Summer 7-30-2024

# Industria 4.0. Internet de las Cosas: ciberseguridad y aplicaciones

Jairo Eduardo Márquez Díaz

Arles Prieto Moreno

Luz Jaddy Castañeda Rodríguez

Luis Gonzalo Benavides Ramírez

# Industria 4.0.

## Internet de las Cosas:
### ciberseguridad y aplicaciones


Jairo Eduardo Márquez Díaz
Compilador

Jairo Eduardo Márquez Díaz
Arles Prieto Moreno
Luz Jaddy Castañeda Rodríguez
Luis Gonzalo Benavides Ramírez
Autores

# Industria 4.0.
# Internet de las Cosas:
## ciberseguridad y aplicaciones

# Industria 4.0. Internet de las Cosas: ciberseguridad y aplicaciones

Jairo Eduardo Márquez Díaz
Compilador

Jairo Eduardo Márquez Díaz
Arles Prieto Moreno
Luz Jaddy Castañeda Rodríguez
Luis Gonzalo Benavides Ramírez
Autores

Autores: Márquez Díaz, Jairo Eduardo, Prieto Moreno, Arles, Castañeda Rodríguez, Luz Jaddy y Benavides Ramírez, Luis Gonzalo
Industria 4.0. Internet de las cosas, Ciberseguridad y Aplicaciones, Fusagasugá, Cundinamarca, Colombia, Sello Editorial, Universidad de Cundinamarca
Industrias 4,0. —Internet de las cosas. —Malware. —Firmware. —Rasomware. —Drones. —Inteligencia Artificial. —Ciberseguridad.
Fusagasugá: Sello Editorial Universidad de Cundinamarca
2024, 284 páginas; 17 cm x 23,5 cm, contiene figuras y tablas
Incluye referencias bibliográficas

ISBN: 978-628-7621-85-5
eISBN: 978-628-7621-86-2



1.a edición, 30 de julio de 2024



John Alexander Moreno Sandoval
Director Editorial

Daniel Alonso Mattern Hernández
Coordinación Editorial

César Augusto Buitrago Quiñones
Editor de Publicaciones

Cindy Catherine Martínez Martínez
Corrección de Estilo

Rubén Alberto Urriago Gutiérrez
Diseño y Diagramación

Impresión: Multi Impresos S.A.S.

Universidad de Cundinamarca
Fusagasugá, Colombia
Diagonal 18 No. 20-29
Teléfono: (+571) 828 1483
editorial@ucundinamarca.edu.co
https://www.ucundinamarca.edu.co

Primera edición, 2024

Esta obra tiene una versión de acceso abierto disponible en el Repositorio Institucional de la Universidad de Cundinamarca: https://repositorio.ucundinamarca.edu.co
Universidad de Cundinamarca
Vigilada Mineducación
Reconocimiento personería jurídica: Resolución No. 19530, de diciembre 30 de 1992

# Contenido

# Lista de figuras

# Lista de tablas

# Glosario

AIoT: Internet de las Cosas e Inteligencia Artificial
APT: Amenaza Persistente Avanzada (Advanced Persistent Threat)
DDoS: Denegación de Servicio Distribuido (Destributed Denial of Service)
DL: Deep Learning
DoS: Denegación de Servicio (Denial of Service)
DSM. Deep Soil Mixing
Endpoint: Puntos Finales de Dispositivos en Una Red
GCP: Ground Control Points
GPS: Sistema de posicionamiento global (Global Posistion System)
IA: Inteligencia artificial
IIoT: Internet industrial de las cosas
IoT: Internet de las cosas (Internet of Thinks)
LiDAR: Light Detection and Ranging
Malware: Software malicioso
ML: Machine Learning
PLC: Controladores Lógicos Programables
PPK: Kinematic postprocesado
SCADA: Supervisory Control and Data Acquisition
SOC: Centro de Operaciones de Seguridad
TI: Tecnologías de la Información
TIC: Tecnologías de la Información y la Comunicación
TO: Tecnologías Operativas
VPN: Red Privada Virtual (Virtual Privacy Network)
ZTNA: Zero Trust Network Access

# Prólogo

El propósito de este libro consiste en mostrar cómo la Cuarta revolución industrial —o Industria 4.0— está transformando la industria con la automatización avanzada y las tecnologías digitales. La Industria 4.0 ofrece numerosos beneficios, como mayor eficiencia, productividad y flexibilidad a través de la integración de sistemas, automatización y tecnologías disruptivas. Este cambio industrial está impulsado por diversas tecnologías que facilitan el monitoreo y el control remoto de instalaciones industriales y hogares.

En el libro se explican conceptos básicos sobre la Industria 4.0 y la automatización industrial, así como sus pilares tecnológicos como el Internet de las cosas (IoT), la impresión 3D, el Big data, la inteligencia artificial (IA), la realidad aumentada, entre otros y se analiza cómo estos están revolucionando la industria. Posteriormente, se profundiza en la transformación digital como el IoT industrial, la ciberseguridad, el uso de drones en la seguridad laboral, con el fin de proveer conocimientos y recomendaciones prácticas para maximizar los beneficios y minimizar los riesgos que conlleva la implementación

de las nuevas tecnologías —como, por ejemplo— en la operación minera.

De manera particular, se aborda el IoT como tecnología clave de la Industria 4.0, que permite la monitorización y control remoto de procesos industriales y de servicios. Sin embargo, esta industria conlleva riesgos de ciberseguridad que amenazan la disponibilidad, integridad y confidencialidad de los datos e infraestructuras. Por lo tanto, se requieren estándares y tecnologías de seguridad como la IA y el *blockchain*, entre otros, para mitigar las vulnerabilidades en diversos entornos de la industria, como, por ejemplo, con los vehículos autónomos y las tecnologías inmersivas.

La tecnología de drones en combinación con los sistemas de Detección de Rango de Luz (LiDAR —por sus siglas en inglés— *Light Detection and Ranging*) y la fotogrametría están revolucionando operaciones de diversas índoles, en particular, en el sector minero, caracterizado por ser difícil y peligroso. El sistema LiDAR puede emplearse para realizar escaneo de topografías en campos abiertos y minas abandonadas o subterráneas, sin exponer a los trabajadores, mostrando su valía en la exploración, sondeo, monitoreo y detección de minerales y de potenciales peligros relacionados con la acumulación de gases, las fallas geológicas, etc.

El uso de drones y tecnologías digitales mejoran la seguridad y el cumplimiento de normativas, lo

que reduce los incidentes y enfermedades laborales. No obstante, se requiere abordar desafíos tecnológicos, económicos y ambientales para asegurar el futuro sostenible de la industria, en particular, de la industria de la minería de carbón.

En el caso concreto de la minería de carbón en Colombia, el contexto regulatorio sobre la salud ocupacional enfrenta varios desafíos a futuro, en especial, en lo que respecta a los problemas de salud y seguridad para los mineros, como las enfermedades respiratorias, los trastornos musculoesqueléticos, los riesgos de seguridad y cómo las regulaciones, las métricas y las mejores prácticas pueden contribuir con los resultados exitosos de los trabajadores mineros. Este será un insumo valioso para seguir avanzando hacia una minería más sostenible, productiva y humana.

Los aspectos técnicos y las consideraciones prácticas para transformar digitalmente las operaciones de la industria y los servicios conducentes a lograr una verdadera Industria 4.0 en Colombia, se presentan al final del presente texto.

## Capítulo 1

# Industria 4.0 y la transformación digital

*Arles Prieto M., Jairo E. Márquez D., Luz J. Castañeda R.* y *Luis G. Benavides R.*

La Industria 4.0 —también llamada Cuarta Revolución Industrial— integra las tecnologías digitales inteligentes en los procesos industriales y de fabricación, abarca un conjunto de tecnologías que incluyen "redes industriales de internet de las cosas (IoT), inteligencia artificial (IA), aprendizaje automático, Big Data, robótica y automatización, sistemas autónomos, entre otras, que permite la fabricación y la creación de fábricas inteligentes" (Márquez, 2020, p. 15). Este tipo de industria se caracteriza por tener gran influencia de la digitalización, la interconexión y la automatización en los procesos productivos. La Industria 4.0

> está revolucionando la forma en que la que las empresas fabrican, mejoran y distribuyen sus productos. Los fabricantes están integrando nuevas tecnologías, equipadas con sensores avanzados, software integrado

> y robótica que recopilan y analizan datos permitiendo una mejor toma de decisiones. (IBM, 2023, p. 5)

La Cuarta Revolución Industrial es un concepto utilizado para identificar a la industria moderna que hace uso de diferentes tecnologías emergentes, las plataformas informáticas y las herramientas de las Tecnologías de la Información y la Comunicación (TIC), con el fin de agilizar los procesos internos, por medio de sistemas de producción reconfigurables que interpretan las tendencias de consumo de los clientes, a través de algoritmos complejos de (IA) y mejora los estándares de calidad, posiciona los productos en el mercado y conecta a un mundo globalizado, con el objetivo de que en el futuro inmediato se logre una integración —por medio de las redes— y se pueda ofertar sistemas de producción más robustos, capaces de interactuar entre sí y con los operarios a través de interfaces inteligentes.

Esta revolución también se caracteriza por la integración de lo físico con lo digital, permitiendo la comunicación entre máquinas, sistemas y personas, lo que deriva en varias ventajas competitivas entre las empresas que ingresan a estos nuevos modelos de producción, compuesta por sensores y actuadores, los cuales brindan la capacidad de proporcionar información en tiempo real y se pueden adaptar con gran facilidad a las necesidades propias de cada proceso con plena autonomía, permitiéndole a los operarios realizar otras actividades.

Finalmente, la Cuarta Revolución Industrial tiene como objetivo mejorar la eficiencia, productividad, calidad y sostenibilidad de la producción, lo que genera un impacto significativo en la economía mediante la creación de nuevos modelos de negocio. Al combinar "los datos de operaciones de producción con los datos operativos, la cadena de suministro, el servicio de atención al cliente y otros sistemas empresariales permite niveles completamente nuevos de visibilidad y conocimiento, a partir de información almacenada previamente" (Sección industrial, 2023, s. p.). Estas tecnologías digitales han impulsado de manera progresiva la automatización y "el mantenimiento predictivo, la optimización de procesos, la eficiencia y la capacidad de respuesta a los clientes" (Villegas, 2023, p. 64). En un entorno globalizado y digitalizado la adopción de estas nuevas tecnologías se vuelve cada vez más crucial para que las empresas mantengan su competitividad.

## Revolución Industrial

Según un artículo publicado en la *Enciclopedia Británica* (2022), "el término revolución industrial fue acuñado por el historiador inglés Arnold Toynbee para describir el desarrollo económico de Gran Bretaña, entre 1760 y 1840" (s. p.). Se define como un proceso histórico asociado a la transformación

económica y social que resultó en cambios significativos a nivel mundial. A lo largo del tiempo, el término ha adquirido un significado más amplio, refiriéndose a una transformación económica en lugar de un periodo específico en un medio determinado. Esto explica por qué algunos países como China e India experimentaron su propia revolución industrial en el siglo xx, mientras que en países como Estados Unidos y algunos de Europa occidental, experimentaron una segunda revolución industrial a fines del siglo xix.

Los avances tecnológicos de la revolución industrial posibilitaron un uso más amplio de los recursos naturales y la producción masificada de bienes manufacturados (Rincón, 2019). A continuación, se presentan algunos ejemplos de estos cambios:

- Introducción de nuevos materiales a la industria, especialmente hierro y acero.
- Empleo de fuentes de energía como combustibles y fuerza motriz, como, por ejemplo, el carbón, el petróleo, la electricidad, la máquina de vapor y el motor de combustión interna.
- Nuevas máquinas como la hiladora y el telar mecánico.
- Implementación de una nueva forma de organización laboral, creando mayores divisiones de trabajo, especializaciones y funciones.

- Desarrollos significativos en el ámbito del transporte y las comunicaciones.
- Mayor aplicación de los conocimientos científicos a la industria.

Villas (2006) sostiene que "históricamente se denomina revolución a aquellas transformaciones que presentan tres características esenciales: producirse en un tiempo comparativamente corto; transformar profundamente las estructuras: económica, política, social o cultural; e implicar un punto de no retorno" (p. 50). Además, están estrechamente relacionadas con los cambios poblacionales que se dieron en ciertos periodos de tiempo, especialmente, por la migración masiva de personal del campo a las ciudades en busca de un mejor futuro y oportunidades laborales. Asimismo, Chaves (2004) afirma que "la industrialización fue impulsada por una sucesión interrelacionada de cambios tecnológicos que sustituyeron a la capacidad humana por instrumentos mecánicos, así como la energía liberada por animales" (p. 93). Durante este periodo se observaron nuevos avances en áreas no industriales, que incluyeron:

- Mejoras agrícolas que permitieron suministrar alimentos a una población cada vez más creciente.
- Cambios económicos conducentes a una repartición más equitativa de la riqueza. "Es-

to redujo la importancia de la tierra como fuente primaria de riqueza frente al aumento de la producción industrial y el comercio internacional" (Banca electrónica, 2022).

- Transformaciones políticas que reflejaron el surgimiento del poder económico y llevaron a la implementación de políticas estatales, acordes con las necesidades de una sociedad industrializada.

En este contexto, los trabajadores adquirieron habilidades distintivas y experimentaron un cambio en su relación con el trabajo. Hubo una transición de ser artesanos para convertirse en operadores de máquinas. En consecuencia, a lo largo de la historia, se han dado lugar a cuatro revoluciones industriales, tal como se detalla a continuación.

## Primera revolución industrial (1760 - 1830)

El aumento poblacional que se presentó en el siglo xviii en Estados Unidos y en algunos países europeos como el Reino Unido, Alemania, Francia, entre otros, dio origen a diferentes movimientos que propiciaron el desarrollo y crecimiento de la industria, liderado principalmente por el sector agrario, que llevó a los granjeros de la época a realizar grandes inversiones en infraestructura, con el objetivo de ser más productivos y así, dar prioridad a las necesidades de una población cada vez más creciente,

lo que demandaba un mayor consumo de alimentos. Este fenómeno además de generar aumentos en las ganancias de los granjeros también permitió el desarrollo de otros sectores como el textil, en el que hizo uso de nuevas fuentes de energía y de maquinaria especializada para aumentar la manufactura y el lucro, con menos mano de obra.

En esta revolución se presentaron grandes desarrollos —como la metalurgia a gran escala— con el uso del carbón de madera y el mineral, la invención de la energía hidráulica, fundamental para el crecimiento de la economía, las máquinas a vapor que dieron origen a las locomotoras, los barcos y la construcción de grandes calderas, vitales para los procesos masificados. Lo anterior se simplifica en la Figura 1:


**Figura 1.** *Fábricas movidas por calderas a vapor agrupadas en grandes espacios e infraestructuras*
Fuente: elaboración propia.

*Industria minera:* con la explotación de grandes yacimientos de carbón mineral para combustible de los hornos y las máquinas a vapor, así como hierro y otros minerales, surgieron paralelamente otras industrias complementarias como los sistemas de ventilación, la fabricación de rieles para los equipos mineros de socavón, fundición de piezas pesadas para maquinaria industrial, entre otras.

*Industria siderúrgica:* con el desarrollo de controles para hornos especiales de altas temperaturas fue posible forjar metales como el hierro y el acero que se convirtieron en las principales materias primas para la construcción de herramientas agrícolas, máquinas textiles, locomotoras, rieles de ferrocarril, embarcaciones, etc., que se convirtieron en uno de los principales propulsores del desarrollo industrial del momento.

*Industria del transporte:* con el crecimiento de las industrias surgió la necesidad de llevar los productos manufacturados y las materias primas para exportación a los puertos de cargas, a las fábricas y a las ciudades donde eran distribuidas, de modo que el ferrocarril fue el medio de transporte más utilizado por su capacidad de carga —tanto de materiales como de pasajeros—, que generó dividendos para las compañías que inicialmente hicieron grandes inversiones en infraestructura, terminales de carga, construcción de plantas físicas, adquisición de

maquinaria y vehículos —estructurando la nueva industria—, impulsando la mano de obra y el crecimiento comercial sin precedentes.

## Segunda Revolución Industrial (1870 - 1914)

Esta revolución inició con el surgimiento de nuevas industrias como la industria química, las exploraciones petroleras, la industria automotriz, las comunicaciones eléctricas, la organización del trabajo, la aviación, nuevas máquinas a vapor y la introducción de otras fuentes de energía como la electricidad y el gas, por mencionar algunas. También se presentó la primera globalización al ampliarse el comercio con otros continentes, lo que generó un cambio económico mundial que llevó a los Estados Unidos y Alemania a liderar la producción industrial.

Esta revolución generó un cambio significativo en el orden económico mundial. González et ál. (2021) señalan que fue el detonante para que existiera una mayor interrelación entre la ciencia y la tecnología, sentando las bases para el avance económico que se vio reflejado en el siglo xx. En este periodo también se dio una mejora sustancial del nivel de vida de las clases media y trabajadora, al aumentar el poder adquisitivo por el bajo costo de los productos; además se realizaron adelantos significativos en investigaciones científicas y tecnológicas.

## Tercera Revolución Industrial

Inició a mediados del siglo xx, tecnológicamente tuvo su auge después de la creación del transistor en los laboratorios de la Bell Telephone, en 1948. En 1958 el ingeniero norteamericano, Jack Clair Kilvy, logró miniaturizar la creación con un oscilador funcional —conformado por unos pocos transistores y componentes electrónicos— en una oblea de silicio, dando origen a los Circuitos Integrados (ic). Posteriormente, a inicios de los años setenta, varias compañías de tecnología compitieron por integrar más transistores en los ic, hasta que, a finales de la década, se crearon los primeros microprocesadores, con lo que se logró revolucionar el mercado tecnológico, así como sentar las bases del desarrollo tecnológico moderno.

Entre los desarrollos más destacados de esta revolución industrial —en la década de los setenta— está la fibra óptica, el Internet, los videojuegos de consola, el microprocesador, los computadores y la electrónica de consumo, representada en electrodomésticos y equipos para la industria, así como los primeros desarrollos de software, la estandarización de las redes informáticas, la automatización de maquinaria para mejorar los procesos industriales, el desarrollo de las Tecnologías de la Información y Comunicación (tic). Joyanes (2017) afirma que

> esta revolución es conocida como la de inteligencia y se caracterizó por la microelectrónica como la base de procesamiento, el computador como máquina más destacada, el Internet como gran dinamizador del cambio y el uso de energía atómica y renovable. (p. 6)

Además, desde el punto de vista social, se dieron grandes cambios especialmente en la globalización, el desarrollo de las comunicaciones, el incremento demográfico, las tendencias de consumo y el comercio electrónico.

## Cuarta Revolución Industrial

También conocida como "Industria 4.0" es un término propuesto por académicos, empresarios y personajes de la política alemana, quienes propusieron en el año 2011 aumentar la competitividad de la industria manufacturera en la producción en línea, integrando Sistemas Ciberfísicos (CPS —por sus siglas en inglés— *Cyber Physical Sistems*). Asimismo, Joyanes (2017) sostiene "que los CPS es un término genérico para hacer alusión a la integración de las máquinas inteligentes conectadas a la red y la mano de obra humana con el objetivo de ofrecer mejores ambientes laborales" (p. 10).

