencia en 16 sectores esenciales. • Enfocado en la colaboración interinstitucional y una respuesta integrada.

Ámbito	Normativa	Enfoque principal	Detalles adicionales
Internacional	Directiva NIS2	Armonización de las medidas de ciberseguridad en la Unión Europea, abarcando sectores críticos como energía, transporte, salud y banca.	- Fortalecer la resiliencia y la supervisión de operadores esenciales. - Establece requisitos más estrictos en gestión de riesgos, notificación de incidentes y supervisión. - Fomenta la cooperación y el intercambio de información entre los Estados miembros.
Internacional	Convenio de Budapest sobre la Ciberdelincuencia	Tratado internacional orientado a fomentar la cooperación entre las naciones, a fin de combatir los delitos informáticos, incluidos aquellos que amenazan a las IC.	- Armonizar las legislaciones nacionales en materia de delitos informáticos. - Establece procedimientos que promuevan la cooperación internacional en la investigación y el enjuiciamiento por delitos informáticos. - Contempla disposiciones sobre la obtención de pruebas electrónicas y la asistencia entre Estados.
Nacional	CONPES 3995	La Política de Seguridad Digital tiene como objetivo fortalecer la capacidad del país para prevenir, detectar y responder a los riesgos y amenazas en el entorno digital, con especial énfasis en la protección de las IC.	- Define los objetivos y las estrategias que orientan la protección y el fortalecimiento de la seguridad digital en Colombia. - Establece un marco para la cooperación entre el sector público y el sector privado. - Promueve el desarrollo de capacidades en materia de seguridad digital.
Nacional	Decreto 338 de 2022	Establece lineamientos para fortalecer la gobernanza de la seguridad digital; identificar ICC y servicios esenciales; gestionar los riesgos asociados; y responder eficazmente a los incidentes de seguridad digital.	- Busca fortalecer la coordinación entre las entidades del Estado en materia de seguridad digital. - Define las responsabilidades de las partes interesadas en la protección de las ICC. - Establece la obligación de implementar medidas de seguridad para salvaguardar los sistemas de información y los datos.
Nacional	Decreto 472 de 2024	Define las directrices para la identificación, designación y protección de las ICC en Bogotá.	- Establece un marco para la gestión de riesgos y la respuesta a incidentes de seguridad cibernética, específicamente en el contexto de las ICC. - Define las responsabilidades de las entidades distritales en la protección de las ICC.

Fuente: Elaboración propia.

A pesar de los avances significativos, Colombia aún carece de una legislación que garantice la protección de las IC, tanto físicas como digitales. A nivel internacional, la tendencia apunta hacia la integración de la protección física, cibernética y de datos personales bajo un marco de resiliencia nacional. En este contexto, normativas como la NIS2 y el NIST CSF se consolidan como referencias clave para la formulación de políticas públicas en América Latina.

Gestión de la identidad en las infraestructuras críticas cibernéticas

Al igual que cualquier sistema de información o aplicación cibernética, toda ICC utiliza mecanismos de autenticación y autorización basados en la gestión de identidades, los cuales se agrupan bajo el concepto de *identidad digital*. Esta última permite o deniega acciones específicas de autenticación y autorización en los distintos componentes de una IC.

A continuación, se evalúan los requisitos y aspectos clave de la gestión de identidad en las ICC.

Requisitos para la gestión de la identidad en las infraestructuras críticas cibernéticas

En las ICC, la gestión de la identidad es un proceso fundamental para garantizar la seguridad y la continuidad de los servicios esenciales. Este proceso incluye la autenticación, que consiste en verificar la identidad de un usuario o dispositivo, y la autorización, que determina los permisos y privilegios otorgados a una entidad autenticada.

Dada la naturaleza crítica de estos sistemas, la gestión de la identidad debe ser robusta y adaptable para hacer frente a amenazas cibernéticas en constante evolución. Sin embargo, en estas infraestructuras, la convergencia entre las TI y las TO plantea desafíos únicos, como la heterogeneidad de los sistemas y la necesidad de equilibrar la seguridad y la usabilidad.

Investigaciones recientes han destacado la importancia de implementar soluciones de gestión de identidad basadas en estándares, que integren tecnologías como la autenticación multifactor (MFA) y la gestión de privilegios. A diferencia de los enfoques tradicionales, estas soluciones ofrecen una mayor protección contra amenazas como el robo de credenciales y los ataques de fuerza bruta.

- Definición de privilegios: la política de control de acceso más adecuada debe asignar permisos y derechos con base en los roles, las tareas y los atributos de los usuarios. Un principio clave es la política de menor

privilegio, que establece que los usuarios solo deben contar con los accesos estrictamente necesarios para desempeñar sus funciones.

En este contexto, el control de acceso basado en atributos (ABAC) permite definir privilegios con un alto nivel de granularidad, ya que las decisiones relacionadas con el acceso se toman a partir de condiciones booleanas aplicadas a los valores de distintos atributos. Esta flexibilidad es fundamental para garantizar la seguridad en los esquemas de control de acceso de los CPS.

- MFA: los esquemas de autenticación basados en un solo factor no son lo suficientemente resistentes como para hacer frente a ataques cibernéticos. Por esta razón, se requiere la combinación de dos o más factores, como *lo que eres* (huellas dactilares, escaneo del iris, etc.), *lo que sabes* (passwords), y *lo que tienes* (tokens), con el fin de incrementar la robustez del proceso. Esta estrategia es esencial para reducir falsos positivos y dificultar los intentos de acceso no autorizado, ya que permite establecer múltiples niveles de autenticación.
- Proceso de *hashing* dinámico y contraseñas fuertes: periódicamente, las contraseñas deben ser sometidas a un proceso de rehashing, utilizando un nuevo *nonce* dinámico para cada usuario y funciones *hash* criptográficas seguras, como SHA-3 y SHA-2 (variante 512). Este enfoque ayuda a prevenir ataques como los de las tablas arco iris, los de colisión o de cumpleaños.
- Auditoría segura y protegida: para mitigar los intentos de acceso no autorizado desde el interior de un CPS y preservar la evidencia digital de ataques tanto internos como externos, es necesario contar con un sistema de gestión de auditoría que recopile y almacene los registros en un sistema distribuido. Este aspecto, relacionado con la auditoría en ciberseguridad, es perentorio.
- Soluciones no criptográficas mejoradas: para prevenir brechas de seguridad derivadas de la explotación de vulnerabilidades, es fundamental implementar sistemas híbridos (IDS/IPS) o basados en IA, utilizando algoritmos de aprendizaje automático, junto con *firewalls* avanzados y *honeypots* dinámicos. Estos elementos deben ser considerados como un ecosistema dinámico y altamente interactivo.
- Copias de seguridad seguras y verificadas: es esencial garantizar la disponibilidad de los datos del CPS y prevenir su destrucción o alteración. Por esta razón, es necesario implementar soluciones de protección eficientes y ligeras que aseguren la integridad de las copias de seguridad. Así, se preserva su robustez frente a ataques DoS/DDoS y *ransomware*.

- Esfuerzos forenses: son esenciales para la recolección de evidencias. Es necesario implementar soluciones innovadoras que neutralicen las técnicas antiforenses, garantizando así la preservación de la evidencia digital y reduciendo al mínimo los intentos de reconocimiento por parte de los atacantes.

El objetivo de estos requisitos es garantizar la integridad, confidencialidad y disponibilidad de los sistemas ciberfísicos ante diversas amenazas y ataques, asegurando así su operación en un entorno seguro y confiable.

Conceptualización de la identidad digital

La identidad digital hace referencia a la representación electrónica de la información personal y profesional que define a un individuo o entidad en entornos virtuales. Está compuesta por un conjunto de atributos digitales, como credenciales de acceso, perfiles de usuario, historiales de transacciones y cualquier otro dato que pueda ser utilizado para identificar a una persona o a un dispositivo dentro de un sistema digital (Elwell, 2014).

Con respecto a la ciberseguridad, la identidad digital es un componente esencial, ya que determina quién puede acceder a qué recursos y bajo qué condiciones. En términos generales, la identidad digital está compuesta por dos elementos fundamentales: la autenticación, que verifica la identidad del usuario, y la autorización, que permite o restringe el acceso a los recursos.

Otra definición relevante es la de credenciales digitales, que hace referencia a los mecanismos utilizados para autenticar y verificar una identidad digital. Estas adoptan diversas formas, como contraseñas, certificados digitales, claves criptográficas o datos biométricos.

Con la creciente digitalización de las IC, el control efectivo de estas credenciales es crucial para la seguridad operativa, ya que cualquier vulnerabilidad podría ser aprovechada por actores maliciosos que buscan acceder indebidamente a sistemas sensibles (NIST, 2018).

Evolución histórica

El concepto de *identidad digital* ha evolucionado considerablemente. En un principio, las identidades digitales se limitaban a nombres de usuario y contraseñas simples, un método de autenticación que, aunque eficaz en su momento, ha demostrado ser insuficiente para satisfacer las necesidades de seguridad actuales.

En los primeros sistemas informáticos, las identidades se gestionaban de forma centralizada. Si bien esto facilitaba su administración, también introducía vulnerabilidades, como el riesgo de un único punto de fallo (Fang et al., 2009).

Con el auge de la conectividad global y el desarrollo del Internet en la década de 1990, surgió la necesidad de mejorar las técnicas de autenticación y autorización. A medida que las organizaciones comenzaron a depender de sistemas más complejos y distribuidos, las contraseñas dejaron de ser seguras.

Fue entonces cuando se introdujo la autenticación de dos factores (2FA) y, más tarde, la MFA, que incorporó elementos adicionales, como *lo que soy* (huellas dactilares y reconocimiento facial), *lo que tengo* (tokens de seguridad) y *lo que sé* (contraseñas) (Roman et al., 2013).

Esta evolución ha sido impulsada por el crecimiento de la computación en la nube, en la niebla y el IoT, así como por las infraestructuras distribuidas, que requieren una gestión descentralizada o itinerante de las identidades digitales.

En las últimas dos décadas, ha surgido un enfoque más sofisticado y seguro para la gestión de identidades digitales, basado en criptoidentidades y *blockchain*. Estas tecnologías permiten una gestión descentralizada, proporcionando a los usuarios un mayor control y seguridad sobre su información personal (Zhang et al., 2020).

Simultáneamente, la IA y el aprendizaje automático se utilizan para detectar patrones anómalos en el comportamiento de las identidades digitales, lo que refuerza la prevención de ataques como la suplantación de identidad y el acceso no autorizado.

Datos como los lugares frecuentados, los tipos de comercio, los artículos adquiridos y la frecuencia de tipeo se convierten en indicadores clave para definir el comportamiento esperado, generando métricas de desviación que permiten identificar posibles violaciones a la seguridad.

La evolución de la identidad digital refleja una adaptación constante a las crecientes amenazas a la seguridad cibernética y a la complejidad de los sistemas interconectados. En el ámbito de las ICC, esta evolución ha sido acelerada, debido a que la seguridad de estos sistemas es fundamental para garantizar la continuidad de los servicios esenciales de un país.

Urge generar alertas sobre el rezago tecnológico que afecta a las IC de la mayoría de los países, lo que las hace altamente vulnerables debido a la convergencia forzada de las TI y las TO, así como a la falta de un componente de ciberseguridad adecuado.

Relevancia actual de la identidad digital

La identidad digital, responsable de la autenticación y del acceso a los CPS, constituye el pilar sobre el cual se asientan las políticas de ciberseguridad en IC, previniendo el acceso no autorizado.

Una gestión adecuada de la identidad digital no solo facilita el control del acceso a sistemas sensibles, sino que también protege la integridad y confidencialidad de los datos. Las amenazas más comunes, como la suplantación de identidad y el uso indebido de credenciales robadas, destacan la necesidad de una gestión robusta y actualizada (Ponemon Institute, 2021).

Con el aumento de la digitalización, la importancia de la identidad digital trasciende el ámbito técnico. La ética y la privacidad de la identidad digital se han convertido en áreas de gran preocupación, especialmente en las IC, dado que un acceso indebido podría comprometer tanto los datos personales como la seguridad física de las instalaciones (Elwell, 2014).

La implementación de regulaciones como la Ley 1273 de 2009 y el Reglamento General de Protección de Datos (Parlamento Europeo, 2016) subraya la necesidad de una gestión segura y ética de las identidades digitales. Esto requiere que las organizaciones no solo acaten las normativas legales, sino que también garanticen la protección de los derechos de los usuarios.

Desafíos actuales en la identidad digital

La gestión de la identidad digital es fundamental para garantizar la seguridad y resiliencia de las IC ante amenazas cibernéticas. Sin embargo, enfrenta desafíos importantes, como la complejidad de los procesos de autenticación y autorización, la protección de la privacidad, la interoperabilidad entre sistemas heterogéneos y la prevención de la suplantación de identidad.

Las tendencias emergentes en IA, *blockchain* y autenticación sin contraseñas abren paso a soluciones más seguras y eficientes. Sin embargo, su éxito depende, en gran medida, de la coordinación organizacional y la adopción de estándares abiertos, la implementación de tecnologías avanzadas de detección y mitigación, y el fomento de una cultura de seguridad tanto a nivel organizacional como individual.

Autenticación y autorización

La autenticación permite el acceso a un sistema, mientras que la autorización define los privilegios otorgados. En esencia, estos procesos constituyen el objetivo fundamental de una identidad digital y representan un desafío significativo ante

la creciente sofisticación de las amenazas que buscan vulnerar la integridad, la confidencialidad y la disponibilidad de los sistemas. La autenticación garantiza que solo los usuarios legítimos accedan a los sistemas críticos, mientras que la autorización delimita sus acciones.

Las IC demandan soluciones de autenticación avanzadas, como la MFA, que combina factores de conocimiento (contraseñas), posesión (dispositivos) y biometría (huellas dactilares y reconocimiento facial) (Roman et al., 2013). Sin embargo, la implementación de la MFA en entornos operativos sensibles puede ser compleja y generar fricciones, especialmente en situaciones de emergencia, donde el acceso rápido y seguro es crucial.

Se recomienda implementar sistemas de autorización multinivel que requieran múltiples fuente de confirmación. Sin embargo, al igual que en el caso anterior, este enfoque puede generar complicaciones en situaciones de emergencia que demanden una respuesta rápida.

Por otro lado, la autorización demanda un control granular que permita administrar las acciones permitidas a cada usuario según su rol en la infraestructura. Los sistemas basados en políticas de control de acceso, como el Role-Based Access Control (RBAC) o el Attribute-Based Access Control (ABAC), son fundamentales para garantizar la seguridad de estos sistemas.

Sin embargo, la integración progresiva de las IC con tecnologías emergentes, como el IoT, incrementa exponencialmente la cantidad de dispositivos y actores que requieren autenticación y autorización, lo que, a su vez, eleva la complejidad y el riesgo de fallos en la seguridad.

Privacidad y protección de datos

La gestión de la identidad digital plantea desafíos significativos en materia de privacidad y protección de datos. Este proceso implica el manejo de grandes volúmenes de información personal y profesional, los cuales son susceptibles a accesos no autorizados y posibles violaciones de la confidencialidad.

En el contexto de las IC, esta información puede incluir datos sensibles de empleados, contratistas o usuarios que acceden a las redes. Además, como se mencionó anteriormente, la mayoría de estas infraestructuras están sujetas a estrictas regulaciones en materia de privacidad, como el Reglamento General de Protección de Datos, la Ley 1581 de 2012 y la Ley 1273 de 2009, las cuales exigen un tratamiento seguro y ético de los datos personales.

El incumplimiento de estas regulaciones, ya sea por ciberataques o por una gestión inadecuada de las identidades digitales, puede tener graves consecuencias legales y financieras para las organizaciones encargadas de gestionar las IC (O'Reilly et al., 2021). Además, la vulneración de la privacidad pueden erosionar la confianza de los empleados y el público en general, comprometiendo la integridad y la fiabilidad de los sistemas.

Para mitigar estos riesgos, es necesario que las organizaciones implementen técnicas avanzadas de cifrado y anonimización de datos, junto con políticas de protección de datos que garanticen el cumplimiento de las normativas vigentes en materia de privacidad.

Interoperabilidad entre sistemas

La complejidad inherente a las ICC, compuesta por sistemas heterogéneos operados por múltiples entidades o fabricantes, representa un obstáculo para la implementación de soluciones coherentes y estandarizadas. Esta fragmentación también amplifica los riesgos asociados a la cadena de suministro.

En este contexto, la interoperabilidad es fundamental para garantizar una autenticación consistente de los usuarios en diversas plataformas y dispositivos, sin sacrificar la seguridad ni la eficiencia operativa.

La falta de estándares universales en la gestión de la identidad digital agrava este problema. A menudo, las organizaciones utilizan sistemas de autenticación y autorización incompatibles, lo que puede dar lugar a brechas de seguridad o a la necesidad de desarrollar soluciones *ad hoc* para integrar sistemas heterogéneos (Suleski et al., 2023; Wang & Zhao, 2023; Zhang et al., 2020).

Una posible solución radica en la adopción de estándares abiertos, como OAuth 2.0 y OpenID Connect, que facilitan la interoperabilidad y permiten gestionar las identidades digitales, de manera más flexible y segura, en entornos heterogéneos. Sin embargo, la implementación de estos estándares demanda un compromiso y una coordinación sustancial entre las partes interesadas.

Prevención de la suplantación de identidad

La suplantación de identidad representa un riesgo significativo para la seguridad de las ICC, especialmente en lo que respecta a los procesos de autenticación y autorización. Los atacantes pueden robar o falsificar credenciales para hacerse pasar por usuarios legítimos y acceder a sistemas y redes sensibles.

El *phishing*, el robo de contraseñas y la explotación de vulnerabilidades en los sistemas de autenticación y protocolos de comunicación son algunos de los

métodos más utilizados para llevar a cabo este tipo de ataques (Shameli-Sendi et al., 2016).

Para mitigar estos riesgos, es fundamental implementar enfoques avanzados de detección de anomalías, en los que la IA y el aprendizaje automático desempeñan un papel clave. Estas tecnologías analizan patrones de comportamiento en tiempo real, identificando actividades sospechosas indicativas de suplantación de identidad.

Por ejemplo, si un usuario accede a un sistema desde una ubicación inusual o realiza acciones que no coinciden con su comportamiento habitual, el sistema puede bloquear el acceso o generar alertas. Este tipo de soluciones adaptativas y proactivas es cada vez más necesario para proteger las identidades digitales de ataques sofisticados.

Además, las soluciones sin contraseñas, basadas en claves criptográficas o biometría, están ganando popularidad debido a su capacidad para mitigar los riesgos asociados a las contraseñas tradicionales, que son susceptibles a suplantaciones y robo. Estas tecnologías proporcionan una capa adicional de seguridad al eliminar uno de los puntos más exánimes en los procesos de autenticación: el uso de contraseñas débiles o filtradas.

Impacto de las amenazas cibernéticas en la identidad digital

El crecimiento de las ICC y la dependencia de identidades digitales ha incrementado el riesgo de ataques cibernéticos. Factores como la hiperconectividad —es decir, el aumento de dispositivos conectados a un sistema— y la administración remota a través de redes de comunicación han ampliado significativamente la superficie de ataque. Esto ha dado lugar a la aparición de nuevas amenazas, siendo los ataques dirigidos a la identidad digital una de las formas más comunes y efectivas de comprometer estos sistemas.

A continuación, se presentan las tipologías de ataques cibernéticos y algunos estudios de caso relevantes.

Tipologías de ataques cibernéticos

Las ciberamenazas contra la identidad digital se clasifican en tipologías que explotan las vulnerabilidades en los procesos de autenticación, autorización y protección de datos.

A continuación, se analizan las más comunes:

- *Phishing* y *spear phishing*: técnicas de ingeniería social diseñadas para engañar a los usuarios y obtener sus credenciales de acceso. La principal

diferencia entre el *spear phishing* y el *phishing* radica en que el primero adopta un enfoque más dirigido, en lugar de centrarse en la calidad.

En el contexto de las IC, los ataques de *spear phishing* suelen estar dirigidos a empleados con acceso privilegiado. Al comprometer sus credenciales, los atacantes pueden obtener acceso a sistemas sensibles.

- Ataques de fuerza bruta y *credential stuffing*: los ataques de fuerza bruta consisten en probar repetidamente combinaciones de nombres de usuario y contraseñas hasta encontrar la correcta. Por otro lado, el *credential stuffing* implica el uso de credenciales robadas de otras plataformas para intentar acceder a un sistema.

Ambos métodos explotan las malas prácticas en la gestión de contraseñas, como la reutilización de credenciales en múltiples sistemas. En el caso de los ataques de fuerza bruta, una forma efectiva de contrarrestarlos es mediante el *bloqueo de sesión*.

- Ataque de MITM: estos ataques interceptan las comunicaciones entre un usuario y el sistema, lo que permite al atacante capturar credenciales en tiempo real o interceptar el flujo de datos. Esto puede afectar la disponibilidad, la confidencialidad y la integridad, dependiendo de cómo se manipulen las unidades de datos del protocolo (PDU). En el contexto de las IC, los ataques MITM pueden comprometer los SCI, que dependen de comunicaciones seguras.
- Suplantación de identidad: implica la creación de identidades falsas o el uso de credenciales robadas para hacer pasar por un usuario legítimo. Este tipo de ataque puede tener consecuencias devastadoras en las IC, ya que permite el acceso subrepticio a sistemas sensibles.
- Explotación de vulnerabilidades en *software* de autenticación: las fallas en los sistemas de autenticación, como las debilidades en la implementación de la MFA o en los protocolos de cifrado, pueden ser explotadas por los atacantes para acceder a identidades digitales y a recursos críticos.

Estudios de caso relevantes

Algunos estudios de caso destacan el impacto de las amenazas cibernéticas en la identidad digital y la seguridad de las IC (tabla 2).

Tabla 2. Casos de afectación a la identidad digital y su impacto sobre las ICC

Año	País	Infraestructura crítica afectada	Tipo de ataque	Compromiso de la identidad digital	Impacto
2010	Irán	Planta nuclear de Natanz (Irán)	Malware (Stuxnet)	Uso de certificados digitales falsos	Sabotaje de centrifugadoras nucleares
2015	Ucrania	Red eléctrica	Ataque APT (BlackEnergy)	Suplantación de identidades administrativas	Apagones masivos en varias regiones
2019	Noruega	Norsk Hydro (Industria metalúrgica)	Ransomware (LockerGoga)	Robo de credenciales	Paralización de operaciones a nivel mundial
2021	EE. UU.	Ataque a Colonial Pipeline (energía)	Ransomware	Acceso a través de credenciales comprometidas	Cierre temporal del suministro de combustible
2021	EE. UU.	Planta de agua en Oldsmar, Florida	Acceso remoto no autorizado	Uso indebido de TeamViewer sin 2FA	Intento de envenenamiento del agua potable
2022	Costa Rica	Ministerios y servicios públicos	Ransomware (Conti)	Acceso vía a cuentas comprometidas	Paralización de sistemas estatales por semanas
2023	Colombia	EPS Sanitas (salud)	Ciberataque tipo ransomware	Posible uso de accesos internos	Afectación a atención médica y fuga de datos personales
2024	Reino Unido	NHS (sistema de salud)	Phishing masivo y ransomware	Robo de credenciales del personal médico	Fuga de información clínica y su impacto en la atención médica

Fuente: Adaptado de Beerman et al. (2023); Lee et al. (2016) y Zhang et al. (2020).

- Ataque a Colonial Pipeline (2021): este ataque es considerado uno de los más graves contra las IC en los últimos años. Un grupo de *ransomware*, conocido como *DarkSide*, comprometió las credenciales de una cuenta de acceso remoto, lo que permitió a los atacantes infiltrarse en los sistemas de la empresa.
El vector inicial fue una contraseña filtrada y reutilizada, que otorgó acceso a una VPN sin MFA. Aunque el objetivo principal del ataque era obtener un rescate financiero, sus repercusiones afectaron gravemente el suministro de combustible en Estados Unidos, destacando la importancia de la identidad digital y la autenticación robusta en la seguridad de las IC (Beerman et al., 2023).

- Ataque a la red eléctrica de Ucrania (2015): este ataque, ejecutado por un grupo de ciberespionaje, comprometió las credenciales de los operadores de los sistemas SCADA, que controlaban sectores de la red eléctrica ucraniana. A través de técnicas de *spear phishing* y *malware* avanzado, los atacantes lograron infiltrarse en los sistemas, provocando apagones que afectaron a más de 230 000 personas (Lee et al., 2016; Zhang et al., 2020). Este incidente demostró cómo las identidades digitales comprometidas pueden ser utilizadas para sabotear las IC y causar daños significativos.
- Ataque a Norsk Hydro (2019): la empresa productora de aluminio fue víctima de un ataque de *ransomware* denominado *LockerGoga*, que afectó a terminales con Windows.

Los atacantes utilizaron las credenciales robadas para desactivar los sistemas de producción de la compañía, lo que provocó la paralización de las operaciones a nivel mundial. Este incidente demostró, una vez más, el impacto de las vulnerabilidades en las ICC cuando las identidades digitales se ven comprometidas.

- Natanz-Stuxnet (Irán, 2010): aunque el objetivo principal de Stuxnet era el sabotaje físico, robó los certificados digitales legítimos de algunas empresas de *hardware* para hacerse pasar por un *software* confiable. Esto permitió que se propagara sin ser detectado, causando daños a las centrifugadoras nucleares. Este ataque marcó un precedente en el uso de la identidad digital como un vector de intrusión sofisticado.
- Planta de agua en Oldsmar, Florida (2021): un actor no identificado accedió remotamente al sistema de control de una planta de tratamiento de agua mediante TeamViewer y credenciales expuestas. Intentó aumentar los niveles de hidróxido de sodio en el agua potable, pero el ataque fue detenido a tiempo. Este incidente reveló la falta de una autenticación segura y de controles de identidad en las IC municipales.
- EPS Sanitas (Colombia, 2023): el sistema de atención de una de las principales EPS del país sufrió un ciberataque, posiblemente relacionado con elementos del *ransomware*. Aunque los detalles técnicos son limitados, se presume que hubo acceso interno no autorizado o suplantación de identidad, lo cual tuvo un impacto negativo en la atención a los pacientes y expuso datos personales y clínicos sensibles.

Estos casos demuestran que la identidad digital es una de las primeras líneas de defensa en la protección de las IC. Los accesos no autorizados, derivados del

robo de credenciales, la suplantación de identidad o el uso indebido de cuentas internas, son cada vez más comunes.

La implementación de controles como la MFA, la gestión de accesos privilegiados (PAM), la segmentación de redes, la detección temprana de anomalías y la capacitación continua son medidas esenciales que deben ser impulsadas y reguladas por el Estado.

Relevancia del fortalecimiento de la identidad digital

Los estudios de caso demuestran cómo las identidades digitales se han convertido en un vector crucial en los ataques a las IC. Es evidente que, cuando los sistemas de autenticación y autorización no son lo suficientemente robustos, los atacantes pueden aprovechar credenciales comprometidas para tener acceso y controlar sistemas críticos.

Esto resalta la importancia de implementar políticas y tecnologías de seguridad más avanzadas, como la MFA, el monitoreo continuo de la identidad digital y la adopción de tecnologías como *blockchain* (Zhang et al., 2020).

Además, las organizaciones responsables de gestionar las IC deben invertir en la capacitación de su personal, a fin de que comprendan los riesgos asociados con la gestión de identidades digitales y adopten buenas prácticas, como el uso de contraseñas fuertes, la MFA y la supervisión de accesos inusuales. Estas medidas preventivas no solo fortalecen la seguridad, sino que también reducen la probabilidad de que un ataque exitoso a las identidades digitales comprometa toda la infraestructura.

Un aspecto fundamental en el funcionamiento de una IC es la implementación de la autorización multinivel, que exige la confirmación de dos o más fuentes para realizar acciones de alto impacto, como el cierre o la apertura de una compuerta. Este proceso debe seguir una lógica AND (todo o nada).

Tecnologías emergentes y su integración

Las tecnologías emergentes están desempeñando un papel fundamental en la transformación de la gestión de las identidades digitales. A medida que los ataques cibernéticos se vuelven más sofisticados y las amenazas evolucionan, las tecnologías avanzadas, como el *blockchain*, la IA, la biometría y los sistemas de identidad federada, ofrecen nuevas herramientas y enfoques para proteger las identidades digitales y optimizar los procesos de autenticación.

En esta sección, se analiza cómo estas tecnologías emergentes se están integrando en la gestión de las identidades digitales y su impacto en la seguridad de las IC.

Blockchain y gestión de identidades

La tecnología *blockchain* emerge como una solución innovadora para la gestión descentralizada de las identidades digitales. Tradicionalmente, esta gestión ha sido centralizada, por lo que no adolece de vulnerabilidades, como el riesgo de un único punto de fallo, en el que un compromiso de la base de datos central podría afectar a todas las identidades almacenadas.

El *blockchain* ofrece una alternativa distribuida, permitiendo que las identidades digitales sean gestionadas a través de una red descentralizada, lo que dificulta la manipulación y el acceso no autorizado a los datos (Sameera et al., 2024).

En el contexto de las IC, el *blockchain* facilita la creación de identidades soberanas, otorgando a los usuarios un mayor control sobre sus credenciales y eliminando la dependencia de un único proveedor de servicios.

Cada transacción o acceso se registra, de forma inmutable, en la cadena de bloques, garantizando la transparencia y la trazabilidad de las interacciones con los sistemas críticos. Esto es especialmente importante en entornos industriales, donde las identidades de los dispositivos IoT pueden gestionarse, de manera segura, mediante el uso del *blockchain*.

Un ejemplo de aplicación es la integración del *blockchain* en los sistemas SCADA, esenciales para el control y el monitoreo de las IC, como las redes eléctricas y los sistemas de distribución de agua.

Al implementar el *blockchain*, tanto las credenciales de los operadores como los dispositivos pueden ser verificados de manera distribuida, lo que reduce significativamente las posibilidades de suplantación de identidad o accesos no autorizados (Zhang et al., 2020).

Finalmente, esta tecnología posibilita la creación de sistemas autosoberanos, capaces de realizar auditorías de forma local (sin necesidad de recurrir a redes *blockchain* de terceros o integradas a redes WAN).

Para garantizar múltiples puntos de confirmación de acciones de alto impacto, como órdenes convergentes e inclusivas, esta tecnología no solo incrementa los puntos de control, sino que también promueve el uso de contratos inteligentes.

Inteligencia artificial en la autenticación

La IA está revolucionando la forma en que los seres humanos interactúan y comprenden el mundo, y la gestión de identidades digitales no es ajena a esta transformación. Su aplicación es especialmente valiosa en los procesos de autenticación y la detección de amenazas.

Los sistemas de autenticación basados en IA son capaces de analizar grandes volúmenes de datos en tiempo real, identificando patrones de comportamiento anómalos que podrían revelar intentos de acceso no autorizado o ataques en curso.

Los algoritmos de aprendizaje automático permiten que estos sistemas se adapten y mejoren de forma continua, ajustando las políticas de autenticación según el comportamiento habitual del usuario o del dispositivo.

Por ejemplo, si un usuario accede a un sistema crítico desde una ubicación o un dispositivo inusual, el sistema basado en IA puede activar una alerta o exigir una autenticación adicional, como la MFA. Este enfoque ayuda a prevenir la suplantación de identidad y el uso indebido de credenciales comprometidas.

Una aplicación relevante de la IA en las IC es la autenticación adaptativa, que ajusta los niveles de seguridad según el contexto del usuario, como la hora, el dispositivo o la ubicación. Este enfoque no solo reduce los riesgos relacionados con el acceso no autorizado, sino que también mejora la experiencia del usuario al evitar pasos de autenticación innecesarios en situaciones de bajo riesgo (Shameli-Sendi et al., 2016).

Además, la IA puede integrarse con sistemas de detección de amenazas internas. Para identificar actividades sospechosas después de la autenticación inicial, estos sistemas, al igual que un sistema de detección de intrusiones (IDS), no solo verifican las credenciales de acceso, sino que también monitorean el comportamiento continuo del usuario o el dispositivo. Esto es crucial para proteger las IC de actores internos maliciosos, quienes, al tener acceso legítimo a los sistemas, podrían abusar de sus privilegios.

Biometría como método de autenticación

El uso de sistemas que incorporan la autenticación basada en *lo que soy* representa, sin duda, una alternativa con altos niveles de seguridad debido a la dificultad de falsificar o suplantar las características biométricas de cada individuo.

Sin embargo, esta dificultad tiende a disminuir con el avance tecnológico, lo que refuerza la necesidad de implementar mecanismos de MFA. Los métodos biométricos, como el reconocimiento de huellas dactilares, iris, rostro y voz, son más difíciles de replicar o sustraer, y ofrecen mayor seguridad que los métodos tradicionales basados únicamente en contraseñas.

En el contexto de las IC, la biometría representa una ventaja significativa al garantizar que solo el personal autorizado pueda acceder físicamente a instalaciones sensibles o virtualmente a sistemas críticos. Por ejemplo, en una planta de

energía nuclear o en una estación de control de agua, el uso de escáneres biométricos asegura que únicamente los operadores con permisos específicos puedan acceder a sistemas SCADA o a áreas restringidas.

Uno de los principales desafíos de la biometría es la protección de los datos biométricos. Si bien métodos como las huellas dactilares o el reconocimiento facial son más seguros que las contraseñas, la exposición de los datos biométricos es irreversible.

Para garantizar un cifrado robusto y una gestión segura, se requiere protección adicional. Además, las organizaciones que implementan biometría deben cumplir con estrictas regulaciones de privacidad.

Otro aspecto importante es la falta de inmutabilidad de algunos registros biométricos, lo cual debe tenerse en cuenta en sistemas críticos con tiempos de interacción más cortos. Por ejemplo, la voz, como factor de autenticación, puede variar debido a fenómenos como un resfriado, lo que debe considerarse al diseñar el sistema de autenticación.

Implementación de los sistemas de identidad federada

Los sistemas de identidad federada permiten que organizaciones o plataformas compartan un conjunto de credenciales de identidad. En lugar de autenticarse repetidamente en diferentes sistemas, los usuarios pueden disfrutar de un único inicio de sesión, reconocido por todos los miembros de la federación. Esto no solo mejora la eficiencia y la experiencia del usuario, sino que también fortalece la seguridad al reducir la cantidad de credenciales a gestionar.

En el ámbito de las IC, la identidad federada es especialmente útil cuando múltiples actores y entidades colaboran en la gestión de un mismo sistema, como ocurre en consorcios de energía o grandes sistemas de transporte.

La federación de identidades permite que estas organizaciones compartan la gestión de credenciales sin comprometer la seguridad. Un ejemplo de este tipo de tecnología es el Security Assertion Markup Language (SAML), que facilita la federación de identidades entre diferentes dominios (Lewis & Lewis, 2009).

La implementación de la identidad federada es esencial para la transición hacia un modelo de confianza cero (*zero trust*), en el que ningún usuario o dispositivo se considera confiable, ni siquiera dentro de la red interna. En un enfoque *zero trust*, cada solicitud de acceso se verifica y autentica individualmente, y las identidades federadas garantizan que estas verificaciones sean eficientes y seguras, especialmente en sistemas distribuidos y complejos.

Otros desarrollos relevantes

Además de las tecnologías previamente mencionadas, otras soluciones emergentes están destacándose en la gestión de identidades digitales para las IC. Los *tokens* de seguridad físicos y las claves criptográficas avanzadas proporcionan una mayor protección contra ataques de suplantación de identidad o interceptación de credenciales. Dispositivos como las llaves de seguridad basadas en el estándar Fast Identity Online 2 (FIDO2) permiten a los usuarios autenticarse mediante claves criptográficas que solo funcionan en el dispositivo autenticado.

Tendencias en la gestión de la identidad digital

Para abordar los desafíos de seguridad, privacidad y eficiencia en entornos cada vez más interconectados, la gestión de identidades digitales está evolucionando a pasos agigantados. Entre las tendencias más destacadas se encuentran las identidades autosoberanas y las identidades federadas y descentralizadas, que ofrecen enfoques innovadores, a fin de superar los problemas asociados con la gestión centralizada de las identidades digitales.

A continuación, se analizan estas tendencias, así como su impacto en la seguridad y la gestión de las IC.

Identidades autosoberanas

La identidad autosoberana es un modelo emergente que otorga a individuos y entidades el control total de sus identidades digitales, eliminando la necesidad de intermediarios centralizados, como empresas o gobiernos.

En este sistema, las credenciales son emitidas por entidades de confianza (como gobiernos, instituciones académicas o empresas), pero son los usuarios quienes las almacenan y gestionan a través de billeteras digitales seguras. La verificación de estas credenciales se realiza mediante tecnologías criptográficas, lo que permite a los usuarios compartir solo la información necesaria para cada interacción o transacción.

Este enfoque de identidad descentralizada aborda algunos de los problemas relacionados con los modelos tradicionales de identidad digital. En primer lugar, reduce la dependencia de proveedores de identidad centralizados, que, a menudo, son blanco de ataques cibernéticos y pueden representar un único punto de fallo.

Además, las identidades autosoberanas otorgan mayor control y privacidad a los usuarios, quienes deciden qué datos compartir y con quién, lo que limita la

exposición de su información personal y reduce el riesgo de violaciones de privacidad (Tobin & Reed, 2017).

El *blockchain* desempeña un papel clave en las identidades autosoberanas al proporcionar una capa de seguridad y verificación descentralizada. La naturaleza inmutable y distribuida de la cadena de bloques permite verificar las credenciales sin necesidad de un ente central.

En el contexto de las IC, la adopción de identidades autosoberanas podría mejorar significativamente la seguridad al eliminar los intermediarios que gestionan las credenciales de acceso. Por ejemplo, en una planta de energía, tanto los operadores como los dispositivos podrían gestionar sus credenciales de manera soberana, verificándolas mediante una red *blockchain*.

Este enfoque no solo incrementaría la seguridad, sino que también promovería la interoperabilidad entre diversos sistemas de identidad, permitiendo el uso de credenciales autosoberanas en distintas IC sin depender de un único proveedor (Dehalwar et al., 2022; Weigl et al., 2023).

Sin embargo, la adopción generalizada de identidades autosoberanas enfrenta desafíos considerables. La complejidad técnica inherente a la gestión de credenciales puede ser un obstáculo, especialmente en las IC, donde la eficiencia y la simplicidad son primordiales. Además, la ausencia de una regulación clara y estandarizada dificulta su implementación a gran escala, dado que distintas jurisdicciones y organizaciones podrían establecer normativas dispares para la gestión y verificación de identidades.

A pesar de estos desafíos, las identidades autosoberanas emergen como una tendencia clave con el potencial de transformar la gestión de las identidades digitales, especialmente en entornos donde la seguridad y la privacidad son primordiales.

Identidades federadas y descentralizadas

Otro enfoque emergente son las identidades federadas y descentralizadas. A diferencia de las autosoberanas, las federadas permiten que un conjunto de organizaciones o sistemas confíen en el mismo proveedor de identidad, lo que facilita el acceso a múltiples plataformas con una sola autenticación. Por lo general, este modelo se implementa en entornos empresariales y académicos mediante protocolos como OAuth 2.0 y SAML.

En una identidad federada, el usuario inicia sesión a través de un proveedor de identidad (como Google o Microsoft), que actúa como un intermediario confiable

para verificar su identidad en múltiples servicios. Este enfoque presenta claras ventajas, como la simplicidad y la reducción de la carga asociada a la gestión de múltiples credenciales.

En el contexto de las IC, la identidad federada resulta especialmente útil cuando varias organizaciones o sistemas colaboran en la gestión de un servicio o una red. Por ejemplo, en la gestión de una red eléctrica que involucra a múltiples empresas y agencias gubernamentales, la identidad federada puede simplificar el acceso de los operadores a sistemas compartidos, sin comprometer la seguridad.

El principal desafío de las identidades federadas radica en la confianza centralizada en los proveedores de identidad. Si el proveedor se ve comprometido, todas las plataformas que dependen de él pueden verse afectadas. Además, este modelo depende de la disponibilidad del proveedor, por lo que, en caso de una interrupción del servicio o un ataque dirigido, los usuarios podrían perder el acceso a los sistemas críticos.

El *blockchain* permite que las identidades descentralizadas otorguen a los usuarios un control total sobre sus credenciales. Este enfoque descentraliza la verificación, eliminando la dependencia de una autoridad central. La verificación de credenciales se realiza a través de una red distribuida. Esto mejora tanto la seguridad como la privacidad al mitigar el riesgo de un único punto de fallo y evitar el almacenamiento centralizado de la información personal.

En las IC, las identidades descentralizadas pueden mejorar la seguridad y reducir la exposición a ciberataques. Por ejemplo, en plantas de energía, los operadores de sistemas SCADA podrían autenticar su acceso a distintos subsistemas mediante identidades descentralizadas. Esto sería especialmente valioso en escenarios de resiliencia cibernética, ya que las identidades descentralizadas seguirían operando, incluso si uno o varios nodos de la red se vieran comprometidos.

No obstante, la implementación de identidades descentralizadas enfrenta importantes desafíos, como la complejidad técnica inherente a estos sistemas. Para su implementación y gestión efectiva, las organizaciones deben invertir en infraestructura y capacitación.

Además, la interoperabilidad entre los sistemas de identidad descentralizada sigue siendo un desafío, puesto que la compatibilidad no es una característica universal. La falta de estándares y normativas claras también representa un riesgo para su implementación en el contexto de las IC, donde la compatibilidad y la seguridad son primordiales.

Otras tendencias relevantes

Además de las identidades autosoberanas, federadas y descentralizadas, varias tendencias emergentes en la gestión de identidades digitales están ganando relevancia. Un ejemplo es la autenticación sin contraseñas, cuya popularidad ha aumentado, especialmente con el desarrollo de estándares como FIDO2. Este enfoque permite la autenticación mediante claves criptográficas y dispositivos de seguridad, eliminando la necesidad de contraseñas, que, a menudo, son un punto débil en los sistemas de autenticación.

Otra tendencia importante es el auge de los sistemas de autenticación adaptativa, que evalúan el riesgo y personalizan el proceso de autenticación basándose en patrones de comportamiento, ubicación geográfica y tipo de dispositivo, entre otros.