Luego, en 2014, esta iniciativa fue acogida por grandes compañías norteamericanas como General Electric, AT&T, IBM, Intel, entre otras, quienes relacionaron paulatinamente este témino con las fábri-

cas inteligentes. Este escenario generó una serie de cambios significativos, especialmente en la forma en la que se organizaron los medios de producción, mediante las tecnologías emergentes, la digitalización de la información, el uso de las herramientas TIC y tecnologías disruptivas como: Cloud Computing, IoT, sistemas Ciberfísicos, computación Ubicua, Big Data, impresión 3D, automatización industrial, virtualización de redes 6G, comunicaciones, realidad aumentada, nanotecnología, etc., que están revolucionando la manera de comprender la tecnología y cómo los seres humanos interactúan con ella.

Por su parte, Barona y Velasteguí (2021) señalan que "esta nueva revolución industrial se ha caracterizado por lograr la interconexión de los sistemas productivos industriales con la sociedad digital, con el propósito de satisfacer las demandas de consumo de las personas a un nivel acelerado" (s. p.). Algunas de las principales características e impactos son:

1. *Automatización y autonomía:* los sistemas de producción son cada vez más capaces de tomar decisiones basadas en datos suministrados en tiempo real por sensores, robots y sistemas ciberfísicos, quienes tienen un rol fundamental en la automatización de los procesos, ideales para la industria moderna y su interacción con el mundo exterior.

Los mercados globalizados han llevado a la industria moderna a estructurar nuevas estrategias para responder a las demandas de nuevos clientes con otras culturas de consumo.

2. *Fabricación inteligente y personalizada:* con el surgimiento de las máquinas computarizadas y reprogramables se hace posible adaptar los sistemas de producción, para la fabricación de productos personalizados con técnicas de fabricación aditiva (impresión 3D) y la fabricación ágil. Esto converge en que se pueda responder rápidamente a las demandas del mercado, para quienes cuentan con este tipo de infraestructura, porque sus mercados van dirigidos a clientes que requieren prototipos de pocas unidades.
3. *Colaboración humano-máquina:* los operarios interactúan con tecnologías avanzadas y sistemas automatizados, aprovechando las capacidades de la IA y la robótica, para mejorar la productividad y la seguridad en el trabajo, reduciendo los riesgos y optimizando los recursos de las compañías. Para ello es esencial el uso de los Controladores Lógicos Programables (PLC). De lo anterior, Newball (2014) afirma que "estos equipos pueden contar puertos de comunicaciones, pines de

> entradas y salidas análogas y digitales, siendo una evolución a los sistemas de control basados en circuitos electrónicos relés, interruptor y lógica combinacional" (s. p.).

## Beneficios de la Industria 4.0

A medida en que el concepto de Industria 4.0 se ha popularizado e integrado con otras tecnologías emergentes en los diferentes campos de aplicación, se evidencia una serie de beneficios en los procesos productivos y modelos de negocios, proporcionando algunos elementos estratégicos señalados por Beliz (2018):

> Se han generado una serie de cambios y nuevos conceptos como el nuevo estadio de la globalización, la cual se denomina glocal (global + local); el surgimiento de la inteligencia artificial para constituir un nuevo factor de producción; las ventajas comparativas (basadas en recursos naturales) y competitivas (basadas en costos inferiores); surge el concepto de integración hibrida; la disrupción tecnológica haciendo énfasis en nuevos escenarios de trabajo; la producción y comercialización de bienes basada en el contenedor de la era industrial, entre otras. (p. 8)

Algunos de los principales beneficios de esta nueva tendencia tecnológica son:

- *Eficiencia:* la integración de las diferentes tecnologías desarrolladas en los últimos años ha permitido la realización de procesos pro-

ductivos más eficientes y rápidos, que dejan como valor agregado la optimización de recursos energéticos y mejor aprovechamiento de las materias primas. Se evitan reprocesos de productos terminados gracias a que las máquinas modernas —en su gran mayoría— están dotadas de sistemas de control electrónico con interfaces amigables para los operarios, así como de software para trabajar de forma automática.

- *Agilidad:* gracias la digitalización moderna y al desarrollo de medios físicos para el almacenamiento de información se puede tratar la optimización y análisis de datos que fortalecen la toma de decisiones. Esto agiliza los procesos de cada evento significativo, los cuales son registrados una línea de tiempo de las actividades internas de las compañías, lo que permite la flexibilidad de la empresa y el intercambio de los recursos de un producto a otro, de una manera más rápida y acorde a las necesidades de los clientes.
- *Innovación:* todas las tecnologías que soportan la Industria 4.0 están originando nuevos modelos de negocio y formas de creación, investigación e innovación. Este hecho hace que tanto la academia como la industria patrocinen el desarrollo de proyectos que se destaquen en el mercado y que a sus líde-

res se les ofrezcan ciertas garantías laborales para que continúen las investigaciones. Desde luego, muchas empresas dedicadas al desarrollo investigativo destinan grandes recursos económicos para acondicionar las infraestructuras y realizar una mejor selección de talento humano, debido a que ello genera mejores resultados.

- *Experiencia de usuario y personalización de producto:* a diferencia de las revoluciones anteriores, donde los fabricantes se caracterizaron por crear grandes líneas de producción para tener mayores stocks de mercancías en bodegas, esta revolución va enfocada hacia la fabricación personalizada, buscando un mayor grado de satisfacción del cliente y, de esta manera, elevar la experiencia de usuario al ofertar un mejor servicio.
- *Reducción de costos:* las compañías modernas hacen uso de las TIC, para lograr una mayor eficiencia en los procesos internos, una mejor administración de los recursos y un incremento en la agilidad y rapidez de producción. Esto conlleva a la disminución considerable de los tiempos de inactividad de las máquinas, lo que permite reducir costos de producción y con ello, ofrecer mejores beneficios a los clientes.
- *Mejora de ingresos:* la implementación de las TIC en la industria ha generado mejoras sig-

nificativas en los ingresos, se ha observado un aumento en la automatización de las líneas de producción completas, lo cual ha llevado a una disminución de los costos de producción y de mano de obra. Además, esta implementación ha permitido ampliar los portafolios de servicios, que a su vez han conducido a un incremento en las ventas y en los ingresos de la industria.

## Automatización Industrial 4.0

Se define como una serie de técnicas, métodos y tareas que, por lo general, no requiere de la intervención humana para su funcionamiento. Dada la versatilidad, la reducción de costos de producción es evidente, lo que mejora la competitividad entre compañías para lograr un mejor posicionamiento de los productos manufacturados en los mercados, sumado a que permite resolver problemas de distintas naturalezas, como la técnica. Witorg (2019), afirman que "toda empresa busca la eficiencia económica y productiva para ser sostenible en el mundo actual, que conlleva a que los productos manufacturados evolucionen a la denominada cuarta revolución industrial" (s. p.).

En la Figura 2 se observa lo que sucede al interior de las compañías que han entrado al boom de la tecnología, en las que se evidencia el uso de las redes ubicuas para la supervisión remota de las má-

quinas; gracias a las plataformas informáticas e interfaces de potencia —diseñadas para estos fines—, el control automático es una realidad y es una de las tantas ventajas que ofrece la industria moderna para el procesamiento de información —suministrada en tiempo real y por sensores—, lo que ha dado origen al desarrollo de equipos electrónicos inteligentes, fundamentados en sistemas embebidos para la ejecución de complejos algoritmos en diferentes lenguajes de programación.

**Figura 2.** *Control remoto de robots en una fábrica de producción*
Fuente: elaboración propia.

El desarrollo de microprocesadores industriales de la década de los ochentas llevó a las compañías de electrónica a diseñar nuevos sistemas de control y a aumentar significativamente la capacidad de procesamiento de los autómatas programables, lo que impulsó la revolución industrial y el desarrollo de

técnicas más complejas para mejorar las capacidades en la maquinaria industrial, caracterizadas por poseer una mayor eficiencia, seguridad y calidad, así como conectividad con las TIC que integran la Industria 4.0.

## Características de los automatismos eléctricos

Los automatismos eléctricos son muy útiles en la cadena de producción de la industria, pues son la base del procesamiento de la información —suministrada por sensores— para la toma de decisiones, promover la competitividad, reducir costos, ganar tiempo y ofrecer calidad en los productos. Entre sus principales características se encuentran:

- Intervención directa en los procesos industriales.
- Son desarrollados para realizar tareas complejas, repetitivas y optimizar tiempos.
- Poseen flexibilidad para transformar las materias primas.
- Se puede realizar una mejora constante en la calidad de los productos.
- Aumenta la seguridad operativa, especialmente cuando se realizan actividades de riesgo para los operarios.
- Son especiales en procesos donde se opera a temperaturas elevadas, se manipulan sus-

tancias toxicas o existen otro tipo de altos riesgos.

Los automatismos eléctricos se diseñan para ofrecer a la Industria 4.0 una mayor flexibilidad, integración y conectividad. También permiten el control y monitorización remota a través de Internet y la integración de distintos sistemas de automatización. Algunas características importantes son:

1. Conectividad abierta y protocolos estandarizados: se basan en protocolos Ethernet e IP para facilitar la comunicación e integración con otros sistemas.
2. Electrónicos programables (PLC): se caracterizan por recoger y procesar datos de forma remota para tomar decisiones autónomas en tiempo real.
3. Interfaces hombre-máquina (HMI): permiten supervisar y controlar los procesos de manera intuitiva a través de pantallas táctiles.
4. Internet industrial (IIoT): los dispositivos están conectados a Internet industrial para permitir una comunicación rápida y segura entre máquinas, sistemas y personas.
5. Integración de la cadena de suministro: la conectividad permite "integrar todos los elementos de la cadena de suministro desde proveedores hasta clientes" (Portugal et ál., 2023, p. 7207).

6. Análisis de datos: los datos recopilados por los diferentes sensores permiten realizar análisis predictivos que mejoran la eficiencia, productividad y flexibilidad de los procesos.

## Pirámide de automatización

Representa los niveles de automatización e integración que debe poseer la empresa moderna para que los procesos de fabricación y manufactura estén alineados con los sistemas de gestión y administración de los recursos, a fin de lograr una comunicación ideal con los eslabones de la cadena de valor, como se muestra en la Figura 3.


**Figura 3.** *Pirámide de la automatización*
Fuente: elaboración propia.

Las cinco etapas de la pirámide de la automatización se distribuyen en los diferentes niveles que debe ejecutar la alta gerencia para tener una producción con los últimos estándares de calidad. La descripción de cada nivel es la siguiente:

***Nivel I o de Campo:*** está conformado por una amplia variedad de dispositivos (sensores) que tienen como función tomar las señales del ambiente y convertirlas en pulsos eléctricos para su control, son similares a actuadores que se activan según la etapa del proceso, para el monitoreo de las variables y protocolos de comunicaciones —con instrumentos de medición—, que luego se envía a las capas superiores de la pirámide.

***Nivel II o de Control:*** aquí se encuentran los dispositivos que procesan las señales recibidas en el nivel I: Computadores Personales (PC), Controladores Lógicos Programables (PLC), Sistemas de Control Proporcional, Integral Derivativo (PIDs), algunos sistemas embebidos, entre otros, cuya función es ejecutar algoritmos de funcionamiento de los procesos, para que las máquinas ejecuten las tareas de forma secuencial y autónoma.

***Nivel III o de Supervisión:*** lo conforman los Sistemas de Control y Adquisición de Datos (SCADA, por sus siglas en inglés, *Supervisory Control and Data Acquisition*), que son los encargados del monitoreo de los procesos productivos, el almacenamiento de la información, la representación gráfica

de las variables controladas, la generación de alarmas, entre otros, así como lograr la conectividad con otras aplicaciones, bien sean locales o distribuidas en la nube.

***Nivel IV o de Planificación:*** tiene como función gestionar los Sistemas de Ejecución de la Producción (MES —por sus en siglas en inglés— *Manufacturing Execution Systems*), generalmente conformado por un software integral que sigue el proceso de fabricación de un producto y realiza analítica de datos para su documentación, con el objetivo de optimizar las actividades de producción. Con este sistema se realiza una gestión constante que permite tener una visión más amplia y en tiempo real del estado de la producción para obtener información clave que apoye la gestión relacionada con la cadena de suministro y las actividades de mercadeo de los productos finales.

***Nivel V o de Gestión:*** se encuentra en la cúspide de la pirámide y su función principal es la Administración de los Recursos de la Empresa (ERP —por sus siglas en inglés— *Enterprise Resource Managenet*), los cuales se integran en una serie de módulos de software para la recolección, almacenamiento y disposición de la información, con el propósito de auspiciar la toma de decisiones en tiempo real, así como permitir la toma correctivos y dar soluciones a problemas que no se solucionaban antes porque

los módulos trabajaban por separado y dificultaba su gestión.

## Tecnologías esenciales de la Industria 4.0

El avance tecnologíco al que se ha llegado en las últimas décadas, ha traido consigo una serie de desarrollos, tanto en el campo de la informática como en la electrónica industrial y de consumo, permitiendo que se complementen, para dar origen a diferentes tecnologias emergentes que hoy facilitan la adquisición, procesamiento, interpretación de datos y conexión global. Garrell y Guilera (2019) sostienen que

> que muchos de los avances tecnologicos que hoy son la base de la Industria 4.0 permitirán en el futuro inmediato transformar drasticamente la producción, llevano a las fábricas a una mayor eficiencia y productividad, por encontrarse totalmente integrada y automatizada. (s. p.)

En la Figura 4 se relacionan algunas de las tecnologías adoptadas por la Industria, que actualmente se están implementando en muchos sectores con resultados positivos. A continuacion, se hace una breve descripción de cada una de ellas, así:


**Figura 4.** *Tecnologías esenciales en la industria 4.0*
Fuente: elaboración propia.

La Industria 4.0 está conformada por otras tecnologías que la complementan y que se convierten en los pilares fundamentales que soportan la infraestructura de la industria moderna, las cuales se mencionan a continuación.

### *Fabricación Aditiva*

La fabricación aditiva o impresión 3D se caracteriza por ser una tecnología revolucionaria de la Industria 4.0, permite modelar objetos tridimensionales, a través de la aplicación de capas sucesivas de ma-

teriales como resinas, ABS, PLA, Nylon, PETG, como se muestra en la Figura 5. Esta tecnología facilita el diseño de prototipos que, a diferencia de los métodos tradicionales de fabricación, donde se invertían horas de trabajo eliminando material (fabricación sustractiva), esta construye los objetos capa por capa, a partir de un modelo digital diseñado en un software especial, conocido como Diseño Asistido por Computador (CAD).

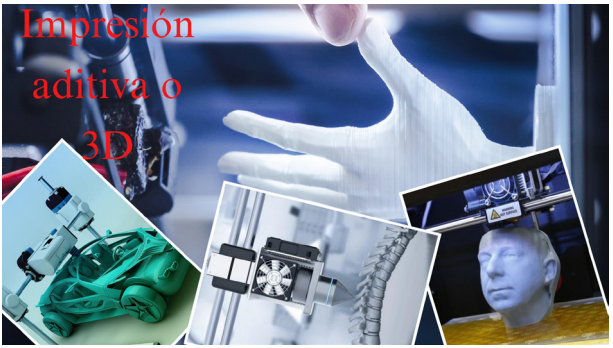



**Figura 5.** *Impresión aditiva o 3D*
Fuente: elaboración propia.

El proceso de fabricación inicia con la creación del modelo en 3D —a través de un software de diseño— del objeto que se quiere imprimir; luego se genera un archivo que se convierte en la información suministrada a los motores de la impresora 3D para que inicie a depositar el material, capa por capa y con una precisión milimétrica, hasta formar la fi-

gura. Para generar esta impresión, existen diferentes tipos de tecnologías como las siguientes:

- Deposición de material fundido.
- Sinterización selectiva por láser.
- Fusión de láser selectiva.
- Estereolitografía.

Este tipo de impresión se está utilizando para la fabricación de piezas que ya no se encuentran en los mercados especializados, así como para prótesis y productos exclusivos. Además, esta tecnología permite hacer prototipos en tiempos muy cortos a bajo costo y realizar correctivos *in situ*. Zahera (2012), afirma que:

> Las fábricas no son ajenas a este fenómeno y existen otros términos relacionados con el prototipado rápido conocidos como Software de Fabricación Asistida por Computador (CAM) o para la asistencia a la Ingeniería (CAE), así como el empleo de autómatas y Robots en planta, la inspección por visión artificial, el control del avance de la producción en tiempo real (MES), o incluso la modelización y recreación virtual de procesos y fábricas enteras con software de simulación (CAPE). (p. 2)

La fabricación aditiva se caracteriza porque ofrece a los usuarios finales ventajas como:

- Diseño y personalización: su función principal es la fabricación de objetos con geometrías complejas y diseños personalizados,

que se dificultan fabricarlos con métodos tradicionales.

- Eficiencia y reducción de costos: puede minimizar el desperdicio de material, así como costos asociados con moldes, lo que implica que se pueda realizar producción bajo demanda y evitar tener productos en stock a la espera de ser adquiridos.
- Producción rápida y prototipado: realiza prototipos en tiempos récord, evitando que los clientes hagan grandes inversiones económicas en la fabricación de moldes. Además, reduce el tiempo necesario para la fabricación de nuevos productos y acelera los ciclos de desarrollo.
- Reparación y mantenimiento: replicar piezas de máquinas —que antes eran muy difíciles de encontrar en el mercado— se ha convertido en una fortaleza para esta tecnología, porque además de reducir costos, permite prolongar la vida útil de los equipos.

Esta tecnología tiene un amplio rango de aplicaciones en varios campos de la industria, como en la automotriz, aeroespacial, médica, arquitectónica, joyería, alimentaria, robótica, etc.

## Sistemas de integración horizontal y Vertical

El término hace referencia a la forma como se coordinan diferentes procesos al interior de las organizaciones e industrias, para alinearse a las tendencias actuales del mercado, que conlleva a ser más competitivos al lograr superar el clímax incierto que se generan en ciertas compañías, cuando se pierde el horizonte, se sienten amenazados por una competencia fuerte o surgen productos sustitutos a mejores precios para los consumidores. En este sentido, Ariza (2018) afirma que

> es necesario plantear una estrategia de integración que lleve a las empresas a crecer y posicionarse en el mercado, identificando las amenazas del entorno para así sacarle provecho a las oportunidades, logrado con ello mejores ventajas competitivas ante la competencia. (s. p.)

Como se observa en la Figura 6, existen dos tipos de estrategias que buscan reducir los riesgos asociados a las operaciones del negocio, dependiendo de los objetivos de las compañías, el objeto social, el capital humano y económico que disponen. Para conocer mejor estas estrategias, a continuación, se hace una breve descripción de cada una:

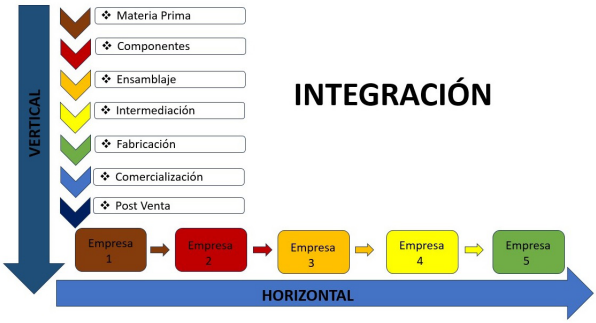



**Figura 6.** *Sistema de integración horizontal y vertical*
Fuente: elaboración propia.

La Figura 6 representa las formas verticales y horizontales en las que interactúan las compañías modernas para ser más competitivas y aprovechar mejor los mercados emergentes, formas de integración que se explican a continuación:

- *Integración vertical:* las empresas o grupos empresariales pueden realizar varias actividades en las diferentes etapas del proceso —como la extracción o adquisición de materias primas, comercialización con otras compañías y transformación en productos terminados—, lo que implica una integración entre proveedores, fabricantes, distribuidores y los clientes finales. Por ejemplo, una empresa del sector textil que importa materias primas tendrá ventas al por mayor y al detal, además, tendrá talleres de confección y tiendas para la comercialización de sus pro-

ductos terminados. Esto genera una ventaja competitiva porque tiene control de toda la línea de producción y puede ofrecer mejores precios.