A esto se suma el uso avanzado de tecnologías como el aprendizaje automático y la IA. En conjunto, estos avances mejoran tanto la seguridad como la experiencia del usuario al proporcionar un acceso más fluido en escenarios de bajo riesgo y una protección reforzada en situaciones de alto riesgo (Bakar & Haron, 2014).

Autenticación sin contraseñas

La autenticación sin contraseñas es una tendencia en auge, impulsada por la imperiosa necesidad de robustecer la seguridad y mejorar la experiencia del usuario al eliminar las contraseñas, consideradas uno de los eslabones más débiles de la autenticación tradicional. Dada su susceptibilidad a ataques de fuerza bruta, *phishing* y reutilización, las contraseñas representan un riesgo significativo.

En cambio, la autenticación sin contraseñas utiliza claves criptográficas, dispositivos de seguridad físicos, biometría o MFA, como huellas dactilares o reconocimiento facial, para validar la identidad de los usuarios.

El estándar FIDO2 representa uno de los avances más significativos en este campo. Este protocolo utiliza un sistema de claves públicas y privadas, generadas directamente en el dispositivo del usuario. De este modo, se refuerza la seguridad y se elimina el riesgo de robo o interceptación de credenciales.

Ventajas:

- Seguridad reforzada: al eliminar las contraseñas, se reducen significativamente los riesgos de ataques de *phishing*, fuerza bruta y reutilización de credenciales.
- Mejor experiencia para el usuario: al prescindir de la memoria y eliminar la necesidad de gestionar múltiples contraseñas, se optimiza la accesibilidad y se simplifica el uso.

Desafíos:

- Implementación: la adopción generalizada de sistemas sin contraseñas puede representar un desafío para las organizaciones con infraestructuras heredadas que aún dependen de contraseñas tradicionales.
- Acceso en dispositivos compartidos o públicos: la autenticación sin contraseñas debe contemplar cómo garantizar un acceso seguro.

Gestión de las identidades en el internet de las cosas

El crecimiento exponencial del IoT está generando la necesidad de gestionar identidades digitales no solo para humanos, sino también para millones de dispositivos conectados. Cada dispositivo IoT requiere una identidad digital única para su autenticación y autorización en las redes a las que está vinculado. Esto plantea desafíos significativos en términos de escalabilidad, interoperabilidad y seguridad, ya que muchos dispositivos IoT presentan limitaciones en su capacidad de procesamiento y almacenamiento.

Los sistemas de gestión de identidades deben ser capaces de autenticar estos dispositivos de forma rápida y segura, garantizando que solo los autorizados puedan interactuar con los sistemas críticos. En este contexto, se están explorando soluciones como las identidades descentralizadas basadas en *blockchain*, que permiten autenticar dispositivos IoT sin depender de un proveedor centralizado, lo que reduce significativamente el riesgo de suplantación o manipulación de identidades (Roman et al., 2013).

Asimismo, la autenticación de *alcance cercano*, facilitada por el Edge Computing, se presenta como una alternativa para establecer la autenticación en distintos segmentos de red.

Ventajas:

- Escalabilidad: las soluciones avanzadas gestionan millones de dispositivos con distintos niveles de acceso y privilegios.
- Seguridad distribuida: las tecnologías descentralizadas, como el *blockchain*, proporcionan mayor seguridad y reducen el riesgo de compromisos centralizados.

Desafíos:

- Limitaciones de los dispositivos: muchos dispositivos IoT presentan limitaciones técnicas que dificultan la implementación de métodos avanzados de autenticación y cifrado.

- Estándares de interoperabilidad: la falta de estándares universales puede dificultar la implementación y la interoperabilidad entre dispositivos desarrollados por diferentes fabricantes.

Autenticación multifactor adaptativa

A diferencia de la MFA tradicional, que requiere dos o más factores de autenticación, la AMFA ajusta los métodos de autenticación basándose en el contexto y el riesgo evaluado en tiempo real. Este enfoque considera aspectos como la ubicación geográfica, el dispositivo utilizado, la hora del día o el historial de comportamiento del usuario.

Si el sistema detecta una actividad inusual, como un intento de inicio de sesión desde un país diferente o un dispositivo desconocido, puede solicitar autenticación adicional. En situaciones de bajo riesgo, como un inicio de sesión desde una ubicación habitual o un dispositivo confiable, el sistema puede simplificar la autenticación para mejorar la experiencia del usuario (Shameli-Sendi et al., 2016).

Ventajas:

- Mayor seguridad dinámica: la AMFA ajusta la autenticación según las amenazas detectadas en cada contexto, reforzando así la protección contra accesos no autorizados.
- Experiencia de usuario mejorada: simplificar la autenticación en situaciones de bajo riesgo reduce la fricción en las interacciones de los usuarios.

Desafíos:

- Complejidad en la implementación: la AMFA exige sistemas avanzados capaces de analizar múltiples factores en tiempo real y realizar ajustes rápido.
- Privacidad y recopilación de datos: para implementar la autenticación adaptativa, las organizaciones deben recopilar y analizar grandes volúmenes de datos, especialmente los relacionados con el comportamiento del usuario, lo que genera preocupaciones sobre su privacidad.

Conclusiones

La protección de las ICC demanda una estrategia integral que aborde aspectos tecnológicos y humanos, con la gestión de identidades digitales como pilar fundamental. Este enfoque mitiga las vulnerabilidades derivadas de la convergencia entre las TI y las TO, garantizando la seguridad, la confidencialidad y la integridad de los sistemas.

Además, la implementación de tecnologías emergentes, como el *blockchain*, la IA y la autenticación biométrica, refuerza la capacidad de respuesta ante amenazas cibernéticas. Sin embargo, su implementación plantea desafíos técnicos, normativos y de interoperabilidad, lo que destaca la necesidad de marcos regulatorios claros y estándares abiertos que faciliten su integración en entornos heterogéneos y críticos para el funcionamiento de la sociedad.

En lo que respecta a la gestión de la identidad digital para la protección de las IC, esta se ha convertido en un eje transversal en normativas como la NIS2, el NIST CSF V 2.0 y el CONPES 3995 debido a la proliferación de ataques basados en la suplantación de identidad o el robo de credenciales. Además, se observa que las normativas modernas tienden a integrar la protección física y digital, reconociendo la creciente dependencia tecnológica de las IC.

Finalmente, en un escenario en el que el ataque a una IC ya no es una posibilidad, sino una certeza temporal, es imperativo implementar estrategias de mitigación y respuesta. Esto requiere el desarrollo de sistemas resilientes, el uso de tecnologías avanzadas de monitoreo y control, y la adopción de una defensa integrada con la metodología *zero trust*.

Referencias

- Alirio, M. H., Sierra, B., & Silva, J. M. (2016). *Importancia de definir la infraestructura crítica en Colombia*.
- Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*, 68, 81-97. <https://doi.org/10.1016/j.cose.2017.04.005>
- Aydin, H., & Sertbaş, A. (2022). Cyber security in industrial control systems (ICS): A survey of Rowhammer vulnerability. *Applied Computer Science*, 18(2), 86-100. <https://doi.org/10.35784/acs-2022-15>
- Bakar, K. A. A., & Haron, G. R. (2014). Adaptive authentication based on analysis of user behavior. *Proceedings of 2014 Science and Information Conference (SAI 2014)*, 601-606. <https://doi.org/10.1109/SAI.2014.6918248>
- Beerman, J., Berent, D., Falter, Z., & Bhunia, S. (2023). A review of Colonial Pipeline ransomware attack. *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, 8-15. <https://doi.org/10.1109/CCGridW59191.2023.00017>
- Centro Nacional de Inteligencia (CNI). (2008). *Directiva 2008/114/CE del Consejo*.
- Check Point Software Technologies. (s.f.). *What is spear phishing?* <https://tinyurl.com/2yn9f4et>
- Chen, T. M., & Abu-Nimeh, S. (2011). Lessons from Stuxnet. *Computer*, 44(4), 91-93. <https://doi.org/10.1109/MC.2011.115>
- Comando Conjunto Cibernético (CCOC). (2015). *Guía para la identificación de infraestructura crítica cibernética (ICC) de Colombia*. Comando General de las Fuerzas Militares. <https://tinyurl.com/mvvd3xfr>
- Dehalwar, V., Kolhe, M. L., Deoli, S., & Jhariya, M. K. (2022). Blockchain-based trust management and authentication of devices in smart grid. *Cleaner Engineering and Technology*, 8, 100481. <https://doi.org/10.1016/j.clet.2022.100481>
- Dragos, Inc. (2021). *Industrial cyber risk management*. <https://tinyurl.com/mw7hsnz8>
- Elwell, J. S. (2014). The transmediated self: Life between the digital and the analog. *Convergence*, 20(2), 233-249. <https://doi.org/10.1177/1354856513501423>
- Fang, J., Yan, C., & Yan, C. (2009). Centralized identity authentication research based on management application platform. *2009 First International Conference on Information Science and Engineering*, 2292-2295.
- Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of Internet of Things (IoT). *International Journal of Computer Applications*, 111(7), 1-6. <https://doi.org/10.5120/19547-1280>
- FIDO Alliance. (s.f.). *FIDO2: Moving the world beyond passwords*. <https://fidoalliance.org/fido2/>
- Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security -- A survey. *arXiv*. <http://arxiv.org/abs/1701.04525>

- Kebande, V. R., & Awad, A. I. (2024). Industrial Internet of Things ecosystems security and digital forensics: Achievements, open challenges, and future directions. *ACM Computing Surveys*, 56(5). <https://doi.org/10.1145/3635030>
- Lee, R. M., Assante, M. J., & Conway, T. (2016). *SANS ICS 2016 defense use case 4 1: Analysis of the recent reports of attacks on US infrastructure by Iranian actors*. <https://www.secureworldexpo.com/tags/bowman->
- Lewis, J. E., & Lewis, K. D. (2009). Web single sign-on authentication using SAML. *IJCSI International Journal of Computer Science Issues*, 2. <https://doi.org/10.48550/arXiv.0909.2368>
- Ley 1273. (2009, 5 de enero). *Por medio de la cual se modifica el Código Penal...* Congreso de la República de Colombia. <https://tinyurl.com/2bf5r745>
- Ley 1581. (2012, 17 de octubre). *Por la cual se dictan disposiciones generales para la protección de datos personales*. Congreso de la República de Colombia. <https://tinyurl.com/yzqspuwD>
- Luque Juárez, J. M. (2024). La seguridad humana y su implementación en la operación de las Fuerzas Armadas: análisis documental. *Revista Científica General José María Córdova*, 22(45), 237-258. <https://doi.org/10.21830/19006586.1237>
- Maglaras, L., Janicke, H., & Ferrag, M. A. (2022). *Cyber security and critical infrastructures*. <https://www.mdpi.com/topics>
- Moteff, J., & Parfomak, P. (2004). *CRS report for Congress: Critical infrastructure and key assets: Definition and identification*.
- Muth, R., Galal, T., Heiss, J., & Tschorsch, F. (s.f.). *Towards smart contract-based verification of anonymous credentials*. <https://github.com/hyperledger/indy-sdk>
- National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity*. U.S. Department of Commerce.
- O'Reilly, P., Rigopoulos, K., Feldman, L., & Witte, G. (2021). *2020 cybersecurity and privacy annual report*. <https://doi.org/10.6028/NIST.SP.800-214>
- Palleti, V. R., Adepu, S., Mishra, V. K., & Mathur, A. (2021). Cascading effects of cyber-attacks on interconnected critical infrastructure. *Cybersecurity*, 4(1). <https://doi.org/10.1186/s42400-021-00071-z>
- Parlamento Europeo. (2016). *Reglamento general de protección de datos (GDPR) (Reglamento 2016/679)*. <https://gdpr-info.eu/>
- Qu, Y., Gao, L., Luan, T. H., Xiang, Y., Yu, S., Li, B., & Zheng, G. (2020). Decentralized privacy using blockchain-enabled federated learning in fog computing. *IEEE Internet of Things Journal*, 7(6), 5171-5183.
- Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6), 11-25. <https://doi.org/10.1109/37.969131>
- Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10), 2266-2279. <https://doi.org/10.1016/j.comnet.2012.12.018>

- Sameera, K. M., Nicolazzo, S., Arazzi, M., Nocera, A., R. R. K., P. V., & Conti, M. (2024). Privacy-preserving in blockchain-based federated learning systems. *Computer Communications*. <https://doi.org/10.1016/j.comcom.2024.04.024>
- Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers and Security*, 57, 14-30. <https://doi.org/10.1016/j.cose.2015.11.001>
- Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. *Digital Health*, 9. <https://doi.org/10.1177/20552076231177144>
- Tobin, A., & Reed, D. (2017). *The inevitable rise of self-sovereign identity: A white paper from the Sovrin Foundation*.
- Vesić, S., & Bjelajac, M. (2023). Cyber security of a critical infrastructure. *Pravo - Teorija i Praksa*, 40(2), 77-88. <https://doi.org/10.5937/ptp2302077v>
- Wang, C., & Zhao, J. (2023). Network approaches in blockchain-based systems: Applications, challenges, and future directions. *Computer Communications*, 212, 141-150. <https://doi.org/10.1016/j.comcom.2023.09.018>
- Weigl, L., Barbereau, T., & Fridgen, G. (2023). The construction of self-sovereign identity: Extending the interpretive flexibility of technology towards institutions. *Government Information Quarterly*, 40(4). <https://doi.org/10.1016/j.giq.2023.101873>
- Zhang, J., Zhong, S., Wang, T., Chao, H. C., & Wang, J. (2020). Blockchain-based systems and applications: A survey. *Journal of Internet Technology*, 21(1), 1-14. <https://doi.org/10.3966/160792642020012101001>

Capítulo 3

La inteligencia artificial y la transformación digital en el ámbito de la ciberseguridad*

DOI: <https://doi.org/10.25062/9786287818002.03>

Lucas Adolfo Giraldo Ríos

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este capítulo explora la intersección de la inteligencia artificial y la transformación digital en el ámbito de la ciberseguridad, destacando cómo estas tecnologías avanzadas están revolucionando la protección de sistemas y datos. Se detallan las aplicaciones del aprendizaje automático, el aprendizaje profundo y las redes neuronales en la detección y respuesta a amenazas, así como el uso de técnicas como el aprendizaje por refuerzo y las redes generativas adversarias (GAN). Además, se examina la integración de IA en plataformas de seguridad unificadas y la personalización de estrategias de ciberseguridad para adaptarse a amenazas dinámicas. También se discuten las mejores prácticas, como la formación continua y la colaboración con expertos, y se destacan tendencias emergentes que incluyen la optimización de políticas de seguridad y la simulación de ataques avanzados.

Palabras clave: aprendizaje automático; aprendizaje profundo; ciberseguridad; detección de amenazas; inteligencia artificial; transformación digital.

* Capítulo de libro resultado del proyecto de investigación "Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales" del grupo de investigación "Ciberespacio Tecnología e Innovación", de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado C por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) y registrado con el código COL0181179. Los puntos de vista y los resultados de este capítulo pertenecen al autor y no reflejan necesariamente los de las instituciones participantes.

Lucas Adolfo Giraldo Ríos

Candidato a doctor en Ingeniería, Industria y Organizaciones, Universidad Nacional de Colombia. Magíster en Administración de Empresas de Base Tecnológica, Universidad Antonio de Nebrija, España. Magíster en Innovación, Universidad EAN, Colombia. Especialista en Gestión Financiera Empresarial, Universidad de Medellín, Colombia. Administrador de Empresas, Universidad de Antioquia, Colombia.

<https://orcid.org/0000-0002-9947-7882> - Contacto: lucas.giraldo@esdeg.edu.co

Citación APA: Giraldo Ríos, L. A. (2025). La inteligencia artificial y la transformación digital en el ámbito de la ciberseguridad. En M. E. Realpe Díaz & G. A. Gómez Rodríguez (Eds.), *Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales* (pp. 79-118). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818002.03>

CIBERSEGURIDAD EN LA FRONTERA DIGITAL: DESAFÍOS Y OPORTUNIDADES EN LOS NUEVOS ECOSISTEMAS TECNOLÓGICOS EMPRESARIALES

ISBN impreso: 978-628-7602-99-1

ISBN digital: 978-628-7818-00-2

DOI: <https://doi.org/10.25062/9786287818002>

Colección Ciberseguridad y Ciberdefensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2025



Introducción

La ciberseguridad se refiere a las "prácticas, tecnologías y procesos diseñados para proteger sistemas, redes y datos de ataques, daños o accesos no autorizados. En un mundo cada vez más digitalizado, la ciberseguridad se ha convertido en una prioridad fundamental para individuos, empresas y Gobiernos" (Agea, 2023, s.p.). Su alcance va desde la protección de información personal hasta la defensa de infraestructuras críticas a nivel nacional (Stallings, 2021).

La evolución tecnológica ha incrementado la dependencia de las organizaciones en los sistemas de información, haciendo de la ciberseguridad un componente esencial para la continuidad del negocio. La ciberseguridad no solo abarca la protección de los datos, sino también la integridad y disponibilidad de los sistemas, garantizando que estos funcionen correctamente y estén accesibles para los usuarios autorizados (Whitman & Mattord, 2022).

Además, la ciberseguridad implica la gestión de riesgos, identificando, evaluando y mitigando amenazas potenciales. Esto requiere una combinación de estrategias proactivas y reactivas, como la implementación de medidas preventivas y la capacidad de responder de manera efectiva a incidentes de seguridad (Anderson, 2020).

La ciberseguridad también se extiende a la educación y concienciación de los usuarios. La capacitación continua y la promoción de buenas prácticas entre los empleados son cruciales para crear una cultura de seguridad dentro de las organizaciones. La protección efectiva contra amenazas cibernéticas depende en gran medida del comportamiento y la cooperación de todos los usuarios (Srinivas et al., 2019).

En resumen, la ciberseguridad es un campo dinámico y multidimensional que abarca una amplia gama de actividades y disciplinas. Su objetivo principal es proteger la información y los sistemas en un entorno cada vez más interconectado y vulnerable a amenazas sofisticadas. En la era digital, donde la información se mueve a velocidades sin precedentes y la interconexión es una realidad omnipresente, la ciberseguridad es vital. Los datos son el nuevo petróleo y, como tal, son objeto de codicia por parte de actores malintencionados. Sin una ciberseguridad robusta, las organizaciones se enfrentan a riesgos significativos, incluyendo pérdidas financieras, daño reputacional y compromisos legales (Hentea et al., 2008).

La dependencia de la tecnología en prácticamente todos los aspectos de la vida moderna ha hecho que la ciberseguridad sea una prioridad crítica. Desde las finanzas y la atención médica hasta la educación y el entretenimiento, todos los sectores dependen de sistemas seguros para operar de manera efectiva. Una brecha en la seguridad puede resultar en interrupciones graves que afecten la confianza del público y la estabilidad de las organizaciones (Gordon & Loeb, 2022).

Las amenazas cibernéticas están en constante evolución, adaptándose rápidamente a las nuevas tecnologías y estrategias de defensa. Esto requiere que las organizaciones mantengan una vigilancia constante y actualicen regularmente sus políticas y prácticas de seguridad. La ciberseguridad debe ser vista como un proceso continuo y no como una solución estática (Baker, 2020).

Además, la creciente adopción de tecnologías emergentes como el internet de las cosas (IoT), la computación en la nube y la inteligencia artificial (IA) ha ampliado la superficie de ataque, introduciendo nuevas vulnerabilidades y desafíos. La interconexión de dispositivos y sistemas significa que una falla de seguridad en un área puede tener repercusiones en cadena en otros sistemas interconectados (Sicari et al., 2015).

La ciberseguridad también tiene un componente regulatorio significativo. Con la implementación de normativas como el Reglamento General de Protección de Datos (GDPR), en Europa, y la Ley de Privacidad del Consumidor de California (CCPA), en Estados Unidos, las organizaciones deben cumplir con estrictos requisitos de protección de datos. El incumplimiento puede resultar en sanciones severas y pérdida de confianza del consumidor (Solove & Schwartz, 2021).

Este capítulo utiliza una metodología cualitativa basada en la revisión y análisis de literatura existente para explorar la intersección de la IA y la transformación digital en el ámbito de la ciberseguridad. La pregunta de investigación central es: ¿Cómo puede la inteligencia artificial mejorar la eficacia de la ciberseguridad en un

entorno digital cada vez más complejo? El objetivo general del capítulo es identificar y analizar las aplicaciones, beneficios, desafíos y consideraciones éticas de la IA en la ciberseguridad, proporcionando una visión comprensiva de su impacto y potencial futuro (Goodfellow et al., 2016; Buczak & Guven, 2016; Floridi et al., 2018).

El alcance de este capítulo se centra en la intersección de la IA y la transformación digital en el ámbito de la ciberseguridad, proporcionando una visión comprensiva de las aplicaciones, beneficios, desafíos y consideraciones éticas asociadas. Sin embargo, hay ciertas limitaciones por tener en cuenta: 1) la rápida evolución de las tecnologías y las amenazas cibernéticas pueden hacer que algunos de los hallazgos y recomendaciones se vuelvan obsoletos en un corto periodo; 2) la implementación de IA en ciberseguridad es altamente contextual, variando significativamente entre diferentes sectores y organizaciones, lo que limita la generalización de las conclusiones presentadas, y 3) el análisis está basado principalmente en una revisión de literatura existente, lo que puede no capturar completamente las últimas innovaciones y prácticas emergentes en el campo.

Las amenazas a la ciberseguridad son variadas y evolucionan constantemente. Entre las principales se encuentran el *malware* (programa maligno), los ataques de *phishing*, el *ransomware* y las amenazas internas. Cada una de estas amenazas explota diferentes vulnerabilidades, como el *software* desactualizado, las configuraciones de seguridad deficientes y la falta de conciencia entre los usuarios (Sharma & Chen, 2019).

El *malware* es un tipo de *software* malicioso diseñado para causar daño o acceder a sistemas sin autorización. Incluye virus, troyanos, *spyware* y *adware*. Estos programas pueden robar información, dañar datos y sistemas, y permitir a los atacantes controlar dispositivos de manera remota. La detección y eliminación del *malware* requiere herramientas avanzadas y prácticas de seguridad robustas (Tounsi & Rais, 2018).

Los ataques de *phishing* buscan engañar a los usuarios para que revelen información confidencial, como contraseñas y datos financieros, a través de correos electrónicos o sitios web fraudulentos. A menudo, estos ataques se presentan como comunicaciones legítimas de entidades confiables. La concienciación y educación de los usuarios son esenciales para prevenir el *phishing*, junto con tecnologías de filtrado y autenticación (Aleroud & Zhou, 2017).

El *ransomware* es una forma de *malware* que cifra los datos de la víctima y exige un rescate para restaurar el acceso. Este tipo de ataque ha aumentado en frecuencia y sofisticación, afectando tanto a individuos como a organizaciones. La

mejor defensa contra el *ransomware* es una combinación de medidas preventivas, como copias de seguridad regulares y la educación de los empleados sobre las tácticas de los atacantes (Richardson & North, 2017).

Las amenazas internas, que incluyen acciones malintencionadas o negligentes por parte de empleados o contratistas, representan un riesgo significativo para la seguridad de la información. Los sistemas de monitorización y control de acceso, así como políticas claras y entrenamiento en seguridad, son esenciales para mitigar este riesgo. La implementación de estrategias de defensa en profundidad puede ayudar a proteger contra estas amenazas internas (Colwill, 2009).

Además de estas amenazas específicas, las vulnerabilidades en los sistemas y redes también representan un riesgo importante. Esto incluye *software* sin parches, configuraciones de seguridad débiles y la falta de segmentación de red. La gestión proactiva de vulnerabilidades y la implementación de controles de seguridad rigurosos son esenciales para minimizar estos riesgos (LeMay et al., 2011).

Transformación digital: impacto en la ciberseguridad

Concepto de transformación digital

“La transformación digital implica la integración de tecnologías digitales en todas las áreas de una organización, cambiando fundamentalmente la forma en que opera y entrega valor a sus clientes” (“El desafío de la transformación digital”, 2023). Esto incluye el uso de tecnologías como la nube, el IoT, la inteligencia artificial y el análisis de *big data*. La transformación digital no es solo una adopción tecnológica, sino una reinención de los modelos de negocio y procesos operativos (Vial, 2019).

La adopción de tecnologías en la nube es un componente crucial de la transformación digital. La computación en la nube ofrece flexibilidad y escalabilidad, permitiendo a las organizaciones acceder a recursos y servicios según sea necesario sin la necesidad de invertir en infraestructura física costosa. Esto no solo reduce costos, sino que además facilita la innovación y la adaptación rápida a los cambios del mercado. Sin embargo, la migración a la nube también introduce nuevos riesgos de seguridad que deben gestionarse adecuadamente (Rittinghouse & Ransome, 2017).

El Internet de las Cosas (IoT) es otra tecnología central en la transformación digital. Los dispositivos IoT están interconectados y pueden comunicarse entre sí, proporcionando datos en tiempo real y automatizando procesos. Por ejemplo, en la industria manufacturera, los sensores IoT pueden monitorear maquinaria y predecir fallas antes de que ocurran, optimizando el mantenimiento y reduciendo el tiempo de inactividad. Sin embargo, la proliferación de dispositivos IoT amplía la superficie de ataque, introduciendo vulnerabilidades adicionales que deben ser gestionadas de manera efectiva (Sicari et al., 2015).

La inteligencia artificial (IA) y el análisis de *big data* también juegan un papel fundamental en la transformación digital. Estas tecnologías permiten a las organizaciones analizar grandes volúmenes de datos para obtener *insights* valiosos y tomar decisiones informadas. La IA puede automatizar tareas repetitivas, mejorar la eficiencia operativa y personalizar las interacciones con los clientes. Por ejemplo, los chatbots impulsados por IA pueden proporcionar soporte al cliente 24/7, mejorando la experiencia del cliente y liberando recursos humanos para tareas más complejas. Sin embargo, la protección de estos datos y la garantía de su integridad y confidencialidad son desafíos críticos que deben abordarse para garantizar la seguridad en un entorno digital (Chen et al., 2014).

Además, la transformación digital implica un cambio cultural dentro de las organizaciones. Para aprovechar plenamente las tecnologías digitales, las empresas deben fomentar una cultura de innovación y agilidad. Esto puede incluir la adopción de metodologías ágiles, la formación continua de los empleados y la promoción de una mentalidad de mejora continua. La transformación digital no es solo una cuestión de tecnología, sino también de personas y procesos (Fitzgerald et al., 2014). La transformación digital es un proceso multifacético que involucra la adopción de tecnologías avanzadas, la reinención de modelos de negocio y procesos, y un cambio cultural dentro de las organizaciones. Aunque presenta numerosos beneficios, también introduce nuevos desafíos en términos de seguridad y gestión de riesgos. Las organizaciones deben abordar estos desafíos de manera proactiva para garantizar una transición exitosa hacia un entorno digital más eficiente y seguro.

Transformación digital: impacto en la ciberseguridad

La transformación digital, aunque ofrece numerosas ventajas, también presenta nuevos desafíos en términos de ciberseguridad. La adopción de tecnologías avanzadas amplía la superficie de ataque, introduciendo nuevas vulnerabilidades

y vectores de amenaza. La interconexión de dispositivos IoT, por ejemplo, puede crear puntos de entrada adicionales para los atacantes (Weber, 2010). La mayor cantidad de datos generados y compartidos aumenta el riesgo de que la información sensible sea comprometida. Además, las soluciones en la nube, aunque beneficiosas por su escalabilidad y flexibilidad, pueden ser vulnerables a problemas de configuración y accesos no autorizados si no se gestionan correctamente (Rittinghouse & Ransome, 2017).

Uno de los principales desafíos es la complejidad creciente de los entornos tecnológicos. A medida que las organizaciones adoptan múltiples tecnologías y plataformas, la gestión de la seguridad se vuelve más complicada. La integración de sistemas dispares y la interoperabilidad pueden crear brechas de seguridad que los atacantes pueden explotar. Por lo tanto, es esencial tener una estrategia de ciberseguridad holística que abarque todos los componentes del ecosistema digital (Von Solms & Van Niekerk, 2013). Además, la velocidad de la transformación digital puede ser un problema. Las organizaciones a menudo priorizan la innovación y la rapidez sobre la seguridad, lo que puede llevar a la implementación de tecnologías sin una evaluación adecuada de los riesgos de seguridad. Este enfoque puede resultar en la exposición a amenazas que podrían haberse mitigado con una planificación y evaluación de riesgos más rigurosa (Schneier, 2015).

Además, la dependencia de proveedores externos de servicios en la nube y otras tecnologías puede introducir riesgos adicionales. Las organizaciones deben confiar en que estos proveedores implementen medidas de seguridad adecuadas. Esto requiere una gestión cuidadosa de las relaciones con los proveedores y la implementación de acuerdos de nivel de servicio que incluyan requisitos de seguridad específicos (Bandyopadhyay et al., 2009). Por ejemplo, un proveedor de servicios en la nube debe garantizar que los datos de la organización estén protegidos contra accesos no autorizados y que se sigan las mejores prácticas de seguridad. La falta de control directo sobre los datos y los sistemas alojados en la nube puede ser una fuente de preocupación para muchas organizaciones.

La transformación digital puede afectar la ciberseguridad al cambiar la dinámica del trabajo. Con el aumento del trabajo remoto y la movilidad, los empleados acceden a los sistemas corporativos desde ubicaciones y dispositivos diversos. Esto puede aumentar el riesgo de acceso no autorizado y la exposición a amenazas si no se implementan medidas de seguridad adecuadas, como la autenticación

multifactor y la gestión de dispositivos móviles (Columbus, 2020). La política de "lleva tu propio dispositivo" (BYOD) también presenta desafíos adicionales, ya que los dispositivos personales pueden no estar tan protegidos como los dispositivos corporativos, aumentando así la vulnerabilidad a ataques cibernéticos.

Desafíos y oportunidades

Los desafíos incluyen la necesidad de actualizar constantemente las estrategias de seguridad para mantenerse al día con las amenazas emergentes y la dificultad de proteger entornos tecnológicos cada vez más complejos. La rápida evolución de las tecnologías y las tácticas de los atacantes requieren una adaptabilidad y agilidad constante en las defensas de ciberseguridad (Huang & Nicol, 2010). Uno de los principales desafíos es la escasez de profesionales capacitados en ciberseguridad. A medida que las amenazas se vuelven más sofisticadas, la demanda de expertos en seguridad supera la oferta. Las organizaciones deben invertir en la formación y desarrollo de su personal, así como en la atracción y retención de talento en ciberseguridad (ISACA, 2019).

Otro desafío significativo es la gestión de la privacidad y el cumplimiento normativo. Con regulaciones como el GDPR y la CCPA, las organizaciones deben asegurarse de que sus prácticas de ciberseguridad cumplan con las normativas de protección de datos. Esto implica no solo proteger los datos contra amenazas externas, sino también gestionar adecuadamente el acceso y uso de los datos dentro de la organización (Solove & Schwartz, 2021). A pesar de estos desafíos, la transformación digital también ofrece oportunidades significativas para mejorar la ciberseguridad. Las tecnologías avanzadas, como la IA y el aprendizaje automático, pueden mejorar la capacidad de las organizaciones para detectar y responder a amenazas. Estas tecnologías permiten un análisis más rápido y preciso de grandes volúmenes de datos, identificando patrones y anomalías que podrían pasar inadvertidas para los analistas humanos (Buczak & Guven, 2016).

La transformación digital también fomenta la colaboración y el intercambio de información. Las organizaciones pueden aprovechar plataformas y comunidades de seguridad para compartir conocimientos y mejores prácticas. Esta colaboración puede mejorar la resiliencia general del ecosistema digital y facilitar la respuesta coordinada a incidentes de seguridad (European Union Agency for Cybersecurity [ENISA], 2019).

Inteligencia artificial en ciberseguridad

La inteligencia artificial (IA) se refiere a la capacidad de las máquinas para realizar tareas que tradicionalmente requieren inteligencia humana, como el aprendizaje, la resolución de problemas y la toma de decisiones. En ciberseguridad, la IA se utiliza para analizar grandes volúmenes de datos y detectar patrones que podrían indicar una amenaza. La IA abarca diversas tecnologías, incluyendo el aprendizaje automático, el aprendizaje profundo y la lógica difusa (Russell & Norvig, 2016). Estas tecnologías permiten a los sistemas de ciberseguridad no solo responder a las amenazas actuales, sino también anticiparse a futuras vulnerabilidades. El aprendizaje automático (*machine learning*) es una subdisciplina de la IA que permite a los sistemas aprender y mejorar a partir de la experiencia sin ser explícitamente programados para cada tarea. En ciberseguridad, se utiliza para identificar patrones en los datos que pueden ser indicativos de actividades maliciosas. Los algoritmos de aprendizaje automático pueden clasificarse en *supervisados*, *no supervisados* y *de refuerzo*, cada uno con sus propias aplicaciones y ventajas (Goodfellow et al., 2016). Por ejemplo, en la detección de intrusiones, los algoritmos supervisados pueden ser entrenados con datos etiquetados de tráfico de red normal y malicioso para identificar futuras intrusiones.

El aprendizaje profundo (*deep learning*), una subdisciplina del aprendizaje automático, utiliza redes neuronales artificiales con múltiples capas para analizar datos complejos. Esta técnica es particularmente efectiva para tareas como el reconocimiento de imágenes y el procesamiento del lenguaje natural. En ciberseguridad, el aprendizaje profundo se aplica para mejorar la precisión de los sistemas de detección y respuesta. Por ejemplo, las redes neuronales convolucionales (CNN) pueden analizar grandes volúmenes de datos de tráfico de red para identificar patrones de ataques sofisticados que podrían pasar inadvertidos para los métodos tradicionales (LeCun et al., 2015).

La lógica difusa (*fuzzy logic*) es otra técnica de IA que se utiliza para manejar la incertidumbre y la imprecisión en los datos de ciberseguridad. La lógica difusa permite a los sistemas tomar decisiones basadas en información incompleta o ambigua, lo que es común en entornos de seguridad. Por ejemplo, un sistema de detección de intrusiones basado en lógica difusa puede evaluar múltiples factores de riesgo que no son claramente definidos como seguros o inseguros, proporcionando una evaluación más flexible y adaptable de la amenaza (Zadeh, 1996).

Una de las ventajas clave de la IA en ciberseguridad es su capacidad para manejar y analizar grandes volúmenes de datos en tiempo real. En un entorno donde los ataques pueden ocurrir en fracciones de segundo, la capacidad de la IA para procesar datos rápidamente y detectar anomalías es crucial. Los sistemas basados en IA pueden monitorizar continuamente el tráfico de red, los registros de eventos y otros datos de seguridad, proporcionando alertas inmediatas y permitiendo una respuesta rápida a las amenazas (Kim et al., 2014). La IA también permite la automatización de muchas tareas de ciberseguridad que tradicionalmente requerirían intervención humana. Esto incluye la detección de *malware*, la gestión de vulnerabilidades y la respuesta a incidentes. La automatización no solo mejora la eficiencia operativa, sino que también reduce el margen de error humano. Por ejemplo, los sistemas automatizados pueden aplicar parches de seguridad y actualizar reglas de *firewall* sin necesidad de intervención manual, asegurando que las defensas estén siempre actualizadas y optimizadas (Seymour & Tully, 2016).

Además, la IA tiene el potencial de mejorar la capacidad de las organizaciones para predecir y prevenir ataques. Los modelos predictivos basados en IA pueden analizar patrones históricos de amenazas y comportamientos maliciosos para anticipar futuras vulnerabilidades. Esta capacidad de predicción permite a las organizaciones implementar medidas preventivas y fortalecer sus defensas antes de que ocurra un ataque. Por ejemplo, los algoritmos de predicción pueden identificar comportamientos inusuales en el tráfico de red que podrían indicar un ataque inminente, permitiendo a los equipos de seguridad tomar medidas proactivas (Hastie et al., 2009).

Las aplicaciones de IA en ciberseguridad son diversas e incluyen la detección de anomalías, la identificación de amenazas, la automatización de respuestas y la mejora de la gestión de incidentes. Los sistemas de IA pueden analizar tráfico de red en tiempo real, identificar comportamientos sospechosos y alertar a los equipos de seguridad para que tomen medidas preventivas (Sommer & Paxson, 2010).

Una de las aplicaciones más comunes es la detección de anomalías en la red. Los sistemas de detección de intrusiones basados en IA pueden monitorear el tráfico de red y utilizar algoritmos de aprendizaje automático para identificar patrones anómalos que podrían indicar una actividad maliciosa. Esto permite a las organizaciones responder rápidamente a posibles amenazas antes de que puedan causar daño significativo (Patcha & Park, 2007).

Otra aplicación importante es la identificación de amenazas y la clasificación de *malware*. Los sistemas de IA pueden analizar archivos y comportamientos

de *software* para determinar si representan una amenaza. Esto incluye la identificación de nuevas variantes de *malware* que pueden no ser detectadas por los métodos tradicionales de firmas. La IA también puede categorizar el *malware* en diferentes familias, lo que ayuda a los analistas a entender mejor la naturaleza de la amenaza (Schultz et al., 2001).

La automatización de respuestas es otra área donde la IA puede mejorar la ciberseguridad. Los sistemas de respuesta automatizada pueden tomar medidas inmediatas para contener una amenaza una vez que ha sido detectada. Esto incluye la cuarentena de dispositivos infectados, el bloqueo de direcciones IP maliciosas y la actualización de reglas de *firewall*. La automatización reduce el tiempo de respuesta y libera a los analistas para que se concentren en tareas más complejas (García-Teodoro et al., 2009).

Además, la IA puede mejorar la gestión de incidentes al proporcionar herramientas avanzadas de análisis y visualización. Los sistemas de gestión de información y eventos de seguridad (SIEM) basados en IA pueden correlacionar eventos de seguridad de múltiples fuentes, identificar patrones y tendencias, y proporcionar recomendaciones sobre cómo mitigar las amenazas. Esto mejora la capacidad de los equipos de seguridad para gestionar y resolver incidentes de manera eficiente (Chuvakin et al., 2013).

Los beneficios de la IA en ciberseguridad incluyen la capacidad de procesar y analizar datos a una velocidad y escala inalcanzables para los humanos, mejorando así la eficiencia y eficacia de las operaciones de seguridad. No obstante, la IA también tiene limitaciones, como la dependencia de datos de calidad para el entrenamiento de modelos y la posibilidad de errores en la detección, lo que podría llevar a falsos positivos o negativos (Buczak & Guven, 2016). Uno de los principales beneficios de la IA es su capacidad para manejar grandes volúmenes de datos en tiempo real. En ciberseguridad, donde los ataques pueden ocurrir en cuestión de segundos, la velocidad de respuesta es crucial. Los sistemas de IA pueden analizar el tráfico de red, los registros de eventos y otros datos de seguridad de manera continua, identificando y respondiendo a amenazas más rápido que los métodos tradicionales (Kim et al., 2014).

La precisión de la detección es otro beneficio significativo. Los algoritmos de aprendizaje automático pueden mejorar su precisión con el tiempo a medida que se entrenan con más datos. Esto permite a los sistemas de IA identificar patrones complejos y sutiles que podrían pasar inadvertidos para los analistas humanos. La capacidad de aprender y adaptarse a nuevas amenazas es una ventaja clave de

la IA en ciberseguridad (Seymour & Tully, 2016). Sin embargo, la IA también tiene limitaciones. Una de las más importantes es la calidad y cantidad de datos necesarios para entrenar los modelos. Si los datos de entrenamiento son incompletos o sesgados, los modelos de IA pueden producir resultados inexactos. Esto puede llevar a la identificación incorrecta de amenazas, lo que resulta en falsos positivos (alarma innecesaria) o falsos negativos (no detectar una amenaza real) (Chio & Freeman, 2018). Además, los sistemas de IA pueden ser vulnerables a ataques de adversarios. Los atacantes pueden intentar engañar a los modelos de IA mediante técnicas como el envenenamiento de datos, donde se introducen datos maliciosos en el conjunto de entrenamiento para manipular los resultados. También pueden utilizar ataques de evasión, diseñados para evitar la detección por sistemas de IA (Biggio & Roli, 2018).

Finalmente, la implementación de IA en ciberseguridad requiere una inversión significativa en infraestructura y capacitación. Las organizaciones deben asegurarse de que tienen los recursos necesarios para desplegar y mantener sistemas de IA efectivos. Esto incluye la contratación de personal capacitado y la inversión en *hardware* y *software* adecuado (Buczak & Guven, 2016).

Técnicas y herramientas de IA en ciberseguridad

Algoritmos de aprendizaje automático

El aprendizaje automático (*machine learning*) es una subdisciplina de la inteligencia artificial (IA) que implica el uso de algoritmos que permiten a las máquinas aprender de los datos y mejorar su desempeño con el tiempo. En ciberseguridad, estos algoritmos se utilizan para detectar patrones en los datos que podrían indicar comportamientos maliciosos. Los algoritmos de aprendizaje automático pueden clasificarse en supervisados, no supervisados y de refuerzo, cada uno con sus propias aplicaciones y ventajas (Goodfellow et al., 2016). Los algoritmos supervisados son aquellos que se entrenan con un conjunto de datos etiquetados, donde cada entrada de datos está asociada con una etiqueta que indica su clase o categoría. En ciberseguridad, estos algoritmos se utilizan para tareas como la detección de *spam* y la clasificación de *malware*. Los modelos se entrenan para reconocer patrones en los datos etiquetados y luego aplican este conocimiento a nuevos datos para identificar amenazas. Un ejemplo común es el uso de máquinas

de vectores de soporte (SVM) para clasificar correos electrónicos como *spam* o legítimos (Maloof, 2006).

Por otro lado, los algoritmos no supervisados no requieren datos etiquetados. En su lugar, buscan patrones y relaciones en los datos sin ninguna guía predefinida. Estos algoritmos son útiles para la detección de anomalías, donde se busca identificar comportamientos inusuales que podrían indicar una amenaza. Los métodos de *clustering* y análisis de componentes principales son ejemplos de técnicas no supervisadas utilizadas en ciberseguridad. Por ejemplo, el *clustering* puede agrupar eventos de seguridad similares, ayudando a identificar patrones de ataque que no se habían observado previamente (Hastie et al., 2009).