- *Integración horizontal:* hace referencia a la colaboración entre organizaciones o dependencias que estén en un mismo nivel jerárquico o que pertenecen a una misma actividad comercial, con el propósito de buscar un mejoramiento continuo en diferentes actividades comunes como la comunicación, la coordinación e intercambio de información para mejorar los procesos internos, la toma de decisiones y realización de sinergias entre compañías para la interconexión entre proveedores, fabricantes y distribuidores.

Este tipo de integración también se puede lograr mediante la implementación de sistemas de gestión empresarial, para conectar diferentes actividades al interior de las organizaciones.

## Ciberseguridad

La digitalización de la información y la realización de diferentes actividades en línea, hacen que las empresas estén expuestas a constantes ataques informáticos, lo que pone en riesgo la información —secretos industriales, suplantación de identida-

des, transacciones comerciales fraudulentas, etc.— y las operaciones internas que garantizan el normal desarrollo de esta. Ayerbe (2017) afirma que "los sistemas de control industrial son vulnerables fundamentalmente en dos tipos de amenazas informáticas, las Tecnologías de la Información (TI) y la de las Tecnologías Operativas TO que aún carecen de soluciones integrales de seguridad" (s. p.).

Los ataques más comunes al sector industrial están dirigidos hacia la parte comercial y administrativa, el atacante puede encontrar información valiosa que explota con fines económicos. Una de las formas de minimizar estos impactos negativos consiste en mantener los sistemas de seguridad actualizados y aplicar políticas de seguridad de estricto cumplimiento al interior de las organizaciones.

Un ciberataque puede tener diferentes niveles de gravedad: en el nivel más bajo se encuentran los *Spam* o *Adware,* los cuales producen molestias a las organizaciones. Los *Spyware* que tienen como finalidad el monitoreo de hábitos de navegación y el *Phishing* como una técnica de ataque para suplantar páginas web, especialmente del sector bancario, con el objetivo de engañar a los cuentahabientes para que suministren información confidencial como las contraseñas de sus cuentas, números de tarjetas de crédito, entre otros.

Los *RooKit* y las Amenazas Persistentes Avanzadas (APT —pos sus siglas en inglés— *Advance*

*Persistent Threats*), según Márquez (2017), utilizan técnicas de hackeos avanzadas para acceder a los sistemas informáticos, con la finalidad de permanecer allí por un periodo de tiempo prolongado, que dejan consecuencias fatales para las organizaciones atacadas. Además de las diferentes técnicas utilizadas para acceder a la información, quizá los más comunes se deben a los errores humanos, por desconocimiento. Hay otras clasificaciones de ataques muy comunes en la industria, y en este sentido Ayerbe (2017) sostiene que los "ciberataques pueden clasificarse en dirigidos y accidentales, los dirigidos persiguen un objetivo concreto, como un ataque por denegación de servicios, mientras que los accidentales cuando se infecta con un virus propagado desde un área específica de la empresa" (s. p.).

## Realidades inmersivas

Las realidades inmersivas se distribuyen en las siguientes tecnologías:

*Realidad Virtual* (VR): conocida por sus siglas en inglés, *Virtual Reality*, se caracteriza porque sumerge a los usuarios en un mundo digital en el que se vive una experiencia sensorial, gracias a algunos periféricos diseñados para esa inmersión como cascos cerrados, gafas, auriculares, guantes hápticos, trajes especiales, mandos o sensores de movimiento, para

la simulación del entorno. Contar con un procesador —que organice las escenas que ve el usuario— es necesario para esta tecnología. Cruz et ál. (2006) afirman que

> existen dos tipos de VR, la inmersiva, aquella que se desarrolla en un ambiente 3D a través de los accesorios propios de esta tecnología y la no inmersiva, donde los usuarios interactúan de forma sencilla con los periféricos del computador. (p. 96)

En el ámbito empresarial y de marketing, la VR ha tenido una gran acogida entre los usuarios, porque pueden experimentar mejor los productos antes de ser adquiridos y al ser una tecnología en expansión, los emprendedores pueden beneficiarse con las aplicaciones u otros periféricos para captar más clientes interesados en vivir este tipo de experiencias.

*Realidad Aumentada*: identificada con las siglas AR (de las siglas en inglés *Aumented Reality*) fue creada con el objetivo de incorporar fragmentos de información virtual a través de gafas especiales y Smartphone. Permite la combinación de imágenes u objetos virtuales con el entorno, sin que los usuarios se salgan del mundo físico o real; en otras palabras, se logra el aumento de la realidad con información digital. Uno de los ejemplos más representativos de esta tecnología es el juego de Pokémon Go, en el que los jugadores capturan varios personajes de la serie —en diferentes escenarios— con móvil como medio de rastreo.

Así como en la VR se hace uso de accesorios para sumergirse al mundo virtual, con esta tecnología también es necesario utilizar gafas especiales, cascos y teléfonos celulares. Sin embargo, el entorno debe ser visible y permitir obtener la información que está superpuesta. Muchas empresas ven fortalezas en el desarrollo de esta tecnología, especialmente en el campo del marketing, para minimizar las devoluciones de los productos por una mala elección de los clientes, como en el caso de los menús de los restaurantes. En el arte, por ejemplo, esta tecnología también se convierte en una gran aliada para la restauración de obras porque permite proyectar los detalles originales. Otros usos se dan con los GPS de los vehículos, los cuales despliegan información de los destinos y ubican a los usuarios en una cartografía virtual.

Una de las ventajas de esta tecnología —en comparación con la RV— consiste en que no se requiere de la inmersión total en el escenario, ni de auriculares u otros dispositivos externos, basta con portar las gafas o revisar la pantalla del móvil eventualmente. Esta tecnología, según Reinoso (2013), se puede resumir en

> cuatro niveles de acuerdo con la forma de trabajo, parámetros, sistemas de seguimiento y técnicas empleadas así:

- Nivel 0 – Hiperenlaces en el mundo físico.

- Nivel 1 – Realidad Aumentada basada en marcadores.
- Nivel 2 – Realidad Aumentada *markerless*.
- Nivel 3 – Visión aumentada. (p. 10)

*Realidad Mixta:* es la integración de las dos tecnologías anteriores —también es conocida como realidad híbrida— en escenarios tridimensionales, a los que se les agrega información digital. El propósito consiste en recrear escenarios donde los objetos reales y virtuales interactúen entre sí, donde los usuarios se sumergen en el mundo virtual desde un espacio físico. Bockholt (2017) afirma que "el término hace referencia a los vídeos donde se hace la mezclan y superponen secuencias en tiempo real, en un contenido de realidad virtual" (s. p.).

Para lograr los resultados en esta tecnología es necesario grabar con una cámara y con una pantalla verde de fondo, a la persona que se va a sumergir en el entorno virtual, luego se conecta otra cámara en la misma posición de la anterior, para que quien está viendo la escena, pueda observar lo que está experimentando el usuario en el entorno virtual. Esta técnica presenta algunas características como:

- Los usuarios y accesorios físicos están presentes en el entorno virtual, lo que genera una experiencia real para quienes la utilizan.
- Se puede experimentar la sensación de que los objetos poseen volúmenes, gracias a las

facultades cerebrales para captar las tres dimensiones.

- Los objetos se aprecian con realismo extremo, logrando que los usuarios los asuman como parte del escenario.

## Computación en la nube

Es una tecnología emergente que permite a los usuarios acceder a los recursos informáticos —como archivos, programas— y hacer procesamiento de datos, entre otras actividades de manera remotamente, por medio de Internet, sin necesidad de estar conectados a servidores u ordenadores personales; Ortiz et ál. (2018) sostienen "que la computación en la nube hace referencia a los servicios ofrecidos a través de internet, mediante aplicaciones configuradas, haciendo uso de la convergencia de software y hardware desde cualquier lugar de planeta" (p. 70).

Sumado a lo anterior, esta tecnología se puede clasificar en tres tipos: pública, privada y mixta o híbrida, los cuales se relacionan con algunas características como el costo, la disponibilidad de la información y las expectativas del cliente. También ofrece algunos servicios que son aprovechados por otras tecnologías emergentes como la IoT, para representar los resultados a los clientes finales a través de analítica de datos, interfaces y servicios como:

SAAS *(Software como Servicio):* desde esta interfaz los usuarios pueden acceder a software libre que se encuentra alojado en servidores, pero con la diferencia de que algunos recursos están limitados y en caso de ser requeridos es necesario hacer el pago de una membrecía.

PAAS *(Plataforma como Servicio):* en este modelo se ofertan ambientes completos de desarrollo *On Demand* —que son servicios ofrecidos por una empresa de tecnología para satisfacer una demanda de consumo—, donde los usuarios pueden hacer modificaciones de las herramientas con el objetivo de optimizar las aplicaciones. Una de las ventajas principales es la incorporación automática de Sistemas Operativos, algunas herramientas de desarrollo, servicios de negocios inteligentes, así como ofertar la infraestructura para configurar aplicaciones web y móviles.

IAAS *(Infraestructura como Servicio):* los proveedores tienen autonomía para alquilar diferentes recursos de infraestructura como los servidores o periféricos que permiten la trasmisión y almacenamiento de la información a los clientes. Con este servicio solo se pagan por los recursos consumidos y son escalables y adaptables a necesidades puntuales.

## Robots autónomos

La industria moderna emplea herramientas tecnológicas que facilitan las tareas de los operarios, especial-

mente, aquellas labores repetitivas o que demandan ciertos cuidados y conocimientos, tales como la aplicación de soldaduras especiales, la manipulación de químicos o de sustancias nocivas para la salud o tareas de alto riesgo que comprometan la integridad física de los empleados. El desarrollo de interfaces robotizadas y robots autónomos facilitan las tareas antes mencionadas y solo requieren de programación para ejecutar los algoritmos.

Jiménez (2021), afirma que "los robots autónomos inteligentes pueden obtener sus conocimientos y entrenamientos a través de diferentes procedimientos y de fuentes diversas, utilizando algoritmos de aprendizaje neutros en principio, pero que a medida que las máquinas lo requieren se hacen más complejos" (p. 8).

Actualmente hay dos tipos de robots: los industriales y los colaborativos. Los primeros son programados para realizar tareas específicas y predefinidas dentro de un área de trabajo físico, mientras que los colaborativos o *cobot*, están diseñados para interactuar con los seres humanos dentro de un espacio de trabajo compartido y de forma segura, asistiendo en diferentes tareas y procesos. En la era de las fábricas modernas, muchas máquinas están dotadas de IA compartida con IOT, por lo que varios estudios de mercado prevén en el futuro inmediato, un aumento en la comercialización de robots colaborativos,

debido a los bajos precios y usos adaptables de cada compañía.

Un robot colaborativo ocupa espacios pequeños y están compuestos de brazos robóticos y accesorios, además, las actualizaciones constantes los hacen seguros para que los operarios puedan hacer sus actividades cerca de ellos y sin barreras protectoras; mientras que los robots industriales se construyen para que los humanos interactúen con ellos a través de controles electrónicos y sean apagados en caso de ocurrir algún incidente relevante.

## Internet industrial de las cosas

El Internet de las Cosas (IoT —por sus siglas en inglés— *Internet of Thing*) no es un concepto nuevo —como se afirma en muchos artículos y libros actuales—, desde 1982 se contempló la posibilidad de que en el futuro los dispositivos inteligentes debían ser conectados en una gran red, un artículo publicado por Valencia y Portilla (2018), lo definen como:

> Una tendencia que está transformando el mundo de la industria en cuanto a fabricación y automatización, ya que se trata de una red de dispositivos que se pueden conectar y transferir datos entre sí, es decir, es la integración e interacción de sistemas de red ciber-físicos como: máquinas, sensores, personas y el *cloud computing*, que se pueden comunicar e interactuar en tiempo real para monitorizar, controlar y analizar grandes volúmenes de datos, lo cual permite

> la reducción de costos, la mejora de la productividad y el incremento de los ingresos. (p. 3)

El IoT es un concepto que actualmente está asociado a la Industria 4.0 con el nombre de IIoT (*Industrial Internet* of Things), que utiliza el poder sensórico moderno para crear máquinas inteligentes, con capacidad de analizar variables en tiempo real. También es considerada como una tecnología que está en pleno crecimiento y cuyo objetivo principal es la resolución de problemas —a través de las redes inalámbricas, actuadores, servidores en la nube, software y sensores—, toma variables del ambiente, las procesa, almacena, grafica, analiza y facilita la automatización industrial.

Con el desarrollo de esta tecnología, también surgen las redes de baja potencia y áreas ampliadas, mejor conocidas como Redes de Área Amplia de Baja Potencia (LPWAN —por sus siglas en inglés— *Low Power Wide Área Network*), a las que se les pueden dar diferentes usos como el envío de datos generados por sensores y la conexión de hardware, con muy bajos consumos de energía. Una de las grandes ventajas es el cubrimiento de grandes distancias e incluso, en lugares donde el internet tradicional no tiene cobertura, como túneles, sótanos o áreas rurales.

Para dar solución a esta problemática, la industria de la electrónica ha creado hardware inalámbrico a bajo costo —mejor conocido como *transceivers*

de datos configurables y reprogramables—, con unas coberturas superiores a veinte millas, en línea de vista y sin repetidores, para la transmisión de datos planos como las lecturas de sensores o comandos de control para actuadores.

A diferencia del internet tradicional, los dispositivos que soportan estas redes y su funcionamiento no requieren de cambios constantes en las baterías, por lo que son ideales para las compañías de telecomunicaciones. Las cuatro organizaciones que lideran las IoT en el mundo son: Lora Wan, Sigfox, Narrow Band IoT y LTE-M, como se muestra en la Figura 7.


**Figura 7.** *Operadores que lideran el mercado mundial de IoT*
Fuente: elaboración propia.

Estas compañías suministran varios de los servicios de IoT a nivel mundial, actualmente están haciendo sinergia con las compañías de telefonía celular para ofrecer una cobertura más amplia y rápida. Lora Wan es una de las principales compañías y también es un protocolo que se especializa en equipos para zonas rurales y áreas urbanas.

Sigfox —competidor de Lora Wan— es una empresa francesa que opera en las bandas ISM (del inglés, *Industrial Scientific and Medical*), cuenta con cobertura en las zonas urbanas de la Unión Europea, Rusia, América, Oceanía y algunos países de África, con los distintos operadores de cada país han configurado una red de baja velocidad y de largo alcance para atender las necesidades de la IoT.

Narrow Band IoT es una compañía de grupos asociados en telecomunicaciones enfocada en el tratamiento de datos —avalado por el Proyecto de Asociación de Tercera Generación (3GPP —del inglés— *3rd Generation Project*)—, una de sus principales características es que usa la arquitectura de red celular a través de bandas licenciadas.

El estándar LTE-M fue desarrollado por las agencias espaciales para que los sensores se comuniquen a corto alcance a través de las redes WLAN y WSN; Bonafini y Sacchi (2019), sostienen que "esta solución se basa en el desarrollo de una infraestructura de red inalámbrica marciana basada en LTE on Mars

(LTE-M), por ser robusta y flexible, caracterizada por el amplio ancho de banda para comunicaciones con *Rovers* o drones terrestres" (p. 752). Este estándar fue liberado y capitalizado por un grupo empresarial para el intercambio de información con una amplia presencia en Argentina, México, Asia y Europa.

La IIoT es un mercado masivo que apunta a que los periféricos que se utilizan para obtener las variables sean lo más baratos posibles, debido a que uno de sus objetivos es la obtención de información de sensores para la analítica de datos y toma de decisiones. Liñan et ál. (2015) afirman que "los objetos pueden adquirir inteligencia por medio de la toma de decisiones relacionadas con el entorno y aprovechar los canales de comunicación disponibles para suministrar información sobre sí mismos, así como acceder a la acumulada por otros objetos inteligentes" (s. p.).

## IA como herramienta clave para la IIoT

La IA es la combinación de varios algoritmos matemáticos que tienen como objetivo emular en las máquinas la capacidad de tomar decisiones. Esta tecnología ha ido evolucionando a pasos agigantados, muchas de las tecnologías emergentes se complementan con esta, lo que ha ampliado el rango de las aplicaciones como la detección facial para

la identificación de personas, los asistentes virtuales en los *call-center*, el aprendizaje de idiomas, los diagnósticos médicos, los sistemas expertos para el análisis de información, finanzas, educación, E-comerce, agricultura, logística y transporte, etc.

En un artículo publicado por Burke (2020), manifiesta que "para el 2022 más del 80 % de los proyectos IoT empresariales, van a incluir un componente de IA, frente al 10 % que se registra en la actualidad, teniendo un crecimiento muy grande en el corto tiempo" (s. p.). Lo anterior demuestra que la IoT se hace cada vez más inteligente, lo que ha permitido que los principales proveedores de software para estas plataformas ofrezcan paquetes más robustos e integrados, capaces de realizar un análisis basado en aprendizaje automático para detectar patrones y posibles fallas en los sensores.

## Big Data y análisis

Hoy se cuenta con grandes volúmenes de información o conjunto de datos que se transportan por diferentes medios y cuya velocidad dificulta su captura y procesamiento. Este escenario dio origen al término Big Data o grandes volúmenes de información, utilizados por las industrias para mejorar la producción, predecir fallos, realizar mantenimientos, optimizar el rendimiento y tomar decisiones, convirtiéndose en una herramienta muy útil en la

industria moderna, porque permite llevar una trazabilidad de todos sus procesos internos.

Actualmente, no hay una medida exacta para determinar a partir de qué cantidad de datos se puede considerar una Big Data. Los expertos consideran que pueden ser desde los 30 Terabytes (1000 GB), hasta varios Petabytes (1000 TB). Vilaplana (2019), afirma que "las compañías del futuro serán aquellas que sepan integrar satisfactoriamente la tecnología con las personas. Lo anterior implica que las compañías deben hacer un gran esfuerzo, para disponer de talento humano capacitado que afronte los retos inmediatos" (p. 121).

Las nuevas generaciones vienen con una gran disposición a interactuar con los entornos virtuales, recibiendo el apelativo de la generación digital, los cuales están mejor acondicionados para interactuar con la información en entornos distribuidos. Barea et ál. (2020), sostienen que "los datos se pueden estructurar en diferentes formas y tamaños, a través de múltiples sistemas de gestión, tales como: Bases de datos relacionales; Base NoSQL; Infraestructuras de computación en paralelo y Hadoop" (p. 39). Cada una de estas herramientas, permite desarrollar tareas más complejas en el campo de la informática, mezclando el análisis de grandes volúmenes de datos a través de múltiples sistemas de gestión.

*Simulación:* es una réplica digital de un proceso o producto para obtener información sobre sí

mismo y predecir su comportamiento bajo ciertas características. Este concepto se ha ido extendiendo a diferentes escenarios para identificar problemas a través de prototipos virtuales, antes de que se manifiesten físicamente, minimizando los costos de producción. La simulación de líneas de producción contribuye al mejor uso de las materias primas y eliminar desperdicios, para lograr altos estándares de producción.

Con el apoyo de la simulación se puede determinar qué cantidad de productos finales se pueden realizar, así como reducir los tiempos inactivos de los equipos, identificar cuellos de botella y obtener una vista preliminar de los productos terminados y se puede observar el funcionamiento de los modelos virtuales antes de ser llevados a producción.