El aprendizaje por refuerzo es otra técnica utilizada en ciberseguridad. En este enfoque, los agentes de IA aprenden a tomar decisiones mediante la interacción con un entorno y la recepción de recompensas o castigos en función de sus acciones. Este enfoque es útil para desarrollar sistemas de respuesta automatizada que pueden adaptarse a amenazas cambiantes y optimizar sus estrategias con el tiempo. Por ejemplo, un agente de refuerzo podría aprender a ajustar dinámicamente las reglas del *firewall* en respuesta a nuevos tipos de ataques (Sutton & Barto, 2018). Además de estos enfoques básicos, se utilizan técnicas avanzadas como las redes neuronales convolucionales (CNN) y las redes neuronales recurrentes (RNN) para tareas específicas.

Las CNN son especialmente útiles para el análisis de imágenes y la detección de patrones en datos estructurados, mientras que las RNN son efectivas para el procesamiento de secuencias de datos, como registros de eventos y tráfico de red. Estas técnicas avanzadas permiten una mayor precisión en la detección de amenazas complejas y sutiles (LeCun et al., 2015).

El aprendizaje profundo, una subdisciplina del aprendizaje automático, utiliza redes neuronales con múltiples capas para analizar datos complejos. Esta técnica es especialmente útil en ciberseguridad para la detección de *malware* y la identificación de anomalías en el tráfico de red. Las redes neuronales profundas pueden aprender representaciones complejas de los datos y detectar patrones que los métodos tradicionales podrían pasar por alto. Por ejemplo, una red neuronal profunda puede analizar el tráfico de red en busca de patrones de comportamiento que indiquen la presencia de un atacante (Goodfellow et al., 2016).

Además de mejorar la precisión en la detección de amenazas, los algoritmos de aprendizaje automático también permiten una respuesta más rápida a los incidentes de seguridad. Los sistemas basados en aprendizaje automático pueden analizar datos en tiempo real y tomar decisiones automatizadas para mitigar

amenazas. Esto reduce el tiempo de respuesta y minimiza el impacto de los ataques. Por ejemplo, un sistema de detección de intrusiones basado en aprendizaje automático puede identificar y bloquear automáticamente un ataque DDoS en curso (García-Teodoro et al., 2009).

Es importante destacar que la efectividad de los algoritmos de aprendizaje automático en ciberseguridad depende en gran medida de la calidad de los datos utilizados para su entrenamiento. Los datos deben ser representativos de los escenarios de amenazas reales y deben estar limpios y libres de ruido. La recopilación y preparación de datos son etapas críticas en el desarrollo de modelos de aprendizaje automático efectivos. Además, es necesario actualizar y ajustar regularmente los modelos para mantener su eficacia en un entorno de amenazas en constante evolución (Chio & Freeman, 2018).

Redes neuronales y aprendizaje profundo

Las redes neuronales y el aprendizaje profundo representan una evolución del aprendizaje automático. Estas técnicas permiten el análisis de datos complejos y no estructurados, como el tráfico de red y los registros de eventos, mejorando la capacidad de los sistemas de ciberseguridad para identificar amenazas avanzadas. Las redes neuronales imitan el funcionamiento del cerebro humano, utilizando capas de neuronas artificiales para procesar la información (Schmidhuber, 2015).

Las redes neuronales convolucionales (CNN) son un tipo de red neuronal diseñada específicamente para el reconocimiento de patrones en datos estructurados, como imágenes y secuencias de datos. En ciberseguridad, las CNN se utilizan para analizar el tráfico de red y detectar anomalías que podrían indicar ataques. Estas redes son capaces de identificar características específicas en los datos que pueden ser indicativas de comportamientos maliciosos. Por ejemplo, una CNN puede detectar patrones inusuales en el tráfico de red que sugieren la presencia de un *malware* avanzado (Krizhevsky et al., 2012).

Las redes neuronales recurrentes (RNN) son otro tipo de red neuronal, particularmente útil para el procesamiento de secuencias de datos. Las RNN tienen una memoria interna que les permite considerar el contexto temporal, lo que es esencial para analizar registros de eventos y patrones de tráfico en tiempo real. Esto las hace ideales para tareas como la detección de intrusiones y la identificación de comportamientos anómalos. Por ejemplo, una RNN puede analizar una serie de eventos de inicio de sesión para detectar patrones que indiquen un intento de ataque de fuerza bruta (Hochreiter & Schmidhuber, 1997).

El aprendizaje profundo también incluye técnicas como el aprendizaje de transferencia, donde un modelo preentrenado en una tarea se ajusta para realizar una tarea similar. Esto es útil en ciberseguridad, donde los datos etiquetados pueden ser escasos y costosos de obtener. El aprendizaje de transferencia permite utilizar modelos entrenados en grandes conjuntos de datos públicos y adaptarlos a contextos específicos de ciberseguridad. Por ejemplo, un modelo de detección de objetos entrenado en un conjunto de datos de imágenes puede ser ajustado para detectar tipos específicos de *malware* (Pan & Yang, 2010).

Además, las redes generativas adversarias (GAN) son una técnica avanzada de aprendizaje profundo que se utiliza para generar datos sintéticos. En ciberseguridad, las GAN pueden generar ejemplos de ataques para entrenar y evaluar sistemas de defensa. Las GAN consisten en dos redes neuronales que compiten entre sí: una genera datos sintéticos mientras que la otra evalúa su autenticidad, mejorando continuamente la calidad de los datos generados. Esto es especialmente útil para crear conjuntos de datos balanceados y diversos para entrenar modelos de detección de amenazas (Goodfellow et al., 2014). Otra técnica relevante en el contexto de las redes neuronales y el aprendizaje profundo es el autoencoder, que se utiliza para la reducción de dimensionalidad y la detección de anomalías. Un autoencoder es una red neuronal que aprende a comprimir los datos de entrada en una representación más pequeña y luego a reconstruirlos. Las diferencias entre los datos originales y reconstruidos pueden revelar anomalías. Esto es útil en la detección de comportamientos anómalos en el tráfico de red y en los registros de eventos, donde las anomalías pueden indicar la presencia de actividades maliciosas (Sakurada & Yairi, 2014).

En suma, las redes neuronales y el aprendizaje profundo ofrecen poderosas herramientas para mejorar la ciberseguridad. Su capacidad para analizar datos complejos y no estructurados, junto con técnicas avanzadas como el aprendizaje de transferencia y las GAN, permite a las organizaciones detectar y responder a amenazas de manera más efectiva. La aplicación de estas tecnologías requiere una comprensión profunda de los algoritmos y una infraestructura adecuada para manejar el procesamiento intensivo de datos (LeCun et al., 2015).

Análisis predictivo y detección de anomalías

El análisis predictivo utiliza técnicas estadísticas y algoritmos de aprendizaje automático para predecir eventos futuros basados en datos históricos. En ciberseguridad, se utiliza para anticipar ataques y tomar medidas preventivas. La detección

de anomalías, por su parte, identifica desviaciones inusuales en el comportamiento del sistema que podrían indicar una brecha de seguridad (Chandola et al., 2009). El análisis predictivo en ciberseguridad implica el uso de modelos de predicción para identificar posibles amenazas antes de que ocurran.

Esto se basa en el análisis de patrones históricos de ataques y comportamientos maliciosos. Los modelos predictivos pueden identificar indicadores tempranos de un ataque, como un aumento en el tráfico de red anómalo o intentos de acceso fallidos, y alertar a los equipos de seguridad para que tomen medidas preventivas. Por ejemplo, los sistemas de predicción pueden analizar el comportamiento de los usuarios y detectar patrones que preceden a un ataque interno (Hastie et al., 2009).

La detección de anomalías es una técnica crítica en ciberseguridad, ya que muchas amenazas se manifiestan como comportamientos anómalos en los sistemas. Los algoritmos de detección de anomalías analizan los datos en busca de desviaciones respecto de patrones normales de comportamiento. Esto puede incluir picos inesperados en el tráfico de red, accesos no autorizados a sistemas y cambios inusuales en los archivos de configuración. Por ejemplo, un sistema de detección de anomalías puede identificar una cantidad inusual de datos salientes desde un servidor, lo que podría indicar una filtración de datos (Patcha & Park, 2007).

Existen varios métodos para la detección de anomalías, incluidos los métodos basados en estadísticas, los modelos de aprendizaje automático y las técnicas de minería de datos. Los métodos estadísticos se basan en modelos probabilísticos para identificar datos que no se ajustan a la distribución esperada. Los modelos de aprendizaje automático, como las máquinas de vectores de soporte (SVM) y los bosques aleatorios, pueden aprender patrones normales a partir de datos históricos y detectar anomalías en tiempo real. Las técnicas de minería de datos, como el *clustering* y la reducción de dimensionalidad, se utilizan igualmente para identificar patrones ocultos en los datos (Chandola et al., 2009).

La detección de anomalías también puede mejorarse mediante el uso de técnicas de aprendizaje profundo, como las redes neuronales autoencoder. Los autoencoders son redes neuronales diseñadas para aprender una representación comprimida de los datos, lo que les permite identificar desviaciones significativas respecto de los patrones normales. Esta técnica es particularmente útil para detectar ataques sofisticados que pueden no ser capturados por métodos tradicionales. Por ejemplo, un autoencoder puede detectar patrones de tráfico de red que difieren significativamente de la actividad normal, indicando un posible ataque (Sakurada & Yairi, 2014).

Además de la detección de anomalías en tiempo real, el análisis predictivo también puede utilizarse para la planificación de la capacidad y la gestión de recursos en ciberseguridad. Los modelos predictivos pueden anticipar picos en la carga de trabajo y ajustar los recursos en consecuencia para garantizar que los sistemas de seguridad puedan manejar la demanda. Esto es especialmente útil en entornos de red altamente dinámicos, donde la carga de trabajo puede variar significativamente en función de eventos externos, como campañas de *marketing* o lanzamientos de productos (Hastie et al., 2009).

Otra aplicación importante del análisis predictivo en ciberseguridad es la identificación de vulnerabilidades potenciales antes de que sean explotadas. Los modelos predictivos pueden analizar datos de vulnerabilidades conocidas y anticipar las más probables de ser explotadas en el futuro. Esto permite a las organizaciones priorizar sus esfuerzos de reparación y centrarse en las vulnerabilidades más críticas. Por ejemplo, un modelo predictivo puede identificar que ciertas configuraciones de *software* son más susceptibles a ataques y recomendar actualizaciones específicas para mitigar estos riesgos (Sutton & Barto, 2018).

El análisis predictivo y la detección de anomalías también pueden ayudar a mejorar la respuesta a incidentes de seguridad. Al anticipar posibles ataques y detectar anomalías en tiempo real, los equipos de seguridad pueden responder de manera más rápida y efectiva a los incidentes. Esto incluye la implementación de contramedidas automatizadas, como el aislamiento de sistemas comprometidos y la aplicación de parches de seguridad, para mitigar el impacto de los ataques. La capacidad de respuesta rápida es crucial para minimizar el daño y garantizar la continuidad operativa (García-Teodoro et al., 2009).

El análisis predictivo y la detección de anomalías son herramientas esenciales para la ciberseguridad proactiva. Estas técnicas permiten a las organizaciones anticipar y mitigar amenazas antes de que causen daños significativos, mejorando la resiliencia y la capacidad de respuesta a incidentes de seguridad. La implementación de estas tecnologías requiere una combinación de conocimientos técnicos y estrategias de gestión de riesgos para maximizar su eficacia y mantener la seguridad en un entorno de amenazas en constante evolución (Chandola et al., 2009).

El aprendizaje automático (*machine learning*) y el aprendizaje profundo (*deep learning*) desempeñan un papel crucial en la ciberseguridad al permitir el análisis avanzado de grandes volúmenes de datos y la detección de patrones complejos asociados a amenazas. Los algoritmos supervisados, no supervisados y de refuerzo se aplican para identificar comportamientos maliciosos y responder

rápidamente a incidentes. Las redes neuronales convolucionales (CNN) y recurrentes (RNN) mejoran la precisión en la detección de anomalías y ataques sofisticados, mientras que técnicas avanzadas como los autoencoders y las redes generativas adversarias (GAN) proporcionan herramientas adicionales para la identificación de amenazas y la generación de datos sintéticos. El análisis predictivo y la detección de anomalías permiten anticipar ataques y gestionar recursos de manera proactiva, mejorando la resiliencia y la capacidad de respuesta a incidentes de seguridad.

Casos de uso de IA en ciberseguridad

Detección de *malware* y prevención de fraudes

La IA se utiliza para mejorar la detección de *malware* mediante el análisis de patrones en el código y el comportamiento del *software*. Los sistemas basados en IA pueden identificar y clasificar nuevas variantes de *malware* más rápidamente que los métodos tradicionales. Esto se debe a la capacidad de la IA para aprender y adaptarse a nuevas amenazas, mejorando continuamente su precisión y eficacia (Schultz et al., 2001). Un enfoque común es el uso de algoritmos de aprendizaje automático para analizar el código del *software* y detectar características que son indicativas de *malware*.

Estos algoritmos pueden ser entrenados con grandes conjuntos de datos de muestras de *malware* conocidas y archivos benignos, aprendiendo a distinguir entre los dos. Una vez entrenados, pueden analizar nuevos archivos y determinar si contienen características similares a las del *malware* conocido (Ye et al., 2017). Además del análisis de código, la IA también se utiliza para monitorear el comportamiento del *software* en tiempo real. Los sistemas basados en IA pueden analizar cómo interactúa un programa con el sistema operativo, el uso de la red y otros comportamientos que podrían indicar una actividad maliciosa. Este enfoque permite la detección de *malware* que puede no ser identificable a través del análisis estático del código (Saxe & Berlin, 2015).

Las técnicas de aprendizaje profundo, como las redes neuronales recurrentes (RNN) y las redes neuronales convolucionales (CNN), también se aplican en la detección de *malware*. Estas redes pueden aprender representaciones complejas de los datos y detectar patrones sutiles que podrían pasar inadvertidos para los

métodos tradicionales. Las RNN son particularmente útiles para analizar secuencias de comportamiento del *software*, mientras que las CNN pueden identificar características estructurales en el código (LeCun et al., 2015). Un ejemplo práctico de la aplicación de IA en la detección de *malware* es la utilización de sistemas de *sandboxing* automatizados. Estos sistemas ejecutan archivos sospechosos en entornos virtualizados y monitorean su comportamiento en busca de actividades maliciosas. La IA puede analizar los resultados del *sandboxing* y tomar decisiones sobre si un archivo es seguro o no, mejorando la velocidad y precisión de la detección de *malware* (Egele et al., 2012).

En el ámbito financiero, la IA se aplica para detectar y prevenir fraudes mediante el análisis de transacciones en tiempo real y la identificación de patrones sospechosos. Esto permite a las instituciones financieras actuar rápidamente para mitigar riesgos. Los sistemas basados en IA pueden analizar grandes volúmenes de datos transaccionales, identificando comportamientos anómalos que podrían indicar fraude (Ngai et al., 2011).

Uno de los enfoques más comunes es el uso de algoritmos de aprendizaje automático para clasificar transacciones como fraudulentas o legítimas. Estos algoritmos se entrenan con datos históricos de transacciones, donde se etiquetan las transacciones fraudulentas y legítimas. Los modelos resultantes pueden detectar patrones en las transacciones en tiempo real, alertando a los equipos de seguridad cuando se identifican comportamientos sospechosos (Buczak & Guven, 2016). Además de la clasificación, la IA también se utiliza para realizar análisis de red, identificando relaciones entre diferentes entidades (como cuentas bancarias, tarjetas de crédito y direcciones IP) que podrían indicar fraude organizado. Los algoritmos de detección de fraude basados en grafos pueden descubrir conexiones ocultas entre entidades que de otro modo podrían pasar inadvertidas (Chen et al., 2012).

Las técnicas de aprendizaje profundo también se aplican en la prevención de fraudes. Las redes neuronales convolucionales (CNN) y las redes neuronales recurrentes (RNN) pueden analizar secuencias de transacciones y detectar patrones temporales que indican actividades fraudulentas. Estas técnicas permiten una detección más precisa y en tiempo real, lo que es crucial para mitigar los impactos del fraude (Zheng et al., 2018). Un ejemplo práctico de la aplicación de IA en la prevención de fraudes es el uso de sistemas de autenticación basados en el comportamiento. Estos sistemas analizan patrones de comportamiento del usuario, como la forma en que escriben, mueven el ratón y navegan por un sitio web. La IA puede identificar desviaciones en estos patrones que podrían indicar que un

fraude está ocurriendo, permitiendo a las instituciones financieras tomar medidas preventivas de manera proactiva (Monaco & Tappert, 2016).

Gestión de incidentes y respuesta automatizada

La IA puede automatizar la gestión de incidentes de seguridad, desde la detección hasta la respuesta. Esto incluye la identificación de la causa raíz de un incidente, la contención de la amenaza y la reparación de los sistemas afectados, reduciendo el tiempo de respuesta y mejorando la eficiencia. Los sistemas basados en IA pueden analizar grandes volúmenes de datos de seguridad en tiempo real, proporcionando información crítica para la toma de decisiones (García-Teodoro et al., 2009).

Uno de los aspectos clave de la gestión de incidentes es la correlación de eventos. Los sistemas de gestión de información y eventos de seguridad (SIEM) basados en IA pueden correlacionar datos de múltiples fuentes, como registros de red, sistemas de detección de intrusiones y aplicaciones de seguridad. La IA puede identificar patrones y relaciones entre estos eventos, proporcionando una visión holística de la situación de seguridad. Esto permite a los equipos de seguridad comprender mejor el contexto y la gravedad de un incidente, facilitando una respuesta más efectiva (Chuvakin et al., 2013). La respuesta automatizada a incidentes es otro beneficio significativo de la IA. Los sistemas de respuesta a incidentes pueden tomar medidas inmediatas para contener una amenaza una vez que ha sido detectada. Esto incluye la cuarentena de dispositivos infectados, el bloqueo de direcciones IP maliciosas y la actualización de reglas de *firewall*. La automatización de estas tareas reduce el tiempo de respuesta y minimiza el impacto de los incidentes de seguridad. Por ejemplo, un sistema de respuesta automatizada puede detectar un ataque de *ransomware* en curso y aislar rápidamente los sistemas afectados para prevenir la propagación del *malware* (National Institute of Standards and Technology [NIST], 2020).

La IA también puede ayudar en la identificación de la causa raíz de los incidentes. Los algoritmos de análisis de causa raíz pueden rastrear la secuencia de eventos que llevaron a un incidente, identificando la fuente del problema. Esto es crucial para la reparación efectiva y la prevención de futuros incidentes. La capacidad de la IA para analizar datos complejos y descubrir relaciones causales es una herramienta poderosa en la gestión de incidentes. Por ejemplo, un análisis de causa raíz podría identificar que una configuración incorrecta del *firewall* permitió un acceso no autorizado, lo que llevó a una filtración de datos (Sommestad et al., 2013). Además, los sistemas basados en IA pueden proporcionar recomendaciones

sobre las mejores prácticas para la reparación de incidentes. Utilizando bases de datos de conocimiento y experiencias pasadas, la IA puede sugerir acciones específicas para resolver problemas y mejorar la postura de seguridad. Esto ayuda a los equipos de seguridad a tomar decisiones informadas y a implementar soluciones efectivas. Por ejemplo, después de un ataque de *phishing*, la IA podría recomendar medidas como la capacitación adicional de los empleados y la implementación de autenticación multifactor para reducir el riesgo de futuros ataques (IBM, 2018).

La integración de la IA en la gestión de incidentes también permite una monitorización continua y en tiempo real de los sistemas de seguridad. Esto es crucial para detectar y responder a incidentes rápidamente. Los sistemas de IA pueden analizar flujos de datos en tiempo real y generar alertas instantáneas cuando se detectan comportamientos anómalos. Esto mejora significativamente la capacidad de respuesta a incidentes, permitiendo a los equipos de seguridad actuar antes de que las amenazas puedan causar daños significativos (García-Teodoro et al., 2009). Otro beneficio importante de la IA en la gestión de incidentes es la reducción del estrés y la carga de trabajo de los equipos de seguridad. La automatización de tareas repetitivas y el análisis de datos liberan a los analistas de seguridad para que se concentren en problemas más complejos y estratégicos. Esto no solo mejora la eficiencia operativa, sino que también ayuda a retener talento en el campo de la ciberseguridad, donde la demanda de profesionales capacitados supera la oferta (ISACA, 2019).

La IA también facilita la creación de informes detallados y la documentación de incidentes de seguridad. Los sistemas basados en IA pueden generar informes automáticos que incluyen una descripción del incidente, las acciones tomadas para contener la amenaza y recomendaciones para prevenir futuros incidentes. Estos informes son esenciales para el cumplimiento normativo y para la comunicación con las partes interesadas, como la alta dirección y los auditores (NIST, 2020). Además, la capacidad de la IA para aprender y adaptarse continuamente mejora la eficacia de la gestión de incidentes a lo largo del tiempo. Los sistemas de IA pueden ajustar sus modelos y algoritmos basándose en nuevos datos y experiencias, mejorando su capacidad para detectar y responder a amenazas emergentes. Esto es especialmente importante en un entorno de amenazas en constante evolución, donde los atacantes desarrollan continuamente nuevas técnicas para evadir las defensas de seguridad (Buczak & Guven, 2016). Por último, la IA puede facilitar la colaboración entre diferentes equipos y organizaciones en la gestión de incidentes de seguridad. Los sistemas de IA pueden compartir información y alertas con

otros equipos de seguridad, mejorando la coordinación y la respuesta conjunta a amenazas. Esto es particularmente útil en el contexto de ataques coordinados a gran escala, donde una respuesta rápida y bien coordinada es crucial para mitigar el impacto. La colaboración y el intercambio de información entre organizaciones también ayudan a mejorar la resiliencia global frente a las amenazas cibernéticas (ENISA, 2019).

Integración de IA en sistemas de seguridad

La integración de IA en los sistemas de seguridad implica la incorporación de tecnologías de IA en las infraestructuras de seguridad existentes. Esto puede incluir la implementación de sistemas de detección y respuesta automatizados, así como la mejora de las capacidades de análisis de datos. La integración exitosa de IA requiere una planificación cuidadosa y la alineación con los objetivos de seguridad de la organización (Buczak & Guven, 2016).

Uno de los primeros pasos en la integración de IA es la evaluación de las necesidades de seguridad de la organización. Esto incluye la identificación de áreas donde la IA puede agregar valor, como la detección de amenazas, la gestión de incidentes y la respuesta automatizada. La evaluación también debe considerar la infraestructura tecnológica existente y las capacidades del personal de seguridad (Colwill, 2009). La selección de las herramientas y tecnologías de IA adecuadas es crucial para una integración exitosa. Las organizaciones deben evaluar diferentes soluciones de IA en función de sus capacidades, compatibilidad con la infraestructura existente y facilidad de uso. Esto puede incluir la evaluación de plataformas de aprendizaje automático, herramientas de análisis de *big data* y sistemas de respuesta automatizada (Goodfellow et al., 2016).

La implementación de IA en los sistemas de seguridad también requiere la formación y capacitación del personal de seguridad. Los equipos de seguridad deben estar familiarizados con las nuevas tecnologías y saber cómo utilizarlas de manera efectiva. La formación continua y la actualización de habilidades son esenciales para mantener la eficacia de las soluciones de IA (ISACA, 2019). Por último, la integración de IA debe incluir un enfoque en la gestión del cambio. La introducción de nuevas tecnologías puede generar resistencia entre los empleados y requerir cambios en los procesos operativos. Es importante comunicar los beneficios de la IA y proporcionar apoyo durante la transición. La gestión del cambio efectiva puede facilitar la adopción y maximizar los beneficios de la integración de IA (Kotter, 1996).

Aplicaciones de IA en ciberseguridad militar y defensa nacional

La inteligencia artificial está transformando profundamente el panorama de la ciberseguridad en el ámbito militar y de defensa nacional. Las Fuerzas Armadas y agencias de seguridad han comenzado a integrar algoritmos avanzados para detectar amenazas cibernéticas en tiempo real, analizar patrones de comportamiento en redes complejas y responder de forma automatizada a ataques sofisticados. Esta adopción responde a la creciente necesidad de proteger infraestructuras críticas, sistemas de mando y control, y datos estratégicos frente a actores estatales y no estatales cada vez más organizados y habilitados tecnológicamente.

Uno de los casos más destacados es el uso de IA en programas de defensa cibernética desarrollados por el Departamento de Defensa de los Estados Unidos (DoD), como parte del Joint Artificial Intelligence Center (JAIC). Este centro ha promovido soluciones que combinan aprendizaje automático y *big data* para identificar intrusiones en redes militares clasificadas. Estas soluciones permiten una supervisión continua de sistemas complejos como el Command, Control, Communications, Computers, and Intelligence (C4I), donde la latencia en la respuesta podría tener consecuencias críticas para la seguridad nacional (Cummings, 2017).

A nivel internacional, la OTAN ha implementado mecanismos de cooperación e investigación en IA aplicados a la ciberseguridad a través del Cooperative Cyber Defence Centre of Excellence (CCDCOE). En sus ejercicios anuales *Locked Shields*, se utilizan simulaciones que replican ataques a gran escala contra infraestructuras digitales de defensa. En este contexto, agentes basados en IA son empleados para evaluar escenarios, coordinar defensas y proponer contramedidas automáticas frente a amenazas emergentes. Estas experiencias prácticas permiten validar algoritmos en entornos complejos y estresados operativamente (NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE], 2020).

Otro uso crítico de la IA en contextos militares es la protección de sistemas SCADA (Supervisory Control and Data Acquisition) y redes de defensa industrial. Estas infraestructuras, al ser fundamentales para operaciones logísticas, vigilancia aérea o control de armamento, son blanco frecuente de ciberataques sofisticados. La IA se emplea para monitorizar señales anómalas, prevenir sabotajes cibernéticos y generar respuestas autónomas en tiempo real. Además, el uso de *deep learning* y *reinforcement learning* permite optimizar defensas cibernéticas incluso en situaciones de incertidumbre operacional o ataques de tipo adversarial (Brundage et al., 2018).

Asimismo, se ha observado un creciente interés en el uso de redes generativas adversarias (GAN) para entrenar sistemas de defensa ante ataques desconocidos o de día cero (*zero-day attacks*). En entornos militares, donde el acceso a datos reales de ataques puede ser limitado por motivos de clasificación, las GAN permiten generar escenarios sintéticos que alimentan modelos predictivos de defensa. Estos enfoques han sido particularmente útiles en pruebas realizadas en entornos simulados por agencias como DARPA, que buscan desarrollar capacidades de respuesta anticipada frente a amenazas futuras (Goodfellow et al., 2014).

La adopción de IA en la ciberseguridad militar plantea desafíos importantes en cuanto a ética, gobernanza y transparencia. La toma de decisiones autónoma en contextos bélicos debe ser regulada bajo marcos legales internacionales, como el derecho internacional humanitario y las directrices de uso responsable de tecnologías emergentes. En este sentido, la coordinación entre aliados, la interoperabilidad entre plataformas y la vigilancia institucional serán clave para garantizar que la IA se utilice como una herramienta de protección y no de escalamiento cibernético ofensivo (Floridi et al., 2018).

Mejores prácticas y recomendaciones

Entre las mejores prácticas para la implementación de IA en ciberseguridad se incluyen la realización de pruebas exhaustivas de los sistemas de IA antes de su despliegue, la formación continua de los equipos de seguridad y la colaboración con expertos en IA y ciberseguridad para garantizar una implementación efectiva. La adopción de un enfoque basado en riesgos y la evaluación continua de la eficacia de las soluciones de IA también son esenciales (NIST, 2020).

Una de las mejores prácticas es realizar pruebas exhaustivas de los sistemas de IA antes de su despliegue. Esto incluye la validación de los modelos de IA con datos de prueba y la simulación de diferentes escenarios de amenaza. Las pruebas exhaustivas pueden identificar posibles problemas y asegurar que los sistemas de IA funcionen como se espera en entornos reales. Es crucial que estas pruebas incluyan una variedad de escenarios de ataque para evaluar la capacidad del sistema de IA para detectar y responder a diferentes tipos de amenazas (Goodfellow et al., 2016). La formación continua de los equipos de seguridad es esencial para garantizar que puedan utilizar las soluciones de IA de manera efectiva. La ciberseguridad es un campo en constante evolución, y los equipos deben estar actualizados con las últimas técnicas y tecnologías. La inversión en capacitación y desarrollo profesional puede mejorar la eficacia de las soluciones de IA y fortalecer la

postura de seguridad de la organización. Esto puede incluir cursos de formación, talleres y certificaciones en IA y ciberseguridad (ISACA, 2019). La colaboración con expertos en IA y ciberseguridad es otra práctica recomendada. Las organizaciones pueden beneficiarse de la experiencia y el conocimiento de expertos externos para guiar la implementación de IA. Esto puede incluir la colaboración con proveedores de tecnología, consultores y comunidades de práctica en ciberseguridad. La colaboración también puede facilitar el intercambio de mejores prácticas y lecciones aprendidas, lo que puede mejorar la eficacia de las soluciones de IA (ENISA, 2019).

Adoptar un enfoque basado en riesgos es crucial para la implementación efectiva de IA en ciberseguridad. Esto implica la identificación y priorización de los riesgos de seguridad más críticos y la implementación de soluciones de IA para mitigar esos riesgos. La evaluación continua de la eficacia de las soluciones de IA y la adaptación de las estrategias de seguridad en función de los resultados también son importantes. Este enfoque asegura que los recursos se utilicen de manera eficiente y que las medidas de seguridad se centren en las áreas de mayor impacto (NIST, 2020). La implementación de controles de calidad en el desarrollo y el uso de modelos de IA es también una práctica importante. Esto incluye la revisión periódica y la auditoría de los modelos de IA para asegurar que sigan siendo efectivos y que no hayan desarrollado sesgos o errores con el tiempo. Los controles de calidad también pueden incluir la validación cruzada de los modelos y la comparación de su rendimiento con otros enfoques de ciberseguridad (Chio & Freeman, 2018).

Otra recomendación es la integración de la IA en una arquitectura de seguridad en capas. La IA no debe ser la única línea de defensa, sino parte de una estrategia de seguridad más amplia que incluya otras medidas, como *firewalls*, sistemas de detección de intrusiones y políticas de seguridad sólidas. La combinación de IA con otras tecnologías y prácticas de seguridad puede proporcionar una defensa más robusta y efectiva contra las amenazas cibernéticas (Buczak & Guven, 2016).

Es importante mantener una evaluación continua de la eficacia de las soluciones de IA. Esto incluye el monitoreo de su desempeño y la revisión regular de los resultados para identificar áreas de mejora. La retroalimentación continua y la actualización de los modelos de IA pueden garantizar que sigan siendo efectivos en un entorno de amenazas en constante cambio. La implementación de un proceso de mejora continua puede ayudar a las organizaciones a adaptarse rápidamente a nuevas amenazas y a mejorar continuamente su postura de seguridad (Goodfellow et al., 2016).

Futuro de la IA en la ciberseguridad

Tendencias emergentes

Las tendencias emergentes en la IA y la ciberseguridad incluyen el uso de técnicas de IA más avanzadas, como el aprendizaje por refuerzo y los modelos generativos, así como la integración de IA en plataformas de seguridad unificadas. Estas tendencias prometen mejorar la capacidad de las organizaciones para detectar y responder a amenazas de manera más eficiente y efectiva (Goodfellow et al., 2016). El aprendizaje por refuerzo es una técnica de IA que se está volviendo cada vez más importante en la ciberseguridad. En el aprendizaje por refuerzo, los agentes de IA aprenden a tomar decisiones mediante la interacción con su entorno y la recepción de recompensas o castigos. Esta técnica es útil para desarrollar sistemas de respuesta automatizada que pueden adaptarse y optimizar sus estrategias con el tiempo (Sutton & Barto, 2018).

Los modelos generativos, como las redes generativas adversarias (GAN), también están emergiendo como una herramienta poderosa en la ciberseguridad. Las GAN pueden generar datos sintéticos que son indistinguibles de los datos reales, lo que es útil para entrenar y evaluar sistemas de IA. Además, las GAN pueden utilizarse para simular ataques y desarrollar defensas más robustas (Goodfellow et al., 2014). La integración de IA en plataformas de seguridad unificadas es otra tendencia importante. Estas plataformas combinan múltiples capacidades de seguridad, como la detección de amenazas, la gestión de incidentes y la respuesta automatizada, en un solo sistema. La IA puede mejorar la interoperabilidad y la eficiencia de estas plataformas, proporcionando una visión integral y coordinada de la seguridad (Gartner, 2020).

Además, la IA está facilitando la personalización y la adaptación en la ciberseguridad. Los sistemas basados en IA pueden ajustar sus estrategias en función de las características específicas de la organización y las amenazas a las que se enfrenta. Esto permite una ciberseguridad más efectiva y adaptada a las necesidades particulares de cada organización (Huang & Nicol, 2010).

Aprendizaje por refuerzo en ciberseguridad

Introducción al aprendizaje por refuerzo

El aprendizaje por refuerzo (RL) es una técnica de IA donde los agentes aprenden a tomar decisiones mediante la interacción con su entorno, recibiendo recompensas

o castigos en función de sus acciones. En ciberseguridad, esta técnica se aplica para desarrollar sistemas que pueden adaptarse dinámicamente a nuevas amenazas y optimizar sus estrategias de defensa con el tiempo (Sutton & Barto, 2018).

Aplicaciones en la detección de intrusiones.

El RL se utiliza para mejorar la detección de intrusiones. Los agentes de RL pueden ser entrenados para identificar patrones de tráfico de red que indican ataques. A medida que interactúan con el entorno, aprenden a reconocer comportamientos maliciosos y a tomar medidas para mitigarlos, como ajustar las reglas del *firewall* o aislar segmentos de red comprometidos (Buczak & Guven, 2016).

Optimización de políticas de seguridad

Una de las principales ventajas del RL es su capacidad para optimizar políticas de seguridad. Los agentes pueden evaluar diferentes configuraciones y estrategias de seguridad, seleccionando las más efectivas en función de las recompensas recibidas. Esto permite a las organizaciones mantener políticas de seguridad dinámicas que se adaptan a las amenazas en evolución (Sutton & Barto, 2018).

Simulación de ataques y respuesta

El RL también se utiliza para simular ataques y respuestas en entornos controlados. Los agentes pueden aprender a llevar a cabo ataques complejos y a desarrollar contramedidas eficaces. Esta simulación es útil para evaluar la resiliencia de los sistemas de seguridad y para entrenar a los equipos de respuesta a incidentes (Goodfellow et al., 2016).

Desafíos y limitaciones

A pesar de sus ventajas, el RL presenta desafíos. Requiere grandes cantidades de datos y recursos computacionales para entrenar los agentes. Además, los modelos de RL pueden ser difíciles de interpretar, lo que complica la comprensión de las decisiones tomadas por los agentes. La implementación de RL en entornos reales también puede ser compleja debido a la necesidad de ajustar continuamente las políticas en respuesta a nuevas amenazas (Buczak & Guven, 2016).

Futuro del RL en ciberseguridad

Se espera que el uso de RL en ciberseguridad continúe creciendo. La capacidad de los agentes de RL para adaptarse y optimizar políticas en tiempo real es una herramienta poderosa para enfrentar amenazas cibernéticas cada vez más sofisticadas. Con el avance de la tecnología y la disponibilidad de más datos, el RL

se convertirá en una parte integral de las estrategias de ciberseguridad (Sutton & Barto, 2018).

Redes generativas adversarias (GAN) en ciberseguridad

Introducción a las GAN

Las redes generativas adversarias (GAN) son una técnica avanzada de aprendizaje profundo que involucra dos redes neuronales que compiten entre sí: una generadora y una discriminadora. La red generadora crea datos sintéticos, mientras que la red discriminadora evalúa su autenticidad. Esta competencia mejora continuamente la calidad de los datos generados (Goodfellow et al., 2014).

Generación de datos sintéticos

En ciberseguridad, las GAN se emplean para generar datos sintéticos que pueden ser utilizados para entrenar y evaluar sistemas de detección de amenazas. Estos datos incluyen ejemplos de ataques y comportamientos maliciosos que son difíciles de obtener en cantidades suficientes en el mundo real. Las GAN pueden crear conjuntos de datos balanceados y diversos, mejorando la capacidad de los sistemas de detección para identificar amenazas (Goodfellow et al., 2014).

Detección de anomalías y fraudes.

Las GAN también se aplican en la detección de anomalías y fraudes. La red generadora puede crear ejemplos de comportamientos normales, mientras que la red discriminadora aprende a identificar desviaciones de estos comportamientos. Esto es útil para detectar fraudes financieros y otras actividades maliciosas que se desvían de los patrones normales (Chio & Freeman, 2018).

Simulación de ataques avanzados.

Las GAN pueden simular ataques cibernéticos avanzados, proporcionando a los equipos de seguridad la oportunidad de probar y mejorar sus defensas contra amenazas sofisticadas. Estas simulaciones permiten a las organizaciones prepararse para escenarios de ataque que de otro modo serían difíciles de replicar en un entorno de prueba (Goodfellow et al., 2014).

Mejoras en el desarrollo de *software* seguro

Las GAN se utilizan para identificar vulnerabilidades en el *software* y sugerir mejoras. La red generadora puede crear código que intenta explotar vulnerabilidades, mientras que la red discriminadora evalúa la seguridad del código. Este proceso

puede ayudar a los desarrolladores a identificar y corregir fallas de seguridad antes de que el *software* se implemente (Goodfellow et al., 2014).

Desafíos y futuro de las GAN

A pesar de sus beneficios, las GAN presentan desafíos, como la necesidad de grandes cantidades de datos y recursos computacionales. También pueden ser vulnerables a ataques adversariales. Sin embargo, el potencial de las GAN para mejorar la ciberseguridad es significativo, y se espera que su uso continúe expandiéndose a medida que se desarrollen nuevas técnicas y se mejoren los modelos existentes (Goodfellow et al., 2014).

Integración de IA en plataformas de seguridad unificadas

Concepto de plataformas de seguridad unificadas

Las plataformas de seguridad unificadas integran múltiples herramientas y tecnologías de ciberseguridad en una única solución cohesiva. Esto incluye sistemas de detección de intrusiones, *firewalls*, gestión de información y eventos de seguridad (SIEM), y más. La IA mejora la interoperabilidad y la eficiencia de estas plataformas, proporcionando una visión integral de la seguridad (Gartner, 2020).

Detección y respuesta en tiempo real

La integración de IA en plataformas de seguridad unificadas permite la detección y respuesta en tiempo real de amenazas cibernéticas. Los algoritmos de IA pueden analizar datos de múltiples fuentes y correlacionar eventos para identificar patrones de ataque. Esto facilita una respuesta rápida y coordinada a incidentes de seguridad, mejorando la protección general (Chuvakin et al., 2013).

Automatización de tareas de seguridad

La IA automatiza tareas repetitivas y de bajo nivel en la gestión de seguridad, como la clasificación de alertas, la actualización de reglas de *firewall* y la implementación de parches de seguridad. Esto libera a los analistas de seguridad para que se concentren en problemas más complejos y estratégicos, mejorando la eficiencia operativa (NIST, 2020).

Análisis predictivo y proactivo

Las plataformas de seguridad unificadas con IA incorporada pueden realizar análisis predictivos para anticipar amenazas y vulnerabilidades antes de que ocurran.

Esto permite a las organizaciones implementar medidas preventivas y fortalecer sus defensas de manera proactiva. Los modelos predictivos basados en IA analizan patrones históricos y comportamientos para identificar posibles ataques futuros (Hastie et al., 2009).

Mejora de la colaboración y la comunicación.

La integración de IA en plataformas de seguridad unificadas mejora la colaboración y la comunicación entre diferentes equipos de seguridad. Los sistemas de IA pueden compartir información y alertas en tiempo real, facilitando una respuesta coordinada a amenazas cibernéticas. Esto es particularmente útil en organizaciones grandes y complejas donde la comunicación eficiente es crucial (ENISA, 2019).

Desafíos y futuro de las plataformas unificadas con IA

Aunque las plataformas de seguridad unificadas con IA ofrecen numerosos beneficios, también presentan desafíos, como la complejidad de la integración y la necesidad de una gestión continua de los modelos de IA. Además, es crucial garantizar la seguridad y privacidad de los datos utilizados por los sistemas de IA. A pesar de estos desafíos, el futuro de las plataformas unificadas con IA es prometedor, con el potencial de transformar la ciberseguridad y mejorar significativamente la protección contra amenazas (Gartner, 2020).

Personalización y adaptación en ciberseguridad

Introducción a la personalización en ciberseguridad

La personalización en ciberseguridad implica adaptar las estrategias y herramientas de seguridad para satisfacer las necesidades específicas de una organización. La IA juega un papel crucial en esta personalización, permitiendo el desarrollo de soluciones de seguridad que se ajustan a las características y requisitos únicos de cada entorno (Huang & Nicol, 2010).

Análisis de comportamiento de usuarios.

La IA permite el análisis detallado del comportamiento de los usuarios, identificando patrones normales y detectando anomalías que pueden indicar actividades maliciosas. Este enfoque personalizado permite la implementación de medidas de seguridad adaptadas a los comportamientos individuales de los usuarios, mejorando la eficacia de la detección de amenazas (Seymour & Tully, 2016).

Adaptación a amenazas dinámicas

Las soluciones de seguridad basadas en IA pueden adaptarse dinámicamente a nuevas amenazas. Los modelos de IA aprenden continuamente de los datos y ajustan sus estrategias en función de las amenazas emergentes. Esta capacidad de adaptación es crucial en un entorno de ciberseguridad en constante evolución, donde las técnicas de ataque cambian rápidamente (Goodfellow et al., 2016).

Segmentación y protección de activos críticos

La personalización también incluye la segmentación y protección de activos críticos. La IA puede identificar los activos más valiosos y vulnerables dentro de una organización y desarrollar medidas de seguridad específicas para protegerlos. Esto incluye la implementación de controles de acceso granulares y la monitorización continua de estos activos (Columbus, 2020).

Automatización de respuestas personalizadas

La IA permite la automatización de respuestas personalizadas a incidentes de seguridad. Los sistemas pueden analizar el contexto de un incidente y tomar decisiones adaptadas a la situación específica. Esto incluye la contención de amenazas y la notificación a los equipos de seguridad con información relevante para una respuesta eficaz (García-Teodoro et al., 2009).

Desafíos y futuro de la personalización en ciberseguridad

La implementación de soluciones de seguridad personalizadas presenta desafíos, como la necesidad de datos de alta calidad y la complejidad de desarrollar modelos adaptativos. Sin embargo, el potencial de la personalización para mejorar la ciberseguridad es significativo. A medida que las tecnologías de IA avanzan, la capacidad de desarrollar soluciones de seguridad altamente personalizadas y adaptativas seguirá mejorando, ofreciendo una protección más robusta y efectiva (Huang & Nicol, 2010).

Potenciales desarrollos y avances

Se espera que los avances en la IA mejoren la capacidad de los sistemas de ciberseguridad para identificar y responder a amenazas desconocidas, así como para predecir y prevenir ataques con mayor precisión. Además, la IA podría facilitar la automatización completa de ciertos aspectos de la ciberseguridad, liberando a los analistas humanos para que se concentren en tareas más estratégicas (Goodfellow et al., 2016).

Un área de desarrollo potencial es la mejora de la detección de amenazas avanzadas. Los algoritmos de IA están evolucionando para identificar amenazas sofisticadas que utilizan técnicas de evasión para evitar la detección. Esto incluye la capacidad de detectar amenazas persistentes avanzadas (APT) y ataques dirigidos que son difíciles de identificar con métodos tradicionales (Buczak & Guven, 2016).

Otro avance importante es la capacidad de la IA para predecir ataques antes de que ocurran. Los modelos predictivos pueden analizar patrones históricos y comportamientos para anticipar amenazas futuras. Esto permite a las organizaciones tomar medidas preventivas y fortalecer sus defensas antes de que se produzca un ataque. La predicción precisa de amenazas es una herramienta poderosa para la ciberseguridad proactiva (Hastie et al., 2009).

La automatización completa de ciertos aspectos de la ciberseguridad es otra área de desarrollo prometedora. Los sistemas de respuesta automatizada pueden gestionar y resolver incidentes de seguridad sin intervención humana, mejorando la velocidad y eficacia de la respuesta. Esto libera a los analistas humanos para que se concentren en tareas más estratégicas, como la planificación y la evaluación de riesgos (García-Teodoro et al., 2009). Además, los avances en el procesamiento del lenguaje natural (NLP) están mejorando la capacidad de los sistemas de IA para analizar y comprender datos de texto. Esto es útil para tareas como la detección de *phishing* y la clasificación de correos electrónicos. Los sistemas de NLP pueden identificar patrones de lenguaje que son indicativos de ataques y alertar a los equipos de seguridad (Chio & Freeman, 2018).

En el futuro, la IA jugará un papel cada vez más importante en la ciberseguridad, no solo como herramienta de defensa, sino también como elemento clave en la creación de sistemas de seguridad más proactivos y resilientes. La colaboración entre humanos y máquinas será esencial para abordar las amenazas de ciberseguridad de manera efectiva (Goodfellow et al., 2016). La IA permitirá la creación de sistemas de seguridad proactivos que puedan anticipar y mitigar amenazas antes de que causen daño. Esto incluye la capacidad de identificar vulnerabilidades y aplicar parches de seguridad de manera automatizada. La proactividad en la ciberseguridad es crucial para mantenerse un paso adelante de los atacantes (Huang & Nicol, 2010).

La resiliencia es otro aspecto clave donde la IA jugará un papel importante. Los sistemas de IA pueden aprender y adaptarse a nuevas amenazas, mejorando continuamente su capacidad de defensa. La resiliencia en ciberseguridad significa la capacidad de recuperarse rápidamente de los incidentes y mantener la

continuidad operativa (Von Solms & Van Niekerk, 2013). La colaboración entre humanos y máquinas será esencial para aprovechar al máximo el potencial de la IA en ciberseguridad. Los analistas humanos pueden proporcionar el juicio y la intuición necesarios para interpretar los resultados de los sistemas de IA, mientras que la IA puede manejar tareas repetitivas y análisis de datos a gran escala. Esta colaboración puede mejorar la eficacia general de la ciberseguridad (Columbus, 2020).

Entonces la IA también facilitará la creación de ecosistemas de seguridad más integrados y coordinados. Los sistemas basados en IA pueden compartir información y colaborar en tiempo real, mejorando la capacidad de las organizaciones para responder a amenazas de manera coordinada. La integración y la cooperación son esenciales para enfrentar las amenazas cibernéticas en un entorno cada vez más interconectado (ENISA, 2019).

Consideraciones éticas y normativas en el uso de la IA en ciberseguridad

El uso de inteligencia artificial en ciberseguridad plantea importantes desafíos éticos y normativos que deben abordarse con responsabilidad. A medida que los sistemas basados en IA asumen funciones críticas en la detección, análisis y respuesta a amenazas cibernéticas, surgen preocupaciones sobre la transparencia de los algoritmos, la equidad en las decisiones automatizadas y la posibilidad de errores que afecten negativamente a individuos u organizaciones. Uno de los principales riesgos es la generación de falsos positivos o negativos, que pueden llevar a medidas de seguridad inapropiadas, incluyendo bloqueos de usuarios legítimos o la omisión de amenazas reales. Por lo tanto, garantizar la confiabilidad, explicabilidad y auditabilidad de los sistemas de IA es fundamental para una implementación ética.

Además, existe una preocupación creciente respecto del uso malicioso de la IA en entornos cibernéticos. Así como la IA puede ser utilizada para defender redes y sistemas, también puede ser empleada por actores malintencionados para automatizar ataques, desarrollar *malware* adaptativo o ejecutar campañas de desinformación con alta precisión. Este fenómeno, conocido como *dual use*, exige que las instituciones desarrollen marcos de gobernanza que minimicen el uso ofensivo indebido de estas tecnologías. Iniciativas, como el informe *The Malicious Use of Artificial Intelligence*, advierten sobre la necesidad urgente de políticas internacionales que regulen tanto la creación como el despliegue de IA en entornos críticos (Brundage et al., 2018).

Desde el punto de vista normativo, distintas regiones del mundo están avanzando en la construcción de marcos regulatorios orientados a la IA segura y

confiable. En Europa, el *Artificial Intelligence Act* propone clasificar los sistemas de IA según su nivel de riesgo (bajo, medio, alto e inaceptable), con obligaciones diferenciadas en función de su aplicación. En el ámbito de la ciberseguridad, esto incluye requisitos estrictos en torno a la protección de datos personales, la trazabilidad de decisiones automatizadas y la supervisión humana en sistemas de alto riesgo. Asimismo, el *Reglamento General de Protección de Datos (GDPR)* establece limitaciones al procesamiento automatizado que afecte significativamente los derechos de las personas, reforzando el principio de control humano significativo sobre los sistemas automatizados.

Otra dimensión clave en este debate es la ética del diseño algorítmico. La IA debe desarrollarse siguiendo principios como la justicia, la no discriminación, la responsabilidad, y el respeto por los derechos fundamentales. Esto implica garantizar que los modelos no perpetúen sesgos históricos ni tomen decisiones que afecten de forma desproporcionada a ciertos grupos. En ciberseguridad, esto se traduce en la necesidad de evitar la vigilancia masiva sin control judicial, la discriminación algorítmica en políticas de acceso o monitoreo, y la manipulación de información por parte de sistemas autónomos. La ética algorítmica no solo es un requisito moral, sino una condición técnica para construir confianza en el uso de IA.

Con lo que la gobernanza de la IA en ciberseguridad requiere una acción coordinada entre Gobiernos, sector privado, academia y sociedad civil. Las políticas deben ser multidisciplinarias y adaptables, capaces de responder a un entorno tecnológico en constante evolución. Asimismo, es fundamental promover la educación ética en los profesionales del sector, así como la participación de expertos en derecho, filosofía, seguridad y tecnología en los procesos de diseño, evaluación y auditoría de soluciones basadas en IA. La inclusión de estas consideraciones garantizará que la inteligencia artificial no solo sea efectiva desde el punto de vista técnico, sino también legítima, justa y segura desde una perspectiva social y jurídica.

Conclusiones

Este capítulo ha explorado la intersección crítica entre la inteligencia artificial (IA), la transformación digital y la ciberseguridad, identificando no solo los beneficios técnicos y operativos de la IA en la detección, análisis y respuesta ante amenazas, sino también sus limitaciones, riesgos emergentes y desafíos normativos. La implementación de sistemas basados en IA mejora significativamente la velocidad y

precisión de las operaciones de ciberseguridad, pero requiere una infraestructura robusta, datos de calidad y supervisión humana responsable.

Desde una perspectiva institucional, la adopción de IA en ciberseguridad exige una reconfiguración de las capacidades organizativas, tanto en el sector público como privado. Las entidades encargadas de proteger infraestructuras críticas deben integrar doctrinas de ciberdefensa que reconozcan el papel estratégico de la automatización, el análisis predictivo y la respuesta autónoma. Esto implica no solo la inversión en tecnología, sino también en la formación de talento humano con competencias interdisciplinarias que incluyan análisis de datos, ingeniería de seguridad, ética algorítmica y regulación tecnológica.

En el ámbito doctrinal, las organizaciones de seguridad y defensa deben actualizar sus marcos de operación para incorporar modelos de colaboración híbrida entre humanos y máquinas, definiendo claramente los límites del control automatizado en escenarios críticos. La IA no debe sustituir el juicio estratégico, sino potenciarlo. Las doctrinas militares, de inteligencia y de gestión de crisis deben incluir protocolos para la validación, supervisión y auditoría de decisiones automatizadas, especialmente en contextos donde el margen de error es inaceptable.

Asimismo, la cooperación internacional se vuelve indispensable. La naturaleza transnacional de las amenazas cibernéticas y el uso ofensivo de IA por parte de actores hostiles hacen necesario establecer mecanismos de interoperabilidad entre aliados, así como marcos normativos globales que regulen el desarrollo, uso y limitación de tecnologías autónomas en el ciberespacio. Organismos como la OTAN, la ONU y el G7 deben liderar la creación de acuerdos vinculantes que fomenten el uso ético y seguro de la IA en seguridad digital.

A futuro, la IA tendrá un rol creciente en la creación de sistemas de ciberseguridad resilientes, proactivos y adaptativos. Sin embargo, este avance tecnológico debe ir acompañado de una madurez institucional que asegure el respeto por los derechos fundamentales, la transparencia en la toma de decisiones y la rendición de cuentas. Solo así será posible aprovechar el potencial de la IA para fortalecer la seguridad digital, sin comprometer los principios democráticos, la soberanía tecnológica y la confianza ciudadana.

Referencias

- Agea, L. A. (2023). Todo sobre las auditorías de ciberseguridad y su importancia. *Ciberseguridad Hoy*. <https://tinyurl.com/2yp9c943>
- Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, 68, 160-196. <https://doi.org/10.1016/j.cose.2017.04.006>
- Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems*. John Wiley & Sons.
- Baker, W. H. (2020). *The complete guide to cybersecurity risks and controls*. CRC Press.
- Bandyopadhyay, T., Mookerjee, V., & Rao, R. (2009). Why IT managers don't go for security products. *Communications of the ACM*, 52(11), 68-73. <https://doi.org/10.1145/1592761.159278>
- Barocas, S., Hardt, M., & Narayanan, A. (2019). *Fairness and machine learning*. fairmlbook.org
- Binns, R. (2018). Fairness in machine learning: Lessons from political philosophy. En *Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency* (pp. 149-159).
- Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Ó hÉigeartaigh, S., Beard, S. J., Belfield, H., Farquhar, S., ... & Amodei, D. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. arXiv. <https://arxiv.org/abs/1802.07228>
- Brynjolfsson, E., & McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. W.W. Norton & Company.
- Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153-1176. <https://doi.org/10.1109/COMST.2015.2494502>
- Cavoukian, A. (2010). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario, Canada.
- Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), 1-58. <https://doi.org/10.1145/1541880.1541882>
- Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. *MIS Quarterly*, 36(4), 1165-1188. <https://doi.org/10.2307/41703503>
- Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. *Mobile Networks and Applications*, 19(2), 171-209. <https://doi.org/10.1007/s11036-013-0489-0>
- Chio, C., & Freeman, D. (2018). *Machine learning and security: Protecting systems with data and algorithms*. O'Reilly Media.
- Chuvakin, A., Schmidt, K., & Phillips, C. (2013). *Logging and log management: The authoritative guide to understanding the concepts surrounding logging and log management*. Syngress.
- Columbus, L. (2020). *Cybersecurity in the age of digital transformation*. McGraw-Hill Education.
- Colwill, C. (2009). Human factors in information security: The insider threat – who can you trust these days? *Information Security Technical Report*, 14(4), 186-196. <https://doi.org/10.1016/j.istr.2010.04.004>
- Comisión Europea. (2020). *Libro blanco sobre la inteligencia artificial: un enfoque europeo hacia la excelencia y la confianza*. <https://tinyurl.com/ykw9aa73>
- Comisión Europea. (2021). *Propuesta de reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión*. <https://tinyurl.com/yhdbwtyr>

- Cummings, M. L. (2017). *Artificial intelligence and the future of warfare* [Research Paper]. The Royal Institute of International Affairs. <https://tinyurl.com/yxshha83>
- Egele, M., Scholte, T., Kirda, E., & Kruegel, C. (2012). A survey on automated dynamic malware-analysis techniques and tools. *ACM Computing Surveys*, 44(2), 1-42. <https://doi.org/10.1145/2089125.2089126>
- El desafío de la transformación digital*. (2023). El-Cafe.es. <https://tinyurl.com/238kcjcl>
- European Union Agency for Cybersecurity (ENISA). (2019). *ENISA threat landscape report*.
- Fitzgerald, M., Kruschwitz, N., Bonnet, D., & Welch, M. (2014). Embracing digital technology: A new strategic imperative. *MIT Sloan Management Review*, 55(2), 1. <https://tinyurl.com/5hc9kcyj>
- Foridi, L., Cows, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P. & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, 28(4), 689-707. <https://doi.org/10.1007/s11023-018-9482-5>
- García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, 28(1-2), 18-28. <https://doi.org/10.1016/j.cose.2008.08.003>
- Gartner. (2020). *Magic quadrant for security information and event management*. Gartner.
- Gellman, R. (2019). *Fair information practices: A basic history*. SSRN. <https://tinyurl.com/yavccbnr>
- Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. The MIT Press.
- Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. En Z. Ghahramani, M. Welling, C. Cortes, N. Lawrence, & K. Q. Weinberger (Eds.), *Advances in neural information processing systems* (Vol. 27, pp. 2672–2680). Curran Associates.
- Gordon, L. A., & Loeb, M. P. (2022). *Managing cybersecurity resources: A cost-benefit analysis*. McGraw-Hill Education. <https://tinyurl.com/22bctvnj>
- Hastie, T., Tibshirani, R., & Friedman, J. (2009). *The elements of statistical learning: Data mining, inference, and prediction*. Springer.
- Hentea, M., Dhillon, H. S., & Dhillon, S. (2008). Towards a science of cybersecurity: A perspective. En *Proceedings of the 5th Annual Conference on Information Security Curriculum Development* (pp. 1-7).
- HIPAA. (1996). *Health Insurance Portability and Accountability Act*. Public Law 104-191.
- Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation*, 9(8), 1735-1780. <https://doi.org/10.1162/neco.1997.9.8.1735>
- Huang, C. D., & Nicol, D. M. (2010). A formal-semantics-based calculus of trust. *IEEE Internet Computing*, 14(5), 38-46. <https://doi.org/10.1109/MIC.2010.83>
- IBM Security. (2018). *IBM X-Force Threat Intelligence Index 2018*. IBM.
- ISACA. (2019). *State of Cybersecurity 2019*.
- Kim, J., Lee, J., & Kim, J. (2014). Towards a deep learning model for cyber attack detection and classification. En *Proceedings of the 2014 IEEE Conference on Big Data* (pp. 1036-1042). <https://tinyurl.com/ymap54t8>

- Kotter, J. P. (1996). *Leading change*. Harvard Business Review Press.
- Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). Imagenet classification with deep convolutional neural networks. *Advances in Neural Information Processing Systems*, 25, 1097-1105. <https://tinyurl.com/389fdb26>
- LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436-444. <https://doi.org/10.1038/nature14539>
- LeMay, E., Ford, M., Keefe, T., & Sanders, W. H. (2011). Model-based security metrics using ADversary View Security Evaluation (ADVISE). En *Proceedings of the 8th ACM International Conference on Quantitative Evaluation of Systems* (pp. 191-200).
- Maloof, M. A. (2006). *Machine learning and data mining for computer security: Methods and applications*. Springer Science & Business Media.
- Monaco, J. V., & Tappert, C. C. (2016). Behavioral biometrics for continuous authentication in online exams. *Journal of Educational Computing Research*, 54(3), 425-447.
- National Institute of Standards and Technology (NIST). (2020). *Framework for improving critical infrastructure cybersecurity*.
- NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2020). *Locked Shields: The world's largest and most complex live-fire cyber defence exercise*.
- Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, 50(3), 559-569.
- Office of the Comptroller of the Currency (OCC). (2020). *Cybersecurity risk management and resilience*.
- Pan, S. J., & Yang, Q. (2010). A survey on transfer learning. *IEEE Transactions on Knowledge and Data Engineering*, 22(10), 1345-1359. <https://doi.org/10.1109/TKDE.2009.191>
- Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks*, 51(12), 3448-3470. <https://doi.org/10.1016/j.comnet.2007.02.001>
- Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, 13(1), 10-21.
- Rittinghouse, J. W., & Ransome, J. F. (2017). *Cloud computing: Implementation, management, and security*. CRC Press.
- Russell, S., & Norvig, P. (2016). *Artificial intelligence: A modern approach*. Pearson Education Limited.
- Sakurada, M., & Yairi, T. (2014). Anomaly detection using autoencoders with nonlinear dimensionality reduction. En *Proceedings of the 2nd Workshop on Machine Learning for Sensory Data Analysis (MLSDA 2014)* (pp. 4-11).
- Saxe, J., & Berlin, K. (2015). Deep neural network based malware detection using two dimensional binary program features. En *Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security* (pp. 11-20).
- Schmidhuber, J. (2015). Deep learning in neural networks: An overview. *Neural Networks*, 61, 85-117. <https://doi.org/10.1016/j.neunet.2014.09.003>

- Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. W.W. Norton & Company.
- Schultz, M. G., Eskin, E., Zadok, E., & Stolfo, S. J. (2001). Data mining methods for detection of new malicious executables. *Proceedings of the 2001 IEEE Symposium on Security and Privacy*, 38-49.
- Seymour, J., & Tully, P. (2016). Weaponizing data science for social engineering: Automated E2E spear phishing on Twitter. *Black Hat USA*.
- Sharma, R., & Chen, L. (2019). A survey on phishing attacks and countermeasures. En *Proceedings of the 2019 11th International Conference on Machine Learning and Computing* (pp. 1-5).
- Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146-164. <https://doi.org/10.1016/j.comnet.2014.11.008>
- Solove, D. J., & Schwartz, P. M. (2021). *Information privacy law*. Wolters Kluwer Law & Business.
- Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. En *2010 IEEE Symposium on Security and Privacy* (pp. 305-316).
- Sommestad, T., Holm, H., & Sandström, K. (2013). The impact of password policies on the usability and security of passwords. *Journal of Information Security and Applications*, 18(4), 144-157.
- Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, 92, 178-199.
- Stallings, W. (2021). *Effective cybersecurity: A guide to using best practices and standards*. Pearson Education.
- Sutton, R. S., & Barto, A. G. (2018). *Reinforcement learning: An introduction*. The MIT Press.
- Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, 72, 212-233. <https://doi.org/10.1016/j.cose.2017.09.001>
- Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *Journal of Strategic Information Systems*, 28(2), 118-144. <https://doi.org/10.1016/j.jsis.2019.01.003>
- Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer International Publishing.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102.
- Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, 26(1), 23-30.
- Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security*. Cengage Learning.
- Ye, Y., Li, T., Adjeroh, D., & Iyengar, S. S. (2017). A survey on malware detection using data mining techniques. *ACM Computing Surveys*, 50(3), 1-40.
- Zadeh, L. A. (1996). Fuzzy logic = computing with words. *IEEE Transactions on Fuzzy Systems*, 4(2), 103-111.
- Zheng, Y., Zhang, Q., Yu, L., Liu, T., Gu, T., & Zhang, W. (2018). Fraud detection with deep learning. En *2018 IEEE International Conference on Big Data (Big Data)* (pp. 3991-3997).

Capítulo 4

Articulación de la ciberseguridad y la ciberdefensa en la planeación estratégica de las organizaciones^{*}

DOI: <https://doi.org/10.25062/9786287818002.04>

Lucas Adolfo Giraldo Ríos

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El capítulo aborda la integración estratégica de la ciberseguridad y la ciberdefensa como pilares esenciales para la protección de los activos digitales en un entorno empresarial digitalizado y amenazado. Destaca cómo han evolucionado las ciberamenazas y subraya la necesidad de adoptar medidas proactivas y reactivas para salvaguardar la confidencialidad, la integridad y la disponibilidad de la información. Se hace hincapié en la importancia de incorporar la ciberseguridad a la planificación estratégica, establecer políticas, asignar recursos y fomentar una cultura organizativa orientada a la seguridad. Además, el texto destaca el papel complementario de la ciberdefensa, que no solo responde a los ataques, sino que refuerza la resiliencia de las organizaciones, incorporando tecnologías avanzadas, formación continua y colaboración interinstitucional. Se concluye que la sinergia entre prevención, respuesta eficaz y resiliencia es crucial para hacer frente a las complejas ciberamenazas actuales porque garantiza la continuidad operativa y una ventaja competitiva sostenible.

Palabras clave: amenazas cibernéticas; ciberdefensa; ciberseguridad; confidencialidad; resiliencia organizacional; planeación estratégica.

^{*} Capítulo de libro resultado del proyecto de investigación "Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales" del grupo de investigación "Ciberespacio Tecnología e Innovación", de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado C por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) y registrado con el código COL0181179. Los puntos de vista y los resultados de este capítulo pertenecen al autor y no reflejan necesariamente los de las instituciones participantes.

Lucas Adolfo Giraldo Ríos

Candidato a doctor en Ingeniería, Industria y Organizaciones, Universidad Nacional de Colombia. Magíster en Administración de Empresas de Base Tecnológica, Universidad Antonio de Nebrija, España. Magíster en Innovación, Universidad EAN, Colombia. Especialista en Gestión Financiera Empresarial, Universidad de Medellín, Colombia. Administrador de Empresas, Universidad de Antioquia, Colombia.

<https://orcid.org/0000-0002-9947-7882> - Contacto: lucas.giraldo@esdeg.edu.co

Citación APA: Giraldo Ríos, L. A. (2025). Articulación de la ciberseguridad y la ciberdefensa en la planeación estratégica de las organizaciones. En M. E. Realpe Díaz & G. A. Gómez Rodríguez (Eds.), *Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales* (pp. 119-156). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818002.04>

CIBERSEGURIDAD EN LA FRONTERA DIGITAL: DESAFÍOS Y OPORTUNIDADES EN LOS NUEVOS ECOSISTEMAS TECNOLÓGICOS EMPRESARIALES

ISBN impreso: 978-628-7602-99-1

ISBN digital: 978-628-7818-00-2

DOI: <https://doi.org/10.25062/9786287818002>

Colección Ciberseguridad y Ciberdefensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2025



Introducción

En la última década, el aumento exponencial de las amenazas cibernéticas ha puesto en primer plano la importancia de la ciberseguridad y la ciberdefensa en el ámbito empresarial. Las organizaciones ya no solo se enfrentan a problemas tradicionales de seguridad física, sino que deben adoptar un enfoque integral que aborde también la protección de sus activos digitales. Este enfoque es esencial, ya que un ciberataque puede comprometer no solo la información y los sistemas críticos de una empresa, sino también su reputación y su capacidad para operar de manera continua (Ramírez, 2024). Ante este panorama, las estrategias de ciberseguridad y ciberdefensa se han convertido en herramientas indispensables para garantizar la estabilidad y la protección de las organizaciones en el entorno digital.

La ciberseguridad, en su esencia, se enfoca en prevenir los posibles ataques mediante la implementación de medidas y controles que protejan los sistemas y la información. Estas medidas incluyen la protección de la confidencialidad, la integridad y la disponibilidad de la información, que son los pilares fundamentales de cualquier estrategia de seguridad. Sin embargo, con el aumento de la sofisticación de los ataques cibernéticos, la ciberdefensa ha emergido como un complemento esencial. La ciberdefensa no solo responde a los ataques una vez que han ocurrido, sino que también se encarga de mitigar sus efectos y garantizar la recuperación rápida de las operaciones (Rincón-Gallón, 2022).

En este contexto, la colaboración interna dentro de las organizaciones y la cooperación externa con entidades gubernamentales y organismos internacionales son elementos cruciales para una ciberdefensa eficaz. Las empresas deben trabajar de la mano con el sector público y otros actores clave para intercambiar información sobre amenazas emergentes y aprender de las mejores prácticas en

el campo de la seguridad cibernética. La falta de una estrategia de ciberdefensa coordinada y global puede dejar a las organizaciones vulnerables a ataques devastadores que comprometan no solo sus datos, sino también su capacidad operativa (Guzmán-Pacheco, 2022).

A medida que las organizaciones dependen cada vez más de la tecnología para sus operaciones diarias, la integración de la ciberseguridad y la ciberdefensa en la planeación estratégica se vuelve más importante que nunca. La protección de los activos digitales ya no puede ser vista como una cuestión técnica aislada, sino como un componente clave de la estrategia empresarial general. En este sentido, aquellas organizaciones que logren implementar medidas proactivas y reactivas de ciberdefensa estarán mejor posicionadas para enfrentar los desafíos del entorno cibernético actual y para garantizar la continuidad de sus operaciones en un mundo cada vez más digital (Valderrama, 2024).

Importancia de la ciberseguridad y la ciberdefensa

La ciberseguridad y la ciberdefensa se han convertido en elementos fundamentales para la protección de los activos digitales de las organizaciones debido al crecimiento exponencial de las amenazas cibernéticas en la última década (Ramírez, 2024). Hoy en día, las empresas enfrentan riesgos que van más allá de los problemas tradicionales de seguridad física, lo cual las obliga a adoptar un enfoque proactivo y preventivo frente a posibles ataques. Además, el enfoque estratégico que integra estas disciplinas resulta clave para la continuidad operativa y la protección de los datos tanto propios como de los clientes.

Confidencialidad de la información

La confidencialidad de la información se ha posicionado como uno de los pilares fundamentales dentro de la ciberseguridad, ya que los datos representan activos de gran valor para las organizaciones. En la era digital, la mayor parte de las operaciones de las empresas depende de la recolección, procesamiento y almacenamiento de información sensible. Esta puede abarcar desde datos financieros hasta información personal de los clientes y otros detalles estratégicos relacionados con la operación diaria de la organización (Rincón-Gallón, 2022).

Relevancia de la confidencialidad

La protección de la confidencialidad de la información no solo es esencial para evitar filtraciones, sino que también asegura la integridad de la relación con los clientes, socios comerciales y otros actores involucrados en la cadena de valor de la organización. La pérdida de confidencialidad puede tener efectos devastadores no solo en términos económicos, sino también en la percepción pública y la reputación organizacional. Un fallo en esta área podría generar desconfianza en los servicios de una empresa, lo que a largo plazo afectaría su competitividad en el mercado.

Según Guzmán-Pacheco (2022), cualquier acceso no autorizado a información confidencial puede causar graves daños, tanto financieros como reputacionales. Por ejemplo, una violación de datos podría exponer detalles sensibles, como números de tarjetas de crédito o información de cuentas bancarias, lo que podría llevar a multas regulatorias, acciones legales por parte de los clientes afectados y una pérdida de confianza en la marca.

Ejemplos de violaciones de confidencialidad

Uno de los casos más emblemáticos de violación de confidencialidad ocurrió en Yahoo entre 2013 y 2014, cuando la empresa sufrió una filtración masiva que afectó a más de tres mil millones de cuentas de usuario. Esta violación no solo comprometió la información personal de los usuarios, sino que también impactó negativamente la confianza en los servicios de la empresa. Como resultado, Yahoo se vio forzada a reducir significativamente el precio de su venta a Verizon, con lo cual perdió aproximadamente 350 millones de dólares en valor de la transacción (Guzmán-Pacheco, 2022).

Este caso subraya el impacto de una falla en la protección de la confidencialidad, que no solo afecta las finanzas de la empresa directamente, sino también su valor de mercado y su posición competitiva a largo plazo. Yahoo, una de las compañías pioneras de internet, nunca pudo recuperarse del golpe reputacional causado por este incidente, lo que la debilitó frente a sus competidores.

Otro ejemplo relevante fue la violación de datos que sufrió Equifax en 2017, la cual comprometió la información personal de más de 147 millones de consumidores, incluyendo números de la seguridad social, fechas de nacimiento y direcciones. Este incidente no solo expuso a los consumidores al fraude y robo de identidad, sino que también condujo a sanciones económicas para Equifax y a una demanda colectiva, lo que subraya las posibles consecuencias legales y financieras de la pérdida de confidencialidad (Rutz, 2021).

Implicaciones legales y regulatorias

Las regulaciones sobre protección de datos, como el Reglamento General de Protección de Datos (GDPR) en Europa y la Ley de Privacidad del Consumidor de California (CCPA) en los Estados Unidos, establecen sanciones significativas para las organizaciones que no protejan adecuadamente la confidencialidad de la información de sus usuarios. Estas normativas no solo buscan proteger a los consumidores, sino también garantizar que las empresas adopten las mejores prácticas en cuanto a la ciberseguridad y la gestión de la información (Pereyra, 2021).

El incumplimiento de estas regulaciones puede resultar en multas millonarias y restricciones adicionales sobre las operaciones de la empresa. Por ejemplo, según el GDPR, las multas pueden alcanzar hasta el 4 % de la facturación anual global de la compañía o veinte millones de euros, lo que sea mayor. Esto resalta la importancia de adoptar un enfoque preventivo y garantizar que todas las medidas necesarias estén en su lugar para evitar violaciones de la confidencialidad.

Medidas preventivas para garantizar la confidencialidad

La protección de la confidencialidad de la información no solo depende de la implementación de tecnología avanzada, sino también de un enfoque integral que incluya políticas claras, procedimientos operativos y la capacitación del personal (Sánchez, 2023). Algunas de las principales medidas preventivas incluyen:

1. *Cifrado de datos*: el uso de técnicas avanzadas de cifrado asegura que, incluso si los datos son interceptados, no puedan ser leídos sin la clave adecuada. El cifrado debe aplicarse tanto a los datos en tránsito como a los datos en reposo.
2. *Gestión de accesos*: implementar políticas de control de acceso que limiten quién puede ver o modificar información confidencial es clave para reducir el riesgo de accesos no autorizados. Esto incluye la autenticación multifactor y el uso de privilegios mínimos.
3. *Auditorías de seguridad*: realizar auditorías regulares para identificar posibles vulnerabilidades en los sistemas de seguridad y corregirlas antes de que puedan ser explotadas. Esto también implica pruebas de penetración y simulaciones de ataques.
4. *Capacitación continua*: capacitar al personal sobre las mejores prácticas en el manejo de información confidencial y sensibilizarlo sobre la importancia de la ciberseguridad en su día a día.

5. *Políticas claras de confidencialidad:* desarrollar y comunicar políticas de confidencialidad que definan claramente cómo se maneja y protege la información sensible en la organización.

Integridad de los datos

La integridad de los datos es uno de los pilares fundamentales de la ciberseguridad y está directamente relacionada con la calidad, la precisión y la fiabilidad de la información. Garantizar que los datos no sean manipulados, alterados o destruidos de manera no autorizada es crucial para asegurar que las organizaciones puedan operar con confianza y tomar decisiones informadas basadas en información correcta (Valderrama, 2024). Sin integridad, la información pierde su valor, ya que no se puede confiar en que sea precisa o representativa de la realidad.

Importancia de la integridad de los datos

En el contexto de las operaciones empresariales, la integridad de los datos tiene un impacto directo en la toma de decisiones y en las relaciones con clientes, socios y proveedores. La alteración de datos, ya sea por acción maliciosa o por error humano, puede tener repercusiones significativas en la credibilidad de una organización. Esto se debe a que la información que se utiliza para tomar decisiones estratégicas o para interactuar con terceros debe ser exacta y fiable. Si los datos son manipulados o corrompidos, la empresa corre el riesgo de tomar decisiones equivocadas, lo que podría generar pérdidas económicas o dañar su reputación (Muñoz-Zambrano & Zambrano-Rendón, 2023).

Un ejemplo clásico de la importancia de la integridad de los datos es el uso de bases de datos en el sector financiero. Las transacciones, los balances y la información contable deben ser exactos y no estar sujetos a cambios no autorizados. Cualquier alteración en estos datos podría afectar la credibilidad financiera de la empresa y generar multas regulatorias o pérdidas financieras. En sectores altamente regulados, como la banca, incluso una pequeña alteración de datos puede tener consecuencias legales graves.

Ataques que comprometen la integridad

Uno de los tipos de ataques más dañinos para la integridad de los datos es la manipulación deliberada de la información. Los atacantes pueden infiltrarse en los sistemas para alterar registros críticos, modificar transacciones financieras o incluso alterar datos sensibles relacionados con operaciones o clientes. Estos ataques no solo afectan la precisión de los datos, sino que pueden tener un efecto

dominó en otros aspectos de la ciberseguridad, como la confidencialidad y la disponibilidad de la información.

Un ejemplo significativo de un ataque que comprometió la integridad de los datos fue el incidente de la cadena de suministro de SolarWinds en 2020. Durante este ataque, los hackers lograron insertar código malicioso en las actualizaciones del software de gestión de red de SolarWinds, lo cual permitió a los atacantes obtener acceso no autorizado a redes gubernamentales y corporativas en todo el mundo. Este ataque no solo comprometió la confidencialidad de los datos, sino que también planteó serias preocupaciones sobre la integridad de la información procesada por las entidades afectadas (Muñoz-Zambrano & Zambrano-Rendón, 2023).

El ataque a SolarWinds destacó la vulnerabilidad de los sistemas críticos y la necesidad de implementar medidas de protección robustas para garantizar la integridad de los datos. La manipulación del código fuente de las actualizaciones no solo comprometió a SolarWinds, sino que también afectó a miles de sus clientes, que confiaban en que el software que recibían no había sido alterado. Este tipo de violaciones puede tener efectos catastróficos, ya que los datos corruptos pueden propagarse a través de sistemas interconectados y afectar múltiples capas de una infraestructura tecnológica.

Consecuencias de la pérdida de integridad

La pérdida de integridad de los datos puede tener consecuencias devastadoras para las organizaciones. En primer lugar, los datos alterados pueden llevar a decisiones erróneas que afecten tanto a la estrategia empresarial como a las operaciones diarias. Por ejemplo, en el ámbito de la manufactura, si los datos sobre la producción o los inventarios son manipulados, las empresas podrían enfrentarse a problemas de suministro, interrupciones en la cadena de valor y pérdidas financieras.

En segundo lugar, la manipulación de datos puede erosionar la confianza entre la organización y sus clientes, socios comerciales y reguladores. En sectores como el de la salud, por ejemplo, la alteración de los datos de los pacientes puede tener implicaciones legales y éticas. La falta de integridad en los registros de salud podría poner en riesgo la vida de los pacientes y exponer a las organizaciones a demandas por negligencia (Valderrama, 2024).

Mejores prácticas para garantizar la integridad de los datos

Para evitar la manipulación o alteración no autorizada de los datos, las organizaciones deben implementar una serie de medidas y prácticas de seguridad que protejan la integridad de su información. La tabla 1 presenta un conjunto de prácticas

de seguridad cibernética que son clave para garantizar la integridad de los datos dentro de una organización, las cuales se centran en proteger los datos contra accesos no autorizados, alteraciones y manipulaciones que podrían comprometer la confiabilidad y precisión de la información. Cada una está acompañada de una descripción, los elementos esenciales que la componen, y referencias bibliográficas en formato APA para ofrecer una visión completa y respaldada sobre su implementación. Cabe señalar que estas herramientas son fundamentales para mantener la integridad de los datos y asegurar que la información se mantenga exacta y confiable en todo momento dentro del entorno empresarial.

Tabla 1. Medidas clave para garantizar la integridad de los datos dentro de una organización

Medida de seguridad	Descripción	Elementos clave	Referencias
Control de acceso basado en roles (RBAC)	Limitar el acceso a los datos a los empleados que lo necesiten para cumplir con sus funciones. De esta manera se previene que personas no autorizadas modifiquen los datos.	Roles bien definidos, autenticación, permisos basados en funciones y gestión de privilegios.	Valderrama (2024).
Cifrado de datos	El cifrado asegura que los datos, tanto en tránsito como en reposo, no puedan ser alterados sin la clave adecuada, con lo cual se protege la integridad en caso de interceptación.	Claves de cifrado, algoritmos de cifrado, cifrado de datos en tránsito y en reposo, y gestión de claves.	Sánchez (2023).
Registros de auditoría y control	Mantener un registro detallado de todas las interacciones con los datos para detectar intentos de manipulación. Esto permite rastrear accesos y modificaciones realizadas.	Registro de eventos, auditorías de seguridad, control de acceso y rastreo de actividades sospechosas.	Muñoz-Zambrano & Zambrano-Rendón (2023).
Integridad de los datos mediante firmas digitales	Las firmas digitales y algoritmos hash verifican que los datos no han sido alterados desde su creación, validando su autenticidad y detectando cualquier modificación.	Firmas digitales, algoritmos hash, verificación de autenticidad y detección de modificaciones no autorizadas.	Valderrama (2024).
Pruebas de integridad periódicas	Realizar pruebas periódicas para identificar vulnerabilidades antes de que sean explotadas. Incluye simulaciones de ataques y revisiones de los procedimientos.	Simulacros de ataques, pruebas de penetración, revisiones de políticas y simulaciones de incidentes de seguridad.	Muñoz-Zambrano & Zambrano-Rendón (2023).

Fuente: Elaboración propia

Disponibilidad de la información

La disponibilidad de la información es un aspecto crítico dentro de la ciberseguridad, ya que asegura que los sistemas y servicios estén accesibles cuando los usuarios los necesiten. En el mundo empresarial moderno, la dependencia de sistemas digitales para gestionar operaciones clave ha crecido exponencialmente, lo que significa que cualquier interrupción puede tener consecuencias devastadoras para la continuidad del negocio. Por lo tanto, garantizar la disponibilidad de la información es tan importante como proteger la confidencialidad e integridad de los datos (Muñoz-Zambrano & Zambrano-Rendón, 2023).

Importancia de la disponibilidad

La disponibilidad de los sistemas es fundamental para el funcionamiento diario de una organización. Un fallo en la disponibilidad de los sistemas críticos puede paralizar operaciones clave, interrumpir servicios, afectar las cadenas de suministro o incluso llevar a la pérdida de clientes y reputación. Las organizaciones deben asegurar que los sistemas estén disponibles 24/7, ya que cualquier tiempo de inactividad puede traducirse en pérdidas financieras significativas, particularmente en sectores como la banca, la salud o el comercio electrónico, donde los servicios en línea son esenciales para la operación.

Un concepto importante vinculado a la disponibilidad es el “tiempo de actividad” (*uptime*), que se refiere a la cantidad de tiempo en que un sistema está operativo y disponible para los usuarios. Las organizaciones buscan mantener el mayor tiempo de actividad posible, y las interrupciones del servicio pueden ser perjudiciales. Por ejemplo, si una tienda en línea experimenta una interrupción durante una gran venta o un evento promocional, puede perder millones en ingresos debido a la imposibilidad que tendrían los clientes de realizar transacciones (Rutz, 2021).

Uno de los mayores desafíos para la disponibilidad de la información son los ataques de Denegación de Servicio (DoS) y Denegación de Servicio Distribuida (DDoS). Estos ataques intentan sobrecargar los servidores de una organización con un volumen masivo de tráfico falso, haciendo que los sistemas no puedan gestionar las solicitudes legítimas de los usuarios. Los ataques DDoS pueden derribar sitios web, interrumpir servicios en línea y afectar la capacidad de una empresa para operar de manera normal.

Un ataque emblemático de DDoS ocurrió en 2016, cuando los hackers afectaron al proveedor de DNS Dyn. Esto perjudicó a empresas importantes como Twitter, Spotify y Reddit, pues interrumpió sus servicios y causó inconvenientes a millones

de usuarios en todo el mundo. Al explotar las vulnerabilidades en la infraestructura de DNS, los hackers demostraron lo fácil que es para un ataque masivo incidir en múltiples empresas dependientes de un mismo servicio (Casale, 2022). Este suceso subraya la importancia de proteger los sistemas críticos de las organizaciones y de diseñar infraestructuras que puedan resistir ataques de este tipo.

Otra amenaza creciente que afecta la disponibilidad es el *ransomware*, donde los hackers cifran los sistemas de la organización para impedir el acceso a los datos y solicitar un rescate para restaurar la funcionalidad. Este tipo de ataque puede ser igualmente destructivo, ya que impide a las empresas operar hasta que se resuelva el problema, lo cual genera tiempos de inactividad prolongados y pérdidas de ingresos.

La ciberdefensa como complemento a la ciberseguridad

La ciberdefensa, a diferencia de la ciberseguridad, se centra principalmente en las estrategias reactivas para mitigar los efectos de un ataque cibernético que ha tenido éxito en superar las barreras preventivas establecidas. Mientras que la ciberseguridad engloba las medidas preventivas que buscan proteger los sistemas informáticos y las redes de posibles intrusiones y vulnerabilidades, la ciberdefensa se activa una vez que las amenazas han logrado penetrar en los sistemas. En este sentido, la ciberdefensa puede considerarse una respuesta complementaria y necesaria a los fallos que puedan producirse en las estrategias de ciberseguridad (Casale, 2022).