A través de la simulación se puede ampliar los portafolios de servicios como valor agregado, por ejemplo, se puede perfeccionar la ergonomía en un puesto de trabajo, ensamblar una máquina con la ayuda de planos virtuales, realizar la interacción de los operarios con sistemas robotizados, materiales y herramientas, así como emular todas las etapas de fabricación en un medio virtual con el objetivo de optimizarlo.

A partir de la información suministrada a través de las redes de IoT o IIoT de una máquina, se puede crear una réplica digital para analizar el funciona-

miento y comportamiento de los materiales. A través de la técnica de los "gemelos digitales" —creados para que asuman un comportamiento similar al original—, los usuarios pueden determinar qué partes de la máquina presenta anomalías (como recalentamientos o desgastes en un momento determinado cuando son expuestos a condiciones extremas) para determinar el comportamiento y tomar medidas correctivas antes de iniciar con la línea de producción.

## Sistemas de la cadena de bloques y computación cuántica

Los sistemas de cadena de bloques o *blockchain* y la computación cuántica son dos tecnologías emergentes que tienen el potencial de revolucionar la industria 4.0 (Soori et ál., 2023). El *blockchain* es una tecnología de contabilidad distribuida que se puede utilizar para registrar transacciones de manera segura, es a prueba de manipulaciones. Es un sistema descentralizado —no hay autoridad de quien controla la cadena de bloques en una transacción— que se mantiene por una red de computadoras llamadas "nodos", encargadas de efectuar las operaciones.

Cuando se realiza una transacción en el *blockchain*, se hace por medio de un registro de una transferencia de valor, como una criptomoneda, de una dirección a otra (Han et ál., 2023). Cuando un

usuario inicia una transacción, se transmite a la red, donde los nodos la verifican y la agregan a un bloque, así como un "*hash*" del bloque anterior. Este *hash* se utiliza para unir los bloques, creando la cadena de bloques propiamente dicha (Handayani et ál., 2023). El proceso para agregar una transacción a un bloque es el siguiente:

1. *Creación de transacciones:* el usuario inicia una transacción mediante la creación de un mensaje que incluye las direcciones del remitente y del destinatario, la cantidad de criptomonedas que se transfieren y el identificador único de la transacción.
2. *Difusión:* la transacción se transmite a la red donde los nodos la reciben.
3. *Verificación:* los nodos verifican la transacción comprobando que el remitente tenga los fondos necesarios para realizar la transferencia y que la transacción sea válida de acuerdo con las reglas de la cadena de bloques.
4. *Agregar a un bloque:* si la transacción es válida se agrega a un bloque que representa la colección de transacciones, que han sido verificadas y están en espera de ser agregadas a la cadena de bloques.
5. *Minería:* el bloque se entrega a los mineros —quienes usan computadoras de alto

rendimiento para resolver problemas matemáticos complejos— para que validen las transacciones en el bloque y puedan agregarlo a la cadena.

6. *Actualización:* una vez que se ha agregado el bloque a la cadena, la transacción se considera completa y el valor se transfiere del remitente al destinatario.

Los detalles técnicos acerca de la transacción en una cadena de bloques pueden variar según la tecnología que se utilice, pero el proceso básico —descrito anteriormente— lo comparten la mayoría de los sistemas de *blockchain* actuales. Manipular un bloque una vez que se ha agregado a la cadena es muy difícil, lo que garantiza la seguridad, porque cualquier cambio en un bloque requeriría cambiar el *hash* del bloque anterior, que luego requeriría cambiar el *hash* del bloque que le antecede y así sucesivamente. En consecuencia, el proceso resulta difícil porque implicaría que el atacante debería tener el control de la mayoría de nodos al interior de una red. El *blockchain* presenta diversas aplicaciones en la industria 4.0 (Tyagi et ál., 2023; Nuttah et ál., 2023), como:

- Gestión de la cadena de suministro: permite rastrear el movimiento de bienes y materiales en una cadena de suministro, asegurando que sean auténticos y no hayan sido manipulados.

- Fabricación: se puede usar para rastrear la producción de bienes, asegurando que se produzcan de manera segura y ética.
- Finanzas: se utiliza para crear nuevos productos y servicios financieros, como contratos inteligentes e intercambios descentralizados.
- Energía: se ha empezado a usar para rastrear la producción y distribución de energía, asegurando que se produzca de manera sostenible.

Las aplicaciones potenciales del *blockchain* en la industria 4.0 son amplias, teniendo en cuenta el potencial de cambiar el estilo de vida de las personas a gran escala y que muchas tecnologías que la pretenden incorporar aún están en sus primeras etapas de desarrollo. Una de estas tecnologías es la computación cuántica —un nuevo tipo de computación que se fundamenta en los principios de la mecánica cuántica (Levich et ál., 2022)— usada para realizar cálculos exponencialmente más rápidos que los de las computadoras clásicas.

Las implicaciones potenciales de la computación cuántica en la industria 4.0 (Awasthi et ál., 2023) y su relación con el *blockchain* son amplias, en particular, en al campo de la criptografía (Ristov y Koceski, 2023). Esto se debe a que se pueden romper los algoritmos de encriptación usados para

proteger los datos en la cadena de bloques, representando un grave riesgo de seguridad.

No obstante, también se presenta una serie de aplicaciones potenciales para la computación cuántica en el campo del *blockchain*. Por ejemplo, acelerar el procesamiento de las transacciones, al igual que el desarrollo de nuevos protocolos de seguridad. Visto de esta manera, la relación entre el *blockchain* y la computación cuántica aún se encuentra en las primeras etapas de desarrollo, sin embargo, está claro que estas dos tecnologías tienen el potencial de revolucionarse mutuamente. El *blockchain* podría proporcionar una plataforma segura para la computación cuántica, mientras que esta última podría usarse para perfeccionar la seguridad y el rendimiento de los sistemas que soportan el *blockchain*.

## Almacenamiento masivo de datos e IA

El almacenamiento masivo de datos es un término utilizado para describir la capacidad de almacenar grandes volúmenes de datos, a menudo soportado en un servicio en la nube. La IA forma parte de las ciencias de la computación, cuya función es el desarrollo de sistemas que pueden aprender y adaptarse de forma autónoma (Márquez, 2023a).

Los sistemas de IA se emplean cada vez más en el almacenamiento masivo de datos para gestionar y analizar la información de manera eficiente; pe-

ro también, el almacenamiento masivo de datos es importante para la IA porque permite a estos los sistemas almacenar y acceder a grandes cantidades de información y aprender a mejorar sus capacidades. Por ejemplo, un sistema de visión por computador —que se utiliza para el reconocimiento de imágenes— necesita acceder a una gran cantidad de imágenes para aprender a identificar diferentes objetos.

Algunas de las características técnicas (Suganya y Sasipraba, 2023; Alemami et ál., 2023) más relevantes del almacenamiento de datos en la nube incluyen:

1. *Escalabilidad:* las soluciones de almacenamiento deben ser capaces de manejar grandes cantidades de datos y escalar hacia arriba o hacia abajo, según sea necesario, para acomodar volúmenes de datos crecientes o decrecientes.
2. *Durabilidad:* los datos almacenados deben ser altamente disponibles y duraderos, lo que significa que deben estar protegidos contra la pérdida, corrupción de datos y deben soportar fallas de hardware y software.
3. *Rendimiento:* diseñados para proporcionar un alto rendimiento, con velocidades rápidas de ingesta y recuperación de datos, para admitir análisis en tiempo real y otros usos que requieren baja latencia.

4. *Seguridad:* deben proporcionar características de seguridad sólidas para proteger los datos contra el acceso no autorizado, el robo y la manipulación, incluidos el cifrado, los controles de acceso y auditorías.
5. *Gestión de datos:* compresión, duplicación y archivado para ayudar a optimizar la utilización del almacenamiento y reducir los costos.
6. *Integración:* aplicaciones y servicios, incluido el análisis de datos, el aprendizaje automático y otros servicios basados en la nube.
7. *Rentabilidad:* modelos de precios flexibles y facturación de pago por uso, para ayudar a las organizaciones a optimizar sus costos.
8. *Ubicación de datos:* capacidad para almacenar datos en múltiples ubicaciones geográficas para respaldar la soberanía y los requisitos de cumplimiento, así como para proporcionar un acceso más rápido a los datos para los usuarios en diferentes regiones.
9. *Recuperación de datos:* recuperación de datos rápida y confiable, con funciones como cifrado, integridad y confiabilidad.

Estas técnicas de almacenamiento masivo de datos en la nube están ligadas a varios servicios de IA y, debido a su especificidad, las principales empresas que ofrecen estos servicios son líderes en tecnología

y cuentan con una amplia base de usuarios en todo el mundo (Boneder, 2023). Algunos ejemplos de estas empresas son:

- *Amazon Web Services* (AWS): esta plataforma ofrece un amplio portafolio de soluciones de IA como *Amazon SageMaker*, que permite la creación, entrenamiento y despliegue de modelos de aprendizaje automático, y *Amazon Rekognition*, que proporciona capacidades de visión por computadora. Además, la plataforma de asistente de voz *Alexa* es un ejemplo de cómo combinan la IA con la nube para ofrecer servicios innovadores (Zharovskikh, 2023).
- *Google Cloud Platform* (GCP): ofrece herramientas como *Google Cloud AI Platform* y *TensorFlow*, que son ampliamente utilizadas para el desarrollo y entrenamiento de modelos de IA. Google es conocido por su liderazgo en tecnologías de inteligencia artificial y esto se refleja en sus ofertas en la nube. También han desarrollado *Google Home*, un asistente de voz que utiliza IA para brindar servicios en la nube (Parisyan, 2023).
- *Microsoft Azure*: dispone de *Azure Machine Learning* y otros servicios relacionados que expanden las capacidades de IA para respaldar aplicaciones y procesos basados en la nube. Otros servicios son *Azure Virtual*

> *Machines, que* ofrece máquinas virtuales escalables y flexibles para ejecutar aplicaciones empresariales; *Azure Synapse Analytics* es un servicio de análisis de datos que integra otros productos de *Azure* como IA, almacenamiento en la nube de extremo a extremo y procesamiento paralelo; también dispone de *Azure Functions*, que proporciona un servicio de computación sin servidor y facilita ejecutar fragmentos de código en respuesta a eventos (Gupta et ál., 2021).

Estas son solo algunas de las opciones más destacadas en el campo de la IA en la nube. Cada una de estas plataformas ofrece una amplia gama de servicios y herramientas que permiten a las empresas el almacenamiento, proceso y análisis de gran cantidad de datos, utilizando tecnologías de IA (Hussein y ALRikabi, 2023) para obtener *insights o perspectivas* valiosas para tomar decisiones más informadas. Asimismo, el almacenamiento masivo de datos y la IA son dos tecnologías que están estrechamente relacionadas y que se utilizan cada vez más de manera conjunta (Márquez, 2023b). El almacenamiento masivo de datos suministra a los sistemas de IA la información que necesitan para aprender y mejorar sus capacidades, y los sistemas de IA ayudan a gestionar y analizar los datos de forma eficiente.

## Discusión

Con el pasar del tiempo los seres humanos han ido evolucionando gradualmente, generando grandes cambios en los comportamientos sociales y la manera como se percibe la realidad en el entorno. Una de las mayores influencias se presentó en el periodo de la Primera Revolución Industrial, en el siglo xviii, porque se dieron varios cambios en el aspecto tecnológico, social y económico que originaron un antes y un después en diferentes aspectos de la vida y que, a partir de ahí, ha generado una diferencia de vida, que llevó a una migración masiva a las áreas urbanas y establecer las clases sociales.

Posteriormente, a medida que la ciencia fue desarrollándose y explorando otras fuentes de energía, hubo una migración controlada a las siguientes revoluciones industriales, hasta llegar a la actual. Esta última, ha estado influenciada por la era de la digitalización, la ia, las telecomunicaciones, el desarrollo de plataformas informáticas, etc., que han modificado sustancialmente la percepción del mundo, representando un cambio en el paradigma de la industria.

La Industria 4.0 se fundamenta en la aplicación e integración de tecnologías emergentes que están generando grandes cambios —tanto en la industria manufacturera, como en el comportamiento de consumo de la sociedad— en la innovación y ge-

neración de valores agregados en los productos, por medio de herramientas tecnológicas que hoy hacen que las fábricas estén conectadas a la red, compuestas por sensores, actuadores y sistemas autómatas, para ser más eficientes y afrontar al mercado global, un mercado que exige exclusividad y menor cantidad de productos en stock.

Aunque esta revolución industrial está en pleno crecimiento y desarrollo, sus bondades prevén grandes cambios, apoyados por la digitalización de la información, para lograr una mejor gestión y llevar una trazabilidad de los procesos, así como la toma de decisiones. Esto permite identificar hacia dónde convergen las empresas del futuro, buscar nuevas oportunidades de negocios y hacer sinergias con compañías de la misma línea, que ya no serían competencia sino aliados, para afrontar los mercados globales.

En este sentido, la manufactura inteligente está apoyada por plataformas informáticas que ofrecen softwares como herramientas interactivas, para realizar simulaciones, emulaciones y prototipados rápidos, disminuyendo sustancialmente los costos de producción y tiempos de entrega, haciendo un mejor uso de las materias primas y evitando los desperdicios y reprocesos. También se han desarrollado diferentes metodologías que permiten planificar y validar cada una de las etapas de producción: desde el desarrollo del producto hasta su comercializa-

ción, lo que conlleva hacia una mejor calidad del servicio, flexibilidad en la manufactura —al poder, incluso, tercerizar algunas etapas del proceso con compañías aliadas—, reducción de costos y tiempos de entrega.

Con la aplicación de las diferentes herramientas que apoyan esta nueva etapa de producción y mercados, los cambios que se están presentando se deben en gran medida a los aportes de la tecnología, por lo que, Ynzunza et ál. (2017), afirman que "los procesos modernos están altamente marcados por la digitalización de la producción, la automatización, la integración de capacidades a través de sistemas ciberfísicos, la impresión 3D, la ingeniería inversa, el maquinado inteligente, etc." (p. 17).

## Conclusiones

Las Revoluciones Industriales han auspiciado grandes cambios en las sociedades, especialmente, en la mentalidad de las personas —altamente influenciables por el modernismo, dispuestas a adaptarse a nuevos estilos de vida—, quienes constituyen sociedades de consumo.

La Industria 4.0 se caracteriza por la automatización de las empresas a través de la integración de sistemas computarizados. Este enfoque se apoya en el uso de sensóricas inteligentes, la simulación de productos terminados *in situ* y la implementa-

ción de sistemas de gestión para monitorear todas las etapas del proceso: desde la planificación hasta la comercialización de los productos finales. Además, implica que los sistemas de producción inteligentes estén conectados en red, con la capacidad de detectar anomalías, al igual que predecir e interactuar con el mundo físico, tomando decisiones en apoyo a la producción en tiempo real. La aplicación de estos principios en la fabricación de productos y servicios pueden aumentar la productividad, optimizando la eficiencia energética y la sostenibilidad.

Uno de los principales desafíos de la Industria 4.0 consiste en reorganizar las cadenas de valor, de manera que las fábricas se vuelvan más inteligentes y modulares, con sistemas de fabricación reconfigurables y automatización con capacidad de auto-optimización. Tal es el caso de los sistemas ciberfísicos —encargados de monitorear procesos y de recrear de manera virtual el mundo físico— que convergen en la toma de decisiones descentralizadas.

La transformación comprende máquinas inteligentes en red, que se comunican entre sí e intercambian información de manera autónoma y ejecutan decisiones. Esto da como resultado fábricas inteligentes que adaptan la producción en tiempo real a las cadenas de suministro interrumpidas y las demandas fluctuantes del mercado. La adquisición de datos, el control de calidad transparente y los servi-

cios de mantenimiento consistentes son una parte integral del cambio de paradigma que potencia los ciclos rápidos de innovación. En síntesis, la cuarta revolución industrial implica una digitalización de extremo a extremo de las cadenas de valor verticales y horizontales a lo largo de todo el ciclo de vida del producto.

## Capítulo 2

# Internet de las cosas y ciberseguridad

*Jairo Eduardo Márquez Díaz*

El internet de las cosas (IoT) hace referencia al conjunto de dispositivos electrónicos conectados a internet permanentemente, registrando y compartiendo datos. Bajo este escenario, cualquier dispositivo electrónico (microelectrónico, bioelectrónico o nanoelectrónico) incluyendo electrodomésticos, equipos de oficina, maquinaria, aditamentos acoplados al vestuario, artículos personales, drones y vehículos autónomos que comparten datos entre ellos mismos o una central, de modo que pertenecen al mundo del IoT. Para este decenio, el IoT estácompuesto por "diversas variantes como: Internet de los Vehículos (IoV), Internet de Energía (IoE), IoT industrial, IA en el IoT (IAoT), *Internet of Things-Grid* (IoT-G), *Internet of Robotized Thin gs* (IoRT), IoT *on the Battlefield* (IoTotBF)" (Márquez, 2019, p. 86), *Internet of Wearables Things* (IoWT) (Dao, 2023), *Internet of Medical Things* (IoMT) (Ashfaq et ál., 2022), *Internet of Underwater Things* (IoUT), etc.

(LEMO, 2023), que van a cambiar el ritmo de las sociedades en diversos contextos, cuyo objetivo estará enmarcado en mejorar la calidad de vida de las personas, la industria, la ciudades y el medioambiente a través del aumento en la conectividad, navegabilidad, monitoreo, interacción y ubicuidad en entornos urbanos y rurales. Esto trae consigo nuevos retos en materia de seguridad y en normativas, que no solo garanticen el buen uso de las tecnologías y de los algoritmos que las controlan —en este caso particular, a la IA— a través de desarrollos basados en aprendizaje profundo y aprendizaje automático (Lin et ál., 2020).

La demanda de nuevas tecnologías, aplicaciones y soluciones de IOT están marcadas por la atención y el control digital sanitario asistencial en entornos inteligentes —en el campo laboral e industrial, esparcimiento, transporte, hogar y estudio entre otros— que permitan el monitoreo remoto de cualquier variable para mejorar un servicio, a favor del bienestar personal y la optimización de procesos como la detección de fugas de gas o agua, monitoreo de calidad ambiental, seguimiento de activos, telemática, mantenimiento predictivo de máquinas, seguimiento de ocupación de estacionamientos y monitoreo de tapas de alcantarillas, entre otros. Esta demanda implica tecnologías de redes de alta velocidad, dotadas de nuevos protocolos de conectividad con baja latencia y protección contra ciberataques.

La conectividad no solo estará representada en tecnologías 5G, WiFi (incluyendo sus últimas variantes WiFi 6 y próximamente Wifi 7) o LiFi, sino en la comunicación satelital de órbita baja. Esto representa un reto —basados en el hecho de que el espacio en torno a la Tierra está cada vez más colmado de satélites— por lo que se espera que el mercado de servicios se incremente para los próximos decenios. Por ejemplo, la empresa Starlink —que planear tener 12000 satélites— brinda servicios de conectividad de alta velocidad, a nivel mundial —con los 1500 satélites con los que cuenta en el momento de redactar este documento—, sumado a otras flotas de satélites de varios países que pretenden expandir este servicio.

Por esto, las sociedades del siglo xxi están conectadas de manera permanente y en cualquier parte del mundo, con múltiples para los usuario y la industria. Incluso, esta conectividad podrá expandirse muy pronto a otros mundos antes de mitad de siglo, tales como la Luna y Marte, como lo vienen planificando grandes industrias aeroespaciales y gobiernos.

## IoT y vulnerabilidades

El IoT está cada vez más presente en nuestro diario vivir —bien sea en el hogar como en el trabajo— y es esencial para el monitoreo de variables como la

temperatura, humedad, velocidad de flujo, presión, conductividad eléctrica, pH, medición de metales pesados en el aire, control de acceso, seguridad, conducción, compra de artículos, signos vitales, contaminantes biológicos activos, etc., usando como medio de comunicación la internet inalámbrica. Esto implica que el IoT presenta funciones específicas de captura de datos del entorno —que luego son procesados, almacenados y analizados— para la toma de decisiones. Este proceso demanda del uso de redes distribuidas y ajustadas tanto en estándares universales como propios de cada fabricante, para lo cual los dispositivos hacen uso de sensores y actuadores para comunicarse entre sí.

Otro aspecto a tener en cuenta del IoT es que está en permanente evolución, con una demanda de ancho de banda moderada que promete incrementarse con la incorporación de algoritmos de Aprendizaje Automático (*Machine Learning*), ampliando sus servicios, dando paso al denominado *Analytics on the Edge* (Harth et ál., 2018).

Al ser el IoT escalable, varios de sus procesos de captura y registro de datos pueden ser optimizados, lo que repercute en el uso de energía de manera eficiente —pues la mayoría de estos son dispositivos inalámbricos que funcionan con baterías—. De igual manera, el IoT se vale de tecnologías modernas web para su conectividad y transferencia de datos en tiempo real —bien a un servidor local o central

en la nube (servidores/plataformas)—, por lo que sus aplicaciones se extienden a diferentes campos en los que se emplean aplicaciones móviles multiplataforma.

La conectividad inalámbrica de los dispositivos IoT se lleva a cabo a través de redes de amplia cobertura —como LPWAN que incluyen las redes Sigfox, LoRa y NB-IoT—, caracterizadas por trabajar bajo modulaciones y anchos de banda diferentes, según la funcionalidad de cada país (Mekki et ál., 2018).

En cuanto a la manipulación del entorno de operación de la IoT, se presentan diversos problemas de seguridad —bien a través hardware como de software—, tal como se resume a continuación:

1. En los servicios de red alámbrica e inalámbrica se presentan vulnerabilidades por factores como: contraseñas débiles cuya decodificación es fácil para un atacante; sistemas de recuperación de contraseña inseguros; *firmware* de dispositivos desactualizados con puertas traseras activas; desbordamiento de búfer; problemas de las Interfaz de Programación de Aplicaciones (API —por sus siglas en inglés—*Application Programming Interface*) en los dispositivos y *Backend* de fabricantes y terceras partes; Denegación de Servicio Distribuido (DDoS —por sus siglas en inglés— *Destributed Denial of Service*);

bloqueos de cuentas y gestión de credenciales; inyección de *malware* y ataques de repetición y fuerza bruta; servicios sin cifrar o cifrados de manera incorrecta; debilidades en los servicios UDP y protocolos de comunicación UPnP (*Universal Plug and Play*), *Wiegand* o *Clock&Data*; verificación inadecuada del *payload* e integridad de mensajes, entre muchos otros problemas.

2. Factor humano: los mecanismos de actualización y autenticación son responsabilidad del administrador de la red para detectar fallas en las actualizaciones que no aparecen cifradas o con permisos de escritura, o no se deja habilitada la autenticación para el *firmware* y parches, etc.
3. Autenticación: existen variantes que muchos administradores las toman como si fuera una sola —entre dispositivo a dispositivo IoT; de dispositivo IoT a aplicación móvil; de dispositivo IoT a la nube; de aplicación móvil a la nube y de aplicación web a la nube—, sin embargo, con cualquier falla en alguna de estas autenticaciones se compromete la privacidad de toda la red, la ubicación y los datos del o de los usuarios queda expuesta.

La continua expansión del IoT en el mercado de servicios social, sanitario e industrial, sumado a

las sinergias con el Big Data, la IA, la computación en la nube, la Visión Artificial como Servicio (CVaas), la computación en el borde (*Edge computing*), la informática perimetral y el *blockchain* entre otros, ha cimentando las bases para el desarrollo y consolidación de tecnologías como los *Smart Systems* que involucra "*Smart energy, Smart home, Smart buildings, Smart Cities, Smart transport, Smart Health, y la Smart industry*" (Nikpour et ál., 2023, p. 18) y los *Wearables* (IOWR).

Como la relación del IOT con la IA es cada vez mayor, se ha incorporado en dispositivos como electrodomésticos con el fin de mejorar la eficiencia energética y la seguridad de los datos que circulan por la red a la que están conectados en un hogar, edificio o industria. Sin embargo, incorporar programas de aprendizaje profundo en los microcontroladores de los dispositivos IOT —en particular, en los chips de memoria, cuya capacidad es limitada— es uno de los aspectos por superar, de ahí que en la actualidad la data se envíe a la nube, que por supuesto puede ser vulnerable a los ciberataques. Un avance en esta dirección es el algoritmo TibyNAS, que como afirma Ackerman (2020), "genera redes neuronales compactas con el mejor rendimiento posible para un microcontrolador determinado, sin parámetros innecesarios"(p. 35), que se combina con el sistema MCUNet encargado de la clasificación

de imágenes, de manera local, reduciendo con ello el riesgo de robo de información.

Este tipo de adelanto es crucial para las tecnologías actuales y futuras, porque día a día crece el número de electrodomésticos, *wereables* y dispositivos IoT implementados en personas, hogares, edificios, industria, transporte y ciudades, superando incluso el billón en esta década; los limitantes como la memoria y capacidad de procesamiento serán superados rápidamente.

## Vulnerabilidades en protocolos

El rápido aumento en la cantidad de dispositivos IoT ha hecho posible conectar y controlar varios sistemas de forma remota, pero también ha creado una serie de vulnerabilidades de seguridad que deben abordarse. Una de las principales vulnerabilidades en los protocolos IoT es la falta de medidas de seguridad en el diseño e implementación de dichos dispositivos. La falta de estandarización en los protocolos crea un medio fragmentado que dificulta la identificación y resolución de problemas de seguridad. Esto ha llevado a la creación de múltiples protocolos propietarios, cada uno con sus debilidades de seguridad, dificultando a los expertos asegurar la fiabilidad de los dispositivos IoT.

Por muchos años los protocolos que rigen el IoT han sido una de tantas debilidades críticas de segu-

ridad, demandando ser atendidos con el fin de garantizar una comunicación intra e interdispositivos estandarizada. Normalmente, existen protocolos no estandarizados relacionados con el IoT como Zigbee, Z-wave, XBee, bluetooth, WiFi y LoRa entre otros, que funcionan sobre las pilas de código abierto de los protocolos TCP/IP. Estos protocolos también presentan vulnerabilidades en su estructura: desde su creación, hasta la corrupción de memoria en la mayoría de los casos. Estas fallas permiten que se ejecuten diferentes tipos de *malware*, ataques de DDoS, campañas DDoS-as-a-Service, *cryptojacking* e inyección de registros de DNS, que exhiben la información a un ciberataque. Por consiguiente, es recomendable que las organizaciones se familiaricen con la infraestructura defensiva que poseen y evalúen si los recursos anti-DDoS son suficientes para que cumplan con su papel.

Cabe anotar que el modelo TCP/IP, que se muestra en la Figura 8, presenta la estructura de los protocolos de red específicos que permite que cualquier equipo o nodos puedan comunicarse de extremo a extremo bajo direccionamientos determinados, tanto de transmisión-recepción como de enrutamiento.

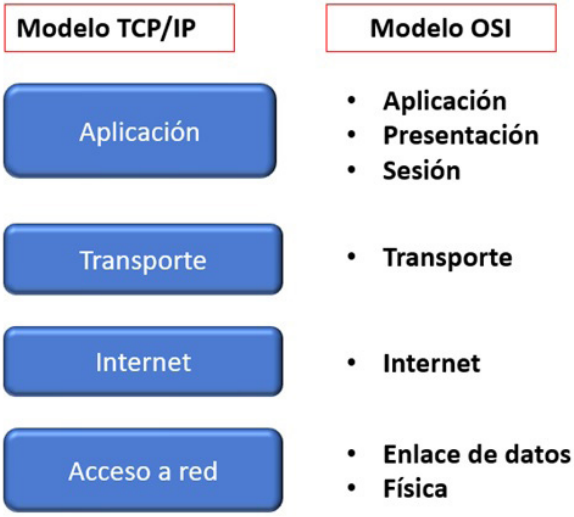



**Figura 8.** *Capas del modelo tcp/ip y su correspondencia con el modelo de Interconexión de Sistemas Abiertos (OSI —por sus siglas en inglés— Open Systems Interconnection)*
Fuente: elaboración propia.

Según la capa, las vulnerabilidades de los protocolos TCP/IP son aprovechadas para realizar ataques de tipo DDOS. Acharya y Tiwari (2016), clasifican las vulnerabilidades de la siguiente manera:

a. *Aplicación*: esta capa involucra protocolos como FTP, NetBIOS, Telnet, SIP, LDAP, SSL, TLS, RPC, RSH, NFS, RCP, Rlogin, RDISC, RIP, SNMP, NIS, DNS, etc (Forouzan, 2020), sujetos a ataques de inyección de código y *phishing*, empleando técnicas como: "HTTP/HTTPS Flooding, FTP Flooding, Telnet DDOS,

Mail Bombs, SQL Slammer y DNS Flood." (Márquez, 2019, p. 11)

*b.* *Transporte*: los ataques son de tipo volumétrico, encaminado a destruir las redes, negando o consumiendo sus recursos hasta que el servidor colapsa, comprometiendo protocolos como TCP, UDP y SCTP (Kozierok, 2019). Los ataques DDoS más comunes son: SYN Flooding y UDP Flooding y TCP Null Flooding.

*c.* *Internet:* los ataques que se producen en esta capa se deben a vulnerabilidades propias del diseño de los protocolos como: IP, IPv4, IPv4+, IPv6, IGMP, ICMP, BGP, ARP, PIM, RIP y OSPF (Tanenbaum y Wetherall, 2019). Los ataques más comunes son de tipo *Smurf* y comprometen el protocolo ICMP, la suplantación de IP, de Denegación de Servicio (DoS —por sus siglas en inglés— *Denial of Service*), Fraggle, TearDrop, ICMP Flooding. Este tipo de ataques también comprometen el enrutamiento de datos desviándolo a una ubicación controlada por el atacante.

d. Acceso: los ataques explotan las debilidades de la capa de red alámbrica o inalámbrica y sus protocolos como PPP, ATM, LLC, MAC, Ethernet, IEEE 802.x, IPFS (Pernet, 2023), Frame Relay y HDLC (Comer y Stevens, 2020). Los ataques DDoS más comunes son:

> VLAN hopping, MAC Flooding, DHCP Attack y ARP Spoofing. "Cualquier ciberataque exitoso puede necesitar moverse entre capas, pero en última instancia el acceso a la red ocurre en la capa física, específicamente, en la propia conexión de red óptica, por cable o inalámbrica" (Ling, 2021).

Dadas las características de ataque en esta capa, la intercepción de señales y el acceso no autorizado es crítico, al igual que el daño físico en algún componente de la red o la manipulación del hardware, instalando dispositivos para el monitoreo, intersección y modificación de datos.

Otras vulnerabilidades relacionadas directamente con los sistemas IoT son las pilas de TCP/IP de código abierto, que no son propiedad de una sola empresa, las cuales son: picoTCP, uIP, FNET y Nut/Net, que se encuentran presentes en los protocolos IPv6, DNS, mDNS, TCP, ICMP y LLMNR, relacionados con la comunicación de dispositivos conectados a internet. Un ejemplo particular sobre TCP son los ataques DDoS a través del protocolo de escritorio remoto de Microsoft (RPD), aprovechando el puerto UDP 3389; aunque se requiere de un conjunto de privilegios, no es descartable este tipo de ataque —aun con los parches y posibles accesos no autorizados— al interior de una red.

Existen vulnerabilidades propias de los sistemas operativos y de la arquitectura que soporta la Internet

actual —que se encuentran conectados a servidores, equipos de cómputo, dispositivos IoT, controles de acceso, etc.— y que supone un verdadero problema a la hora de conocer las características operativas del *firmware* y hardware de conectividad para establecer si están o no en riesgo, sumado a la presencia de malas prácticas en el desarrollo de software. Por ejemplo, existen recursos, software especializado o un simple script —como la herramienta en línea GitHub, cuyo objetivo consiste en determinar si un dispositivo de red de destino ejecuta una pila TCP/IP integrada específica— que permiten el sondeo del protocolo ICMP, las firmas de opciones TCP y el manejo de banderas e estos para detectar vulnerabilidades y tomar las acciones correctivas del caso en aras de prevenir futuros ataques.

Recientemente, se ha planteado el protocolo Thread (Sistu et ál., 2019) que está respaldado por las mayores industrias de la tecnología IoT a través del Thread Group, diseñado para establecer conectividad segura IP inalámbrica —sin la necesidad de concentradores o *hub*— gracias al uso de estándares IPv6 y 6LoWPAN. El protocolo Thread emplea mecanismos de encriptación para garantizar una comunicación segura, incluso vía bluetooth, así como la trasparencia de conectividad entre dispositivos, ampliando una red de ser necesario, tomando en consideración el bajo consumo energético.

El incremento de los dispositivos IoT y la cobertura, los problemas de saturación y rango de acción quedan resueltos porque la red se adapta en caso de que algún dispositivo falle. Por lo tanto, se espera que este protocolo sea adoptado por la industria en pocos años, minimizando el problema de compatibilidad actual con las tecnologías IoT.

Una de las principales preocupaciones de la industria del IoT es la seguridad —que demanda ser atendida con prontitud— de sus dispositivos, pero no hay mucha experiencia en el manejo de los protocolos de ciberseguridad, por lo que muchos protocolos se implementan sin examinar esta protección, lo que crea el escenario ideal para las aparición de vulnerabilidades, que luego son explotadas por parte de la ciberdelincuencia.

La falta de gestión de los dispositivos IoT es un aspecto crítico —representada en el escaso soporte de seguridad en el proceso de producción, hasta que llega al usuario final—, porque, a pesar de que existen sistemas automatizados para realizar esta tarea, la configuración predeterminada y la gestión de las actualizaciones (como la validación de *firmware*, cifrado en tránsito, etc.) no se realiza por olvido y si se hace, no hay una periodicidad constante. Esto mismo sucede con las funciones de monitoreo de los sistemas, la capacidad de respuesta ante incidentes y la metodología de desmantelamiento seguro de los dispositivos.

Como se mencionó, la ciberseguridad del IoT enfrenta grandes retos, por lo que, desde su creación, se requiere que los fabricantes establezcan y extiendan la raíz de confianza de los dispositivos, teniendo en cuenta aspectos como:

- Garantizar el arranque seguro de los dispositivos.
- Cambiar componentes obsoletos e inseguros.
- Facilitar la detección de anomalías empleando las funciones de NXP i.MX 8, entre otras.
- Incorporar el cifrado de datos y depuración de estos, lo que lleva a una gestión de claves ideal.
- *Hardening* físico y lógico que permita disponer de una interfaz segura de entrada/salida.
- Facilitar a las empresas y usuarios finales las actualizaciones necesarias.
- Implementar fuertes medidas de seguridad en el diseño e implementación de dispositivos IoT. Esto incluye el uso de un cifrado sólido y la implementación de la autenticación de dos factores.
- Estandarizar los protocolos utilizados por los dispositivos IoT para facilitar la identificación y resolución de problemas de seguridad.

Existen soluciones en el mercado para ayudar a los desarrolladores a implementar funciones de seguridad de manera rápida y sencilla, mediante herramientas de automatización, software de código abierto y funciones habilitadas para la seguridad en hardware estándar, mencionadas en otros apartes del capítulo.

## Geopolítica e IoT

La pandemia de la COVID-19 dejó grandes lecciones para la sociedad contemporánea, una de ellas es que no puede bajarse la guardia ante una epidemia mundial. El confinamiento obligatorio puso en la palestra la fragilidad del sector sanitario para detectar y atender las afecciones, así como dar tratamiento a enfermedades crónicas en lugares diferentes a las instalaciones hospitalarias y laboratorios. La propuesta del IoT para esta calamidad fue aumentar el número de dispositivos en el hogar, incluso en el cuerpo del paciente, de tal manera que el monitoreo se realizara *in situ*, para controlar el estado de salud y minimizar los riesgos asociados a la enfermedad. Con esta nueva perspectiva de monitoreo, la industria y las empresas de salud han empezado a introducir el IoT de forma masiva en sus instalaciones y en los hogares de sus trabajadores y pacientes, buscando mejorar la seguridad y atención de estos.

Con estas implementaciones se busca mejorar la eficiencia de los recursos utilizados al interior de una empresa, empleando, por ejemplo, sistemas de control energético, de iluminación y ambientales inteligentes, así como sistemas de seguridad y monitoreo en áreas de alto y bajo tráfico, que garanticen el bienestar del trabajador. Sin embargo, aunque ha aumentado el interés de emplear el IoT, así mismo el riesgo de comprometer información sensible a terceros es alto, pues hay que considerar las vulnerabilidades propias de esta tecnología y las inestabilidades geopolíticas que en los últimos años han abierto una brecha a la ciberdelincuencia y a los ataques de diversa índole.

La ubicuidad y dependencia tecnológica llaman la atención de la ciberdelincuencia, sobre todo en tiempos de incertidumbre económica y geopolítica mundial actual. Es así como las APT (Márquez, 2017), los ataques de *ransonware* y DDoS van a ser el común denominador para los próximos años. Estos ciberataques tienen connotaciones económicas, personales, corporativas, políticas y geopolíticas, por mencionar algunos; en el caso de la geopolítica, los ataques están marcados por nuevas innovaciones técnicas y tecnológicas que buscan que objetivos particulares —como diplomáticos, organizaciones gubernamentales y no gubernamentales, centros de salud, centros de investigación, universidades, etc.— caigan en trampas digitales, al descargar ar-

chivos adjuntos, corruptos o maliciosos, con el fin de robar y secuestrar sus sistemas.

En los ciberataques dirigidos a plataformas gubernamentales e infraestructuras críticas —como hospitales o sectores energéticos, de transporte, de carreteras, puentes, edificios, túneles, aeropuertos, puertos marítimos, servicios públicos, etc.— se busca controlar las redes informáticas para hacer colapsar las infraestructuras y economías globales a través de la creación de cadenas de infección, *phishing* y uso de servicios legítimos, haciendo casi imposible poder tomar acciones correctivas. Se estima que estos ciberataques se incrementaran, así como su patrocinio por Estados y organizaciones rusas, chinas, iraníes, norcoreanas, entre otras.

Existen otros grupos de ciberpiratería ubicados en países como Vietnam, quienes a través de sus redes sociales propagan todo tipo de *malware* y *phishing* con objetivos políticos e intereses de ese gobierno, como por ejemplo, el robo de propiedad intelectual y minería de criptomonedas. Estos tipos de ciberataque buscan la recopilación de información comercial confidencial que luego es vendida a la competencia. El *modus operandi* se hace mediante el envío de mensajes a titulares de los correos electrónicos, con direccionamiento a páginas falsas, y con el uso de técnicas de ingeniería social, de *spear-phishing* (Bullee et ál., 2017), de *pharming* (Ortiz, 2019) y otras.