Una de las claves de la ciberdefensa es la capacidad de las organizaciones para detectar rápidamente las amenazas y actuar de forma coordinada para contener y mitigar los daños. Esto requiere la implementación de un plan de respuesta a incidentes bien estructurado, que cubra todos los aspectos del ataque, desde la detección temprana hasta la contención, el análisis forense y la recuperación de los sistemas afectados. La preparación de estos planes debe basarse en la evaluación continua de los riesgos y la simulación de ataques potenciales, de modo que las organizaciones puedan reaccionar con rapidez y eficacia cuando ocurra un incidente real (Fernández, 2023).

En la actualidad, la ciberdefensa ha ganado una relevancia crítica, especialmente en un entorno global donde los ataques a infraestructuras críticas y sistemas gubernamentales se han vuelto más frecuentes. Los ataques cibernéticos no solo afectan a las organizaciones privadas, sino que también ponen en riesgo la seguridad nacional de los países, ya que pueden tener como objetivo sectores clave como la energía, las telecomunicaciones o los sistemas financieros. Como

resultado, la ciberdefensa ha dejado de ser un aspecto meramente técnico y se ha convertido en un tema de importancia estratégica para los gobiernos y las empresas a nivel mundial (González, 2020).

Un componente fundamental de la ciberdefensa es la cooperación internacional. Los ciberataques, debido a su naturaleza transnacional, requieren respuestas coordinadas entre diferentes países y organizaciones. Esto ha llevado al establecimiento de redes internacionales de colaboración, donde los Estados comparten información sobre amenazas, vulnerabilidades y soluciones para mitigar los daños de los ataques. Un ejemplo de ello es la creación de equipos de respuesta a incidentes de seguridad informática (CERT, por sus siglas en inglés), que funcionan tanto a nivel nacional como internacional para ofrecer asistencia técnica y coordinar esfuerzos ante ciberataques de gran magnitud (UNIDIR, 2022).

El ataque Stuxnet, ocurrido en 2010, se ha convertido en un caso paradigmático de cómo la ciberdefensa puede tener un papel crucial en la mitigación de los daños causados por un ciberataque. Stuxnet, un gusano informático sofisticado que fue diseñado para sabotear las centrifugadoras de enriquecimiento de uranio en Irán, demostró la vulnerabilidad de las infraestructuras críticas ante ataques cibernéticos avanzados. Sin embargo, la respuesta del gobierno iraní y la comunidad internacional resaltó la importancia de contar con sistemas robustos de ciberdefensa. A pesar de los daños iniciales, las medidas adoptadas para contener el ataque, analizar su origen y fortalecer las defensas fueron clave para prevenir que Stuxnet lograra su objetivo a mayor escala (Sandoval, 2022).

Otro caso notable es el ataque a la infraestructura energética de Ucrania en 2015, donde un grupo de ciberdelincuentes logró penetrar en las redes de distribución eléctrica y provocar un apagón masivo. La respuesta de Ucrania incluyó no solo la restauración de los sistemas afectados, sino también la implementación de nuevas medidas de ciberdefensa que buscaron proteger sus redes eléctricas de futuros ataques similares. Como en el caso anterior, este evento subrayó la importancia de contar con una ciberdefensa resiliente, que no solo se basa en la capacidad de reaccionar ante ataques, sino también en la adaptación y mejora continua de las defensas ante la evolución de las amenazas (Rodríguez, 2021).

La ciberdefensa, por tanto, no es solo un conjunto de acciones reactivas, sino también un proceso continuo de aprendizaje y adaptación. Las organizaciones deben realizar análisis forenses detallados después de cada incidente para comprender cómo los atacantes lograron penetrar en sus sistemas y qué vulnerabilidades fueron explotadas. Estos conocimientos permiten reforzar las barreras de

ciberseguridad existentes y desarrollar nuevas estrategias de ciberdefensa más efectivas para el futuro (Valencia, 2023).

Asimismo, es importante destacar el papel del sector privado en la ciberdefensa. Dado que gran parte de las infraestructuras críticas y los sistemas digitales están gestionados por empresas privadas, estas tienen un papel esencial en la protección del ciberespacio. En este sentido, el apoyo entre el sector público y el privado es fundamental para garantizar una ciberdefensa sólida y coordinada. Las empresas deben colaborar estrechamente con las agencias gubernamentales para compartir información sobre amenazas emergentes y participar en ejercicios de ciberseguridad que simulen ataques reales y mejoren la preparación colectiva (Nolasco-Mamani et al., 2022).

Por lo anterior, la ciberdefensa complementa a la ciberseguridad al proporcionar las herramientas y estrategias necesarias para reaccionar ante los ciberataques que logran superar las barreras preventivas. La cooperación internacional, la participación del sector privado y la mejora continua de las capacidades defensivas son aspectos clave para enfrentar los desafíos que presenta el panorama actual de ciberseguridad (Casale, 2022).

Resiliencia organizacional

En el entorno actual de crecientes amenazas cibernéticas, uno de los conceptos más importantes en la gestión de la seguridad de la información es la *resiliencia organizacional*. La resiliencia se refiere a la capacidad de una organización para no solo prevenir ataques cibernéticos, sino también para recuperarse de ellos de manera rápida y efectiva, de tal manera que se asegure la continuidad operativa. En términos más generales, la resiliencia organizacional implica la preparación y la capacidad de una empresa para adaptarse a las interrupciones, restaurar las funciones críticas y mitigar el impacto de los incidentes en su infraestructura tecnológica y en sus operaciones comerciales (Carreño & López, 2022).

La resiliencia no debe confundirse con la mera reacción ante un ataque. Va más allá, ya que abarca una estrategia integral que incluye la *gestión de riesgos*, el *fortalecimiento de la infraestructura tecnológica* y la *planificación ante desastres*. Las organizaciones resilientes son aquellas que, además de contar con sistemas de defensa robustos, disponen de planes de respuesta y recuperación bien definidos. Estos planes se diseñan con antelación y deben estar sujetos a revisiones periódicas para asegurar que son efectivos ante las amenazas emergentes. En este sentido, la *cultura de la resiliencia* es fundamental para las organizaciones

modernas, ya que les permite anticiparse a posibles interrupciones, recuperarse de manera eficiente y, por lo tanto, minimizar las pérdidas financieras, operativas y reputacionales (Carlini, 2016).

Un aspecto central de la resiliencia organizacional es la implementación de *planes de recuperación ante desastres* (Disaster Recovery Plans [DRP]) y *planes de continuidad del negocio* (Business Continuity Plans [BCP]). Estos planes proporcionan un marco para que las organizaciones puedan operar durante y después de una crisis, de tal manera que permiten restaurar las funciones críticas en el menor tiempo posible. El BCP, por ejemplo, detalla los pasos que debe seguir una empresa para mantener operaciones esenciales en caso de una interrupción, mientras que el DRP se enfoca más específicamente en los procesos de TI, asegurando que los datos y sistemas puedan recuperarse después de un ataque o fallo técnico (Serrano, 2022).

La *resiliencia tecnológica* también desempeña un papel crucial en este proceso. A medida que las organizaciones dependen cada vez más de la tecnología para sus operaciones, garantizar la solidez y flexibilidad de sus infraestructuras tecnológicas es esencial. Esto incluye la adopción de soluciones en la nube, la creación de copias de seguridad automatizadas, la implementación de sistemas redundantes y la utilización de tecnologías avanzadas de *detección y respuesta ante amenazas*. Todo esto, combinado con una capacitación continua del personal, asegura que las organizaciones puedan no solo sobrevivir a los ataques, sino también adaptarse rápidamente a las condiciones cambiantes (Pacheco-Mangas et al., 2021).

Un ejemplo destacado de resiliencia organizacional es la respuesta del Servicio Nacional de Salud (NHS) del Reino Unido al ataque de *ransomware* WannaCry en 2017. Se trató de uno de los incidentes más grandes de *ransomware* hasta la fecha, pues afectó a miles de sistemas en más de 150 países, incluyendo a muchas organizaciones del sector salud. En el caso del NHS, aunque el ataque causó el cierre de varios hospitales y clínicas —lo cual interrumpió los servicios médicos esenciales—, gracias a la implementación de un plan de resiliencia organizacional sólido, que incluía medidas preventivas y de recuperación, el NHS logró restaurar la mayor parte de sus operaciones en un tiempo relativamente corto. Este caso demostró la importancia de estar preparados no solo para defenderse de ataques, sino también para recuperarse de ellos con rapidez (Sánchez, 2023).

La respuesta del NHS incluyó no solo la restauración de los sistemas afectados, sino también un análisis exhaustivo de las vulnerabilidades explotadas por el ataque. Este enfoque le permitió implementar nuevas medidas de seguridad,

como actualizar sistemas obsoletos y mejorar las defensas cibernéticas. Además, el ataque WannaCry subrayó la importancia de la *resiliencia proactiva*, en la cual las organizaciones no solo se centran en recuperarse, sino también en aprender de los incidentes para prevenir futuros ataques. Este enfoque incluye la actualización constante de los sistemas, la realización de simulacros regulares y la capacitación continua de los empleados para identificar y responder a las amenazas de manera más eficaz (Akbanov et al., 2019)

Además, la *resiliencia organizacional* implica una gestión efectiva de la cadena de suministro y las relaciones con terceros. En el caso de muchas organizaciones, una interrupción en los servicios que prestan proveedores externos puede tener un efecto dominó que afecte la capacidad de la empresa para operar de manera efectiva. Por lo tanto, es fundamental que las organizaciones desarrollen relaciones sólidas con sus proveedores, asegurando que también cuenten con estrategias de resiliencia que puedan complementar las propias de la organización (Ruiz, 2022).

Elementos propios de la ciberresiliencia

La ciberresiliencia es un concepto clave en la estrategia de seguridad de las organizaciones modernas, ya que les permite no solo resistir ataques cibernéticos, sino también recuperarse rápidamente y garantizar la continuidad operativa. En este sentido, la implementación de diversas variables es esencial para fortalecer la capacidad de respuesta y minimizar el impacto de incidentes cibernéticos. La tabla 2 desglosa las principales variables que se deben considerar en la ciberresiliencia y describe sus características, elementos esenciales, condiciones de cumplimiento, riesgos asociados a su omisión y las referencias bibliográficas correspondientes. Este enfoque integral proporciona una guía práctica para las empresas que buscan mejorar su preparación ante posibles amenazas cibernéticas.

Tabla 2. Desglose de las principales variables a considerar en la ciberresiliencia

Variables que se deben tener en cuenta en la ciberresiliencia	Descripción de la variable	Elementos a tener en cuenta	Condiciones de cumplimiento en la empresa	Riesgos de no tenerla en cuenta en una empresa	Referencias
Plan de continuidad del negocio (BCP)	Proceso que garantiza la continuidad de las operaciones durante y después de un incidente.	Identificación de funciones críticas, responsables y procesos alternativos.	El plan está documentado, probado regularmente y actualizado.	Pérdida de operaciones esenciales y caos organizacional.	Serrano (2022).

Variables que se deben tener en cuenta en la ciberresiliencia	Descripción de la variable	Elementos a tener en cuenta	Condiciones de cumplimiento en la empresa	Riesgos de no tenerla en cuenta en una empresa	Referencias
Plan de recuperación ante desastres (DRP)	Estrategia para recuperar sistemas y datos después de un desastre cibernético o físico.	Identificación de tecnologías críticas, plan de copias de seguridad y responsables de tecnologías de la información (TI).	El plan incluye recuperación de datos y redundancia en sistemas clave.	Pérdida de datos críticos e incapacidad de reanudar operaciones.	Carlini (2016).
Cultura de ciberseguridad	Nivel de conciencia y responsabilidad cibernética dentro de la organización.	Capacitación continua, políticas claras y comportamiento proactivo en ciberseguridad.	Empleados capacitados en identificar y prevenir amenazas cibernéticas.	Incremento de vulnerabilidades por errores humanos.	Carreño & López (2022).
Colaboración con terceros	Coordinación con proveedores y socios externos para garantizar la resiliencia en la cadena de suministro.	Asegurar que los proveedores tengan BCP y DRP adecuados, así como hacer evaluación de riesgos de terceros.	Contratos actualizados y auditorías periódicas a terceros.	Brechas de seguridad en proveedores e interrupciones en la cadena de suministro.	Ruiz (2022).
Infraestructura tecnológica redundante	Mecanismos de respaldo para garantizar el funcionamiento continuo de los sistemas críticos.	Implementación de sistemas de respaldo, almacenamiento en la nube, redundancia de servidores.	Sistemas de respaldo disponibles y probados regularmente.	Interrupción prolongada de servicios y pérdida de datos.	Pacheco-Mangas et al. (2021).
Evaluación de riesgos cibernéticos	Análisis de las amenazas y vulnerabilidades que pueden afectar a la organización.	Identificación y clasificación de riesgos y medidas de mitigación.	Análisis regular de riesgos y actualización de políticas.	Falta de preparación ante amenazas emergentes.	(Akbanov et al., 2019)

Variables que se deben tener en cuenta en la ciberresiliencia	Descripción de la variable	Elementos a tener en cuenta	Condiciones de cumplimiento en la empresa	Riesgos de no tenerla en cuenta en una empresa	Referencias
Respuesta ante incidentes	Proceso de manejo y mitigación de incidentes cibernéticos para limitar su impacto.	Equipos de respuesta a incidentes, notificación y contención rápida.	Equipos entrenados y protocolos de respuesta establecidos.	Retraso en la respuesta que agrava los daños y las pérdidas.	Sánchez (2023).
Simulacros y ejercicios de ciberseguridad	Pruebas periódicas que simulan incidentes cibernéticos para evaluar la preparación.	Simulacros de ataques, revisión de tiempos de respuesta y efectividad.	Realización de simulacros anuales y revisión de resultados.	Falta de preparación ante incidentes reales.	Serrano (2022).

Fuente: Elaboración propia

El concepto de resiliencia organizacional ha cobrado relevancia a nivel internacional como respuesta al incremento de ciberataques. Por ejemplo, países como Estonia, tras el ataque cibernético masivo en 2007, reformularon su política nacional de seguridad para incluir la ciberdefensa como pilar estratégico, para lo cual establecieron el Centro de Excelencia en Ciberdefensa Cooperativa de la OTAN en Tallin (Organización del Tratado del Atlántico Norte [OTAN], 2021).

En el ámbito nacional, Colombia ha adoptado un enfoque de ciberresiliencia que vincula al sector defensa, al sector productivo y a la ciudadanía, integrando esfuerzos bajo el marco de la Política Nacional de Seguridad Digital. Esta estrategia ha sido clave para fortalecer la protección de infraestructuras críticas, como el sector eléctrico, el bancario y las telecomunicaciones (MinTIC, 2021).

Por su parte, la experiencia del Reino Unido, con su Centro Nacional de Ciberseguridad (NCSC), es otro referente importante. Esta entidad opera con un modelo de colaboración con empresas privadas, universidades y agencias estatales que promueve campañas educativas, análisis de amenazas y mecanismos de respuesta unificados (UK NCSC, 2020).

En el contexto latinoamericano, México ha formulado la Estrategia Nacional de Ciberseguridad, que enfatiza la protección de infraestructuras críticas, la educación en ciberseguridad y el fomento a la cooperación internacional. Uno de sus mayores avances ha sido el desarrollo de capacidades técnicas en las fuerzas armadas para responder ante amenazas de ciberespionaje y sabotaje digital (OCDE, 2020).

Asimismo, Israel considera la ciberseguridad un asunto de seguridad nacional, de manera que ha integrado capacidades ofensivas y defensivas dentro de su doctrina de defensa. De esta manera, combina vigilancia activa, inversión en *start ups* de ciberseguridad y formación intensiva de talento desde edades tempranas. Cabe señalar que esta visión holística lo ha posicionado como un referente mundial en ciberdefensa (Kaplan & Cohen, 2022).

Estos casos permiten observar cómo distintas naciones han articulado institucionalmente la ciberseguridad y la ciberdefensa con su planeación estratégica. En este sentido, su análisis proporciona insumos valiosos para que las organizaciones diseñen sus propios marcos de actuación, alineados con las mejores prácticas internacionales (Sánchez & Morales, 2022).

Integración de la ciberseguridad en la planeación estratégica

Integrar la ciberseguridad en la planificación estratégica es crucial para garantizar que los activos digitales estén protegidos y las operaciones comerciales puedan continuar sin interrupciones. Específicamente, este proceso debe comenzar con una evaluación exhaustiva de los riesgos cibernéticos, lo cual permite a las organizaciones identificar vulnerabilidades y diseñar medidas para mitigarlas (Muñoz-Zambrano & Zambrano-Rendón, 2023).

El primer paso es identificar los activos más críticos para la organización. Estos pueden incluir bases de datos de clientes, sistemas de gestión financiera, infraestructura de TI y cualquier otro recurso digital esencial para las operaciones. Una vez identificados, se deben evaluar los riesgos específicos asociados a cada uno.

Esta evaluación de riesgos implica no solo identificar amenazas, sino también determinar el impacto que un ataque podría tener en la organización. Este proceso debe realizarse de manera periódica, ya que el entorno cibernético es dinámico y las amenazas evolucionan constantemente. Al realizar evaluaciones regulares, las organizaciones pueden ajustar sus estrategias de ciberseguridad para enfrentar nuevas vulnerabilidades (Guzmán-Pacheco, 2022).

Tras evaluar los riesgos, es necesario diseñar e implementar medidas preventivas que garanticen la protección de los activos digitales, las cuales pueden incluir la implementación de *firewalls*, sistemas de detección de intrusiones, cifrado de datos y controles de acceso. Sin embargo, es importante destacar que la tecnología por sí sola no es suficiente, pues también se deben establecer políticas

y procedimientos que regulen el uso seguro de los sistemas de información (Valderrama, 2024).

La creación de políticas de ciberseguridad debe ser un esfuerzo colaborativo entre el departamento de TI y otras áreas de la organización. Las políticas deben abarcar temas como el acceso a sistemas de información, la gestión de contraseñas y la respuesta ante incidentes de seguridad. Además, deben alinearse con las normativas y regulaciones aplicables, garantizando el cumplimiento legal en materia de protección de datos y seguridad cibernética (Rincón-Gallón, 2022).

Es esencial que estas políticas no solo se implementen, sino que también se comuniquen y sean comprendidas por todos los miembros de la organización, pues la falta de concientización sobre ciberseguridad entre los empleados es una de las principales causas de incidentes de seguridad. Por lo tanto, es fundamental desarrollar programas de formación y concientización que capaciten al personal en buenas prácticas de seguridad (Bermúdez et al., 2023).

Asignar adecuadamente los recursos es clave en la integración de la ciberseguridad, pero requiere inversión financiera y humana, de manera que las organizaciones deben estar dispuestas a invertir en tecnología avanzada y en contratar personal capacitado que pueda gestionar las políticas y medidas de seguridad de manera efectiva (Sánchez, 2023).

La ciberseguridad no puede verse como una solución estática. El panorama de amenazas cibernéticas cambia constantemente, por lo que las organizaciones deben estar preparadas para adaptarse a nuevos desafíos, lo cual implica actualizar regularmente las tecnologías de seguridad, revisar las políticas y los procedimientos, así como mejorar continuamente las capacidades del personal (Casale, 2022).

En este contexto, utilizar indicadores y métricas es útil para evaluar la efectividad de las medidas de ciberseguridad, al tiempo que permiten medir el desempeño de las políticas y procedimientos de seguridad, identificar áreas de mejora y tomar decisiones informadas. Algunos indicadores comunes incluyen el número de incidentes de seguridad detectados, el tiempo de respuesta ante incidentes y el costo de las medidas de ciberseguridad implementadas (Valderrama, 2024).

Además, realizar pruebas regulares de las medidas de ciberseguridad, como simulacros de ataques y auditorías de seguridad, ayuda a identificar posibles debilidades en las defensas de la organización y mejora la capacidad de respuesta ante un ataque real. De igual forma, estas prácticas sensibilizan a los empleados sobre la importancia de seguir las políticas de seguridad y fortalecen la cultura organizacional en torno a la ciberseguridad (Muñoz-Zambrano & Zambrano-Rendón, 2023).

Para realizar estas acciones es muy importante la colaboración con otras dependencias de la organización. Por ejemplo, mientras el área legal puede proporcionar orientación sobre el cumplimiento normativo y las implicaciones legales de un incidente de seguridad, por su parte, el área de TI ofrece soporte técnico para implementar medidas preventivas. Así, esta colaboración asegura que la estrategia de ciberseguridad sea coherente y eficaz (Rutz, 2021).

Asimismo, el compromiso de la alta dirección resulta fundamental, pues sin su apoyo es difícil garantizar que se asignen los recursos necesarios y que las políticas de seguridad se implementen de manera efectiva. Además, la alta dirección debe promover una cultura de seguridad en toda la organización, de tal manera que cada empleado entienda su responsabilidad en la protección de los activos digitales (Pereyra, 2021).

La ciberseguridad también debe integrarse en los procesos de gestión de riesgos. Específicamente, las organizaciones deben considerar los riesgos cibernéticos como parte de su análisis general y desarrollar planes de contingencia que permitan minimizar el impacto de un ataque cibernético. Estos planes deben incluir procedimientos para la recuperación ante desastres, la continuidad del negocio y la comunicación con las partes interesadas en caso de un incidente (Guzmán-Pacheco, 2022). La tabla 3 sintetiza los elementos de la estrategia descritos.

Tabla 3. Elementos ciber en la estrategia

Elemento	Descripción	Prácticas clave	Referencias
Integración en la planificación estratégica	La ciberseguridad debe integrarse en la planificación estratégica de la organización para garantizar la protección de los activos y la continuidad operativa.	Evaluaciones de riesgos periódicas y adaptación continua a nuevas amenazas.	Muñoz-Zambrano & Zambrano-Rendón (2023).
Evaluación de riesgos	Identificar y evaluar los riesgos cibernéticos permite a las organizaciones comprender sus vulnerabilidades y diseñar medidas de mitigación.	Identificación de activos críticos (bases de datos y sistemas TI), determinación del impacto de los ciberataques y realización de evaluaciones periódicas de riesgos.	Guzmán-Pacheco (2022).
Medidas preventivas	Después de evaluar los riesgos, se deben diseñar e implementar medidas preventivas para garantizar la protección de los activos digitales.	Implementación de <i>firewalls</i> , sistemas de detección de intrusos, cifrado de datos, controles de acceso y políticas que regulen el uso seguro de los sistemas de información.	Valderrama (2024).

Elemento	Descripción	Prácticas clave	Referencias
Creación de políticas de ciberseguridad	Las políticas de ciberseguridad deben ser un esfuerzo colaborativo entre TI y otras áreas de la organización.	Políticas que cubran temas como el acceso a sistemas, la gestión de contraseñas y la respuesta a incidentes de seguridad, alineadas con normativas y regulaciones aplicables.	Rincón-Gallón (2022).
Concientización y capacitación	La falta de concientización sobre ciberseguridad entre los empleados es una causa común de incidentes. Es vital capacitar al personal en buenas prácticas de seguridad.	Desarrollo de programas de formación y concientización para todo el personal, con el fin de garantizar el cumplimiento de las políticas de seguridad.	Bermúdez et al. (2023).
Asignación de recursos	Asignar los recursos adecuados, tanto financieros como humanos, es clave para la integración de la ciberseguridad.	Inversión en tecnología avanzada y contratación de personal capacitado para gestionar las políticas y las medidas de seguridad de forma efectiva.	Sánchez (2023).
Actualización continua	La ciberseguridad es dinámica y debe evolucionar con el panorama de las amenazas.	Actualización regular de tecnologías, revisión de políticas y mejora continua de las capacidades del personal.	Casale (2022).
Uso de métricas e indicadores	Las métricas son útiles para evaluar la efectividad de las medidas de ciberseguridad. Permiten medir el rendimiento de las políticas y tomar decisiones informadas.	Uso de indicadores, como número de incidentes detectados, tiempo de respuesta y costo de las medidas implementadas.	Valderrama (2024).
Pruebas y auditorías	Realizar pruebas regulares de las medidas de ciberseguridad ayuda a identificar debilidades y mejorar la capacidad de respuesta ante ataques.	Simulacros de ataques, auditorías de seguridad y programas de sensibilización para los empleados.	Muñoz-Zambrano & Zambrano-Rendón (2023).
Colaboración interdepartamental	Colaborar con áreas como legal y TI asegura que la estrategia de ciberseguridad sea coherente y efectiva.	El área legal puede orientar en el cumplimiento normativo, mientras que el TI puede implementar medidas preventivas.	Rutz (2021).
Compromiso de la alta dirección	El apoyo de la alta dirección es esencial para asignar los recursos necesarios y promover una cultura de seguridad en la organización.	Fomentar una cultura de seguridad en la que cada empleado entienda su responsabilidad en la protección de los activos digitales.	Pereyra (2021).
Gestión de riesgos	La ciberseguridad debe integrarse en los procesos de gestión de riesgos y en los planes de contingencia para minimizar el impacto de un ataque.	Desarrollar planes de recuperación ante desastres, continuidad del negocio y comunicación efectiva en caso de incidentes.	Guzmán-Pacheco (2022).

Elemento	Descripción	Prácticas clave	Referencias
Ciberseguridad y competitividad	Integrar la ciberseguridad no solo protege, sino que también mejora la competitividad al generar confianza en clientes y socios comerciales.	Organizaciones comprometidas con la ciberseguridad mejoran su reputación y se diferencian en el mercado.	Sánchez (2023).

Fuente: Elaboración propia

Por lo tanto, integrar la ciberseguridad en la planificación estratégica no es solo una cuestión de protección, sino también de competitividad. Las organizaciones que demuestran un compromiso sólido con la ciberseguridad ganan la confianza de sus clientes y socios comerciales, lo cual les permite diferenciarse en el mercado y mejorar su reputación (Sánchez, 2023).

No obstante, uno de los principales desafíos en la integración de la ciberseguridad en la planeación estratégica es la ausencia de marcos metodológicos estandarizados dentro de muchas organizaciones. Para superar esta dificultad, es recomendable adoptar marcos como el NIST Cybersecurity Framework (CSF), COBIT o las doctrinas de ciberdefensa de la OTAN, instrumentos que proporcionan directrices estructuradas para gestionar los riesgos cibernéticos de forma proactiva y alineada con los objetivos organizacionales (ISACA, 2019; OTAN, 2021; NIST, 2018).

El marco NIST CSF se compone de cinco funciones esenciales: identificar, proteger, detectar, responder y recuperar. Esta estructura permite a las organizaciones entender su entorno de riesgo y priorizar acciones que aseguren la continuidad del negocio, pues su flexibilidad permite aplicarlas tanto en grandes corporaciones como en pymes, de tal manera que fomentan la resiliencia digital desde un enfoque escalable (NIST, 2018).

Por su parte, COBIT ofrece un enfoque integral para la gobernanza y la gestión de las tecnologías de la información. Con una orientación hacia el cumplimiento, la calidad y la seguridad de los sistemas, COBIT facilita la alineación de las estrategias de TI con los objetivos corporativos. Su enfoque basado en procesos y control permite definir responsabilidades claras, establecer indicadores y gestionar eficazmente la ciberseguridad como un activo estratégico (ISACA, 2019).

En contextos internacionales y de defensa, las doctrinas de la OTAN establecen principios fundamentales para la protección de infraestructuras críticas, la cooperación internacional y la defensa activa ante amenazas persistentes avanzadas (APT). Estas doctrinas integran la ciberdefensa como una dimensión estratégica

de la seguridad nacional y promueven capacidades conjuntas de disuasión, disuasión activa y recuperación operativa (OTAN, 2021).

Es importante tener en cuenta que la implementación de estos marcos debe adaptarse a la cultura organizacional, el nivel de madurez digital y los recursos disponibles. Ahora bien, también es cierto que un enfoque híbrido que combine los lineamientos de NIST con el gobierno estructurado de COBIT puede resultar particularmente eficaz en sectores regulados o críticos como la banca, la salud y las telecomunicaciones. Además de lo anterior, cumplir los estándares internacionales refuerza la reputación institucional ante clientes, socios y entes reguladores (Sánchez, 2023).

Por lo tanto, es recomendable que las organizaciones incluyan en su planeación estratégica no solo políticas generales de ciberseguridad, sino también una hoja de ruta metodológica apoyada en marcos reconocidos. Esto fortalece la capacidad de anticipación, respuesta y recuperación frente a las amenazas del entorno digital, y permite medir el desempeño de las estrategias implementadas con base en prácticas internacionales consolidadas (Muñoz-Zambrano & Zambrano-Rendón, 2023).

Rol de la ciberdefensa en la planeación estratégica

La implementación práctica de estrategias de ciberseguridad y ciberdefensa puede observarse en organizaciones líderes que han logrado integrar estos elementos en su planeación estratégica. Un caso emblemático es el de la NASA, que adoptó el NIST CSF como base para su marco de gestión de riesgos cibernéticos, con lo cual aseguró una protección integral de sus sistemas críticos y datos científicos (NIST, 2018).

En el sector financiero, el banco HSBC ha implementado el marco COBIT para alinear su estrategia de ciberseguridad con sus objetivos corporativos. Esto le ha permitido establecer controles sobre activos digitales, identificar riesgos emergentes y asegurar el cumplimiento normativo en distintas jurisdicciones. En particular, la combinación de marcos técnicos y una cultura organizacional proactiva ha sido clave en su éxito (ISACA, 2019).

Por su parte, en el sector gubernamental, el Departamento de Defensa de los Estados Unidos ha desarrollado una doctrina de ciberdefensa basada en la resiliencia operativa y en compartir inteligencia en tiempo real con agencias aliadas. Además, esta estrategia incluye ejercicios conjuntos con organizaciones civiles

y privadas para simular ciberataques a gran escala, como parte del programa "Cyber Shield" (OTAN, 2021).

En América Latina, Chile ha avanzado en la institucionalización de su ciberdefensa mediante la creación del Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT). Esta entidad trabaja en conjunto con empresas públicas y privadas, promoviendo buenas prácticas, alertas tempranas y estándares de seguridad para infraestructuras críticas (Gobierno de Chile, 2022).

Otro caso interesante es el del Centro Nacional de Ciberseguridad de Colombia (CNCS), que ha desarrollado un marco nacional basado en NIST y la ISO/IEC 27001. Este esfuerzo ha permitido coordinar esfuerzos entre entidades públicas, militares y privadas para aumentar la capacidad de respuesta ante incidentes cibernéticos y proteger el ecosistema digital colombiano (MinTIC, 2021).

Estos ejemplos permiten evidenciar que la integración estratégica de la ciberseguridad no es un ideal teórico, sino una práctica creciente en entornos complejos. Asimismo, sirven como referencia para aquellas organizaciones que buscan estructurar sus esfuerzos en torno a modelos probados, adaptándolos a sus necesidades, capacidades y contexto sectorial (Rutz, 2021).

En un mundo donde las amenazas cibernéticas están en constante evolución, la ciberdefensa ha emergido como un pilar fundamental en la planificación estratégica de las organizaciones. La ciberdefensa no se limita a la simple protección de los sistemas internos, sino que va más allá, proporcionando un enfoque integral que permite a las empresas detectar, responder y recuperarse de ataques cibernéticos con rapidez y eficacia. Finalmente, cabe enfatizar que mientras la ciberseguridad se centra en la prevención de incidentes, la ciberdefensa añade una capa de protección al preparar a la organización para enfrentar incidentes cuando ocurren y mitigar su impacto (Casale, 2022).

Detección temprana de amenazas: el primer paso para una respuesta efectiva

La detección temprana de amenazas es uno de los pilares fundamentales de una estrategia de ciberdefensa efectiva. En un mundo donde las amenazas cibernéticas son cada vez más frecuentes y sofisticadas, la capacidad de identificar y neutralizar ataques en sus primeras etapas es fundamental para mitigar el impacto que pueden causar en una organización.

Por esta razón, como se ha señalado, los ataques cibernéticos, que pueden ocurrir en cualquier momento, exigen una vigilancia constante y el uso de

tecnologías avanzadas para garantizar una respuesta oportuna. Es aquí donde entran en juego herramientas de *monitoreo continuo* y *análisis de tráfico de red*, las cuales desempeñan un papel esencial porque permiten identificar comportamientos sospechosos antes de que los daños sean irreversibles (Muñoz-Zambrano & Zambrano-Rendón, 2023).

Específicamente, el monitoreo continuo es un proceso activo que involucra la supervisión ininterrumpida de los sistemas informáticos y las redes de la organización. A través del uso de tecnologías como los sistemas de detección de intrusiones (IDS) y de herramientas de análisis en tiempo real, es posible obtener una imagen clara de la actividad que se realiza dentro de la red. Estas soluciones no solo detectan actividades inusuales, sino que también alertan de manera inmediata al equipo de seguridad, lo cual permite que se tomen decisiones rápidas para contener y mitigar cualquier ataque en curso. En tal sentido, esta capacidad de respuesta temprana es esencial porque que minimiza el tiempo de exposición a las amenazas y reduce las posibilidades de que estas se conviertan en incidentes cibernéticos graves.

Por su parte, el análisis de tráfico de red es una técnica avanzada que permite identificar patrones anómalos en los flujos de datos que podrían indicar la presencia de un ataque. A través de la correlación de eventos y el análisis de grandes volúmenes de datos, estas herramientas pueden detectar incluso las amenazas más sutiles que podrían pasar desapercibidas para los métodos tradicionales de defensa. Al identificar estos patrones anómalos, las organizaciones pueden activar de inmediato sus *protocolos de respuesta a incidentes*, lo cual les permite contener la amenaza antes de que esta pueda comprometer sistemas críticos.

Este enfoque proactivo es vital porque los atacantes cibernéticos constantemente buscan puntos débiles en las defensas de las organizaciones. Por lo tanto, si se cuenta con sistemas de monitoreo continuo y análisis de tráfico de red, las organizaciones no solo pueden identificar ataques en curso, sino también prevenir los futuros identificando las vulnerabilidades antes de que puedan ser explotadas. De esta forma, la detección temprana contribuye a reducir el impacto inmediato de un ataque y fortalece las defensas a largo plazo, con lo cual ayuda a que las organizaciones se adapten continuamente a las amenazas cambiantes del ciberespacio.

Capacitación continua: la primera línea de defensa

En el contexto de la ciberdefensa, los empleados son un recurso invaluable que, si se capacita adecuadamente, puede convertirse en la primera línea de defensa

frente a los ciberataques. Dado que los ataques cibernéticos no solo se enfocan en vulnerabilidades tecnológicas, sino también en debilidades humanas, es crucial que las organizaciones inviertan en capacitación continua para preparar a su personal contra las amenazas más recientes del ciberespacio. En este sentido, las organizaciones que implementan programas de formación efectivos están mejor posicionadas para enfrentar los desafíos que presenta el panorama actual de ciberseguridad, ya que los empleados desempeñan un papel clave en la prevención de ataques internos y externos (Bermúdez et al., 2023).

La importancia de la capacitación continua

La capacitación del personal debe ser un proceso continuo y dinámico. Sin embargo, no basta con una formación única o esporádica, pues dado que las ciberamenazas evolucionan rápidamente, los empleados necesitan estar al día con las últimas tácticas y métodos empleados por los ciberdelincuentes. Esta formación regular cumple un doble propósito: por una parte mejora la capacidad de los empleados para identificar y mitigar posibles ataques, y, por otra, contribuye a crear una cultura de ciberseguridad dentro de la organización, la cual se convierte en una herramienta poderosa para reducir el riesgo de ataques que aprovechan errores humanos, como el *phishing* o la ingeniería social (Jiménez-Almeira & López, 2023).

Específicamente, entre la variedad de temas que debe abordar la formación continua, uno de los más críticos para la ciberseguridad es la identificación y la prevención de ataques de *phishing*, los cuales siguen siendo una de las principales tácticas utilizadas por los ciberdelincuentes para acceder a sistemas sensibles. Frente a este escenario, los empleados deben aprender a detectar correos electrónicos sospechosos, mensajes maliciosos y sitios web falsificados, así como contar con las herramientas necesarias para reportar estas amenazas al equipo de seguridad de la organización (Rueda, 2020).

Además de continua, la capacitación a los empleados también debe incluir simulacros regulares de incidentes cibernéticos que les permitan familiarizarse con los protocolos de respuesta ante un ataque y saber cómo actuar en situaciones reales. De hecho, las organizaciones que realizan simulacros con regularidad pueden evaluar y ajustar sus planes de respuesta a incidentes, de tal manera que garantizan que sus empleados estén preparados para enfrentar cualquier amenaza. Finalmente, cabe señalar que, según Valencia (2023), los simulacros aumentan la capacidad de respuesta organizacional y permiten identificar debilidades en las estrategias de defensa.

Capacitación adaptada a las nuevas amenazas

Como se ha enfatizado en los apartados anteriores, la evolución de las cibermenazas exige que la capacitación en ciberseguridad no sea estática, pues los atacantes innovan constantemente las tácticas y las técnicas que emplean, como *malware* avanzado, *ransomware* o ataques dirigidos. Frente a esta problemática, Nolasco-Mamani et al. (2022) señalan que uno de los errores más comunes en las organizaciones es confiar en programas de capacitación desactualizados, ya que esto deja a los empleados en una condición de vulnerabilidad ante nuevos vectores de ataque.

Además de la capacitación técnica, es crucial que las organizaciones también incluyan formación sobre aspectos éticos y de cumplimiento normativo. En particular, el creciente enfoque en la privacidad de los datos, así como el surgimiento de regulaciones similares al Reglamento General de Protección de Datos (GDPR), hacen necesario que los empleados comprendan las implicaciones legales de un ataque cibernético y cómo proteger adecuadamente la información personal y sensible.

El papel de la alta dirección en la capacitación

Es fundamental que la alta dirección esté comprometida con la implementación de políticas de seguridad cibernética y que los líderes aseguren los recursos necesarios para capacitar de forma continua al personal. Como argumentan García y argumenta Flores-Romero (2023), la importancia de este compromiso radica en que se crea una cultura organizacional donde todos los empleados, independientemente de su rol, comprenden la importancia de la seguridad digital.

Así pues, la creación de una cultura de ciberseguridad robusta depende de que los empleados de todos los niveles estén alineados con los objetivos de seguridad de la organización. De igual forma, la colaboración entre departamentos, la comunicación clara de las políticas de seguridad y la disponibilidad de recursos para el entrenamiento constante son componentes esenciales para lograrlo (tabla 4).

Tabla 4. Proceso de capacitación que vincula estrategia con ciber

Capacitación en ciberseguridad	Descripción	Roles para su desarrollo
Identificación de phishing	Capacitación para detectar correos electrónicos y mensajes maliciosos.	Equipos de seguridad TI y departamentos de recursos humanos.
Respuesta a incidentes	Entrenamiento en protocolos de acción ante un ciberataque.	Equipos de respuesta a incidentes y alta dirección.

Capacitación en ciberseguridad	Descripción	Roles para su desarrollo
Simulacros de ataques	Realización de simulaciones de ataques para evaluar la capacidad de respuesta.	Equipos de seguridad y gerencia de operaciones.
Protección de datos personales	Formación en cumplimiento de regulaciones, como GDPR y manejo de datos sensibles.	Equipos legales y departamentos de <i>compliance</i> .
Uso seguro de redes sociales	Educación sobre los riesgos asociados con el uso de redes sociales en el trabajo.	Equipos de seguridad y comunicación interna.
Manejo de dispositivos móviles	Capacitación en seguridad para el uso de dispositivos móviles y BYOD.	Equipos de TI y recursos humanos.
Ingeniería social	Entrenamiento para evitar ser víctima de técnicas de manipulación humana.	Seguridad TI, recursos humanos y equipos de psicología organizacional.

Fuente: Elaboración propia.

Implementación de tecnologías avanzadas en la ciberdefensa

El uso de tecnologías avanzadas es un elemento esencial para una estrategia de ciberdefensa efectiva. Herramientas como los sistemas de detección y prevención de intrusiones (IDS/IPS), *firewalls* de próxima generación y soluciones basadas en inteligencia artificial ayudan a las organizaciones a detectar y neutralizar amenazas cibernéticas de manera proactiva. Estas tecnologías permiten automatizar muchas de las respuestas a ataques, lo que reduce significativamente el tiempo de reacción y mejora la eficiencia operativa en la protección de los sistemas críticos (Sánchez, 2023).

La inteligencia artificial, en particular, está transformando la ciberdefensa al proporcionar capacidades avanzadas de detección de amenazas. Mediante el uso de algoritmos de aprendizaje automático, es posible identificar patrones de comportamiento anómalos en grandes volúmenes de datos, lo cual facilita la detección de ataques en etapas tempranas. La IA también ayuda a las organizaciones a anticiparse a posibles amenazas, lo cual les permite implementar medidas de defensa antes de que los atacantes puedan explotar vulnerabilidades.

Colaboración interna y externa en la ciberdefensa

En el entorno actual de amenazas cibernéticas crecientes y cada vez más sofisticadas, la colaboración interna y externa se ha convertido en un componente fundamental de una ciberdefensa efectiva. La ciberseguridad ya no puede abordarse

como una responsabilidad exclusiva del departamento de TI o del equipo de seguridad de una organización; requiere un enfoque holístico que implique a todos los niveles y áreas de la empresa, desde la alta dirección hasta los empleados de línea. Asimismo, la colaboración con entidades externas, como agencias gubernamentales y organismos reguladores, es vital para construir una infraestructura de ciberseguridad robusta y resiliente. Este punto subraya la importancia de la cooperación interna y externa para mitigar los riesgos cibernéticos y garantizar una respuesta coordinada ante incidentes de seguridad.

Colaboración interna: un enfoque transversal

Una ciberdefensa efectiva dentro de una organización comienza con la colaboración entre departamentos. La integración de todos los actores internos es clave para que las medidas de seguridad no solo se implementen, sino que también se mantengan de manera coherente y efectiva. Esto implica la cooperación entre el departamento de TI, que es responsable de la infraestructura tecnológica; el equipo de seguridad encargado de la protección y respuesta ante incidentes; y la alta dirección, que proporciona la visión estratégica y los recursos necesarios para implementar una estrategia integral de ciberdefensa (Guzmán-Pacheco, 2022).