Las técnicas para eludir la seguridad de un sistema físico y lógico se perfeccionan permanentemente, por ejemplo, al soltar binarios *Portable Executable* (PE) para cargar *malware* avanzados, combinados con técnicas básicas o de baja tecnología, con el objetivo de controlar el sistema operativo de la víctima, de tal manera que no le sea fácil reinstalarlo o incluso, deba reemplazar el disco duro.

Otra manera de aumentar la tasa de éxito de ataques *malware*, tipo phishing, es a través de la implantación directa a la entrada del buzón del correo electrónico de la víctima, con herramientas como *Email Appeder*. Con este sistema se burla la seguridad del buzón electrónico, debido a que las credenciales del correo entrante son válidas, por lo que una vez aprobadas, se conecta a las cuentas de correo de la víctima, mediante el protocolo *Internet Message Access Protocol* (IMAP), que se encarga de recibir los mensajes de un servidor de correo. Una vez superado este paso, el ciberdelincuente personaliza los mensajes para que sea creíble y la víctima los acepte, los abra e ingrese su información personal o corporativa. Este tipo de ataque *phishing* no debe subestimarse porque es nuevo, avanzado y cuenta con un alto grado de efectividad.

Otro tipo de *malware* —recientemente descubierto— muestra la nueva generación de gusanos informáticos a la que los sistemas IoT y operativos deberán enfrentar en los próximos años, conocidos

como Gitpaste-12. Este tipo de *malware* empleaba GitHub y Pastebin para almacenar el código de sus componentes y albergar doce módulos de ataque diferentes para atacar vulnerabilidades. Gracias a estas características tiene la capacidad de propagarse gradualmente en una red corporativa —emulando lo que haría una *botnet*, pero a nivel interno—, comprometiendo dispositivos como enrutadores, *firmware* y sistemas operativos, empleando *exploits*, que luego ejecutan un *script* dinámico, con el fin de descargar otros componentes de Gitpaste-12.

Este tipo de *malware* se actualiza permanentemente mientras deshabilita los protocolos de seguridad de los dispositivos *firewall*, software de monitoreo y prevención de ataques; puede tener acceso y control de la infraestructura que conecta y gestiona la computación en la nube, por ende, a la data de los dispositivos IoT y sistemas conectados, aunque existe el módulo apparmor del kernel de Linux, que permite restringir algunos procesos de determinados programas como administrador y comandos relacionados con la seguridad de acceso a la nube.

Sumado a lo anterior, este gusano ejecuta un *criptominer*, cuyo objetivo es secuestrar el procesamiento inactivo de la red, extraer criptomonedas para ataques fraudulentos y servicios externos que pueden incluir a clientes de la víctima. Este tipo de ataque es perverso, ya que no solo tiene acce-

so a todos los datos de la víctima, sino que usa su propia infraestructura para atacar a otros, evitando que el administrador de la red recopile información de aquellos procesos que se están ejecutando y bloqueando instrucciones como: *readdir, tcpdump, sudo, openssl, /proc,* etc. Al momento de descubrirse al gusano Gitpaste-12, este contenía una biblioteca que descargaba y ejecutaba archivos Pastebin que alojaba más código malicioso.

De lo anterior se puede deducir que es este tipo de *malware* es un programa sofisticado, diseñado para lidiar con nuevos desarrollos de seguridad de los sistemas operativos y *firmware* de los dispositivos conectados a una red, atacando de forma selectiva las direcciones IP, comprendidas dentro de un rango aleatorio del enrutamiento entre dominios, sin *Classless Interdomain Routing* (CIDR), ejecución de *scripts* para abrir determinados puertos como el 30004 relacionados con el Protocolo de Control de Transmisión (TCP) y el puerto 30005, relacionado con el protocolo bidireccional SOAP/HTTP, encargados de la comunicación entre dispositivos enrutadores o conmutadores de red, al igual que losservidores de configuración automática.

En síntesis, los nuevos gusanos con características de *botnet* van a aumentar para los próximos años, como el gusano Golang, con el agravante de que van a estar combinados con otras técnicas intrusivas como la criptominería para atacar servi-

dores con sistemas operativos Windows y Linux, sistemas en la nube con *exploits* que relacionan *ransomware*, APT y DDoS con sus variantes (Márquez, 2020). Los gobiernos e industrias han empezado a tomar cartas en el asunto, sin embargo, no solo la ciberdelincuencia va un paso adelante, sino que también las organizaciones apadrinadas por el Estado, contratadas para efectuar ataques selectivos a organizaciones e industrias de otras naciones (Associated Press, 2021; Sanger y Perlroth, 2020).

## Ataques de ransomware

El *ransomware* es un tipo de ciberataque caracterizado por secuestrar la información de un sistema al encriptarlo, para luego cobrar por su rescate a la víctima, con un plazo fijo, a través del pago con moneda electrónica como el bitcoin. De no acceder a estas pretensiones, los cibercriminales proceden a eliminar la información, subastarla o publicarla en sitios de filtración en la darknet para que otros delincuentes se apropien de esta y con ello perpetuar la estafa.

El acoso y la coacción son modalidades de presión recientes para que la víctima pague cuando se niega y van desde la divulgación de información exfiltrada, hasta atentar contra la vida de los empleados y sus familiares. Este tipo de ciberataque ha mostrado estar en constante evolución en la última década con los *ransomware* Rorschach, Wannacry

(Connolly y Wall, 2019), Bad rabbit, Peya, Spora, Reveton, Doxware, Locky, Zcrypt, Goldeneye (Maurya et ál., 2018), Cryptowall, Emotet, jigsaw y Marozka, entre otros (Brewer, 2016).

A parte los desafíos con los que tuvo que lidiar los centros de salud e investigación, escuelas, universidades, sector gubernamental, organizaciones benéficas sin fines de lucro y empresas privadas en general, causados por la pandemia de 2020, se sumaron los ataques masivos de tipo *ransomware*. La razón de estos ciberataques obedeció a que las probabilidades para que estas instituciones pagaran por el rescate de los datos eran altas y así poder recobrar sus servicios. Aunque inicialmente los grupos de *ransomware* prometieron no atacar estas instituciones, la facilidad de obtención de dinero por concepto de secuestro de información fue y sigue siendo alta. De modo que se presentaron acciones "altruistas" en las que los ciberdelincuentes donaron parte del botín a organizaciones benéficas y sin fines de lucro, pero como la acción delincuencial no exime del delito, el dinero fue confiscado por las autoridades.

Sin embargo, aunque haya podido existir una aparente motivación humanitaria, cuando otros acceden a la información, se termina pagando las consecuencias, no importa si la vida de los pacientes se ve comprometida, como se ha evidenciado en diferentes hospitales del mundo (Harkins y Freed,

2018; Collier, 2017), donde países como Estados Unidos (Branch et ál., 2019), Gran Bretaña (Argaw et ál., 2020), Colombia (Gutiérrez, 2023), Francia, Asia, Europa y Oriente Medio han sido golpeados.

Otras razones por las que se ataca al sector sanitario subyacen en el hecho de que su infraestructura informática es débil, con procesos de gestión y administración básica o inexistente. La mayoría de los dispositivos clínicos están conectados en red —como los escáneres de TC, monitores, equipo de radiodiagnóstico, etc.— y actúan como puntos de enlace débiles, transmitiendo datos de forma insegura. Lo crítico es que se comprometen millones de datos de pacientes, accesibles en línea para aquellos que sepan buscarlos.

Periódicamente se crean campañas de *ransomware* disruptivas por parte de los ciberdelincuentes, encaminados a aprovechar las debilidades de determinados sistemas, por ejemplo, credenciales asociadas a bases de datos, en particular, MySQL y PostgreSQL. Lo inquietante de esta situación es que cada vez más son los sistemas que se comprometen, y lo peor del caso es que, "como recordatorio y advertencia a los que no pagan por el rescate, se enumera más de 250 000 bases de datos de 83 000 servidores MySQL y 77 terabytes de datos filtrados" (Johnson, 2020, p. 23).

Aunque se menciona al sector sanitario como objetivo del *ransomware*, no son los únicos, secto-

res como el farmacéutico, financiero, educación, transporte e incluso empresas en ciberseguridad, son fuentes lucrativas para grupos delincuenciales organizados.

Para efectuar un ataque de *ransomware* a este tipo de infraestructuras, se suelen emplear técnicas como *phishing* y software avanzado como Ryuk y TrickBot (Unterfingher, 2020; Gittins y Soltys, 2020), caracterizados para recopilar credenciales y filtrar datos específicos. De igual manera, el *ransomware* se ha venido combinando con sistemas de amenazas APT para potenciar el daño al interior de un sistema, bien sea a través de vigilar el tráfico de información que circula por la misma, robar datos confidenciales para venderlos a la competencia o secuestrar los mismos para su posterior pago.

Otra modalidad de ataque de *ransomware* es el de triple extorsión, que aparte de cifrar los archivos de la víctima y exigir un pago para descifrarlos, amenazan con liberar datos confidenciales robados si no se paga el rescate, e interrumpir las operaciones comerciales al lanzar ataques de DDoS contra su sitio web o red. Los atacantes esperan que al usar estos tres métodos puedan aumentar la presión sobre la víctima para que pague el rescate, incluso si tienen copias de seguridad de sus datos u otras formas para restaurar sus sistemas.

En el caso de las grandes industrias, los ataques de *ransomware* se enfocan en acceder al control

total de los PLC —relacionados con los procesos de producción que, aunque presentan protocolos de seguridad, no están exentos de ser secuestrados—, donde las APT, combinadas con los *ransomware,* se convierten en la navaja suiza para efectuar ataques específicos con daños irreparables en las infraestructuras tecnológicas, de producción, de servicios y logísticas.

Estos ataques suelen ser selectivos, por lo que requieren de tiempo y planificación, ya que debe conocerse el entorno sobre el cual se mueve la víctima y luego, escalar privilegios en el sistema para capturar la mayor cantidad de información. El IOT permite un monitoreo constante de lo que se hace al interior de una organización para después, tener acceso a sus dispositivos.

El panorama del *ransomware* sigue evolucionando y adaptándose a las nuevas tecnologías y estrategias de defensa. Para los líderes de ciberseguridad estar al tanto de estas tendencias y evoluciones es crucial para defenderse contra los nuevos vectores de ataque y prevenir posibles impactos devastadores para las organizaciones. Además, es importante tener en cuenta que las estadísticas sobre el *ransomware* pueden ser difíciles de calcular con precisión, debido a la falta de transparencia y reporte consistente de los ataques.

La colaboración entre gobiernos, empresas y expertos en ciberseguridad es fundamental para abor-

dar eficazmente la amenaza del *ransomware* (Trend Micro, 2023). En la Tabla 1 se muestra de manera simplificada algunos de los ataques más comunes de *ransomware* que existen actualmente.

**Tabla 1.** *Diferentes tipos de ataques de ransomware: características y propiedades*

| Tipo de Ataque | Características | Propiedades |
|---|---|---|
| ***Ransomware* sin carga útil** | Consiste en extorsionar a las víctimas y amenazar con publicar los datos robados en línea si no cumplen con sus demandas. | Los grupos de *ransomware* buscan beneficios cifrando y bloqueando datos, centrando sus esfuerzos en extorsionar a sus víctimas y vender la información robada en el mercado negro con el objetivo de maximizar sus ganancias y minimizar su exposición. |
| ***Ransomware* que roba datos** | Consiste en robar datos sensibles de las víctimas, antes de cifrarlos, con el objetivo de venderlos o utilizar esta información para lucrarse. | Los datos robados se convierten en un activo valioso para los atacantes, quienes pueden vender la información confidencial a la competencia, a otras personas o utilizarla para causar daño adicional a la organización afectada. |
| ***Ransomware* en la nube** | Con el aumento de organizaciones que migran a la nube, los grupos de *ransomware* han adaptados sus estrategias en busca de vulnerabilidades en la configuración y sistemas de la nube para obtener acceso a las redes corporativas. | Se aprovechan las instancias comprometidas de la nube, para llevar a cabo actividades como la criptominería e implementar *ransomware* en sistemas comprometidos, que les permite acceder a datos sensibles de su objetivo. |

Continúa tabla...

| Tipo de Ataque | Características | Propiedades |
|---|---|---|
| ***Ransomware* en plataformas no convencionales** | Consiste en explotar y aprovechar vulnerabilidades en dispositivos o sistemas poco comunes y esenciales para el funcionamiento de las organizaciones, como dispositivos IoT, PLCs o *mainframes* más antiguos. | Las vulnerabilidades en dispositivos poco comunes pueden ser explotadas para obtener un mayor control sobre las operaciones comerciales y logísticas, aumentando con ello el potencial de extorsión a través del bloqueo de estos dispositivos críticos. |
| ***Ransomware* automatizado** | Los grupos de *ransomware* están adoptando prácticas de automatización para aumentar sus ganancias, escalando su alcance y eficiencia en los ataques. | Al igual que las organizaciones profesionales, los grupos de *ransomware* utilizan la automatización en sus ataques para aumentar su rentabilidad, escalándolos para maximizar los ingresos obtenidos de sus víctimas. |
| ***Ransomware* como servicio (RaaS)** | Es un modelo de negocio donde los operadores de RaaS proporcionan a los clientes un kit de herramientas que incluye el *ransomware*, un panel de control para administrar las infecciones y soporte técnico.<br>Además, permite a los operadores de *ransomware* escalar sus operaciones rápidamente, ya que pueden alquilar su malware a un gran número de clientes. | Los clientes de este servicio pueden utilizar el kit de herramientas para lanzar ataques de *ransomware* contra sus víctimas objetivo, sin que tengan conocimiento técnico alguno. |

Fuente: elaboración propia.

Según la información anterior, no sobra preguntarse cómo se puede lidiar con este tipo de problema; una posible respuesta está encaminada hacia la mejora de los protocolos y la seguridad de la información —lo cual no es fácil, bien porque el error humano está presente o por los progresivos avances en los ciberataques, de los cuales nadie se da por enterado hasta que es demasiado tarde—. Si sucede que el sistema ha sido comprometido, lo recomendable es no pagar por las demandas de los ciberatacantes. De manera que, al cortarse el suministro monetario, secuestrar un sistema deja de ser un objetivo. Esto es más fácil decirlo que hacerlo, porque existen diversos motivos e intereses comerciales, corporativos, personales, financieros y políticos que conllevan a pagar e incluso a callar y negar que hubo un ataque y que se pagó por el mismo.

## Botnet y DDoS

Los *botnets* o "redes zombis" se definen como un conjunto de redes informáticas infectadas por *malware* —que permite la ejecución de su procesamiento inactivo—, con el fin de aumentar la potencia informática para atacar a otros sistemas, utilizando la fuerza bruta o técnicas de hackeo, como los ataques de Denegación de Servicio (DoS —por sus siglas en inglés— *Denial of Service*) y sus variantes DDoS y ataques DDoS-*a-as-Service*.

La diferencia básica entre DoS y DDoS radica en el número de computadoras infectadas que hacen solicitudes progresivas y recurrentes a un sistema víctima. Esto implica que este tipo de ataque requiere de un conjunto de redes de equipos informáticos infectados con software malicioso, de diferentes fuentes y que faciliten su control, permitiendo el envío de spam y la propagación de otros tipos de *malware* para continuar infectando progresivamente otras redes.

Con relación a un ataque de clase DDoS, Astudillo (2019), señala que: "consiste en un ataque masivo que busca congestionar el servidor de un objetivo o consumir la totalidad del ancho de banda de salida a Internet de la organización de la víctima" (p. 225). Cualquiera de los dos ataques inutiliza una red haciéndola colapsar en beneficio del atacante, dando paso a infectar y escalar el sistema de los equipos e información disponibles.

En la Figura 9 se muestra, de manera general, la estructura jerárquica de un ataque DDoS y *bonet*, donde el atacante se vale de un conjunto de redes, servidores y equipos, previamente infectados, que actúan como una red zombi o *bots* encargada de distribuir *malware* a la víctima, por medio de peticiones para consumar el ataque de tipo DDoS. Este tipo de ataques no excluye a la tecnología móvil —como smartphones, tablets, *weareables* y por

supuesto, IoT—, disponible y vulnerable, conectada a una red.

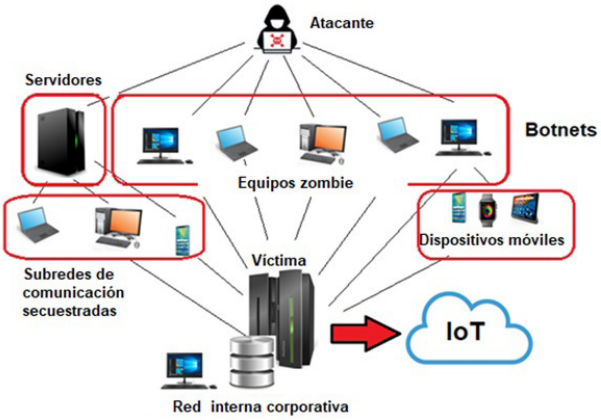



**Figura 9.** *Representación de un ataque de ddos*
Fuente: elaboración propia.

Una característica inherente a las *botnet* es que su nivel de ataque se tecnifica y diversifica continuamente, haciendo casi imposible su erradicación, tal como sucede con la *botnet InterPlanetary Storm, que* detecta y evade los sistemas de seguridad de las redes de cómputo, cuyo sistema operativo puede ser Mac o Android; otro tipo de *botnets* es el *FritzFrog* (Guardicore, 2020), que utiliza la comunicación *peer to peer* (P2) para atacar servidores SSH y el Hoaxcalls, facilitando ataques a gran escala.

Cada vez son más comunes los casos de *botnets* —formados por dispositivos IoT infectados—, que hackean varios sistemas de cómputo con el objetivo

de minar criptomonedas. De igual manera, estos tipos de *botnets* también actúan como vectores de ataque de tipo DDoS, ampliando con ello el espectro de dispositivos con el que se puede vulnerar una red corporativa. Por ejemplo, para armar un *botnet,* empleando dispositivos IoT, se escanean direcciones IP aleatorias en busca de aquellas que puedan presentar vulnerabilidades y cuyas contraseñas se puedan adivinar. Una vez identificadas las direcciones, un software "cargador" implanta *malware* en dichos dispositivos. Al escalar este ataque, los dispositivos infectados como cámaras web "ubicadas en todo el mundo, pueden usarse para ataques DDoS, orquestados por un servidor de comando y control. Cuando no atacan a un objetivo, estos *bots* están listos para buscar más dispositivos vulnerables para infectar" (Shapiro, 2023, s. p.).

La particularidad de las *botnet* es que están diseñadas y alquiladas al servicio del mejor postor para llevar a cabo múltiples actividades delictivas que incluyen ataques DDoS, ejecución de comandos, sabotaje y espionaje industrial, entre otras.

Cualquier vulnerabilidad que presente un sistema de red va a ser utilizado por la ciberdelincuencia para su acceso no autorizado. Estos son algunos de los riesgos a los que están expuestos los dispositivos IoT, frente a ataques de tipo *botnet* y DDoS, relacionados con la activación de servicios de red innecesarios o inseguros, que facilitan el acceso y control

no autorizado a cualquier servicio, lo que vulnera la confidencialidad, integridad, autenticación y disponibilidad de la información.

Dentro de los riesgos asociados a interfaces encargadas de gestionar los dispositivos propietarios o de terceros, se encuentran, por ejemplo, las aplicaciones móviles, los repositorios de datos en la nube e incluso, las páginas web corporativas y las API del *backend* (propias de la programación de aplicaciones). Todas estas fallas conllevan a vulnerabilidades como la implementación de un cifrado débil (o ausencia de este) sobre los datos que circulan por la red, al igual que la ausencia de filtros entrada/salida. En la Tabla 2 se resumen los principales ataques DDoS, los mecanismos empleados y protocolos (objetivos) comprometidos:

**Tabla 2.** *Ataques ddos más comunes*

| Tipo de Ataque | Descripción | Mecanismo de ataque | Objetivo |
|---|---|---|---|
| **TCP SYN Flood** | Envía múltiples solicitudes TCP SYN al servidor objetivo, saturándolo y evitando conexiones legítimas. | Inunda al objetivo con una gran cantidad de paquetes SYN. | Protocolos de capa de red y transporte TCP. |
| **UDP Flood** | Envía una gran cantidad de paquetes UDP al servidor objetivo, con el fin de congestionarlo y así provocar interrupciones del servicio o caídas del servidor. | Inunda al objetivo con una gran cantidad de paquetes UDP. | Protocolos de capa de red y transporte UDP. |

Continúa tabla...

| Tipo de Ataque | Descripción | Mecanismo de ataque | Objetivo |
|---|---|---|---|
| **HTTP Flood** | Lanza un ataque de alta capacidad contra un servidor web, sobrecargándolo con solicitudes y posiblemente bloqueándolo. | Inunda al objetivo con una gran cantidad de solicitudes HTTP. | Protocolos de capa de aplicación **HTTP**. |
| **DNS Amplification** | Envía consultas DNS a resolutores DNS abiertos, que responden con un mayor volumen de tráfico al servidor objetivo, saturándolo. | Utiliza resolutores DNS abiertos para amplificar el ataque, enviando consultas DNS que resultan en un gran volumen de tráfico hacia el objetivo. | Protocolos de capa de red y transporte UDP. |
| **Smurf Attack** | Envía una solicitud de **ping** a la dirección de difusión de una red, utilizando una dirección **IP** falsificada que pertenece al objetivo, provocando que todos los dispositivos en la red le respondan con un alto volumen de tráfico. | Falsifica la dirección **IP** de origen de la solicitud de **ping** para que parezca que proviene del objetivo. | Protocolos de capa de red y transporte **ICMP**. |

Fuente: elaboración propia.

Otras fallas que se encuentran en dispositivos IoT y que pueden ser aprovechadas para su acceso no autorizado son el *firmware* desactualizado, que conlleva a la falta de gestión de procesos de cifrado en tránsito y validación de las actualizaciones sin mecanismos apropiados para ello; el uso de componentes y librerías de software inseguros u obsoletos;

el uso inapropiado de información personal —almacenado en un dispositivo cuyo grado de seguridad es cuestionable—, sumado a la ausencia de un permiso formal o consentimiento informado; ausencia de cifrado de datos y control de acceso a los mismos. Las fallas mencionadas convergen en la falta de gestión y administración de los dispositivos de IoT atribuidos a errores humanos, que no cumplen con las normas y políticas de seguridad de la información corporativas, dictaminadas por entes nacionales e internacionales como la familia de normas ISO 27000 (Baena et ál., 2019; Mintic, 2016), entre otras.

## Ataque persistente avanzado

Un APT es un tipo de ataque cibernético donde se tiene acceso no autorizado a un sistema informático o red, permaneciendo "sin ser detectado durante un período prolongado de tiempo" (Márquez, 2017, p. 7). El objetivo de un ataque APT suele ser el robo de datos confidenciales o interrumpir el funcionamiento de un sistema de manera parcial o total. Para ello, el APT se planifica y diseña cuidadosamente para infiltrarse en una organización, evadiendo las medidas de seguridad existentes y operar sin ser detectado. Los APT suelen constar de varias etapas, cada una con un objetivo específico y con herramientas y técnicas específicas, tal como se resume en la Tabla 3.

**Tabla 3.** *Etapas comunes de un APT*

| Etapa del APT | Descripción |
|---|---|
| Investigación | Recopilación de información sobre el objetivo y la red. |
| Fase de entrada | Uso de una vulnerabilidad o engaño para acceder a la red. |
| Establecimiento de una presencia persistente | Instalación de herramientas de control remoto y otros programas maliciosos en la red. |
| Propagación lateral | Movimiento a través de la red para obtener acceso a sistemas adicionales y robar datos sensibles. |
| Fuga de datos | Extracción de datos sensibles de la red. |
| Mantenimiento | Limpieza de pistas para mantener el acceso no detectado a la red |
| Exfiltración de datos | Transmisión de datos robados por medio de la red de los atacantes |

Fuente: elaboración propia.

Como se observa, los APT son altamente personalizados, por ende, varían en términos de sus objetivos, herramientas y técnicas empleadas. Asimismo, los ataques APT generalmente son llevados a cabo por personal altamente calificado y financiado, como gobiernos u organizaciones criminales. Utilizan una variedad de tácticas y técnicas sofisticadas para obtener acceso a un sistema de destino, incluido el *phishing*, *malware* e ingeniería social, con el objetivo de comprometer una red y mantener el acceso a ella, a menudo, aprovechando las vulnerabilidades de día cero y *malware* personalizado.

Una vez que el atacante ha obtenido acceso al sistema, utilizará métodos sigilosos para evitar la detección y mantener un punto de apoyo en el sistema durante el mayor tiempo posible. Esto puede incluir el uso de herramientas y procesos legítimos para mezclarse con la actividad normal del sistema y el uso de canales de comunicación encriptados para evitar la detección.

Puede ser difícil defenderse de los ataques APT, ya que a menudo implican tácticas sofisticadas y dirigidas, que se adaptan a la red de la organización a la que el ataque ha sido envido. Los atacantes pueden pasar una cantidad significativa de tiempo, estudiando la red y los sistemas del objetivo, antes de lanzar el ataque, para comprender sus defensas y vulnerabilidades. Esto permite evadir la detección y las medidas de seguridad de la red atacada.

Para protegerse contra los ataques APT es importante contar con medidas sólidas de ciberseguridad —tanto para usuarios estándar como privilegiados—, incluidos *firewalls*, antivirus y sistemas de detección de intrusos, entre otros. También es importante educar a los usuarios sobre cómo reconocer y notificar amenazas potenciales que permitan evitar ataques de tipo *phishing* y otras tácticas utilizadas en los ataques APT, al igual que actualizar periódicamente el software y demás sistemas conectados a la red para solucionar las vulnerabilidades.

Los APT pueden combinarse con un ataque de DDoS, ya que este busca sobrecargar una red o un sitio web con tráfico de múltiples fuentes —en un intento de que no esté disponible para los usuarios—, consumiendo todos sus recursos o ancho de banda. Los ataques DDoS generalmente se llevan a cabo mediante *botnets*, dejando a las redes de los dispositivos comprometidos, controladas por el atacante. El atacante digita comandos a la red de *bots* para enviar miles de peticiones a la red o sitio web de destino, que genera una avalancha de tráfico y satura el sistema objetivo para que no esté disponible. También, se falsifican las direcciones de origen del tráfico para ocultar su identidad. Por ejemplo, un atacante puede usar el DDoS para distraer y desviar la atención del personal de las Tecnologías de la Información (TI) de una organización, mientras realiza un ataque APT en segundo plano.

En este orden de ideas, el IoT y las Tecnologías Operativas (TO) están cada vez más conectadas y generalizadas, creando una superficie de ataque más grande para posibles ataques cibernéticos. La integración de dispositivos IoT y el uso creciente de la conectividad en la nube en los sistemas TO y TI, aumenta el riesgo de vulnerabilidades e infracciones. Como resultado, una gama más amplia de industrias y organizaciones ahora corren el riesgo de ataques cibernéticos debido a la rápida expansión de los dispositivos IoT, creando una mayor cantidad

de puntos de entrada, a lo que se suma la integración de las TO con la nube, que aumenta aún más la vulnerabilidad de estos sistemas. El cierre de la brecha entre las TI y las TO también conduce a un acceso menos seguro a los sistemas, facilitando que los atacantes se dirijan a la infraestructura crítica.

Puede ser difícil defenderse de los ataques DDoS porque a menudo involucran una gran cantidad de dispositivos o redes, dificultando rastrear el ataque hasta su origen. Para protegerse contra los ataques DDoS, las organizaciones pueden usar técnicas como la limitación de velocidad, configuración del tráfico y el equilibrio de carga para mitigar el impacto del ataque. También es importante contar con una infraestructura de red sólida que sea capaz de manejar grandes volúmenes de tráfico y contar con un plan para responder y mitigar los ataques DDoS.

En el contexto corporativo e industrial es imprescindible incluir una estrategia para emergencias DDoS en los manuales de ciberseguridad, donde la respuesta a un ataque sea clara para evitar poner en peligro la disponibilidad de los servicios, por lo que se recomienda contar con un enfoque de solución de varias capas que incluya medidas técnicas y organizativas.

Los cortafuegos de última generación ofrecen cierta protección, pero son limitados y no pueden defenderse de las aplicaciones en la nube, ni contra ataques de ejecución, por lo que basarse en la en la

IA puede ser una solución eficaz y mantiene la base de datos actualizada, de forma automatizada. Otra alternativa es utilizar un enfoque híbrido que combine la protección DDoS con la nube, lo que permite filtrar e inspeccionar el tráfico en tiempo real, asegurando una alta protección; implementar una estrategia DDoS integral es esencial para reducir el impacto de los ataques y garantizar que los sistemas sigan operativos frente a un ataque DDoS dirigido.

A medida que se expande el uso de la TO, es más frecuente el *malware* dirigido a estas infraestructuras, diversificándose los ataques a gran escala. Tal es el caso de los ataques de *ransomware*, que anteriormente se consideraban un vector de ataque centrado en las TI, pero que ahora están afectando a los entornos de TO. Los adversarios han reconocido que el impacto financiero y el apalancamiento de extorsión del poder de cierre y de otras infraestructuras críticas, son mucho mayores que en otras industrias. Esto resalta la necesidad de que las organizaciones sean conscientes de la creciente amenaza para los sistemas de TO y TI e implementen medidas de seguridad apropiadas para protegerse de este tipo de ataques.

## Discusión

El riesgo de que se incrementen los ciberataques —para los próximos años— es alto, por el hecho de que existirán millones de servidores en el mundo

con alta dependencia tecnológica y que van a estar comprometidos por fallas en su seguridad. El IoT —con sus diferentes variantes— presenta mayores vulnerabilidades para la industria y sociedad en general, por la razón antes mencionada. Asimismo, los métodos de ataque a mediano plazo están proyectados para contrarrestar las herramientas de seguridad estándar, que supone nuevos modelos de *malware* avanzados, integrados con algoritmos basados en IA.

En este sentido, tanto la manera de ataque como de defensa de los sistemas informáticos deberán evolucionar, demandando recursos importantes, sobre todo para gobiernos e infraestructuras críticas por representar objetivos primarios.

La filtración de datos e incidentes de seguridad puede llevar a la desaparición de una organización como sucede, por ejemplo, con el pago de rescate de la información secuestrada; la pérdida de clientes y de negocios por mala publicidad; la inactividad del sistema; el tiempo de detección y contención de un ciberataque; la pérdida de valor accionario (para aquellas empresas que cotizan en la bolsa). Adicionalmente, se presentan demandas por la exposición de datos personales de miles o millones de usuarios e incumplimiento de la normatividad, acarreando multas regulatorias que pueden redundar en varios millones de dólares.

Resulta evidente que, para los próximos años, el panorama en materia de ciberseguridad no va a cambiar mucho, en parte, por los efectos que derivaron de la pandemia de la COVID-19, como el aislamiento preventivo, el trabajo remoto (International Labour Organization, 2020; Clifford et ál., 2020) y una mayor digitalizaron social e industrial, lo que trajo como consecuencia, el aumento de ciberataques —que para esa época se concentraron en los sectores sanitarios, corporativos e industriales—, lo que da a entrever que los costos por posibles violaciones de datos se puede incrementar, de no tomarse cartas sobre el asunto.

En términos generales, la ciberseguridad hoy es más crítica que nunca, tal como lo ha demostrado los ataques de tipo *ransomware* y DDOS, en los periodos 2020 al 2023, causando importantes interrupciones, daños a los sistemas corporativos y pagos por rescate de información. En consecuencia, el problema tiende a agudizarse para los miles de millones de dispositivos de IOT que se instalan cada año (Márquez, 2022).

Otro aspecto que contemplar son aquellos ciberataques dirigidos a robar el inicio de sesión en navegadores comerciales, para distribuir *malware* encaminado al fraude y robo de credenciales. Aunque los navegadores actuales presentan un nivel de seguridad alto, no están exentos a ciberataques

avanzados que puedan modificar las DLL o inserción de *malware* polimórfico en *cookies* y páginas emergentes, por lo que se espera que evolucionen en esta década.

La mayoría de las fallas mencionadas tienen solución mediante acciones correctivas al interior de una red corporativa. Por ejemplo, actualizar el *firmware*; instalar los parches emitidos directamente por el proveedor; cifrar los dispositivos con contraseñas propias y no dejar la que trae por defecto desde fábrica; autenticación de dos factores (contraseña + código o llave 2FA); inhabilitar servicios no esenciales de protocolos como IPv6 e IPv4+, fallos de configuración en la interfaz web; configurar los dispositivos para que funcionen bajo servidores DNS internos; monitorear el tráfico de paquetes en la red (en busca de anormalidades en los mismos); controlar los accesos y solidificar los cifrados.

Como los ataques cibernéticos evolucionan, se deben mejorar las medidas y protección de la información, activo más importante de cualquier organización. Existen soluciones que minimizan el riesgo de ciberataques como el *Azure Defender* para IoT, de la empresa Microsoft, que integra herramientas de seguridad de tecnologías de información de terceros, de tal manera que permite funcionar con diferentes dispositivos de proveedores de IoT reconocidos. Otra solución propuesta por *Amazon*

*Web Services*, es AWSIoT y AWSIoT Core para redes públicas y privadas de baja potencia y área amplia LoRaWAN (*Low Power Wide Area Network*), diseñado para mejorar la conectividad y seguridad en dispositivos IoT conectados a la nube de AWS.

En el caso de que se haya cometido un ciberdelito y se solicite un rescate por la información, la acción a seguir es notificar a las autoridades y no pagar, ya que al hacerlo se logra perpetuar las intrusiones y mantener estas acciones criminales. Aunque el Estado indica a las organizaciones no pagar el rescate, muchas de ellas ceden ante presiones para evitar la publicación de información confidencial que, en muchos casos, es publicada en sitios de filtración y se combina con una doble extorsión a pesar de haber pagada.

Publicar la información de aquellas empresas o agencias gubernamentales que se han negado a pagar el rescate, es una de las dos modalidades recientes de ciberdelitos; la segunda consiste en publicar algunos datos en la *darknet* para que la víctima vea que se está hablando en serio. En este sentido, hay naciones que prohíben el pago de estos rescates imponiendo fuertes sanciones a quienes realicen estos pagos.

La capacitación y sensibilización de los empleados es una parte crítica de una empresa, puesto que basta que uno solo incumpla con las normas y políticas de seguridad para comprometer todo el

sistema. Para el caso de que se haya consumado el ciberataque, lo recomendable es establecer planes ante incidentes técnicos y de recuperación comercial, que se supone se han diseñado previamente para lidiar con este tipo de escenario.

Basado en lo anterior, tanto los organismos gubernamentales como la industria tecnológica están buscando soluciones plausibles que permitan anular o al menos minimizar el impacto negativo de los ciberataques y de ciberespionaje a sistemas de IoT. Por ejemplo, la *European Telecommunications Standards Institute* (ETSI), es un organismo que lanzó el estándar de seguridad ETSI TS 103 645 (ETSI, 2020); que contempla la protección de datos y seguridad en electrodomésticos y dispositivos de consumo masivo como cámaras inteligentes, controles de acceso, *wereables* y sistemas de consumo, que incluyen puertas de enlace de IoT, estaciones base y concentradores, dispositivos portátiles, sistemas de automatización del hogar, puertas de enlace conectadas, cerradura de puerta y sensores de ventana.

El objetivo de este estándar y de otros en construcción está encaminado a unificar criterios que faciliten llevar un control estricto de los dispositivos IoT que salen y circulan en el mercado, tanto a organizaciones como naciones. Aunque falta que se definan acuerdos comunes a nivel mundial (que permitan definir y asignar responsabilidades y propiedad en asuntos de seguridad y manejo de datos),

es cuestión de tiempo para que logre, esto en parte por el auge de desarrollo e implementación de nuevas tecnologías IoT para los próximos años.

Los ataques centrados en la captura de información almacenada en la nube es un asunto delicado, porque la ciberdelincuencia tendría el control de toda la información de una organización, dejando sus servicios y activos comprometidos, ya sea a un pago extorsivo, un pago periódico,por no ventilar la información de la empresa y de sus clientes.

No obstante, a pesar de las preocupaciones con respecto a la seguridad, el incremento de redes compuestas por dispositivos inteligentes IoT y variantes de estos, será aún mayor para el presente decenio, involucrando diversas tecnologías emergentes para ampliar sus servicios, como aquellas donde gestionan paquetes de datos y de energía, a través de los diferentes nodos de la red, quienes se encargarán de calcular la ruta óptima para su destino. Este nuevo entorno económico abre nuevas oportunidades de negocio para la industria de servicios, de distribución de energía y monitoreo inteligente de las ciudades, hogares y personas e infortunadamente, nuevas oportunidades para los ciberdelincuentes.

## Conclusiones

Para los próximos años, la seguridad de la información se verá cada vez más comprometida por los continuos avances en los sistemas de cómputo

y algoritmos avanzados. Esto trae consigo implicaciones serias sobre el riesgo de comprometer datos sensibles a organizaciones criminales o Estados interesados en lucrarse a costa de las vulnerabilidades de otros, así como desestabilizar la economía de sus contrapartes. Lo cierto de todo esto es que las empresas deben estar mejor preparadas para lidiar con este tipo de escenario. La norma es simple, empresa que no invierte en ciberseguridad está condenada a desaparecer. No sobra mencionar, que las regulaciones y multas por incumplimiento en la protección de datos está llevando a que las empresas tomen en serio este tema, porque no solo está el castigo pecuniario, sino la reputación y potenciales demandas a las que se exponen por no cumplir con la ley.

En cuanto al IoT, se recomienda el uso de cifrado de forma expansiva; el cifrado en bloque AES-XTS (Luo et ál., 2019) para unidades *Flash* y de arranque seguro basado en el algoritmo RSA, junto con sus respectivas variantes; automatizar la seguridad minimizando con ello el riesgo humano; establecer planes de continuidad de negocio y equipos señuelos; capacitar permanentemente a los empleados; realizar respaldos de datos online y offline; usar *blockchain* como sistema de transacción y procesamiento de datos entre otros aspectos para minimizar el riesgo.

Recientemente, con el *blockchain* se están presentando cambios significativos en materia de se-

guridad IoT, expandiéndolo al denominado Internet cognitivo de las cosas (Thapa et ál., 2022), que combina la IA, el IoT y el *blockchain*. Con esta tecnología se crean contratos inteligentes entre los dispositivos y usuarios, sin tener que depender de una autoridad centralizada. Esta transacción aplica tanto si se realiza entre humano/humano, humano/dispositivos/plataformas. Adicional a esto, surgen Plataformas de Tecnologías de Registro Distribuido (DTL —por su siglas en inglés— *Distributed Ledger Technology*), que trabajan de forma similar al *blockchain*, encaminadas a garantizar la seguridad de las transacciones con IoT. DLT se refiere a cualquier sistema de registro distribuido, mientras que *blockchain* es una implementación específica de DLT (Soltani et ál., 2022).