Para que esta colaboración sea exitosa, es necesario que cada área comprenda su rol y cómo su trabajo contribuye a la protección de la organización. El departamento de TI, por ejemplo, es el encargado de asegurar que la infraestructura tecnológica esté actualizada y protegida contra las amenazas. No obstante, sin el apoyo de la alta dirección, que debe asignar los recursos financieros y humanos necesarios, y sin la participación activa de todos los empleados, los esfuerzos del departamento de TI serán insuficientes. Por otro lado, el equipo de seguridad debe coordinarse con todas las áreas para que las políticas y los protocolos de seguridad se implementen de manera coherente en toda la organización.

Además, como se ha señalado, es esencial fomentar una cultura organizacional donde todos los empleados sean conscientes de la importancia de la ciberseguridad. Esto implica que las políticas de seguridad no se vean como algo exclusivo del equipo de TI, sino como una responsabilidad compartida por toda la empresa. Los trabajadores deben ser capacitados regularmente para estar preparados ante posibles ataques, lo cual incluye saber cómo responder y reportar incidentes cibernéticos. Según Fernández (2023), una de las mayores fallas en ciberdefensa ocurre cuando los empleados no tienen claros los protocolos de seguridad o no están preparados para actuar rápidamente ante un incidente.

Respuesta coordinada ante incidentes

La respuesta rápida y coordinada ante incidentes de seguridad es otro aspecto crucial de la colaboración interna. Para que la organización pueda minimizar el impacto de un ataque cibernético, es necesario que los protocolos de respuesta estén bien definidos y que todos los departamentos sepan cómo proceder en caso de un incidente. Esto requiere que los planes de contingencia y las respuestas a incidentes no sean responsabilidad exclusiva del equipo de seguridad, sino que involucren a toda la organización. Los departamentos de TI, operaciones, recursos humanos y comunicaciones, así como la alta dirección deben trabajar de manera conjunta para asegurar que la respuesta sea rápida, eficaz y minimice el impacto operativo y reputacional.

Un ejemplo de esta colaboración es la implementación de simulacros regulares de incidentes, en los cuales todos los departamentos participen para evaluar su preparación y coordinar su respuesta ante posibles ciberataques. Estos simulacros ayudan a identificar debilidades en la estrategia de ciberseguridad de la organización y permiten realizar ajustes en los protocolos de respuesta antes de que ocurra un incidente real. Al respecto, Nolasco-Mamani et al. (2022) argumentan que los simulacros no solo mejoran la capacidad de respuesta, sino que también fomentan la colaboración y la comunicación entre los distintos departamentos.

Colaboración externa: aliados estratégicos

La colaboración externa en la ciberdefensa es igual de importante que la interna. Las organizaciones no operan en un vacío, y cuando enfrentan amenazas cibernéticas, muchas veces la mejor defensa es aplicar un enfoque cooperativo que involucre tanto al sector privado como a entidades gubernamentales y otros organismos de seguridad cibernética. La colaboración con el sector externo es especialmente crítica en caso de un ataque de gran escala, donde los recursos internos pueden no ser suficientes para contener y mitigar el impacto del incidente.

El sector privado y las autoridades gubernamentales pueden proporcionar los recursos, la orientación y la asistencia técnica que resultan vitales para mitigar el impacto de un ciberataque. En particular, las agencias de ciberseguridad gubernamentales suelen disponer de recursos especializados que pueden ayudar a las organizaciones a analizar y gestionar incidentes cibernéticos. En muchos países, existen mecanismos de cooperación público-privada que permiten a las empresas compartir información sobre amenazas y acceder a conocimientos técnicos proporcionados por entidades especializadas, lo cual fortalece la ciberdefensa en su conjunto (Carlini, 2016).

Un buen ejemplo de esta colaboración es el trabajo conjunto entre empresas privadas y los CERT (Computer Emergency Response Teams), que proporcionan soporte y orientación en caso de incidentes cibernéticos. Estas organizaciones tienen acceso a información crítica sobre nuevas amenazas y tácticas utilizadas por atacantes, lo cual permite a las empresas ajustar rápidamente sus defensas. Según Alonso y Tejada (2017), la colaboración con los CERT ha sido fundamental para mejorar la respuesta global a ciberataques, lo cual ha proporcionado a las organizaciones el acceso a herramientas y conocimientos especializados que de otro modo no tendrían.

La colaboración entre sectores: el papel del gobierno y las organizaciones internacionales

La colaboración entre sectores va más allá del simple intercambio de información. En muchos casos, la cooperación con organismos internacionales es clave para enfrentar amenazas cibernéticas que traspasan fronteras. Los ciberataques, por su naturaleza, son problemas globales que requieren soluciones globales. Los organismos internacionales como la Interpol, la OTAN y otros grupos de seguridad globales tienen un papel fundamental porque proporcionan recursos y establecen protocolos de respuesta transnacionales. Esta cooperación es crucial, especialmente cuando se trata de ataques dirigidos a infraestructuras críticas que pueden tener consecuencias regionales o mundiales (Ramírez, 2023).

Además, las organizaciones internacionales trabajan en conjunto para crear normas y estándares de ciberseguridad que las empresas deben cumplir. Como se mencionó, un ejemplo de esto es el Reglamento General de Protección de Datos (GDPR) en la Unión Europea, que establece pautas claras para proteger la información personal y obliga a las empresas a garantizar la seguridad de los datos que manejan. El cumplimiento de estas normativas no solo protege a las organizaciones de sanciones legales, sino que también mejora sus capacidades de ciberdefensa al estandarizar las mejores prácticas en el mundo (Sánchez & Morales, 2022).

Beneficios de la colaboración en la ciberdefensa

Los beneficios de la colaboración en la ciberdefensa son numerosos. En el ámbito interno, la colaboración entre departamentos fortalece la capacidad de respuesta de la organización, mejora la comunicación y fomenta una cultura de seguridad. En el ámbito externo, la cooperación con el sector público y las organizaciones internacionales proporciona a las empresas los recursos y conocimientos necesarios para protegerse de amenazas cibernéticas complejas. Según Ramírez (2023),

las organizaciones que colaboran tanto interna como externamente están mejor preparadas para enfrentar los desafíos de la ciberseguridad y mitigar el impacto de los ciberataques.

En conclusión, la colaboración interna y externa es un componente esencial para consolidar una estrategia de ciberdefensa robusta. Las amenazas cibernéticas modernas requieren un enfoque cooperativo, tanto dentro de las organizaciones como en el contexto global. Al fomentar la colaboración entre departamentos y trabajar de la mano con agencias gubernamentales y entidades internacionales, las organizaciones pueden mejorar significativamente su capacidad de protegerse y responder a los ciberataques.

Conclusiones

La creciente complejidad del entorno digital ha subrayado la importancia crítica de la ciberseguridad y la ciberdefensa en la protección de los activos digitales de las organizaciones. Las amenazas cibernéticas, que han evolucionado en alcance y sofisticación, representan riesgos significativos para la confidencialidad, la integridad y la disponibilidad de la información. Ante estos desafíos, la integración de la ciberseguridad y la ciberdefensa en la estrategia organizacional, lejos de ser opcional, es esencial para garantizar la continuidad operativa y la protección de los datos sensibles, tanto de la empresa como de sus clientes. Las organizaciones que fallan en adoptar medidas preventivas y reactivas adecuadas quedan expuestas a un mayor riesgo de sufrir ataques que pueden comprometer no solo su infraestructura tecnológica, sino también su reputación y posición en el mercado (Ramírez, 2024).

El enfoque de ciberseguridad, con su énfasis en la prevención, debe complementarse con estrategias de ciberdefensa que permitan a las organizaciones detectar, responder y recuperarse de manera efectiva ante los incidentes. Las organizaciones que logran establecer un equilibrio entre la prevención y la respuesta están mejor preparadas para mitigar el impacto de los ciberataques. La implementación de medidas como la detección temprana de amenazas, los planes de respuesta a incidentes y la formación continua del personal se vuelven imprescindibles en este contexto. Sin estas acciones, la capacidad de una organización para enfrentar un ciberataque se reduce drásticamente, exponiéndola a mayores pérdidas financieras y reputacionales (Rincón-Gallón, 2022).

Además, la colaboración interna entre los distintos departamentos de la organización, desde el equipo de TI hasta la alta dirección, es fundamental para asegurar una ciberdefensa efectiva. Cada departamento debe estar alineado con los objetivos de seguridad de la empresa y participar activamente en la implementación y el mantenimiento de las medidas de ciberseguridad. Al mismo tiempo, la colaboración externa con entidades gubernamentales, agencias de seguridad y organismos internacionales es vital para compartir información sobre amenazas emergentes y mejorar las capacidades defensivas de la organización. La falta de colaboración, tanto interna como externa, limita la efectividad de cualquier estrategia de ciberseguridad (Guzmán-Pacheco, 2022).

Por otro lado, la ciberseguridad no solo protege los sistemas y datos de una organización, sino que también contribuye a su resiliencia y capacidad de adaptación frente a las nuevas amenazas. Las organizaciones deben estar preparadas no solo para prevenir ataques, sino también para recuperarse rápidamente y garantizar la continuidad de sus operaciones. En este sentido, la creación de una cultura organizacional sólida en torno a la ciberseguridad y la ciberdefensa, junto con la actualización constante de las tecnologías y estrategias de seguridad, es clave para mantener una ventaja competitiva en el mercado actual (Valderrama, 2024).

En conclusión, el camino hacia una ciberdefensa robusta requiere un enfoque integral que combine la prevención con la capacidad de respuesta ante incidentes, junto con una cultura organizacional orientada hacia la seguridad. Las organizaciones que inviertan en tecnología avanzada, formación continua para sus empleados y colaboración efectiva con agentes externos estarán mejor equipadas para enfrentar las amenazas cibernéticas actuales y futuras. En este sentido, la ciberseguridad y la ciberdefensa ya no pueden ser vistas como cuestiones técnicas aisladas, sino como elementos fundamentales en la estrategia general de cualquier organización que aspire a sobrevivir y prosperar en el entorno digital global (Sánchez & Morales, 2022).

Futuros trabajos

Los futuros trabajos en el área de ciberseguridad y ciberdefensa deben enfocarse en varios aspectos clave para continuar fortaleciendo las estrategias organizacionales frente a las amenazas emergentes. En primer lugar, es necesario investigar nuevas tecnologías, como la inteligencia artificial y el aprendizaje automático para la detección predictiva de amenazas. Estas herramientas tienen el potencial

de mejorar significativamente la capacidad de respuesta porque automatizan la identificación de patrones anómalos y reducen el tiempo de detección de ataques.

En segundo lugar, es fundamental explorar las implicaciones de la ciberseguridad en la cadena de suministro. A medida que las organizaciones dependen cada vez más de proveedores externos y sistemas interconectados, los ataques dirigidos a los socios comerciales pueden representar un riesgo importante. La investigación futura debería centrarse en el desarrollo de marcos de colaboración y protocolos de seguridad que fortalezcan la ciberdefensa en toda la cadena de valor.

Otro aspecto importante para el futuro es la creación de normativas y regulaciones internacionales más robustas y coherentes. A medida que las amenazas cibernéticas se globalizan, la capacidad de los marcos regulatorios nacionales es limitada para gestionar adecuadamente los ataques que traspasan fronteras. Por lo tanto, los futuros trabajos deben centrarse en cómo mejorar la cooperación internacional para abordar estas amenazas mediante la creación de acuerdos y estándares que unifiquen las mejores prácticas en el mundo.

También será esencial investigar el impacto de las nuevas tecnologías disruptivas, como la computación cuántica, en la ciberseguridad. Si bien estas tecnologías presentan oportunidades para mejorar las defensas, también plantean desafíos únicos en términos de la capacidad de los sistemas actuales para resistir ataques. El desarrollo de estrategias de defensa cibernética frente a las amenazas cuánticas debe ser una prioridad en la investigación futura.

Pese al creciente reconocimiento de la importancia de integrar la ciberseguridad y la ciberdefensa en la estrategia organizacional, aún son escasas las investigaciones empíricas que documenten casos exitosos y replicables en el contexto latinoamericano. Esta ausencia representa una oportunidad de investigación y desarrollo de capacidades en materia de gobernanza digital (Carreño & López, 2022).

La mayoría de los estudios se centran en propuestas teóricas o marcos de referencia genéricos, sin abordar cómo estos modelos han sido implementados en escenarios específicos. Por ello, resulta necesario desarrollar estudios de caso que documenten experiencias reales de integración en sectores críticos como salud, energía, banca o educación (Carlini, 2016).

Adicionalmente, los marcos metodológicos disponibles, como NIST CSF o COBIT, deben ser contextualizados a las realidades organizacionales locales, pues la transferencia de estos modelos a países en desarrollo enfrenta barreras como limitación de recursos, escasa capacitación o debilidad institucional (Sánchez, 2023).

En este sentido, la generación de conocimiento contextualizado es clave para fortalecer las capacidades locales. Investigaciones futuras podrían centrarse en cómo adaptar buenas prácticas internacionales a entornos con distintos niveles de madurez digital, infraestructura tecnológica y cultura organizacional (Bermúdez et al., 2023).

Otra línea prometedora de trabajo consiste en el análisis comparativo de políticas públicas regionales de ciberseguridad y ciberdefensa, pues esto permitiría identificar brechas, sinergias y oportunidades de cooperación entre países, con miras a construir un ecosistema digital más resiliente en América Latina (OCDE, 2020).

Referencias

- Akbanov, M., Vassilakis, V. G., & Logothetis, M. D. (2019). WannaCry Ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. *JTIT*, 75(1), 113-124. <https://doi.org/10.26636/jtit.2019.130218>
- Alonso, G. M. P., & Tejada, R. R. (2017). La cooperación público-privada en el fomento de la cultura de ciberseguridad. *Cuadernos de Estrategia*, (185), 217-246. <https://tinyurl.com/2z4dbvb6>
- Bermúdez Oviedo, M. Y., Téllez Florián, M. A., & Conde Urrea, C. A. (2023). *Gestión financiera y administrativa de las inversiones digitales en empresas del sector comercial financiero y de economía solidaria* [trabajo de grado, Universidad Cooperativa de Colombia, Bogotá]. Repositorio Institucional UCC. <https://tinyurl.com/65snauk9>
- Carlini, A. (2016). Ciberseguridad: un nuevo desafío para la comunidad internacional. *Boletín IEEE*, (2), 950-966. <https://tinyurl.com/yt44u768>
- Carreño, J., & López, A. (2022). *Resiliencia organizacional y ciberseguridad: Estrategias para la continuidad del negocio*. Editorial Cibertec.
- Casale, C. G. (2022). *La ciberdefensa como factor crítico en el desarrollo de operaciones militares en el nivel operacional* [trabajo final, Escuela Superior de Guerra Tte Grl Luis María Campos, Buenos Aires]. CEFADigital. <https://tinyurl.com/22tmc7dm>
- Fernández Delgado, L. (2023). *SIC Revista Ciberseguridad, seguridad de la información y privacidad*, 156. <https://revistasic.es/sic156/revistasic156.pdf>
- Flores-Romero, M. B., & González-Santoyo, F. (2023). *La dirección estratégica y su impacto en el desarrollo de la empresa de clase mundial*. Instituto Iberoamericano de Desarrollo Empresarial. <https://tinyurl.com/ys3dtame>
- González, J. (2020). *La ciberseguridad como eje central en la protección de infraestructuras críticas*. Instituto de Estudios Estratégicos.
- Guzmán-Pacheco, J. A. (2022). Importancia de una Ley de ciberseguridad y ciberdefensa para Colombia. *Revista Ciberespacio Tecnología e Innovación*, 1(1), 67-90. <https://doi.org/10.25062/2955-0270.4766>
- Jiménez-Almeira, G. A., & López, D. E. (2023). Ciberseguridad y seguridad integral: Un análisis reflexivo sobre el avance normativo en Colombia. *Revista Ibérica de Sistemas e Tecnologías de Informação*, (E62), 16-31 .
- Muñoz-Zambrano, C., & Zambrano-Rendón, A. D. (2023). Security Operations Center como modelo de gestión de ciberseguridad para el Hospital Especialidades de Portoviejo, Manabí, Ecuador. *MQRInvestigar*, 7(3), 3220-3236. <https://doi.org/10.56048/MQR20225.7.3.2023.3220-3236>

- Nolasco-Mamani, M. A., Vidaurre, S. M. E., & Choque-Salcedo, R. E. (2022). Innovación y Transformación Digital en la Empresa. ACVENISPROH Académico.
- Pacheco-Mangas, J., Palma-García, M. D. L. O., & Hombrados-Mendieta, I. (2020). Resiliencia y cultura organizacional de los Servicios Sociales en la era de la digitalización. *Prisma Social*, (29), 123–137. <https://tinyurl.com/59zj77ec>
- Pereyra Acosta, M. A. (2021). *La ley de gobierno digital y su implicancia en la ciberdefensa del Estado Peruano* [tesis doctoral, Universidad César Vallejo, Lima]. Repositorio Institucional UCV. <https://hdl.handle.net/20.500.12692/68971>
- Ramírez Acosta, A. J. (2024). Ciberdefensa como estrategia para la seguridad y soberanía digital en Paraguay. *Revista Jurídica. Investigación en Ciencias Jurídicas y Sociales*, 7(14), 16-41. <https://tinyurl.com/29l4uts6>
- Ramírez, P. (2023). La cooperación internacional en la ciberseguridad: Desafíos y oportunidades. *Revista de Seguridad Global*, 11(2), 22-40.
- Rincón-Gallón, M. F. (2022). Los factores armados de inestabilidad frente a la ciberseguridad y la ciberdefensa nacional. *Revista Ciberespacio, Tecnología e Innovación*, 1(1), 7-40. <https://doi.org/10.25062/2955-0270.4768>
- Rodríguez Rodríguez, C. G. (2020). La importancia de un plan de continuidad del negocio. <https://tinyurl.com/yc656434>
- Rueda Quintero, J. A. (2020). *Impacto de las técnicas de phishing en Colombia durante los últimos cinco años* [Trabajo de especialización, UNAD]. Repositorio institucional. <https://tinyurl.com/4427s3yc>
- Ruiz, J. (2022). Gestión de la cadena de suministro y resiliencia ante interrupciones tecnológicas. *International Journal of Supply Chain Resilience*, 6(1), 72-85.
- Rutz, G. (2021). Ciberdefensa como campo intelectual: Aportes y propuestas de investigación en ciberdefensa y ciberseguridad para la realidad argentina. *Revista de Estudios y Pesquisas sobre las Américas*.
- Sánchez, A. (2023). *La ciberdefensa en la Fuerza Terrestre ecuatoriana desde una visión prospectiva al 2033* [Tesis de maestría. Universidad de las Fuerzas Armadas ESPE]. Espositorio ESPE. <https://repositoriobe.espe.edu.ec/server/api/core/bitstreams/242f40a2-af64-45c9-b7c4-048f9895f392/content>
- Sandoval, O. (2022). Using cyber threat intelligence to support adversary understanding applied to the Russia-Ukraine conflict. <https://tinyurl.com/4dd3jzmu>
- UNIDIR (2022). *Cooperación internacional para mitigar las operaciones cibernéticas contra la infraestructura crítica*. Instituto de las Naciones Unidas para la Investigación sobre el Desarme. <https://unidir.org/files/2022-03/https://tinyurl.com/mrc3r6ef>

Valderrama Rojas, C. (2024). *Respuestas ante incidentes cibernéticos: Guía práctica para organizaciones*. Editorial Innovatec.

Valencia Soto, E. O. (2023). *Guía para el diseño de simulacros de incidentes de ciberseguridad a través de la adaptación de estándares y metodologías como ISO/IEC 27035, NIST SP 800-61 y NIST SP 800-84 en el Banco Popular* [Trabajo de grado, Universidad Piloto de Colombia]. Repositorio institucional. <https://tinyurl.com/2mz29xek>

Capítulo 5

Guía para la adopción de una cultura de ciberseguridad en juntas directivas^{*}

DOI: <https://doi.org/10.25062/9786287818002.05>

Milena Carvajal Bernal

Caja de Compensación Familiar Compensar

Resumen: Esta investigación propone un instrumento práctico para que las juntas directivas adopten una cultura de ciberseguridad, considerando elementos como la generación de conciencia entre sus integrantes y la gestión temprana de los riesgos que puedan impactar negativamente en la organización. Asimismo, se establece la innovación tecnológica como un factor relevante para la colaboración organizacional. Se reconoce al ser humano como un elemento clave en la solución de los desafíos en seguridad de la información y ciberseguridad, cuyo comportamiento y adopción de estrategias basadas en tecnología contribuyen a mejorar el entorno empresarial en esta materia. Se desarrolla bajo un enfoque cualitativo, basado en los resultados de encuestas y en el análisis de la información recopilada durante su ejecución. Como resultado y conclusión, se presenta una guía con elementos, pasos y recomendaciones para adoptar una cultura de ciberseguridad en las juntas directivas.

Palabras clave: ciberseguridad; cultura organizacional; gestión empresarial; innovación; tecnología.

^{*} Capítulo de libro resultado del proyecto de investigación “Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales” del grupo de investigación “Ciberespacio Tecnología e Innovación”, de la Escuela Superior de Guerra “General Rafael Reyes Prieto”, categorizado C por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) y registrado con el código COL0181179. Los puntos de vista y los resultados de este capítulo pertenecen al autor y no reflejan necesariamente los de las instituciones participantes.

Milena Carvajal Bernal

Magíster en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Especialista en Gerencia de Proyectos de Sistemas, Universidad del Rosario, Colombia. Ingeniera de sistemas, Universidad Manuela Beltrán, Colombia.

<https://orcid.org/0009-0006-9721-8541> - Contacto: carvajalmi@esdeg.edu.co

Citación APA: Carvajal Bernal, M. (2025). Guía para la adopción de una cultura de ciberseguridad en juntas directivas. En M. E. Realpe Díaz & G. A. Gómez Rodríguez (Eds.), *Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales* (pp. 157-196). Sello Editorial ESDEG.
<https://doi.org/10.25062/9786287818002.05>

CIBERSEGURIDAD EN LA FRONTERA DIGITAL: DESAFÍOS Y OPORTUNIDADES EN LOS NUEVOS ECOSISTEMAS TECNOLÓGICOS EMPRESARIALES

ISBN impreso: 978-628-7602-99-1

ISBN digital: 978-628-7818-00-2

DOI: <https://doi.org/10.25062/9786287818002>

Colección Ciberseguridad y Ciberdefensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2025



Introducción

La ciberseguridad debe considerarse un elemento esencial en las organizaciones. Su importancia en el contexto de la transformación digital requiere el respaldo de los niveles directivos para fomentar una cultura preventiva frente a escenarios de riesgo.

En Colombia, la promoción de una cultura de ciberseguridad ha sido objeto de discusión desde hace años. Documentos como el CONPES 3701 (2011) y la resolución AG/RES. 2004 (34-O/04) de la Organización de Estados Americanos (OEA, 2004) ofrecen lineamientos para la implementación de una cultura de ciberseguridad a nivel nacional y regional, respectivamente.

Por otro lado, en la era digital, la cultura y la tecnología están estrechamente relacionadas. La tecnología influye en el comportamiento de una sociedad al cambiar las prácticas culturales, y, a su vez, la dirección en la que avanza la tecnología está ligada estrictamente a lo que determine una sociedad (Goicoechea, 2004). Esta relación puede entenderse a través del principio de equifinalidad de la teoría general de sistemas (TGS), que sugiere que sistemas abiertos como la tecnología pueden alcanzar los mismos objetivos finales a partir de diferentes condiciones iniciales (Bertalanffy, 1989).

Un aspecto relevante en el campo de la tecnología es la cuarta revolución industrial, la cual se desarrolla a un ritmo acelerado, trayendo consigo desafíos significativos en términos de ciberseguridad, como la hiperconectividad de sistemas que genera brechas de seguridad considerables que deben ser abordadas desde todos los puntos de vista posibles. Por tanto, la concientización y comprensión de los riesgos latentes por parte de todos los sectores permitirá crear estructuras más conscientes que fomenten la colaboración entre las personas y las organizaciones, asumiendo una responsabilidad de prevención durante la cuarta revolución industrial (Schwab, 2016).

Sin embargo, una percepción común es que, cuando se habla de ciberseguridad, la mayor parte de las veces se cree que esta es una responsabilidad del equipo de tecnologías de la información (TI) y que no trasciende más allá de las fronteras tecnológicas, cuando, por el contrario, es un tema que debe ser responsabilidad de toda la organización, comenzando por las juntas directivas, quienes “no están tan involucradas en la ciberseguridad como lo están en otras áreas de supervisión” (Gale et al., 2022; Willie, 2023).

Esta mentalidad podría llevar a eventos con impactos negativos para las compañías y, a su vez, para las personas que conforman las juntas directivas. Estas últimas son quienes eventualmente deberán responder legalmente ante cualquier desviación o incumplimiento que se genere por su desconocimiento u omisión. Por lo tanto, para que haya un compromiso de los directores con la ciberseguridad, se requiere en muchos casos que exista una regulación, la cual es denominada por Gale et al. (2022) como “fuerza coercitiva”, que les obligue al cumplimiento de una ley para implementar medidas de ciberseguridad para la protección de la confidencialidad, integridad y disponibilidad de la información.

Tomando el ejemplo que relata Jen Pascua, director de la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA, por sus siglas en inglés), en el “Manual del director sobre supervisión de riesgos cibernéticos”, se plantea el caso de un CISO que propone implementar un sistema de doble factor de autenticación (MFA) para mitigar los riesgos de *phishing* en la compañía. Ante esto, los directores se niegan argumentando que el costo de implementación es muy alto en comparación con la probabilidad de un ataque cibernético, resultando en un ataque real con consecuencias negativas para la empresa (Clinton et al., 2023). Este es un claro ejemplo de cómo la responsabilidad de las juntas directivas es crucial en el contexto actual, en el que hay una gran brecha de conocimientos en cuanto a ciberseguridad y la adopción de una cultura organizacional al respecto.

Según el informe de IBM para el primer trimestre de 2023, los riesgos están aumentando exponencialmente, identificando que los vectores de ataque que más pérdidas generan incluyen atacantes internos, *phishing* y el compromiso de cuentas de correo dirigidas a los directivos (BEC, por sus siglas en inglés) (IBM Security, 2023). Esto evidencia que el ser humano y sus comportamientos son elementos que pueden poner en riesgo la seguridad empresarial, basado en sus prácticas (Cano, 2021), y, por lo tanto, deben contemplarse como parte integral de una estrategia de ciberseguridad corporativa (Willie, 2023).

El informe del Instituto de Auditores Internos (IIA, 2021) indica que, aunque los miembros directivos son conscientes de los riesgos de ciberseguridad, a menudo carecen del conocimiento y la preparación adecuados para abordarlos de manera efectiva. Esta falta de preparación se debe, en parte, a que la ciberseguridad aún se considera como "un problema principalmente técnico" (Gale et al., 2022, p. 4).

Para lograr un compromiso efectivo de la alta dirección en materia de ciberseguridad, resulta fundamental asignar recursos humanos y de infraestructura. No obstante, esto no es suficiente; las organizaciones también deberían establecer un comité directivo específico y un presupuesto exclusivo para la gestión de la ciberseguridad corporativa (Barrero & Bou, 2020).

Otra causa relevante, mencionada por Cano (2021), es el contexto interno, sustentado en la cultura organizacional:

Quando se reconoce el reto que implica analizar, estudiar y tratar de transformar una cultura organizacional, particularmente en seguridad de la información, es necesario ir más allá de la práctica estándar de los talleres de concientización, para dar paso a la comprensión de aspectos más profundos de la dinámica empresarial como pueden ser las estructuras de significados de los colectivos, los imaginarios de las personas sobre la temática y aquellos valores explícitos o tácitos que movilizan comportamientos de las personas más allá de cumplir un requisito normativo. (Cano, 2021)

En línea con lo anterior, un estudio realizado en España por Cyber Risk Culture de PricewaterhouseCoopers reveló que el 86 % de las empresas carecen de una cultura de ciberseguridad sólida en el entorno empresarial o deberían mejorarla. "Solo el 27 % de las compañías ya han realizado iniciativas de concientización a la Alta Dirección, mientras que el 68 % tiene planificado o está considerando realizar iniciativas de concientización a la Alta Dirección" (PricewaterhouseCoopers, 2020).

Dado este panorama, se evidencia un problema relacionado con la adopción de una cultura de ciberseguridad en las juntas directivas. Resulta necesario que estos líderes comprendan y aborden la importancia de fortalecer la ciberseguridad en todos los niveles de la organización, lo cual incluye una adecuada evaluación del impacto y las consecuencias de los riesgos asociados.

La cultura de ciberseguridad abarca múltiples componentes, entre los que se incluyen las personas, la tecnología y los procesos. Estos elementos se complementan con cualidades comportamentales que, según su orientación, pueden robustecer o debilitar la ciberseguridad organizacional. En este sentido, la alta dirección, al

constituirse como eje articulador de los distintos procesos organizacionales, debe promover un comportamiento cibernético seguro (Álvarez & Urrego, 2019).

En este contexto, surge una pregunta crucial: ¿cómo generar la adopción de una cultura de ciberseguridad en las juntas directivas? Como tesis, se plantea que dicha adopción es esencial para el cumplimiento efectivo de la estrategia corporativa y para una adecuada gestión del riesgo cibernético. En consecuencia, quienes ocupan cargos directivos deben contar con habilidades que contribuyan al fortalecimiento de la ciberseguridad organizacional, ya que tienen la responsabilidad de articular los procesos institucionales para el logro de los objetivos estratégicos y misionales.

El objetivo de esta investigación es establecer los elementos orientadores que faciliten la adopción de una cultura de ciberseguridad en las juntas directivas, reconociendo que el componente humano es determinante en la conformación de un ecosistema digital seguro. En tanto nivel estratégico de la organización, las juntas directivas deben liderar una estrategia de resiliencia cibernética adecuada, enfocada en la gestión de riesgos de ciberseguridad con el mismo nivel de prioridad con que se abordan los riesgos financieros u otros riesgos organizacionales (NIST, 2023, p. 25).

Cabe destacar que la adopción de una cultura de ciberseguridad puede variar entre organizaciones, en función de factores como el tamaño, el sector industrial y el nivel de madurez en la gestión de riesgos cibernéticos. Por lo tanto, los elementos orientadores aquí propuestos pueden utilizarse como base, según la etapa en la que se encuentre cada organización.

Metodología

Esta investigación se desarrolló a partir de un enfoque cualitativo, que “parte de la premisa de que el mundo social es ‘relativo’ y sólo puede ser entendido desde el punto de vista de los actores estudiados” (Hernández & Fernández, 2014). Según Vasilachis (2006), la investigación cualitativa se enfoca en el análisis de comportamientos de personas y organizaciones, mediante la recolección de datos y experiencias, que pueden abordarse en cualquier orden (Hernández & Fernández, 2014). Por su parte, la investigación cuantitativa busca “medir y estimar magnitudes de los fenómenos o problemas de investigación” (Hernández & Fernández, 2014, p. 5). En *Estrategias de investigación cualitativa*, Vasilachis (2006) señala que, según Strauss y Corbin, los datos, la interpretación y los escritos constituyen los componentes más relevantes de este tipo de investigación.

Con base en este enfoque, y siguiendo algunas prácticas descritas por Ruiz Olabuénaga (2012), esta investigación se estructuró en las siguientes fases de diseño:

Fase 1: Definición del problema. Se planteó la pregunta de investigación a partir de la identificación de la problemática y su viabilidad de estudio.

Fase 2: Recolección de datos. Se definieron las palabras clave asociadas al objeto de estudio y se realizó la búsqueda de artículos científicos, libros e informes relacionados. La información obtenida se clasificó tras el análisis de los resúmenes (abstracts) y la pertinencia de los documentos. Asimismo, en esta fase se desarrollaron y aplicaron encuestas orientadas a obtener un dato muestral sobre el estado de la cultura de ciberseguridad en juntas directivas.

Fase 3: Análisis de datos. Se procedió a la lectura detallada de los textos seleccionados y al análisis estadístico de los resultados de las encuestas.

Fase 4: Desarrollo de la pregunta de investigación y objetivos. A partir de los hallazgos de la fase anterior, se desarrolló el cuerpo de la investigación, respondiendo a la pregunta planteada y dando alcance a los objetivos, los cuales se abordan en los distintos apartados de este capítulo.

Elementos orientadores para la adopción de una cultura de ciberseguridad a nivel directivo

Este apartado presenta los elementos orientadores que permiten a los integrantes de las juntas directivas reconocer la ciberseguridad como un componente esencial de la estrategia empresarial. La ciberseguridad no puede continuar siendo percibida exclusivamente como una responsabilidad del departamento de TI; por tanto, resulta fundamental comprender no solo los aspectos técnicos, sino también los aspectos culturales organizacionales que favorecen la adopción de una cultura de ciberseguridad sólida en el nivel directivo.

“La alta dependencia de la infraestructura digital y el aumento en el uso y adopción de nuevas Tecnologías de la Información y las Comunicaciones (TIC) traen consigo una serie de riesgos e incertidumbres relacionados con la seguridad digital” (CONPES 3995, 2020, p. 3). Según el *Data Breach Investigation Report 2023*, elaborado por Verizon Business (2023), el 74 % de los incidentes de ciberseguridad tienen origen en errores humanos. Aunque existen soluciones destinadas a proteger a los usuarios y los sistemas tecnológicos frente a ataques cibernéticos, estas cifras evidencian la necesidad de contar con personal capacitado, con

habilidades cibernéticas desarrolladas desde etapas tempranas, que contribuyan a cerrar las brechas vinculadas al comportamiento humano y fomenten una cultura de seguridad digital (González, 2023).

Definición de la cultura de ciberseguridad

De acuerdo con Hofstede (1980), el concepto de cultura contempla cuatro dimensiones que reflejan el comportamiento de los individuos: la *distancia de poder*, que identifica el grado de aceptación de la distribución desigual del poder dentro de una organización; la *evasión de la incertidumbre*, entendida como la resistencia a situaciones ambiguas y la baja tolerancia a ideas o conductas desviadas; el *individualismo frente al colectivismo*, donde el primero refleja un interés centrado en uno mismo y el segundo una cohesión entre grupos internos y externos; y, por último, la *masculinidad*, que indica la orientación de una sociedad hacia valores considerados masculinos, marcando la brecha respecto a los valores femeninos.

En el ámbito investigativo, la cibercultura se define como la interacción compleja entre comunidades humanas, su entorno social, las tecnologías digitales y los medios de comunicación a través de dispositivos computacionales. Esta incluye tres componentes esenciales: cultura del conocimiento, cultura de la información y cultura de la comunicación (González et al., 2007).

La cultura de ciberseguridad se entiende como un conjunto de percepciones, actitudes, valores, suposiciones y conocimientos compartidos en una organización, que determinan su forma de operar y su capacidad para preservar la seguridad de sus activos de información. Este conjunto también tiene como objetivo moldear el comportamiento de los empleados hasta integrarlo como parte de sus *actividades cotidianas* (AlHogail & Mirza, 2014b). Por su parte, la Agencia de Ciberseguridad de la Unión Europea (ENISA, 2017) define la cultura de ciberseguridad organizacional como: "los conocimientos, creencias, percepciones, actitudes, supuestos, normas y valores de las personas en relación con la ciberseguridad y cómo se manifiestan en el comportamiento de las personas con las tecnologías de la información" (p. 7; trad. propia).

A partir de lo anterior, puede afirmarse que el comportamiento de las personas está condicionado por su entorno, las directrices que recibe y su percepción respecto a la interacción con la sociedad. En consecuencia, la adopción de una cultura de ciberseguridad en las organizaciones depende de las exigencias impuestas por un comportamiento considerado aceptable tanto por el grupo como por el entorno organizacional.

Importancia de la cultura de ciberseguridad

La cuarta revolución industrial y el proceso de transformación digital avanzan a un ritmo acelerado, generando desafíos significativos en materia de ciberseguridad, como la hiperconectividad de los sistemas, que da lugar a brechas de seguridad considerables y que deben ser abordadas desde múltiples perspectivas (Schwab, 2016). Uno de los principales riesgos en este contexto está relacionado con el comportamiento humano y el manejo de la información y los sistemas tecnológicos. Diversos estudios sobre cultura de seguridad concluyen que los *insiders* representan una amenaza latente para los activos de información de las organizaciones (AlHogail & Mirza, 2014a).

El informe de IBM Security indica que “las organizaciones con un alto nivel de escasez de habilidades de seguridad tuvieron un costo promedio de 5,36 millones de dólares” (IBM Security, 2023, p. 29), que representa un 30 % más en comparación con aquellas que poseen una postura y conocimientos más sólidos en ciberseguridad.

Esto muestra la importancia de fomentar una cultura de ciberseguridad dentro de las organizaciones, ya que permite mitigar los riesgos a los que estas se encuentran expuestas, en particular los derivados de comportamientos inadecuados por parte de sus colaboradores. Da Veiga y Eloff (2010) destacan que las “organizaciones requieren orientación para establecer una cultura de seguridad de la información” y que “necesitan medir e informar sobre el estado de seguridad de la información en la organización” (p. 1).

Asimismo, el análisis documental realizado por Uchendu et al. (2021) identificó un conjunto significativo de estudios (34 en total) que coinciden en que el apoyo, liderazgo y participación de la alta dirección es un factor fundamental para el desarrollo de una cultura organizacional de ciberseguridad (Uchendu et al., 2021).

En esta misma línea, Al-sartawi (2020) resalta “la importancia de nombrar a miembros de junta directiva con conocimientos y experiencia en TI”, dado que esto favorece la toma de decisiones más adecuadas frente a amenazas y desafíos cibernéticos (p. 1). Esta recomendación refuerza la necesidad de consolidar una cultura de ciberseguridad robusta.

Estudios de caso y ejemplos prácticos

Los siguientes casos ilustran la importancia de desarrollar una cultura de ciberseguridad organizacional como estrategia para reducir riesgos, mediante la concientización del personal.

Cómo Yahoo construyó una cultura de ciberseguridad

De acuerdo con Pearson et al. (2021), el grupo de investigación Sloan (CAMS) del MIT colaboró con Yahoo en la implementación de mecanismos para fortalecer su cultura de ciberseguridad. Inicialmente, se conformaron tres equipos con funciones específicas para promover la participación proactiva de los empleados: uno con capacidades técnicas, encargado de evaluar sistemas, servicios, procesos y personal para detectar vulnerabilidades; un segundo equipo, enfocado en la concientización en seguridad; y un tercero, especializado en ingeniería del comportamiento.

Durante el proceso, se distinguieron las diferencias entre acciones, hábitos y comportamientos, lo que permitió establecer objetivos de comportamiento como punto de partida para la implementación de medidas de cambio. A través del desarrollo de competencias y la introducción de incentivos, se logró modificar el comportamiento de los empleados, consolidando una cultura de ciberseguridad sólida.

Determinación de la madurez de la cultura de ciberseguridad organizacional

El estudio "Determining cybersecurity culture maturity and deriving verifiable improvement measures", realizado por Dornheim y Zarnekow (2023), evaluó el nivel de madurez de la cultura de ciberseguridad en una organización utilizando el marco propuesto por Da Veiga y Eloff (2010). Este marco se basa en seis dimensiones fundamentales que conforman el modelo de evaluación de la cultura en la protección de la información (IPCA), orientadas a medir "cómo los empleados perciben la protección de la información desde una perspectiva de ciberseguridad" (Dornheim & Zarnekow, 2023, p. 6; trad. propia).

El estudio, basado en encuestas aplicadas en dos momentos diferentes a una amplia muestra del personal, reveló que las dimensiones con mayores necesidades de desarrollo eran: 1) responsabilidad en materia de ciberseguridad, 2) compromiso en ciberseguridad y 3) efectividad de las políticas de ciberseguridad. Uno de los principales retos identificados fue aumentar el nivel de compromiso, dado que muchos empleados consideraban la ciberseguridad como un asunto trivial. Esta percepción motivó el diseño de una campaña dirigida a convencer a los directivos sobre la importancia estratégica de la ciberseguridad, desde donde se generó la comunicación hacia el resto del personal.

Adicionalmente, se llevaron a cabo actividades dirigidas tanto a empleados como a directivos y ejecutivos, entre las que se incluyeron talleres prácticos sobre el uso de herramientas de *phishing* y la clonación de sitios web, con el fin de demostrar la facilidad con la que puede ejecutarse un ciberataque.

Responsabilidades de la junta directiva en la creación de una cultura de ciberseguridad

El rol de la junta directiva puede interpretarse desde dos enfoques diferenciados: uno pasivo y otro activo. El enfoque pasivo está basado en una estructura jerárquica en la que el poder se concentra en el gerente general y el presidente, mientras que la junta se limita a aprobar la estrategia definida por el equipo gerencial. En contraste, el enfoque activo contempla a los miembros de la junta como pensadores independientes y autónomos en la definición de la dirección estratégica de la organización, aunque comparten con la gerencia la responsabilidad de cumplir con los objetivos organizacionales (Azuelo et al., 2020).

Actualmente, los altos directivos enfrentan una creciente frecuencia de ataques cibernéticos. De acuerdo con el equipo de Advice Group LATAM (2023), los tipos de ataque más comunes incluyen el *phishing* (44 %), estafas o *scamming* (33 %), *spyware* o *malware* (22 %) y *ransomware* (20 %). Pese a este panorama, los miembros de las juntas directivas consideran que no están preparados para hacer frente a un ataque cibernético. Una encuesta aplicada a 600 miembros de juntas directivas reveló que el 65 % considera que sus organizaciones están en riesgo de ser víctimas de un ciberataque en el corto plazo (Milică & Pearlson, 2023). Asimismo, el Foro Económico Mundial indica que el 95 % de los problemas de ciberseguridad se originan en errores humanos (World Economic Forum, 2022).

Frente a este contexto, la junta directiva debe asumir un papel de liderazgo en la promoción de la cultura de ciberseguridad a todos los niveles de la organización. Esto implica la identificación de responsabilidades, la supervisión de la seguridad organizacional y la implementación de cambios cuando sea necesario (Maurer et al., 2020). Este compromiso debe incluir la asignación de recursos humanos y de infraestructura para garantizar la implementación y el mantenimiento de medidas de ciberseguridad. Sin embargo, la sola disposición de estos elementos no resulta suficiente. Las organizaciones deben garantizar su operatividad mediante la conformación de un comité directivo específico y la asignación de un presupuesto exclusivo para la gestión de la ciberseguridad (Barrero & Bou, 2020).

ENISA (2017) señala que la alta dirección tiene la responsabilidad directa en materia de ciberseguridad, la cual debe entenderse como una fuente para la toma de decisiones estratégicas. Esta debe considerarse una inversión destinada a la reducción de riesgos asociados a pérdidas financieras, daño reputacional, sanciones legales por incumplimiento normativo y exigencias de los accionistas:

Para cambiar la cultura, la alta dirección debe utilizar una serie de instrumentos, como las declaraciones de valores, la comunicación interna, la educación, y debe predicar con el ejemplo a través de sus comportamientos en apoyo de sus declaraciones visionarias. (ENISA, 2017, p. 32)

La OEA (2019) señala que “no es responsabilidad de la junta convertirse en expertos en TI, pero la junta debe saber qué preguntas hacerles a los departamentos de TI” (p. 8). Así, se debe establecer un seguimiento periódico para asegurar que los responsables mantengan los controles de ciberseguridad necesarios para la operación de la organización.

De manera complementaria, la Asociación Nacional de Directores de Empresas (NACD, por sus siglas en inglés) enfatiza la necesidad de contar con un modelo sostenible, empezando por un compromiso de la alta dirección que promueva una cultura de ciber-responsabilidad. Esta debe incluir una gestión efectiva del riesgo cibernético, reconociendo que los miembros de las juntas directivas poseen un poder único para garantizar que los Oficiales de Seguridad de la Información (CISO) dispongan de la influencia y los recursos adecuados para liderar la estrategia de ciberseguridad a nivel corporativo (Clinton et al., 2023).

En el contexto latinoamericano, el documento CONPES 3995 (2020) recomienda el desarrollo de programas de formación para niveles directivos y ejecutivos, con el objetivo de dotarlos de las competencias necesarias para gestionar los riesgos en seguridad digital.

Los ejecutivos deben asumir un rol activo en la integración de la cultura de ciberseguridad, adecuándola a sus perspectivas y necesidades, de modo que puedan reconocer y responder adecuadamente a una realidad transformada por los riesgos emergentes en este ámbito (Cano, 2023).

Uno de los principales desafíos en la consolidación de una cultura de ciberseguridad en las juntas directivas es la falta de concientización. Esta se manifiesta en la carencia de preparación para tomar decisiones informadas, lo que impide dimensionar de forma adecuada el impacto y las consecuencias de los riesgos cibernéticos dentro de las organizaciones.

Las causas identificadas para la limitada adopción de una cultura de ciberseguridad en las juntas directivas son las siguientes:

- *Falta de previsión sobre las consecuencias de la ciberseguridad como riesgo latente.* Para supervisar adecuadamente este tipo de riesgos, es imprescindible que comprendan las responsabilidades que les competen, ya que la toma de decisiones en esta materia no puede ser delegada a estructuras operativas (Clinton et al., 2023).

- *Ausencia de un ecosistema digital robusto o insuficiente presupuesto.* La inversión adecuada es esencial para enfrentar los desafíos de ciberseguridad. De acuerdo con un informe de PricewaterhouseCoopers (2020), solo el 9 % del presupuesto de seguridad de la información de las empresas se destina a actividades de formación y concientización para fortalecer una cultura de ciberseguridad.
- *Percepción de la ciberseguridad como un tema exclusivamente tecnológico.* En la encuesta de la OEA (2018) sobre protección de infraestructuras críticas en América Latina y el Caribe, el 42 % de los encuestados indicó que los esfuerzos de ciberseguridad son supervisados por el departamento de TI. Solo el 13 % señaló que dicha responsabilidad recae en el nivel C-Level, y apenas un 4 % mencionó a otras áreas como encargadas de esta función (OEA, 2018, p. 38).

La falta de reconocimiento del alcance estratégico de la ciberseguridad, la escasa inversión y la limitada conciencia sobre los impactos de los riesgos cibernéticos pueden convertirse en una ventaja para los atacantes, quienes se aprovechan de estas debilidades para obtener beneficios.

Así, esta investigación busca identificar aquellos elementos que favorecen la generación de una cultura de ciberseguridad en los que las juntas directivas deben enfocarse en cuanto a ciberseguridad.

Elementos orientadores para una cultura de ciberseguridad

Para establecer elementos orientadores que guíen de manera eficaz la cultura de ciberseguridad en las juntas directivas, resulta fundamental identificar las características propias de este grupo de líderes que pueden actuar como catalizadores en la adopción rápida y efectiva de prácticas en este ámbito. Álvarez y Urrego (2019) introducen los criterios básicos de éxito (CSF), como componentes esenciales que favorecen el desarrollo organizacional y el logro de objetivos. Estos criterios incluyen la confianza, los sistemas de información, la comunicación intraorganizacional, la estructura organizativa y los mecanismos de incentivos, todos los cuales contribuyen a una transferencia efectiva del conocimiento en ciberseguridad.

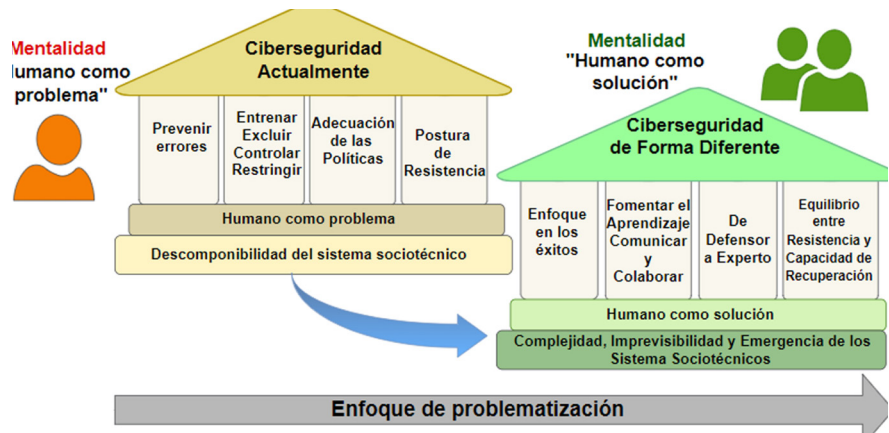
Diferentes elementos conforman el andamiaje necesario para una cultura de ciberseguridad que promueva comportamientos preventivos dentro de la organización. Entre ellos, el factor humano se destaca como un recurso estratégico de

alto valor. En este sentido, Zimmermann y Renaud (2019) proponen un cambio de paradigma al afirmar que:

La mentalidad “diferente” reconoce la capacidad del ser humano bien intencionado para ser un contribuyente importante a la ciberseguridad organizacional, así como su potencial para ser “parte de la solución” en lugar de “el problema”. En esencia, este nuevo enfoque trata inicialmente a todos los humanos en el sistema como si fueran bien intencionados. (p. 168; trad. propia)

Aunque tradicionalmente el ser humano ha sido percibido como el eslabón más débil en la cadena de seguridad de la información, es precisamente en este punto donde debe invertirse dicha percepción. En lugar de concebirlo como una amenaza, debe ser reconocido como un agente clave capaz de robustecer la cultura de ciberseguridad (figura 1).

Figura 1. El ser humano como problema; el ser humano como solución.



Fuente: Elaboración propia con base en Zimmermann y Renaud (2019, p. 179)

Con este contexto, el ser humano se define como un elemento crítico en materia de ciberseguridad. Por tanto, resulta esencial establecer los elementos necesarios para fomentar una cultura de ciberseguridad en las juntas directivas, mediante la implementación de políticas adecuadas y la generación de conciencia. Reconocer al ser humano como un componente clave de esta cultura implica un cambio de perspectiva, en el cual su intervención se concibe como un aspecto positivo y de la cultura de ciberseguridad.

En consecuencia, se seleccionaron tres referentes teóricos que identifican elementos esenciales para el desarrollo de una cultura de ciberseguridad sólida:

ENISA, Isabella Corradini y PricewaterhouseCoopers Asesores de Negocios. Estos autores abordan el tema desde una perspectiva integral que promueve la sinergia entre personas, procesos y tecnología.

De acuerdo con ENISA (2017), una cultura de ciberseguridad eficaz requiere la adopción de un enfoque adecuado que fortalezca la resiliencia de los activos de información. Para ello, identifica elementos clave como los conocimientos, creencias, percepciones, actitudes, suposiciones, normas y valores.

De manera complementaria, Corradini (2020) agrupa los elementos de la cultura organizacional en tres categorías fundamentales: artefactos, valores y supuestos básicos, subdivididos a su vez en concientización, valores y principios, comportamiento. Señala también la relevancia del conocimiento en seguridad de la información.

Por su parte, PricewaterhouseCoopers (2020) propone cuatro dominios principales para evaluar el nivel de cultura de ciberseguridad en las organizaciones: estrategia, conocimiento, comportamiento y perspectiva futura.

En la tabla 1 se presentan los criterios identificados por cada autor, los cuales constituyen la base para el desarrollo de una guía orientadora en la adopción de una cultura de ciberseguridad desde las juntas directivas.

Tabla 1. Elementos orientadores para establecer una cultura de ciberseguridad

Autor	Elementos
ENISA (2017)	Conocimientos
	Creencias
	Percepciones
	Actitudes
	Suposiciones
	Normas
	Valores
Isabella Corradini (2020)	Concientización
	valores y principios
	Interacción con la tecnología
	Comportamiento
	Conocimiento
Pricewaterhouse Coopers Asesores de Negocios, S.L. (2020)	Estrategia
	Conocimiento
	Comportamiento
	Perspectiva futura

Fuente: Elaboración propia

Como resultado del análisis realizado y documentado en la tabla 1, se evidencia la coincidencia de varios elementos entre los autores. Por tanto, para efectos de esta investigación se seleccionaron los elementos orientadores conocimiento, normas, valores, concientización, estrategia y comportamiento, considerados como claves para establecer una guía integrada que permita abordar de manera efectiva la cultura de ciberseguridad en la organización, enfocándose en los miembros de juntas directivas como líderes de la estrategia de ciberseguridad corporativa.

Estos elementos orientadores se toman como base debido a la relevancia que les atribuyen los autores, por lo que los miembros de las juntas directivas deberán identificar cómo se alinean con los valores y estrategias propias de sus organizaciones para el establecimiento de una cultura de ciberseguridad corporativa. Estas validaciones pueden realizarse mediante cuestionamientos que permitan determinar si la junta requiere actualizaciones periódicas en materia de ciberseguridad a través de expertos en la materia. Asimismo, resulta pertinente que los miembros de las juntas incorporen en sus conversaciones datos relevantes sobre ciberseguridad que puedan impactar a la organización, analizando cómo las decisiones comerciales contemplan los riesgos cibernéticos. Una alternativa adicional para mantenerse actualizados consiste en asistir a conferencias especializadas o en optar por certificaciones que fortalezcan su conocimiento en ciberseguridad.

En el siguiente acápite se contrastan los elementos orientadores con los criterios evaluadores que permiten identificar el nivel de familiarización de los miembros de las juntas directivas con las capacidades humanas, administrativas y tecnológicas necesarias para la adopción de una cultura de ciberseguridad.

Criterios evaluadores para medir el nivel de cultura de ciberseguridad en juntas directivas

La ciberseguridad ha adquirido un espacio relevante y urgente como componente estratégico en las organizaciones, por lo que la adopción y el compromiso hacia una cultura de ciberseguridad deben comenzar desde los niveles más altos de la estructura organizativa. Las juntas directivas, en tanto responsables de definir el rumbo estratégico de las organizaciones, deben integrar y fortalecer esta cultura para su adopción en todos los procesos.

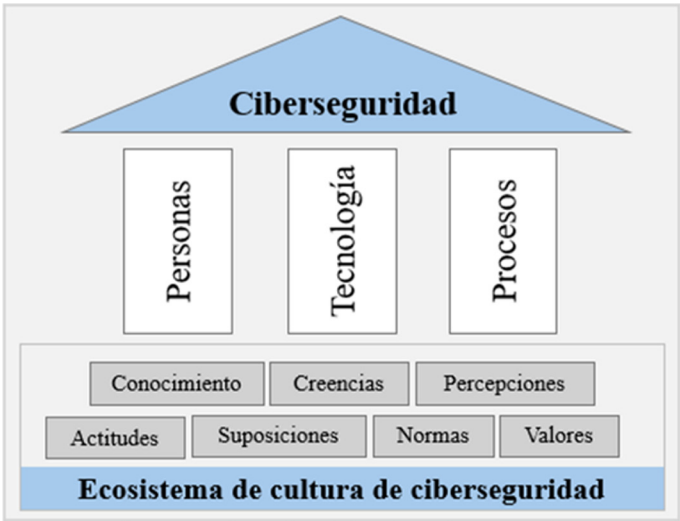
La ciberseguridad se sustenta en tres pilares fundamentales: *personas*, *tecnología* y *procesos*, los cuales son interdependientes y deben funcionar

de manera armónica para el fortalecimiento de una cultura de ciberseguridad (PricewaterhouseCoopers, 2020). Estos pilares se relacionan directamente con las *capacidades humanas, tecnológicas y administrativas* de cada organización.

Definición e importancia de los criterios evaluadores

Establecer una cultura de ciberseguridad implica desarrollar un ecosistema que la respalde, fundamentado en los pilares de personas, tecnología y procesos (Álvarez & Urrego, 2019) (figura 2).

Figura 2. Ecosistema de cultura de ciberseguridad.



Fuente: Álvarez y Urrego (2019).

En primer lugar, se encuentran las personas, por lo que la concientización y capacitación resultan fundamentales para mitigar el error humano, considerado la causa más común de fallas tecnológicas relacionadas con la ciberseguridad (Steele, 2024).

Los procesos constituyen el soporte para establecer políticas y procedimientos destinados a proteger la información, basándose en el cumplimiento de normas, estándares y buenas prácticas, y asegurando que los empleados estén alineados con dichas políticas (Da Veiga & Eloff, 2010).

La tecnología, por su parte, respalda el aseguramiento de la información; no obstante, debe garantizarse la generación de conocimiento respecto al uso

adecuado de las herramientas de TI, de modo que se mantengan alineadas con las necesidades de la organización y actualizadas para prevenir amenazas emergentes. En este sentido, resulta crucial considerar cómo la organización construye valores, conocimientos y comportamientos basados en el uso de las herramientas tecnológicas (AlHogail & Mirza, 2014a).

Estos pilares se consolidan como criterios o capacidades —humanas, administrativas y tecnológicas— orientadoras para proteger la información y generar un ambiente de cibercultura resiliente.

Métodos de evaluación

En el marco de este proyecto de investigación, se llevó a cabo una encuesta destinada a evaluar el nivel de cultura organizacional en materia de ciberseguridad entre miembros de juntas directivas, roles de C-Level, Oficiales de Seguridad de la Información y Gerentes de diversas empresas. A través de esta herramienta se recopilaron datos esenciales de dieciséis participantes pertenecientes a los roles mencionados, conforme se detalla en la tabla 2. Se utilizó un sistema de encuesta semiestructurada por conveniencia, dada la identificación previa de los actores relevantes cuyas respuestas resultaban fundamentales para el desarrollo del ejercicio.

La encuesta incluyó el consentimiento informado, en cumplimiento de lo dispuesto en la Ley 1581 de 2012 y en el Decreto 1377 de 2013. Asimismo, se dejó a voluntad de los encuestados el registro de sus nombres, apellidos y la identificación de la organización a la que pertenecen.

La encuesta se enfocó en medir la comprensión de los participantes respecto a las capacidades humanas, administrativas y tecnológicas de sus organizaciones, alineadas a los elementos orientadores previamente definidos.

Tabla 2. *Participantes por roles*

Rol	Cantidad
Chief information and security officer (CISO)	7
Integrante de junta directiva	4
Director de área	3
Chief executive officer (CEO)	2

Fuente: Elaboración propia.

Capacidades humanas

Ante la pregunta: ¿Qué entiende por cultura de ciberseguridad?, el 75 % de los encuestados asoció el concepto con la adopción de un conjunto de valores, actitudes y buenas prácticas para proteger sus sistemas, redes y datos frente a amenazas cibernéticas. Por su parte, el 25 % relacionó el término más directamente con los procedimientos y tecnologías destinadas a garantizar la confidencialidad, integridad y disponibilidad de la información. Este resultado evidencia la necesidad de implementar programas de concientización y fortalecer el conocimiento en todos los niveles de la organización, comenzando por los miembros de juntas directivas y los cargos ejecutivos.

Una manera de evaluar los esfuerzos de las organizaciones por mejorar la comprensión de la cultura de ciberseguridad es validar la frecuencia con la que se realizan campañas en torno a este tema. Como resultado, el 19 % indicó que se hacen anualmente, otro 19 % señaló que se realizan semestralmente, el 56 % respondió que son llevadas a cabo trimestralmente y el 6 % indicó que no se hacen. Estas respuestas demuestran que, en su mayoría, las organizaciones manifiestan un interés por promover el conocimiento sobre cultura de ciberseguridad a través de campañas periódicas.

Una validación importante en esta investigación fue conocer cómo se perciben las responsabilidades en la organización. Para ello, se formuló la siguiente pregunta: ¿Considera que la ciberseguridad es una responsabilidad del área de TI/ Tecnología? El 25 % respondió afirmativamente, mientras que el 75 % consideró que no lo es. Aunque la mayoría no atribuye la responsabilidad exclusivamente al área tecnológica, preocupa que aún exista un porcentaje que sí lo hace. Esta percepción constituye una de las variables identificadas como parte del problema y refleja la necesidad de un cambio de perspectiva.

La creencia de que el área de TI es la principal responsable puede estar relacionada con la asociación directa del término *ciberseguridad* con aspectos tecnológicos, dejando de lado el componente conductual y la responsabilidad individual que implica la toma de decisiones en esta materia.

Dentro de la medición de cultura de ciberseguridad se buscó identificar si existe un plan de capacitación en esta materia dirigido a los miembros de la junta directiva en sus organizaciones. Los resultados muestran que solo el 56 % de los miembros ha recibido algún tipo de capacitación, mientras que el 44 % no ha sido capacitado.

Este hallazgo pone en evidencia la urgencia de que los miembros de juntas directivas desarrollen una conciencia sólida en torno a la ciberseguridad, que les

permita contar con herramientas cognitivas adecuadas para la toma de decisiones acertadas al respecto.

Como parte de las validaciones realizadas, se investigó lo siguiente: Si su organización ya cuenta con una implementación de cultura de ciberseguridad, ¿cuál considera que fue el reto más complicado de abordar?

El 31 % identificó como principal reto la definición de la estrategia para la implementación de la cultura de ciberseguridad; otro 31 % señaló la asignación de presupuesto para disponer de los recursos necesarios. El 19 % consideró que el mayor desafío fue el gobierno en la definición del modelo de cultura de ciberseguridad, mientras que el 13 % indicó como dificultad la evaluación de la madurez y del comportamiento en torno a dicha cultura. Finalmente, el 6 % manifestó no contar aún con una implementación de cultura de ciberseguridad.

Capacidades administrativas

Las organizaciones deben proveer los recursos necesarios para la ciberseguridad. Con el objetivo de identificar si esta condición se cumple, se planteó la siguiente pregunta: ¿Qué área se encarga de la ciberseguridad en su organización?

El 63 % de las respuestas indicó que esta responsabilidad recae en el área de TI, el 19 % señaló al área de riesgo y cumplimiento, un 6 % mencionó el área de seguridad, otro 6 % indicó la dirección de sistemas de información y el 6 % restante señaló al proceso de continuidad del negocio como encargado. Con estos resultados, se observa que el área de TI concentra una alta asignación de responsabilidades en la gestión de la ciberseguridad.

La siguiente validación se realizó para obtener una aproximación sobre la relevancia de la ciberseguridad en las organizaciones, determinando: ¿Qué porcentaje del presupuesto anual está destinado a la ciberseguridad en su organización?

Los resultados revelan una cifra que sustenta una de las causas de la problemática de esta investigación, relacionada con la ausencia de un ecosistema digital o el bajo presupuesto asignado en las organizaciones. El 38 % de los encuestados indicó que se destina menos del 5 % del presupuesto; el 19 % señaló una asignación entre el 5 % y el 10 %; el 25 % informó que el presupuesto asignado está entre el 10 % y el 20 %, y ningún encuestado reportó asignaciones superiores a este rango. Solo el 6 % indicó que el presupuesto asignado supera el 20 %, mientras que el 13 % manifestó desconocer la cifra correspondiente a su organización.

Se planteó un interrogante con el fin de determinar si se están gestionando de manera adecuada los riesgos cibernéticos: ¿La junta directiva tiene conocimiento

de los riesgos cibernéticos a los que está expuesta la organización y de las posibles consecuencias en términos legales, financieros, operacionales y/o reputacionales?

El 81 % de los encuestados respondió afirmativamente, el 13 % indicó no estar seguro/a y el 6 % manifestó no conocer los riesgos cibernéticos. Este último resultado confirma que algunos integrantes de las juntas directivas toman decisiones para la organización sin tener conciencia del impacto que podría generar la materialización de un riesgo cibernético. Esta validación resulta relevante para conocer las tendencias organizacionales, como una forma de apoyar y mantener actualizados los planes y protocolos de contingencia definidos frente a las amenazas cibernéticas.

Ante la pregunta: ¿Se incluye a la junta directiva en el proceso de toma de decisiones durante incidentes cibernéticos críticos o de alto nivel? El 56 % respondió que siempre, el 25 % indicó que ocasionalmente y el 19 % manifestó que nunca se incluye a la junta para este tipo de decisiones. Esta actividad cobra gran relevancia, ya que, aunque los directivos no deben ser expertos técnicos, sí deben contar con las capacidades generales necesarias para identificar el impacto que un incidente cibernético puede generar en términos legales, económicos o de afectación a la imagen organizacional.

En línea con la pregunta anterior, se investigó lo siguiente: ¿Ha participado en algún ejercicio de simulación de riesgo cibernético en donde la junta directiva deba tomar decisiones frente a un incidente cibernético? El 69 % respondió no haber participado, el 25 % indicó que sí ha participado y el 6 % señaló que, aunque no ha participado, sí ha estado informado. La colaboración de la junta directiva en este tipo de simulaciones proporciona una visión general sobre cuál debería ser su enfoque ante un incidente o la materialización de un riesgo cibernético real.

Capacidades tecnológicas

Respecto a las capacidades tecnológicas, se indagó lo siguiente: ¿Conoce si su organización cuenta con las herramientas tecnológicas y procedimientos necesarios para una adecuada gestión de la ciberseguridad? El 81 % de los encuestados indicó que sí cuentan con herramientas para una adecuada gestión de la ciberseguridad, mientras que el 19 % señaló que no disponen de las herramientas necesarias para su debida gestión.

Frente a la postura de ciberseguridad de su organización, se planteó la siguiente pregunta: ¿Conoce cuáles son los índices de seguridad de sus socios estratégicos o proveedores y cómo podrían impactar a su organización en caso de que estos sufran un incidente cibernético?

El 56 % indicó conocer algunos índices de seguridad de sus terceros, pero no de todos; solo el 6 % conoce el detalle y cómo podría afectarle a su organización; el 19 % tiene una idea general, pero no conoce el detalle ni el impacto que un incidente cibernético de un tercero podría generar; el 13 % señaló que la gestión de la ciberseguridad es manejada por otro departamento o equipo en la organización; y el 6 % manifestó desconocer los índices de seguridad de sus socios o terceros. Dado el resultado de esta pregunta, se infiere que, al delegar la responsabilidad de la gestión de la ciberseguridad en otras áreas, la junta directiva cede su obligación de reconocer la exposición a los riesgos cibernéticos.

Con base en las respuestas anteriores, se identifica que el *conocimiento*, los *valores* y la *concientización* forman parte de los componentes presentes en las juntas directivas. El conocimiento permite que las personas comprendan las reglas, funciones y comportamientos necesarios para la toma de decisiones informadas. A su vez, promover un comportamiento alineado con los valores de la organización facilita que los colaboradores adopten dichos valores en sus actividades cotidianas, mientras que la concientización en ciberseguridad se ha ido normalizando en las organizaciones.

A pesar de esto, los elementos de *norma*, *estrategia* y *comportamiento* no muestran aún un nivel de madurez suficiente y requieren un mayor fortalecimiento en las juntas directivas, según las respuestas obtenidas. Por ejemplo, la inversión en ciberseguridad depende de la autonomía de cada organización, ya que no existe una normatividad que exija destinar un porcentaje específico del presupuesto anual a este aspecto.

Por otra parte, uno de los retos más difíciles de abordar en las organizaciones es el desarrollo de una estrategia efectiva para la formación y concientización en cultura de ciberseguridad. En cuanto al comportamiento, se observa que las responsabilidades en temas de ciberseguridad recaen usualmente sobre el área de TI, y aunque la junta directiva es incluida en el proceso de toma de decisiones durante incidentes cibernéticos críticos, no siempre cuenta con la preparación necesaria que le permita actuar con mayor experticia en este campo.

Estudio de caso

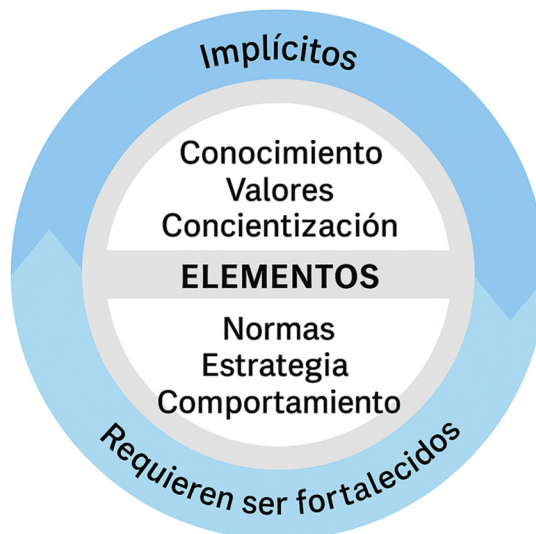
Onumo et al. (2021), en su investigación aplicada a tres empresas, desarrollaron un modelo combinando teorías relacionadas con el comportamiento planificado, valores competitivos, y los factores tecnológicos, organizacionales y ambientales, con el fin de validar los valores culturales asociados a los mecanismos adoptados

por los empleados. Como resultado, identificaron que el comportamiento de las personas se asocia directamente a los elementos organizacionales y a los procesos, mientras que las creencias se ven moderadas por las tecnologías de información. Onumo et al. (2021) señala como un desafío las múltiples interpretaciones de la cultura de seguridad en la literatura, por lo que invita a considerar cómo los factores organizacionales, los mecanismos de comportamiento y el entorno tecnológico pueden persuadir e influir en las personas.

Con base en los resultados obtenidos en esta investigación, se destacan en la figura 3 los elementos que están implícitos o que requieren fortalecimiento en las juntas directivas para la adopción de una cultura de ciberseguridad. Estos elementos demandan la promoción de una mentalidad de seguridad proactiva. Asimismo, es fundamental que las juntas directivas impulsen la formación continua en ciberseguridad y establezcan mecanismos de vigilancia y evaluación que aseguren que las acciones implementadas se mantengan actualizadas y eficaces ante las amenazas emergentes.

En este sentido, vale la pena resaltar que los directivos deben validar y fomentar la cultura de ciberseguridad en sus organizaciones, basándose en las capacidades y elementos que les permitan fortalecer su resiliencia frente a incidentes cibernéticos.

Figura 3. Estado de apropiación de los elementos necesarios para una cultura de ciberseguridad en las juntas directivas.



Fuente: Elaboración propia.

Guía de elementos y pasos para adoptar una cultura de ciberseguridad en juntas directivas

Las juntas directivas, debido a su rol relevante en las organizaciones, deben impulsar las políticas e inclinarse por mantener una estrategia que fomente una cultura de ciberseguridad sólida. Se requiere un compromiso adecuado por parte de las juntas directivas, donde sus capacidades conduzcan a la organización y a todos sus integrantes hacia un nivel adecuado de concientización en temas de ciberseguridad (Cyber Citadel, 2023).

De acuerdo con lo desarrollado en el acápite anterior, en el cual se identificaron los elementos que están implícitos en las organizaciones y que contribuyen al desarrollo de la cultura cibernética, también se evidenciaron algunos aspectos que deben ser fortalecidos para estructurar de manera adecuada las capacidades y aptitudes de los miembros de la junta directiva como estrategias y líderes en la implementación de la ciberseguridad organizacional.

En este acápite se detallan los elementos que guiarán a los directivos en la adopción de una cultura de ciberseguridad, la cual podrá extenderse posteriormente a toda la organización. Estos elementos se apoyan en sus respectivos pasos, que brindan recomendaciones clave para su implementación. Finalmente, se presentan algunas preguntas de reflexión que pueden ser útiles antes y durante el proceso de desarrollo de una cultura de ciberseguridad.

Estrategia

De acuerdo con PricewaterhouseCoopers (2020), la estrategia debe enfocarse en aumentar las capacidades existentes en la junta directiva y profundizar en la concientización sobre el impacto de la ciberseguridad en la organización. La estrategia para desarrollar una cultura de ciberseguridad debe considerar la importancia de vincular a las personas, la tecnología y los procesos. Las personas, como recurso primordial, deben incluirse en planes específicos que contemplen temas como la gestión de incidentes cibernéticos y la toma de decisiones ante la materialización de riesgos de ciberseguridad.

Según Giraldo Ríos (2024), "las empresas deben considerar la estrategia como un todo y empezar a implementarla o corregirla gradualmente, según su ritmo de adaptación" (p. 19). Contar con una estrategia permitirá, a su vez, conocer la postura de la organización frente a la ciberseguridad y facilitar la construcción del programa de concientización (Schneider et al., 2020).

El desarrollo de la estrategia debe contemplar varios pasos que orienten una implementación ordenada. Con base en la literatura estudiada, se proponen los siguientes pasos para desarrollar el elemento orientador *Estrategia*.

Paso 1. Medir el nivel de madurez en cultura de ciberseguridad de la junta directiva

La adopción de una cultura de ciberseguridad debe ser una tarea medible, y uno de los mecanismos para ello es la utilización de un modelo de madurez que permita identificar fortalezas y aspectos de mejora en su implementación y mantenimiento a lo largo del tiempo.

Diversos autores han diseñado marcos aplicables desde distintas perspectivas, entre los cuales se encuentran modelos para determinar comportamientos orientados a la seguridad de la información, cumplimiento de políticas de seguridad de la información, medición de la apropiación de la cultura de ciberseguridad organizacional (AlHogail & Mirza, 2014a; Da Veiga & Eloff, 2010; Da Veiga & Martins, 2015), así como modelos centrados en las personas, como el propuesto por Hayden (2016) (tabla 3).

Tabla 3. Marcos y modelos de medición de cultura de seguridad de la información y ciberseguridad

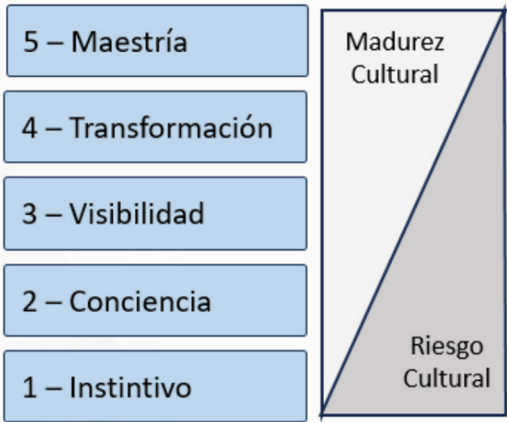
Autor	Marco / modelo	Enfoque
Da Veiga y Eloff (2010)	Information Security Culture Framework (ISCF)	Cultura en seguridad de la información.
Da Veiga y Eloff (2010)	Information Security Culture Assessment (ISCA)	Cultura en seguridad de la información
Da Veiga y Martins (2015)	Information security culture and information protection culture: A validated assessment instrument	Cultura en seguridad de la información.
Hogail (2015)	The Information Security Culture Framework (ISCF)	Cultura en seguridad de la información
Hayden (2016)	Competing Security Cultures Framework (CSCF)	Cultura de seguridad y adopción de comportamientos de seguridad
Hayden (2016)	Culture Capabilities Maturity Model (CCMM)	Identificación de capacidades culturales en las personas de una organización

Fuente: Elaboración propia.

De los documentos antes descritos, se concluye que el modelo presentado por Hayden (2016) tiene un enfoque más cercano al propósito de esta investigación,

ya que puede ser aplicado directamente a los miembros de la junta directiva para determinar sus fortalezas y aspectos de mejora. El modelo de madurez de capacidades de cultura (CCMM) describe cinco niveles y se divide en dos estados transversales: uno identificado como cultura de riesgo, en el cual las personas actúan instintivamente y de manera reactiva sin comprender cómo funciona la organización, y otro en el nivel superior, donde la organización entiende el comportamiento de las personas hasta el punto de poder modificarlo con rapidez y eficacia para enfrentar cualquier reto (Hayden, 2016) (figura 4).

Figura 4. El modelo de madurez de capacidades de cultura.



Fuente: Adaptado de Hayden (2016).

Existen estudios como el de Dornheim y Zarnekow (2023), quienes utilizaron el modelo de Da Veiga y Eloff para determinar la madurez en cultura de ciberseguridad en una compañía australiana, demostrando que los marcos pueden ser adaptados a las necesidades de cada organización.

Paso 2. Designar los recursos necesarios para la gestión de la ciberseguridad
La evolución de las ciberamenazas requiere que los miembros de las juntas directivas asuman un mayor compromiso con la ciberseguridad de sus organizaciones (Nodehi et al., 2024), asegurando la resiliencia corporativa y reduciendo los riesgos identificados a través de ejercicios de evaluación. Por ello, la asignación de recursos, tanto técnicos como humanos, resulta necesaria tanto para el desarrollo de la ciberseguridad organizacional como para la adopción de la cultura de ciberseguridad entre sus miembros (ENISA, 2017).

Concientización

La concientización comprende tres componentes principales. El primero, la conciencia, se refiere al momento en que el individuo reconoce una situación y actúa en consecuencia. El segundo componente es la capacitación, caracterizada por ser un proceso formal orientado a enseñar habilidades específicas. Finalmente, el tercer componente es la educación, que proporciona conocimientos y habilidades bajo un marco teórico integral (Corradini, 2020).

Generar conciencia de ciberseguridad en las juntas directivas implica el reconocimiento de su papel y la comprensión de las implicaciones e impactos de sus decisiones dentro de la organización. Para fortalecer esta conciencia, se debe promover un lenguaje común (Corradini, 2020).

Paso 3. Sensibilizar a los miembros de la junta directiva sobre amenazas cibernéticas y sus consecuencias

La sensibilización en ciberseguridad dirigida a miembros de juntas directivas es relevante, ya que les permitirá mantenerse actualizados y atentos en el cambiante entorno digital. Tal como menciona el SANS Institute (2023) en su publicación *2023 Security Awareness Report*, para alcanzar una madurez en los programas de sensibilización es necesario adoptar un enfoque menos técnico y más orientado a la gestión del riesgo humano. Esto ayudará a que los líderes cambien su percepción sobre la necesidad de contar con una estrategia sólida de ciberseguridad, reforzando su rol y responsabilidad durante los escenarios de respuesta ante incidentes en situaciones de crisis cibernética que pongan en riesgo a la organización.

En este mismo sentido, el programa de sensibilización puede incluir la generación de indicadores que deben ser comunicados a los miembros de la junta directiva para evidenciar el avance en el fortalecimiento de la resiliencia cibernética o para identificar acciones de mejora que deben ser reforzadas.

Se espera que los directivos estén alerta frente a las amenazas cibernéticas a las que pueden estar expuestos, considerando su posición en la organización, así como las consecuencias e impactos que la materialización de un evento cibernético podría acarrear, tales como la indisponibilidad operativa, pérdidas financieras, sanciones legales, pérdida de reputación o incluso acusaciones penales contra los miembros de la junta directiva (Fortinet, 2024).

Conocimiento

El intercambio de conocimiento y el compartir lecciones aprendidas contribuyen a la mejora de la concientización en ciberseguridad (Willie, 2023).

En este sentido, la formación en ciberseguridad debe ser vista como una inversión y no como un costo (Corradini, 2020). Estos programas deben estar diseñados en concordancia con los valores de la organización y orientados al desarrollo de habilidades. Así, el elemento conocimiento en una cultura de ciberseguridad promueve la eficiencia, la innovación y la prosperidad económica en las organizaciones (Da Veiga, 2016).

El incremento de riesgos y amenazas cibernéticas ha llevado a que el conocimiento se convierta en una habilidad esencial, integrada a un comportamiento cibernético de acción inconsciente (Uchendu et al., 2021).

Paso 4. Definir un plan de capacitación en ciberseguridad que contemple sus bases, riesgos y amenazas cibernéticas y las consecuencias para la organización

La planificación de la capacitación debe considerar el contexto específico de cada organización. De acuerdo con Corradini (2020), “los objetivos, etapas, herramientas y técnicas deben planificarse y coordinarse para producir los resultados del aprendizaje que la organización desea lograr”. El método de capacitación puede variar según la necesidad y la forma en que se pretenda su implementación (tabla 4).

Como resultado de la capacitación, se espera lograr una mejora en el comportamiento, las actitudes, el cumplimiento, la comunicación, las normas y las responsabilidades en torno a la ciberseguridad.

Tabla 4. Métodos de capacitación

Método	Medio	Uso
En línea	Correos electrónicos	Pueden ser usados para difundir nuevos materiales de capacitación, como videos, juegos, hojas de consejos, historias y preguntas frecuentes.
	Videos	Pueden utilizarse con fines de formación, incluyendo charlas de expertos en ciberseguridad (internos o externos).
	Juegos	Facilitan el compromiso, la participación y la apertura al conocimiento.
	Seminarios web	Participación de expertos internos o externos de forma interactiva y rentable para transmitir mensajes de ciberseguridad.
	Cursos de formación en línea	Pueden diseñarse como cursos generales o específicos o por grupo objetivo.
	Intranet	Permite la comunicación con los empleados para entregar material de ciberseguridad.
	Redes sociales	Pueden comunicarse buenas prácticas de ciberseguridad, alertar sobre amenazas específicas y compartir recursos útiles. Los empleados deben seguir las cuentas de la organización.

Método	Medio	Uso
Fuera de línea	Ejecutar escenarios, ensayos, <i>sandboxes</i> y ejercicios de juegos de guerra.	Aumenta la preparación para eventos cibernéticos; identifica riesgos; crea comportamientos/respuestas que sean producidas propiamente por el personal.
	Historias	Pueden presentar una respuesta a una amenaza actual, qué medidas tomó el empleado y cuál fue el resultado. Puede estar impresa en folletos o carteleras, o en un video durante una formación en línea. Puede incluir consejos y preguntas.
	Ofrecer incentivos	Puede realizar competencias y brindar productos de la organización a quien haya tenido un mejor desempeño. Estas actividades están ligadas al comportamiento de los individuos.
	Realizar ataques simulados	Pueden incluir ataques en línea con correos electrónicos falsos de <i>phishing</i> . Puede incluir llamadas telefónicas falsas a los integrantes de la junta directiva, con el objetivo de probar procesos y procedimientos correctos. Puede realizar simulaciones de sala de crisis para evaluar el desempeño y actuación de los directivos.
Híbridos	Capacitaciones	Reuniones grupales donde los individuos pueden probar sus habilidades, cometer errores y hacer preguntas en un entorno seguro.
	Folletos / carteles	Pueden incluir consejos, preguntas frecuentes, historias cortas y datos de contacto con el equipo de ciberseguridad.
	Talleres	Entorno interactivo para que las personas reciban capacitación, garantizando un entorno positivo para que se sientan seguros al cometer errores o hacer preguntas.
	Eventos	Se centran en la ciberseguridad en general, amenazas específicas y herramientas contra el cibercrimen.
	Conferencias	Las conferencias permiten obtener una comprensión más amplia y actualizada de las tendencias en ciberseguridad.

Fuente: Elaboración propia con base en ENISA (2017).

Comportamientos

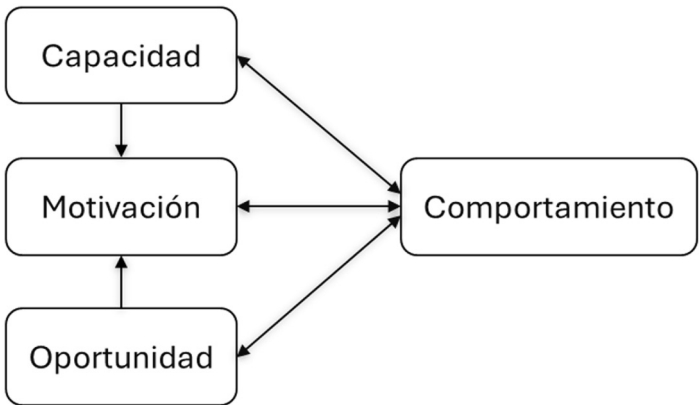
El comportamiento y las actitudes frente a la ciberseguridad por parte de los empleados de una organización están influenciados por la forma en que han adoptado e interiorizado las creencias y valores (González, 2023).

Otros factores, como la capacitación continua, la transmisión de información, ideas y valores, también contribuyen a la formación del comportamiento de cultura de ciberseguridad. Además, fortalecen el empoderamiento de las personas y el desarrollo de capacidades sociológicas y psicológicas, especialmente en contextos que involucran procesos tecnológicos y de ciberseguridad (Álvarez & Urrego, 2019).

Las juntas directivas deben desarrollar estrategias en conjunto con los líderes de proceso para motivar, premiar o, si es necesario, sancionar a los individuos de acuerdo con su comportamiento, ya que este puede fortalecer o debilitar la postura de ciberseguridad de la organización (Hayden, 2016).

Un comportamiento es el resultado de tres variables que todo individuo posee: la habilidad o capacidad de realizar una acción, la motivación que impulsa a llevarla a cabo y la oportunidad de ejecutarla (ENISA, 2021; Michie et al., 2011) (figura 5). Llevando esto al contexto de la cultura de ciberseguridad, puede considerarse el ejemplo de la recepción de un correo de *phishing* por parte de un miembro de la junta directiva, quien debe tener la capacidad de identificar un correo malicioso, la oportunidad de decidir abrirlo o reportarlo, y la motivación para actuar de forma segura.

Figura 5. Modelo COM-B para entender el comportamiento.



Fuente: Adaptado de Michie et al. (2011)

A continuación, se indica el paso que permite desarrollar el elemento Comportamiento en los miembros de la junta directiva.

Paso 5. Evaluar el comportamiento en ciberseguridad de los miembros de la junta directiva

Una de las formas de evaluar el comportamiento de los individuos en cuanto a ciberseguridad es a través de ejercicios de ingeniería social, como pruebas de Rocha y Ekstedt (2012), la verificación del uso de cuentas corporativas para actividades personales como redes sociales, o la identificación de prácticas como el escritorio limpio, entre otras. Las acciones que los empleados adopten ante

actividades reales o simuladas que impliquen algún nivel de riesgo permiten identificar el impacto directo o indirecto en la cultura cibernética (ENISA, 2021).

Valores

Desde la perspectiva de ENISA (2017), la evolución de una cultura organizacional comienza con la modificación de sus valores fundamentales, impulsando así la adopción de nuevos comportamientos. Las juntas directivas son quienes establecen el camino para los valores y objetivos de la organización.

Cano (2021) señala que los valores conscientes determinan el comportamiento y la manera en que se realizan las actividades en una organización, estando intrínsecamente ligados a las conductas y conocimientos previos que definen su historia.

En este sentido, los valores representan teorías oficialmente documentadas que no siempre reflejan la realidad de los valores conscientes o inconscientes. Por tanto, la construcción de valores verdaderos debe basarse en una descripción cualitativa sustentada en observaciones oficiales (Schlienger & Teufel, 2005).

De acuerdo con Schein (2017), el conocimiento adquirido de forma colectiva representa las creencias y valores de un individuo, fomentando la cooperación entre sus integrantes y moderando sus actitudes y comportamientos.

Paso 6. Incluir la ciberseguridad como un valor corporativo

Incorporar la ciberseguridad como un valor corporativo orienta a la organización hacia un enfoque proactivo en la protección de sus activos digitales. Según Hayden (2016), la cultura de ciberseguridad debe diseñarse en armonía con los valores y la cultura preexistente de la organización.

Esto implica que las políticas y prácticas de seguridad deben estar alineadas con la identidad corporativa, de modo que sean percibidas no solo como una obligación, sino como una extensión natural de los principios y objetivos fundamentales de la empresa.

Cuando la junta directiva adopta la ciberseguridad como un valor corporativo y lo proyecta hacia toda la organización en un modelo *top-down*, se genera en los colaboradores un sentido de responsabilidad y compromiso con la protección de la información, fortaleciendo así la resiliencia corporativa frente a posibles amenazas.

Normas

Integrar las normativas que regulan el manejo de la información dentro de la cultura de ciberseguridad se considera una finalidad de aplicabilidad no solo en las organizaciones, sino también en las personas (Valencia-Arias et al., 2020).

Por otro lado, Cano (2016) señala que mantener una cultura organizacional implica un cambio en cada individuo, influenciado por el marco normativo de la organización. Las actuaciones de un individuo impactan tanto a nivel interno como externo, ya que sus comportamientos y decisiones pueden afectar la percepción y las prácticas de ciberseguridad dentro de la organización, así como su imagen ante los grupos de interés. En este contexto, el impacto no solo refuerza la cultura de ciberseguridad interna, sino que también marca una tendencia en su entorno, promoviendo estándares y expectativas similares en otras organizaciones y en la industria en general.

Paso 7. Alinear a la organización en el cumplimiento de normativas, estándares o buenas prácticas en ciberseguridad

Una de las responsabilidades de la junta directiva es liderar la implementación de la ciberseguridad en toda la organización. Esto implica alinearse con estándares y buenas prácticas que proporcionen una visión holística de la seguridad empresarial, incluyendo la ciberseguridad, y garantizar el cumplimiento de las regulaciones y normativas locales aplicables al sector.

Además, la adopción de normas, estándares y buenas prácticas permite desarrollar un modelo de medición que ayuda a la organización a identificar su nivel de madurez y las oportunidades de mejora. Uno de los marcos más utilizados a nivel global es el National Institute of Standards and Technology (NIST), que en su versión más reciente (NIST 2.0) incorpora la función de *Gobernanza*, enfocada en identificar y gestionar los riesgos cibernéticos como parte integral de los riesgos empresariales (NIST, 2023).

Síntesis

Al llegar a este punto, se ha identificado que la adopción de una cultura de ciberseguridad en las juntas directivas implica el desarrollo de los pasos descritos en los apartados anteriores. Estos pasos, en conjunto, permitirán a la organización trazar un objetivo claro en el horizonte, en el cual sus directivos adquieran conciencia sobre la importancia de contar con entornos ciberseguros, dada la naturaleza de las amenazas del mundo moderno, para las cuales deben estar preparados y responder adecuadamente cuando sea necesario, favoreciendo la continuidad y la resiliencia corporativa.

La tabla 5 resume los elementos orientadores y sus pasos para construir una cultura de ciberseguridad a nivel directivo.

Tabla 5. *Pasos para adoptar una cultura de ciberseguridad en juntas directivas*

Elemento	Pasos
Estrategia	Paso 1. Medir el nivel de madurez en cultura de ciberseguridad de la junta directiva.
	Paso 2. Designar los recursos necesarios para la gestión de la ciberseguridad.
Concientización	Paso 3. Sensibilizar a los miembros de la junta directiva sobre amenazas cibernéticas y sus consecuencias.
Conocimiento	Paso 4. Definir un plan de capacitación en ciberseguridad que contemple sus bases, riesgos y amenazas cibernéticas y las consecuencias para la organización.
Comportamientos	Paso 5. Evaluar el comportamiento en ciberseguridad de los miembros de la junta directiva.
Valores	Paso 6. Incluir la ciberseguridad como un valor corporativo.
Normas	Paso 7. Alinear a la organización en el cumplimiento de normativas, estándares o buenas prácticas en ciberseguridad.

Fuente: Elaboración propia.

Preguntas de reflexión

Realizar una revisión periódica de la cultura de ciberseguridad en las juntas directivas permite identificar los aspectos de mejora y evaluar los cambios desde su adopción. ENISA también sugiere que esta cultura debe medirse periódicamente para garantizar su éxito a lo largo del tiempo.

De acuerdo con Cano (2023), “el 51 % de las organizaciones afirma que los altos directivos se han enfrentado a multas, penas de cárcel, pérdida del puesto o pérdida del empleo tras un ciberataque”. Ante este dato, resulta pertinente preguntarse: ¿Qué hace que los miembros de las juntas directivas no muestren un mayor interés en la ciberseguridad?

La junta directiva debe también reflexionar sobre cómo se puede medir su preparación frente a las amenazas cibernéticas y si la organización cuenta con los mecanismos adecuados para enfrentarlas. Es importante que el responsable de ciberseguridad en la organización informe periódicamente a la junta directiva mediante reportes que incluyan estadísticas sobre pérdidas económicas, daños reputacionales o afectaciones operativas (Clinton et al., 2023).

Asimismo, surge el cuestionamiento: ¿Debería la junta directiva contar entre sus integrantes con un experto en ciberseguridad? Esto no implica que dicha persona asuma individualmente la responsabilidad o tome decisiones de manera

aislada ante la materialización de un riesgo o incidente cibernético; más bien, su experticia contribuiría a aumentar el nivel de comprensión de la ciberseguridad dentro de la junta directiva, tal como señalan Clinton et al. (2023).

Conclusiones

Dentro de esta investigación se concluye que la ciberseguridad es contemplada por los directivos, aunque no con la relevancia y frecuencia necesarias. Un punto de partida para la apropiación de este tema es incluir en la agenda de las juntas directivas un espacio específico para discutir asuntos de ciberseguridad, lo cual permitiría abrir el debate sobre ataques dirigidos a la organización o al sector al que pertenece. Surge así la necesidad de preguntarse cuál es el impacto y las consecuencias de la materialización de riesgos.

La perspectiva hacia los integrantes de las juntas directivas es que su postura frente a los riesgos de ciberseguridad sea estratégica. No obstante, esta visión puede verse debilitada por la falta de habilidades, conocimientos y métricas claras, lo que dificulta el análisis y la asignación adecuada de recursos destinados a la ciberseguridad.

Los elementos seleccionados en el desarrollo de esta guía apoyan el fomento de una cultura de ciberseguridad a nivel de juntas directivas. Estos elementos buscan influir en el comportamiento a partir del conocimiento adquirido, promoviendo una toma de decisiones consciente sobre el impacto y la relevancia de la ciberseguridad para la organización. Esta adopción está vinculada tanto a la cultura organizacional interna como a las buenas prácticas observadas desde una perspectiva externa.

La investigación resalta que la concientización y la capacitación en ciberseguridad son fundamentales para las juntas directivas. La falta de conocimiento y preparación puede llevar a decisiones mal informadas que pongan en riesgo la seguridad de la organización. La implementación de programas de sensibilización y formación continua resulta crucial para que los directivos comprendan los riesgos cibernéticos y sus posibles consecuencias.

Las juntas directivas deben asumir un rol estratégico en la gestión de la ciberseguridad. Esto incluye la asignación adecuada de recursos, la creación de comités específicos y la integración de la ciberseguridad en la estrategia corporativa. La investigación destaca que la ciberseguridad no debe ser vista como una responsabilidad exclusiva del departamento de TI, sino como una prioridad organizacional que requiere el compromiso de todos los niveles directivos.

La adopción de una cultura de ciberseguridad en las juntas directivas implica un cambio en la percepción y comportamiento de sus miembros. Es esencial que estos líderes comprendan la importancia de la ciberseguridad y promuevan prácticas seguras dentro de la organización. La investigación propone una guía con elementos orientadores —estrategia, concientización, conocimiento, comportamientos, valores y normas— que puede apoyar a las juntas directivas en el establecimiento de una cultura de ciberseguridad sólida y resiliente.

Recomendaciones

Desarrollo de programas de capacitación personalizados: Crear programas de capacitación en ciberseguridad adaptados a las necesidades específicas de las juntas directivas. Estos programas deben incluir simulaciones de incidentes cibernéticos, estudios de caso y talleres prácticos que permitan a los directivos experimentar y gestionar situaciones reales de ciberseguridad.

Investigación sobre la eficacia de las políticas de ciberseguridad: Realizar estudios longitudinales que evalúen la eficacia de las políticas y estrategias de ciberseguridad implementadas en las organizaciones. Esta información permitirá identificar buenas prácticas y áreas de mejora, proporcionando datos relevantes para la toma de decisiones informadas.

Integración de la ciberseguridad en la cultura organizacional: Investigar métodos para integrar de manera efectiva la ciberseguridad dentro de la cultura organizacional, incluyendo el desarrollo de marcos teóricos y prácticos que faciliten la adopción de comportamientos seguros y fomenten un entorno de trabajo que valore y priorice la ciberseguridad.

Evaluación de la madurez en ciberseguridad: Desarrollar y aplicar modelos de evaluación de madurez en ciberseguridad que permitan medir el progreso organizacional y establecer metas claras. Estos modelos deben considerar factores como la concientización, la capacitación, la asignación de recursos y la implementación de tecnologías de seguridad.

Colaboración intersectorial: Fomentar la colaboración entre sectores y organizaciones para compartir conocimientos y experiencias en ciberseguridad. La creación de redes y alianzas estratégicas fortalecerá las capacidades de ciberseguridad a nivel nacional e internacional, promoviendo un enfoque más cohesivo y coordinado frente a las amenazas cibernéticas.

Referencias

- Advice Group LATAM. (2023, 9 de agosto). *Estadísticas de ciberseguridad en Centroamérica y Colombia*. <https://tinyurl.com/2yu2mkpr>
- AlHogail, A., & Mirza, A. (2014a). A proposal of an organizational information security culture framework. En *Proceedings of International Conference on Information, Communication Technology and System (ICTS) 2014* (pp. 243-250). <https://doi.org/10.1109/ICTS.2014.7010591>
- AlHogail, A., & Mirza, A. (2014b). Information security culture: A definition and a literature review. *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, 1-7. <https://doi.org/10.1109/WCCAIS.2014.6916579>
- AL-sartawi, A. (2020). Information technology governance and cybersecurity at the board level. *International Journal of Critical Infrastructures*, 16(2), 150-161. <https://doi.org/10.1504/IJCIS.2020.10029173>
- Álvarez Dionisi, L. E., & Urrego Baquero, N. (2019, 15 de marzo). Implementing a cybersecurity culture. *ISACA*. <https://tinyurl.com/2ch7q7j7>
- Azuero Zúñiga, F., Cuéllar Boada, F. H., Moya Suárez, J., Serna Hernández, S., Romero Ortiz, L. E., & González Couture, G. A. (2020). *Juntas directivas, eje del gobierno corporativo* (1.ª ed.). Ediciones Uniandes.
- Barrero, V., & Bou, O. (2020). *Estado de preparación en ciberseguridad del sector eléctrico en América Latina*. BID. <https://doi.org/10.18235/0002344>
- Bertalanffy, L. von. (1989). *Teoría general de los sistemas*. Fondo de Cultura Económica.
- Cano, J. (2016, octubre). Modelo de madurez de cultura organizacional de seguridad de la información. Una visión desde el pensamiento sistémico-cibernético. En *XIV Reunión Española sobre Criptología y Seguridad de la Información* (Vol. 1, pp. 24-29). <https://tinyurl.com/24nas3rx>
- Cano, J. (2021, 16 de junio). *Cultura organizacional de seguridad de la información. Una perspectiva sistémica de articulación de sistemas humanos, culturales y sociales*. ISACA. <https://tinyurl.com/4hkbjv63>
- Cano, J. (2023). *Ciberseguridad empresarial: Reflexiones y retos para los ejecutivos del siglo XXI* (2.ª ed.). Ediciones de la U.
- Clinton, L., Marx, A., Swafford, K., & Sandlin, D. (2023). *Director's handbook on cyberrisk oversight* (National Association of Corporate Directors [NACD], Ed.). <https://tinyurl.com/2xemty5x>
- Consejo Nacional de Política Económica y Social (CONPES) 3701. (2011, 14 de julio). *Lineamientos de política para ciberseguridad y ciberdefensa*. Departamento Nacional de Planeación. <https://tinyurl.com/mrb3nfdt>

- Consejo Nacional de Política Económica y Social (CONPES) 3995. (2020, 1 de julio). *Política Nacional de Confianza y Seguridad Digital*. Departamento Nacional de Planeación. <https://tinyurl.com/4xxep7f6>
- Corradini, I. (2020). *Building a cybersecurity culture in organizations: How to bridge the gap between people and digital technology*. Springer International Publishing. <https://doi.org/10.1007/978-3-030-43999-6>
- Cyber Citadel. (2023). *Cyber security guide for board directors*. <https://tinyurl.com/b368dfwd>
- Da Veiga, A. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. *2016 SAI Computing Conference (SAI)*, 1006-1015. <https://doi.org/10.1109/SAI.2016.7556102>
- Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196-207. <https://doi.org/10.1016/j.cose.2009.09.002>
- Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review*, 31(2), 243-256. <https://doi.org/10.1016/j.clsr.2015.01.005>
- Dornheim, P., & Zarnekow, R. (2023). Determining cybersecurity culture maturity and deriving verifiable improvement measures. *Information & Computer Security* (publicación anticipada). <https://doi.org/10.1108/ICS-07-2023-0116>
- European Union Agency for Cybersecurity (ENISA). (2017, noviembre). *Cyber security culture in organisations* [informe/estudio]. <https://tinyurl.com/2a3bae6m>
- European Union Agency for Cybersecurity (ENISA). (2021). *Review of behavioural sciences research in the field of cybersecurity: Technical annex: Evidence reviews*. Publications Office. <https://data.europa.eu/doi/10.2824/717888>
- Fortinet. (2024). *2024 Cybersecurity Skills Gap*. <https://tinyurl.com/4u5auzhs>
- Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. *Computers & Security*, 121, 102840. <https://doi.org/10.1016/j.cose.2022.102840>
- Giraldo Ríos, L. A. (2024). Definición e impacto en la transformación digital y la ciberseguridad. En M. E. Realpe Díaz, & A. M. González González (Eds.), *Tecnologías disruptivas, logística y seguridad y defensa nacional en el ciberespacio* (pp. 15-46). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287602700.01>
- Goicoechea de Jorge, M. (2004). *El lector en el ciberespacio: Una etnografía literaria de la cibercultura* [tesis doctoral, Universidad Complutense de Madrid]. <https://eprints.ucm.es/id/eprint/32979/1/T27652.pdf>
- González Sánchez, D. A. (2023). *Modelo de madurez de cultura organizacional de ciberseguridad para el sector financiero basado en buenas prácticas* [tesis de maestría, Tecnológico de Antioquia, Colombia]. <https://dspace.tdea.edu.co/handle/tdea/3927>

- González, J. A., Amozurrutia, J. A., & Maass, M. (2007). *Cibercultur@ e iniciación en la investigación*. UNAM.
- Hayden, L. (2016). *People-centric security: Transforming your enterprise security culture*. McGraw-Hill Education.
- Hernández Sampieri, R., & Fernández Collado, C. (2014). *Metodología de la investigación* (P. Baptista Lucio, Ed.; 6.ª ed.). McGraw-Hill Education.
- Hofstede, G. (1980). Motivation, leadership, and organization: Do American theories apply abroad? *Organizational Dynamics*, 9(1). [https://doi.org/10.1016/0090-2616\(80\)90013-3](https://doi.org/10.1016/0090-2616(80)90013-3)
- Hogail, A. A. (2015). Cultivating and assessing an organizational information security culture: An empirical study. *International Journal of Security and Its Applications*, 9(7), 163-178. <https://doi.org/10.14257/ijisia.2015.9.7.15>
- IBM Security. (2023). *Cost of a data breach report*. IBM. <https://www.ibm.com/reports/data-breach>
- Institute of Internal Auditors (IIA). (2021). *OnRisk: A guide to understanding, aligning, and optimizing risk*. IIA. <https://iiabelgium.org/wp-content/uploads/2020/11/On-Risk-2021-Report.pdf>
- Maurer, T., Taylor, K., & Grossman, T. (2020, diciembre). *Capacity-Building Tool Box for Cybersecurity and Financial Organizations*. <https://tinyurl.com/3h6pyw2x>
- Michie, S., van Stralen, M., & West, R. (2011). The Behaviour Change Wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science: IS*, 6, 42. <https://doi.org/10.1186/1748-5908-6-42>
- Milică, L., & Pearson, K. (2023, 2 de mayo). Boards are having the wrong conversations about cybersecurity. *Harvard Business Review*. <https://tinyurl.com/2g59rd66>
- National Institute of Standards and Technology (NIST). (2023). *The NIST Cybersecurity Framework 2.0* (NIST CSWP 29 ipd). <https://tinyurl.com/mrymfbf5>
- Nodehi, S., Huygh, T., & Bollen, L. (2024). Six board roles for information security governance. En *Proceedings of the 26th International Conference on Enterprise Information Systems* (pp. 713-720). <https://doi.org/10.5220/0012695900003690>
- Onumo, A., Ullah-Awan, I., & Cullen, A. (2021). Assessing the moderating effect of security technologies on employees compliance with cybersecurity control procedures. *ACM Transactions on Management Information Systems*, 12(2). <https://doi.org/10.1145/3424282>
- Organización de Estados Americanos (OEA). (2004, 8 de junio). *Adopción de una estrategia interamericana integral de seguridad cibernética*. <https://tinyurl.com/5n87uz48>

- Organización de Estados Americanos (OEA). (2018). *Critical infrastructure protection in Latin America and the Caribbean 2018*. <https://www.oas.org/es/sms/cicte/cipreport.pdf>
- Organización de Estados Americanos (OEA). (2019, 27 de septiembre). *Manual de supervisión de riesgos cibernéticos para juntas corporativas*. <https://tinyurl.com/z4vaxhfh>
- Pearlson, K., Sposito, S., Arbisman, M., & Schwartz, J. A. (2021, 30 de septiembre). How Yahoo built a culture of cybersecurity. *Harvard Business Review*. <https://hbr.org/2021/09/how-yahoo-built-a-culture-of-cybersecurity>
- PricewaterhouseCoopers. (2020). *Informe del estado de cultura de ciberseguridad en el entorno empresarial*. <https://tinyurl.com/3ntfz28x>
- Rocha Flores, W., & Ekstedt, M. (2012, 15 de diciembre). A model for investigating organizational impact on information security behavior. En *Proceedings of the 7th International Conference on Availability, Reliability and Security* (pp. 660-667).
- Ruiz Olabuénaga, J. I. (2012). *Metodología de la investigación cualitativa* (5.ª ed.). Universidad de Deusto.
- SANS Institute. (2023). *SANS 2023 Security Awareness Report*. <https://tinyurl.com/3zjbnu8>
- Schein, E. H. (2017). *Organizational culture and leadership* (5.ª ed.). John Wiley & Sons.
- Schlienger, T., & Teufel, S. (2005). Analyzing information security culture: Increased trust by an appropriate information security culture. En *Proceedings of the 14th International Workshop on Database and Expert Systems Applications* (pp. 405-409). <https://doi.org/10.1109/DEXA.2003.1232055>
- Schneider, B., Asprion, P. M., Androvicsova, S., & Azan, W. (2020). *A practical guideline for developing a managerial information security awareness program*.
- Schwab, K. (2016). *La cuarta revolución industrial*. Marcial Pons.
- Steele, G. (2024). *The hidden costs of downtime*, 26.
- Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cybersecurity culture: Current practices and future needs. *Computers & Security*, 109, 102387. <https://doi.org/10.1016/j.cose.2021.102387>
- Valencia-Arias, A., Giraldo, M. C. B., Acevedo-Correa, Y., Garcés-Giraldo, L. F., Quiroz-Fabra, J., Benjumea-Arias, M. L., & Patiño-Vanegas, J. C. (2020). Tendencias investigativas en educación en ciberseguridad: Un estudio bibliométrico. *Revista Latinoamericana de Investigación en Seguridad Informática*, 8(3), 225-239. <https://tinyurl.com/2bwj7moc>
- Vasilachis de Gialdino, I. (2006). *Estrategias de investigación cualitativa* (1.ª ed.). Editorial Gedisa.
- Verizon Business. (2023). *Data Breach Investigation Report 2023 (DBIR)*. <https://tinyurl.com/4zz7z3a5>

- Willie, M. (2023). *The role of organizational culture in cybersecurity: Building a security-first culture*. SSRN. <https://dx.doi.org/10.2139/ssrn.4564291>
- World Economic Forum. (2022). *The Global Risks Report 2022* (Informe 17). <https://tinyurl.com/yc5w4wy6>
- Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset. *International Journal of Human-Computer Studies*, 131, 169-187. <https://doi.org/10.1016/j.ijhcs.2019.05.005>

Epílogo

Desafíos y oportunidades para la ciberseguridad en los ecosistemas empresariales digitales contemporáneos

Milena Elizabeth Realpe Díaz
Giovanni Alberto Gómez Rodríguez

Escuela Superior de Guerra "General Rafael Reyes Prieto"

La transformación digital es un tema ineludible en la mayoría de los procesos y dinámicas corporativas actuales. Tanto las organizaciones privadas como las entidades públicas transitan esta senda a distintos ritmos, evidenciando diversos niveles de compromiso y alcanzando resultados con grados variables de éxito.

En este contexto, los directivos reconocen el impacto significativo de la tecnología en los resultados de sus organizaciones; sin embargo, en algunos casos, carecen de una comprensión profunda sobre cómo se produce dicho impacto y cuáles son sus causas específicas.

El propósito de este libro es responder estos interrogantes, proporcionando una perspectiva académica sobre la importancia de la transformación digital y los entornos donde las organizaciones gestionan y establecen diversas interacciones comerciales, bursátiles o fiscales con actores externos, conocidos como *ecosistemas digitales*. Además, busca exponer información actualizada y relevante sobre su funcionamiento, sus características y requerimientos en materia de ciberdefensa y ciberseguridad.

Los ecosistemas digitales empresariales, configurados en el ciberespacio, se han convertido en un motor de la productividad que debe ser gestionado e incorporado en la planeación estratégica de empresas e instituciones.

No se trata simplemente de herramientas facilitadoras ni de cargos creados para cumplir funciones específicas, asignar procesos o añadir atributos, como la

calidad o la estandarización. Es una verdadera revolución que demanda el diseño de políticas, la implementación de modelos alineados con los fines corporativos y el desarrollo de estrategias que generen valor a través de tecnologías como la inteligencia artificial (IA), el *blockchain*, el *big data*, las técnicas de identificación y autenticación, o los servicios en la nube.

A partir de lo anterior, se puede deducir que los ecosistemas digitales se configuran según la actividad económica y el modelo de negocio diseñado para generar valor. No obstante, las exigencias en materia de seguridad de la información y ciberseguridad tienden a ser relativamente similares, independientemente del sector al que pertenezca la organización. Por esta razón, la mayoría de la información recopilada en esta publicación tiene un valor teórico y práctico aplicable a cualquier ecosistema digital.

La ciberdefensa y la ciberseguridad son temas recurrentes en las reflexiones que giran en torno a los ecosistemas digitales y su gestión. La ciberseguridad se concibe como el conjunto de medidas preventivas y controles destinados a proteger los sistemas y la información ante posibles ataques cibernéticos. Estas acciones buscan garantizar la confidencialidad, integridad y disponibilidad de los datos, pilares fundamentales de cualquier estrategia de seguridad.

Por su parte, la ciberdefensa se refiere a la capacidad del Estado para desplegar medidas reactivas con el fin de mitigar los efectos de un ataque cibernético que ha superado las barreras preventivas previamente establecidas.

Mientras que la ciberseguridad se enfoca en la prevención de intrusiones y vulnerabilidades, la ciberdefensa se activa una vez que dichas amenazas han penetrado los sistemas. En este sentido, la ciberdefensa puede considerarse una respuesta complementaria y necesaria ante las posibles fallas de las estrategias de ciberseguridad.

En síntesis, se aborda la gestión de la ciberdefensa y la ciberseguridad en los ecosistemas digitales empresariales contemporáneos, considerando diversos contextos, niveles y casos, así como el impacto de las nuevas tecnologías.

Algunos textos son descriptivos, mientras que otros adoptan un enfoque reflexivo, a fin de explicar cómo estas tecnologías disruptivas no solo mejoran la seguridad, sino que también amplifican los riesgos o generan nuevas amenazas al estar disponibles para los adversarios en el ciberespacio.

El capítulo uno, titulado "El impacto de la ciberseguridad en los modelos de negocios de las organizaciones", señala que la transformación digital ha reconfigurado la dinámica empresarial, acelerando la implementación de tecnologías disruptivas que permitan procesos más eficientes, flexibles y personalizados.

Sin embargo, esta evolución digital también ha incrementado los riesgos asociados a la ciberseguridad, convirtiéndola en un factor decisivo para el éxito o fracaso de los modelos de negocio contemporáneos. En este sentido, un negocio que opera mediante un ecosistema digital debe alinearse con el modelo de negocio diseñado para generar valor.

La tendencia actual es que las tecnologías de la información (TI) y las tecnologías operativas (TO) sean digitales, y no físicas. Esto significa que el diseño y la configuración del modelo de negocio no solo están condicionados por el entorno digital y la ciberseguridad, sino también por las exigencias tecnológicas, comunicacionales y de seguridad inherentes al ciberespacio.

Un modelo de negocios explica cómo una organización crea, entrega y captura valor, mientras que la ciberseguridad comprende las actividades, políticas y procedimientos implementados para proteger sus sistemas, redes y datos de accesos no autorizados, interrupciones o ataques, cuya contención se torna cada vez más compleja.

Por esta razón, la ciberresiliencia cobra relevancia, y se define como la capacidad de una organización para seguir operando a pesar de ciberataques, incidentes o interrupciones en sus sistemas.

En el panorama digital actual, la creación y la obtención de valor dependen cada vez más de infraestructuras tecnológicas que demandan una protección continua. En este contexto, la ciberseguridad desempeña un papel fundamental al garantizar la protección de los activos digitales críticos de la empresa, reduciendo así las disrupciones operativas y preservando la capacidad de generar ingresos y satisfacer las necesidades de los clientes.

En un entorno empresarial cada vez más digitalizado y expuesto a numerosas amenazas cibernéticas, la ciberseguridad deja de ser una simple medida de protección y se convierte en un diferenciador competitivo.

Las organizaciones que priorizan la seguridad de sus datos y sistemas tienen la oportunidad de utilizar esta inversión como un argumento de venta atractivo para los clientes y socios comerciales que valoran la protección de su información.

Un modelo de negocio bien estructurado depende, en gran medida, de la protección de los activos digitales, lo que convierte a la ciberseguridad en un elemento esencial para garantizar la continuidad operativa y la satisfacción de los clientes. La implementación de medidas de ciberseguridad robustas no solo mitiga los riesgos asociados a los ciberataques, sino que también fortalece la confianza de los clientes y mejora la reputación corporativa.

En síntesis, el capítulo destaca la sinergia entre el modelo de negocio, la ciberseguridad y la ciberresiliencia, elementos esenciales para alcanzar el éxito en un entorno digital cada vez más vulnerable a los ciberataques. Las organizaciones que invierten en estas áreas no solo protegen sus operaciones, sino que también establecen una base sólida para el crecimiento y la innovación.

El capítulo dos, titulado “Desafíos y tendencias en la identidad digital para la seguridad de las infraestructuras críticas”, ofrece una clasificación de las tecnologías más avanzadas que garantizan la identificación y el acceso a sistemas de información esenciales y estratégicos. Además, establece una distinción entre las infraestructuras críticas (IC) y las infraestructuras críticas cibernéticas (ICC).

Este capítulo proporciona al lector una comprensión profunda de cómo estas tecnologías se aplican en la protección de dichos activos, correlacionando las exigencias de seguridad en el acceso a sistemas de control vitales con las técnicas de autenticación más avanzadas, incluyendo las tendencias actuales y los desarrollos emergentes.

Para operar eficientemente, los ecosistemas digitales vulnerables o expuestos deben garantizar que solo las personas autorizadas tengan acceso a la información sensible. El problema radica en la confianza y la idoneidad limitadas de algunas de las formas actuales de identidad digital, lo que demanda técnicas de autenticación más robustas.

Las IC son sistemas físicos y virtuales esenciales para el funcionamiento de una sociedad, como las redes eléctricas, el suministro de agua, el transporte y las telecomunicaciones.

Estos sistemas son fundamentales para el bienestar económico, la seguridad y la salud pública de una nación. Por esta razón, su interrupción o destrucción podría tener un impacto significativo en la seguridad nacional y la estabilidad económica y el tejido social.

Por otro lado, las ICC son los sistemas y activos que controlan, gestionan y soportan las IC a través de medios digitales, como las redes de comunicación y los sistemas informáticos interconectados.

En otras palabras, son infraestructuras estratégicas (IE) respaldadas por las tecnologías de la información y las comunicaciones (TIC) y las tecnologías de operación (TO), cuyo funcionamiento es indispensable. Su suspensión, afectación o destrucción podría tener grave impacto sobre los servicios esenciales del Estado.

Por lo tanto, es esencial proteger las IC mediante la identificación digital, entendida como la representación electrónica de la información personal y profesional

que singulariza a un individuo o entidad en entornos virtuales. La identificación digital comprende un conjunto de atributos digitales, como las credenciales de acceso, los perfiles de los usuarios, los historiales de transacciones y cualquier otro dato que pueda ser utilizado para identificar a una persona o un dispositivo en un sistema digital.

A continuación, se presentan algunas de las técnicas más citadas:

- La tecnología *blockchain* emerge como una solución prometedora para la gestión descentralizada de las identidades digitales. Además, ofrece una alternativa distribuida que permite que las identidades digitales sean gestionadas a través de una red descentralizada, lo que dificulta la manipulación o el acceso no autorizado a los datos.
- La IA está revolucionando la forma en que los seres humanos interactúan y comprenden el mundo, y la gestión de identidades digitales no es ajena a esta transformación. Su aplicación es especialmente valiosa en los procesos de autenticación y la detección de amenazas.
- Los sistemas de autenticación basados en IA son capaces de analizar grandes volúmenes de datos en tiempo real, identificando patrones de comportamiento anómalos que podrían indicar intentos de acceso no autorizado o ataques en curso.
- El uso de sistemas que habilitan la opción de autenticación *lo que soy* representa, sin duda, una alternativa con altos niveles de seguridad debido a la dificultad de falsificar o suplantar las características biométricas de un individuo.
- Los sistemas de identidad federada permiten que organizaciones o plataformas compartan un conjunto de credenciales de identidad. En lugar de autenticarse repetidamente en diferentes sistemas, los usuarios pueden disfrutar de un único inicio de sesión, reconocido por todos los miembros de la federación.

Dos de las tendencias más destacadas en este campo son las identidades autosoberanas y las identidades federadas y descentralizadas, que proponen enfoques innovadores para abordar los problemas relacionados con la gestión centralizada de las identidades digitales.

El capítulo tres, titulado "La inteligencia artificial y la transformación digital en el ámbito de la ciberseguridad", aborda la relación e importancia de la IA en la transformación digital, destacando su enorme potencial para impulsar este proceso. Asimismo, se explora cómo esta tecnología está revolucionando la protección de los datos.

Por otra parte, se detallan las aplicaciones del aprendizaje automático, el aprendizaje profundo y las redes neuronales en la detección y la respuesta a amenazas, así como el aprendizaje por refuerzo y las redes generativas adversarias (GAN).

Se analiza la integración de la IA en plataformas de seguridad unificadas y la personalización de estrategias de ciberseguridad. La implementación efectiva de estas técnicas de IA mejora notablemente la capacidad de respuesta y la resiliencia ante amenazas cibernéticas en un entorno digital en constante evolución. Por lo tanto, cualquier retraso o resistencia en su adopción no solo incrementará las vulnerabilidades, sino que también privará a las organizaciones de la oportunidad de fortalecer sus sistemas de ciberseguridad con capacidades avanzadas.

Finalmente, las perspectivas futuras de la IA en ciberseguridad son prometedoras, anticipándose avances significativos en la detección, la respuesta, la predicción y la prevención de amenazas. La colaboración sostenida entre investigadores, profesionales y reguladores será crucial para liberar todo el potencial de la IA en la defensa cibernética.

El cuarto capítulo, titulado "Articulación de la ciberseguridad y la ciberdefensa en la planeación estratégica de las organizaciones", destaca que, en la actualidad, las organizaciones no solo enfrentan los problemas tradicionales de seguridad física, sino que también deben adoptar un enfoque integral que contemple la protección de sus activos digitales.

Este enfoque es esencial, ya que un ciberataque no solo puede comprometer la información y los sistemas críticos de una empresa, sino también su reputación y su capacidad para operar de manera continua.

Dada su criticidad, es esencial incorporar los requerimientos de ciberseguridad y ciberdefensa en la planeación estratégica de las organizaciones, involucrando a los más altos niveles directivos. Estas se han convertido en factores clave para la salvaguarda de los activos digitales.

Ante el crecimiento exponencial de las amenazas cibernéticas en la última década, las organizaciones requieren sistemas que garanticen la confidencialidad, la integridad y la disponibilidad de su información.

Incorporar la ciberseguridad en la planificación estratégica es esencial para garantizar la protección de los activos digitales y la continuidad de las operaciones comerciales. Este proceso debe comenzar con una evaluación exhaustiva de los riesgos cibernéticos, lo que permite a las organizaciones identificar vulnerabilidades y diseñar medidas de mitigación.

Posteriormente, se deben implementar acciones como la capacitación continua, la adopción de tecnologías avanzadas y la promoción de una colaboración interna y externa en caso de un ciberataque. En síntesis, el enfoque de ciberseguridad, centrado en la prevención, debe complementarse con estrategias de ciberdefensa que permitan a las organizaciones detectar, responder y recuperarse eficazmente de un ataque cibernético.

Las organizaciones que logran establecer un equilibrio entre la prevención y la respuesta están mejor preparadas para mitigar el impacto de los ciberataques. En este sentido, medidas como la detección temprana de amenazas, los planes de respuesta a incidentes y la formación continua del personal son esenciales. Sin estas acciones, la capacidad de una organización para enfrentar un ciberataque se ve gravemente comprometida, lo que la expone a pérdidas financieras y daños en su reputación.

El quinto capítulo, titulado “Guía para la adopción de una cultura de ciberseguridad en juntas directivas”, desarrolla la siguiente tesis: para la ejecución eficaz de la estrategia corporativa y la gestión integral del riesgo cibernético, es fundamental que las juntas directivas adopten una cultura de ciberseguridad. El capítulo sostiene que, tradicionalmente, la ciberseguridad ha sido considerada un asunto técnico, delegado exclusivamente al oficial jefe de seguridad de la información (CISO) o al gestor de las TIC.

No obstante, el capítulo argumenta con solidez la imperiosa necesidad de que la alta dirección y las juntas directivas comprendan la verdadera naturaleza y el impacto devastador de los riesgos cibernéticos. En consecuencia, deben comprometerse activamente e incorporar en sus estrategias corporativas políticas y protocolos de ciberseguridad, destinando los recursos necesarios para su implementación efectiva.

Si bien se busca que las juntas directivas adopten una postura estratégica ante los riesgos de ciberseguridad, la falta de habilidades y conocimientos específicos en este ámbito, sumada a la ausencia de métricas, puede ser un obstáculo a la hora de justificar la inversión en ciberseguridad. Para abordar estas limitaciones, y ofrecer otras recomendaciones, se presenta una guía práctica orientada a fortalecer la cultura de ciberseguridad en las organizaciones y, de manera particular, en sus órganos de gobierno.

Se entiende por cultura de ciberseguridad el entramado de percepciones, actitudes, valores, suposiciones y conocimientos compartidos dentro de una organización, los cuales influyen en su forma de operar y en el cumplimiento de los

requisitos necesarios para proteger su información. Esta cultura busca moldear las conductas de los empleados hasta lograr que las prácticas de seguridad se integren de manera natural en sus actividades cotidianas.

La guía práctica orientada a potencializar la cultura de ciberseguridad en las organizaciones incluye una estrategia orientada a fortalecer las capacidades de los órganos de gobierno y generar conciencia sobre el impacto de la ciberseguridad en la organización. Esta estrategia destaca la importancia de vincular a las personas, la tecnología y los procesos, e incluye los siguientes pasos:

1. Evaluar la madurez de la cultura de ciberseguridad en la junta directiva, utilizando marcos previamente establecidos, entre los que se destaca el modelo de Hayden, que identifica las capacidades culturales de los individuos dentro de una organización.
2. Asignar los recursos necesarios para la gestión de la ciberseguridad.
3. Concientizar a los miembros de la junta directiva sobre las amenazas cibernéticas y sus posibles consecuencias.
4. Establecer un plan de capacitación en ciberseguridad que contemple los fundamentos, los riesgos, las amenazas y las implicaciones de la ciberseguridad para la organización.
5. Analizar el comportamiento de los miembros de la junta directiva en relación con la ciberseguridad.
6. Asumir la ciberseguridad como un valor corporativo, lo que impulsa a la organización a cumplir las normativas y promover buenas prácticas en materia de ciberseguridad.

En síntesis, el capítulo sostiene que la adopción de una cultura de ciberseguridad supone un cambio en la percepción y el comportamiento de los miembros de la organización. Para impulsar esta transformación, es fundamental que los directivos comprendan la importancia de la ciberseguridad y promuevan prácticas seguras, apoyándose en una propuesta que simplifique su implementación.

La conclusión central de este libro es que la transformación digital ha evolucionado hacia la creación de ecosistemas digitales que, además de impulsar el diseño de modelos de negocio adaptados a los entornos digitales, favorecen la integración de los activos de las TI y las TO. En algunos casos, estos ecosistemas asumen la gestión de infraestructuras estratégicas fundamentales para la nación, consolidándose como pilares clave en el desarrollo económico y tecnológico.

El desarrollo y la convergencia de los ecosistemas digitales han provocado un aumento considerable de los requerimientos en materia de ciberdefensa y

ciberseguridad. Esta situación ha impulsado la adopción de tecnologías innovadoras orientadas a fortalecer la detección, la prevención y la mitigación de los efectos adversos de los ciberataques, lo que ha conducido a la consolidación de un enfoque más robusto y proactivo en la protección de los entornos digitales.

Existe un consenso generalizado sobre el hecho de que la principal vulnerabilidad radica en el mal uso de las TIC. Por esta razón, se subraya la imperiosa necesidad de promover una cultura de ciberseguridad, que, en este caso, es liderada por las juntas directivas. Se ha insistido en que, a mayor conectividad y transformación digital, mayores son las amenazas, las cuales requieren sistemas de ciberseguridad y ciberdefensa más avanzados.



Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales

El libro "Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales" aborda la ciberseguridad como un elemento indispensable para la sostenibilidad y competitividad de las organizaciones en un mundo digital interconectado. Destaca la creciente interdependencia de los sistemas digitales y los riesgos asociados, subrayando la necesidad de implementar estrategias robustas que no solo protejan activos, sino que también aseguren la continuidad operativa. A través del libro, se analizan temas relevantes como la gestión de la identidad digital en infraestructuras críticas, el papel de la inteligencia artificial en la ciberseguridad, y la integración de la ciberseguridad y la ciberdefensa en la planificación estratégica. Las conclusiones enfatizan en que una cultura organizacional proactiva y una integración efectiva de la ciberseguridad son esenciales para mitigar riesgos y proteger la reputación empresarial en un entorno en donde emergen rápidamente amenazas y riesgos.



ISBN 978-628-7602-99-1