Es innegable que la seguridad es relevante en cualquier sistema de comunicación, por consiguiente, demandará nuevos desarrollos en hardware como en software; tanto así, que la recolección de datos personales por parte de dispositivos IoT se incrementará en los próximos años, obligando adoptar nuevas técnicas de encriptación *end to end* como la criptografía homomórfica (Zhao y Geng, 2019) y la criptografía ligera o *Lightweight Cryptography*, al igual que los protocolos que involucran la informática confidencial con nivel de seguridad 4 (FIPS 140-3, 2019), razón por la que se está trabajando en una disciplina que combina la criptografía y los

procedimientos de ofuscación o *Whitebox-cryptography* (WBC), para proteger los algoritmos y claves en las memorias Ram de dispositivos IoT, reduciendo con ello las vulnerabilidades relacionadas por la no existencia de protocolos de protección de datos estandarizados.

Las modalidades de *malware* y ataques cibernéticos van a seguir evolucionando, por lo que es necesario preparase para ello. Las campañas de *ransomware* se volverán cada vez más agresivas, con exigencias de rescate más elevadas; aunque los ataques están concentrados en organizaciones, no implica que un ciudadano del común quede exento de ello, todo depende del grado de interés de los ciberdelincuentes o de quien los contrate. Los ataques coordinados pueden ser más efectivos y lucrativos, por lo tanto, es recomendable no bajar la guardia y estar atentos, no solo el personal encargado de los sistemas y redes, sino de cada empleado, puesto que no solo se está comprometiendo la información corporativa, sino la información del personal y de sus familias.

Es importante prever lo que se avecina para los próximos años en materia de tecnologías emergentes como las redes 5G (e incluso la 6G), cuya implementación ha iniciado y también ha empezado a mostrar debilidades en lo que respecta a seguridad, como con la ubicación del usuario y el robo de da-

tos, abriendo oportunidades para secuestrar, escalar un sistema y robar información de forma masiva, mediante ataques en determinados protocolos y de tipo DDoS y APT. Con los servicios centrados en el consumidor móvil, la seguridad, confianza, conveniencia y ubicuidad son factores por considerar bajo los actuales estándares y tecnologías de comunicación venideras.

Para finalizar, con la dinámica de tensión geopolítica presente en la actualidad, entre las grandes superpotencias, se acentuarán aún más los ataques de *ransomware*, APT y DDoS, centrados es destruir infraestructuras críticas e industrias de una nación. Por lo tanto, el sector industrial y los gobiernos deben prever este tipo de ataques, requiriendo ver la seguridad de los datos como una inversión que demanda recursos técnicos y tecnológicos ideales, al igual que diseñar e implementar planes de respuesta ante incidentes, haciendo cumplir las regulaciones en materia de ciberseguridad y otros aspectos.

## Capítulo 3

# Internet de las cosas industriales: estándares y ciberseguridad

*Jairo E. Márquez D., Arles Prieto M.,*
*Luz J. Castañeda R.* y *Luis G. Benavides R.*

La infraestructura de la automatización se ha visto enriquecida debido al creciente número de dispositivos IoT en la industria y en las ciudades inteligentes (*Smart Cities*), en las que presumiblemente se llegue a una cifra cercana al billón, antes del 2030, provocando enormes cambios en la industria 4.0 y en los hogares de todo el mundo. Esta proyección se hace con base en la dinámica de la implementación en múltiples entornos, la conectividad y los datos que capturan permanentemente, bien en el campo de la industria, la medicina, los automóviles y otros sistemas de transporte, dispositivos de seguridad, tecnología vestible, etc.

El IIoT tiene como objetivo mejorar la eficiencia industrial y del lugar de trabajo, mediante la implementación de dispositivos conectados,

como los sensores inteligentes. A diferencia de los productos de IoT, basados en el consumidor, que se utilizan principalmente en los hogares, el IIoT admite su implementación a gran escala, permitiendo la transferencia de un gran volumen de datos a través de redes corporativas. Por ejemplo, una gran empresa que ha adoptado este tipo de tecnologías puede tener cientos o miles de sensores —como se muestra en la Figura 10—, en comparación con una casa inteligente que solo tiene unas pocas docenas. La implementación efectiva de IIoT tiene el potencial de ahorrar tiempo, reducir costos y aumentar la competitividad de la industria.

**Figura 10.** *Representación de gráfica de la conectividad de cientos de sensores a escala industrial*

Fuente: elaboración propia.

La integración de tecnologías de vanguardia como la IA, la realidad virtual y la robótica han mejorado aún más las capacidades del IIoT y como resultado, la productividad, la eficiencia y la rentabilidad en varias industrias, allanando el camino para el desarrollo de fábricas inteligentes, el mantenimiento predictivo y el análisis de datos en tiempo real, entre otras aplicaciones.

Estos beneficios han convertido al IIoT en un factor clave en el crecimiento y el éxito de la industria, lo que ha llevado al desarrollo e implementación de estándares relacionados con los sensores y la seguridad —que juegan un papel crucial en la industria manufacturera y de servicios—. Estos estándares son fundamentales para garantizar el correcto funcionamiento del IIoT, considerados en diferentes contextos, incluida la seguridad autónoma; aunque se han dispuesto diversas alternativas tendientes a reducir los riesgos relacionados con los delitos cibernéticos, el robo de datos y la captura de información, a través de los dispositivos IoT, están a la orden del día, pues el número de vulnerabilidades no deja de crecer.

## Internet de las cosas industriales

El IIoT se refiere a la integración de dispositivos conectados a la intranet o a internet directamente, como los sensores y actuadores en sistemas y procesos indus-

triales, conducentes a recopilar y analizar datos para mejorar la eficiencia y la automatización y la toma de decisiones en tiempo real. "La visión de IIoT incluye todos los aspectos de las operaciones industriales, centrándose no solo en la eficiencia de los procesos, sino también en la gestión de activos, mantenimiento, etc." (Serpanos y Wolfm, 2018, p. 41)

> Esta tecnología se utiliza en una amplia gama de industrias que incluyen la fabricación, logística, energía, petróleo y gas, servicios públicos, transporte, atención médica, etc. El IIoT se considera un facilitador clave para la Industria 4.0, cuyo objetivo es crear sistemas industriales inteligentes y ciudades inteligentes, conectados y autónomos. Tascón y Coullaut (2016) señalan que: En la industria y aquellos lugares con rutinas de trabajo repetitivas como hospitales o granjas, el IIoT permite la optimización del equipamiento y de las operaciones. Desde el punto de vista económico, el impacto es grande, pues incluye cualquier espacio empresarial con producciones en cadena. Abarca todo lo relacionado con mejoras en el mantenimiento de los equipos, la salud y la seguridad de los trabajadores. (p. 77)

El IIoT también permite la integración de tecnologías avanzadas como la robótica, representada por los cobots, la IA por medio del aprendizaje automático y profundo, que convergen a mejorar la automatización y la toma de decisiones en entornos industriales. En consecuencia, las TO y TI conectadas con el Centro de Operaciones de Seguridad

(SOC), si existe, generan una mayor productividad, seguridad y capacidad para predecir y prevenir fallas en los equipos y procesos. Algunos de los beneficios potenciales que puede brindar el IIoT al sector industrial son los siguientes:

1. *Mayor eficiencia:* los dispositivos y máquinas habilitados para el IoT pueden recopilar y transmitir datos en tiempo real, facilitando la supervisión y control de las operaciones relacionadas con las TO. Este escenario conduce a un uso eficiente de los recursos de TI reduciendo el tiempo de inactividad de los equipos.
2. *Mantenimiento predictivo:* los dispositivos IoT pueden monitorear el rendimiento de máquinas y equipos, brindando una advertencia temprana de posibles problemas, permitiendo que se realice un mantenimiento programado antes de que ocurra una falla. Este procedimiento es fundamental para la industria, pues conduce a minimizar problemas en las áreas de producción, de servicios y logística, reduciendo costos y fallas.
3. *Seguridad mejorada:* los dispositivos IoT pueden monitorear la seguridad de los trabajadores y del equipo en tiempo real, brindando una advertencia temprana de peligros potenciales, permitiendo que se to-

men medidas rápidas para mitigar los riesgos, tanto en las TO como en las TI.

4. *Mejor toma de decisiones:* los dispositivos IoT pueden recopilar y transmitir grandes cantidades de datos, proporcionando información valiosa sobre las operaciones que pueden ayudar a los gerentes a tomar decisiones mejor informadas.
5. *Mayor flexibilidad:* los dispositivos IoT se pueden usar para controlar y monitorear operaciones de forma remota, lo que permite una mayor flexibilidad en la gestión y administración de los recursos de las TO, con la capacidad de responder rápidamente a las condiciones cambiantes de las TI.
6. *Ahorro de costos:* se puede ahorrar en los costos a través de la eficiencia mejorada en la reducción del tiempo de inactividad de los dispositivos y de las máquinas habilitados para IoT, así como en la seguridad, a través de la capacidad de tomar decisiones mejor informadas.

Sin embargo, también se presentan desafíos en la implementación del IIoT, como, por ejemplo:

1. *Seguridad:* la integración de dispositivos IoT en sistemas industriales aumenta el riesgo de ciberataques y de filtraciones de datos, tanto en las TO como de las TI. Esto implica garantizar la seguridad de estos dispositivos

y los datos que recopilan, para evitar el acceso no autorizado y proteger la información confidencial.

Con el aumento de *malware* y *ransomware* en la industria en general, extremar las medidas de seguridad no resulta redundante si se intenta mantener a salvo las redes, los dispositivos conectados a la misma y los datos que fluyen permanentemente.

Las redes TO están expuestas a ataques cuando se utiliza la convergencia TI/TO, debido al hecho de que las fábricas inteligentes están en línea. Esto conlleva riesgos significativos, ya que las redes TO son difíciles de proteger. Esto se debe a una variedad de factores, como equipos heredados que no pueden ejecutar software de seguridad y prácticas de seguridad adecuadas de los proveedores de tecnologías operativas.

2. *Interoperabilidad:* garantizar que los diferentes dispositivos, sistemas y plataformas puedan comunicarse y trabajar juntos sin problemas es esencial para la implementación exitosa de IIoT.
3. *Escalabilidad:* conforme crece el número de dispositivos y sistemas conectados, se vuelve cada vez más importante garantizar que la infraestructura y los sistemas que respaldan

el IIoT puedan escalar para satisfacer las demandas de la red.

4. *Confiabilidad:* los sistemas y procesos industriales a menudo son críticos para la operación de una organización y el tiempo de inactividad puede tener consecuencias financieras y operativas significativas. Garantizar la confiabilidad de los sistemas IIoT es esencial para reducir el tiempo de inactividad y garantizar la continuidad del negocio.
5. *Gestión de datos:* el gran volumen de datos generados por los dispositivos y sistemas de IIoT puede ser abrumador, por lo que la gestión y el análisis efectivos de los datos son esenciales para obtener los beneficios que ofrece el IIoT.
6. *Privacidad y protección de datos:* a medida que se recopilan y comparten más datos se vuelve cada vez más importante garantizar que estos se utilicen de manera responsable, cumpliendo con las normas de privacidad y protección de datos que exige cada país.

Como se observa, el IIoT debe afrontar grandes retos en materia técnica y tecnológica, donde la seguridad de los dispositivos juega un papel fundamental, tendiente a proteger la información y la operatividad de la industria.

## La IA y el IIoT

El IoT integrado con la IA o AIoT (Panda y Tripathy, 2018) es uno de los campos del IoT que crece rápidamente, explorando aplicaciones en diversos campos de la industria como: manufactura, cadenas de suministro, sistemas de transporte, comunicación, servicios financieros, salud pública y atención médica, servicios de energía, entre otros. También se le encuentra en varios dispositivos domésticos, incluyendo juguetes y elementos de uso personal. Hay varias tendencias tecnológicas que están impulsando el desarrollo de la AIoT, entre ellas se destacan:

- *Conectividad:* el aumento de la disponibilidad y accesibilidad en la conectividad de redes de baja potencia como 5G, WiFi 6 y Bluetooth 4.0 y 5.X, está permitiendo que cada vez más dispositivos se conecten a internet. Sin embargo, se deben superar obstáculos técnicos que garanticen una conectividad ideal que demanda actualizaciones de las redes y sistemas de comunicación móviles (4G, 4G+ a 5G), que operan en zonas remotas.
- *Sensores y dispositivos de baja potencia:* la miniaturización de los sensores y la creación de dispositivos de baja potencia permiten que los dispositivos sean equipados con la capacidad de recolectar y transmitir datos, esto

incluye emplear el cuerpo humano como conductor natural de señales (Wi-R) (Perry, 2023). Existen tres tipos de sensores IoT para tal efecto (Tascón y Coullaut, 2016):

a. Sensores estáticos: estos sensores se fijan en una determinada ubicación y recopilan datos para diversas aplicaciones prácticas, como la detección de espacios de estacionamiento libres, activar ventanas polarizadoras, medición de temperatura y humedad para el riego de zonas verdes o monitoreo de las condiciones ambientales.

b. Sensores dinámicos: estos sensores se instalan en los dispositivos móviles y pueden detectar diversos parámetros.

c. Sensores de ciudadanos: son personas que utilizan sus teléfonos inteligentes para recopilar datos de diversa índole que ocurren en su ubicación actual y la transmiten a una base de datos central en la nube.

- *Inteligencia artificial y aprendizaje automático:* permiten que los dispositivos IoT sean más autónomos y capaces de tomar decisiones por sí mismos. Los sistemas de aprendizaje automático acompañados con algoritmos predictivos mejoran la calidad de los datos que adquieren los dispositivos IoT. Con esta capacidad, el IoT en la industria ayuda a comprender las amena-

zas potenciales, alertando al equipo de TI o al SOC —encargado para que tome las acciones correspondientes—. También, el hardware dedicado de IA/Machine Learning incorporados en ciertos chips, mejora el consumo energético de los dispositivos, factor importante en la industria y en las ciudades inteligentes.

- *Análisis de datos y aprendizaje automático:* las herramientas para analizar datos, combinadas con el aprendizaje automático, facilitan que estos sean recolectados por los sensores en tiempo real, obteniendo información valiosa que ayuda a las empresas a mejorar la toma de decisiones.
- *Cloud computing:* con el aumento de la capacidad de procesamiento y almacenamiento en la nube, los datos se almacenan y procesan en un solo lugar para permitir el fácil acceso y análisis (Azadi et ál., 2023). Esta tecnología se integra con los "gemelos digitales" —que son representaciones virtuales de activos físicos, como máquinas, dispositivos y sistemas, que se utilizan para analizar y predecir su comportamiento, rendimiento y fallas potenciales—. En el contexto de IIoT e IA, los gemelos digitales se pueden utilizar para supervisar el rendimiento de los dispositivos y sistemas en tiempo real,

proporcionando información sobre su estado e identificando posibles problemas antes de que ocurran.

También admite optimizar las operaciones de los dispositivos y sistemas —ajustando sus configuraciones y parámetros— para mejorar su eficiencia y reducir costos; facilita realizar mantenimientos predictivos, mediante el uso de algoritmos de aprendizaje automático, que analizan los datos recopilados de los dispositivos y sistemas, y predice cuándo es probable que fallen, permitiendo un mantenimiento proactivo. La conectividad y flujo de datos en una red, como se observa en la Figura 11, debe ser permanente, y de presentarse alguna irregularidad, los algoritmos predictivos la detectaran a tiempo.

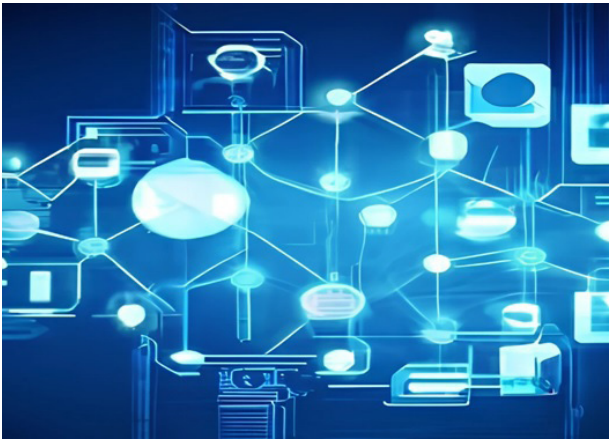


**Figura 11.** *Representación de dispositivos iot gestionados mediante la computación en la nube*

Fuente: elaboración propia.

Sumado a lo anterior, al identificarse las vulnerabilidades y amenazas potenciales, se pueden tomar las medidas adecuadas mejorar la seguridad de los dispositivos y sistemas. En general, los gemelos digitales pueden ayudar en la seguridad al proporcionar visibilidad, información y control sobre los dispositivos y sistemas en la infraestructura de la red, , como se enuncia a continuación:

- *Edge computing:* facilita que los datos se procesen y almacenen en dispositivos IoT en lugar de un centro de datos remoto, mejorando la velocidad de respuesta y reduciendo la carga en la red. La IA y el *Edge Computing* potencian la digitalización de la información clave en cualquier organización, al igual que agiliza las operaciones multidominio y mejora la seguridad de las redes TO y las TI.
- *Seguridad:* la seguridad sigue siendo un desafío importante para el IoT, aunque que cada vez más se desarrollan tecnologías para mejorar la seguridad de los dispositivos y los datos transmitidos. La conexión entre los nodos de sensores con los sistemas de nube escalables integrados con IA se están volviendo cruciales para el análisis de los datos, para presentar la información de forma clara y concisa para la toma de decisiones.

La tendencia de los sistemas inteligentes basados en IIoT ayudan a las organizaciones a prepararse ante desastres de diversa índole, aprovechando la capacidad de los dispositivos conectados en red, al igual que la analítica que proveen en tiempo real. También se toma en cuenta la capacidad de integración de los dispositivos IoT y los puntos finales o *endpoints* —es decir, cualquier dispositivo que esté en la parte final o al borde de una red: computadores, smartphones, portátiles e impresoras, etc.—, que deben estar acompañados de políticas de seguridad, ajustadas a las necesidades del negocio y sus servicios.

- *Integración:* el IoT se está integrando cada vez más con otras tecnologías como *Big Data Analytics*, computación en la nube, *fog-computing, blockchain*, AI, sistemas ciberfísicos, etc., para mejorar la eficiencia y capacidad de los dispositivos controlados desde un sistema central real o simulado mediante gemelos digitales. El registro de datos a través de los diversos sistemas del IoT y los *endpoints*, demandan tecnologías que permitan su gestión y administración, contribuyendo de esta manera a mejorar la toma de decisiones y a minimizar riesgos o amenazas.

La arquitectura de IoT con IA genera estrategias para la AIoT aplicadas a la ingeniería y análisis de datos masivos; la conectividad e integración de redes; el Big Data; la salud; las tecnologías de comunicación; los equipos móviles; la web de las cosas; la transformación y digitalización; el *Edge to Cloud*; el *Edge computing*; los sistemas robóticos; el *blockchain*; la conectividad masiva; la agrotecnología; la interacción humana; la eficiencia energética y la sostenibilidad; la, integración e interoperabilidad con tecnologías 5G en software y en hardware, etc. Este panorama, también abre el espacio para establecer marcos regulatorios acerca de la ética para la AIoT y sus implicaciones con la sociedad en materia de seguridad y privacidad del IoT y del AIoT.

Para proteger cualquier red de IoT, gestionada por TO y TI, utilizar el *blockchain* es una manera viable, porque certifica a cada dispositivo, por medio del Proyecto Hogar Conectado sobre IP (CHIP —por sus siglas en inglés— *Project Connected Home over* IP), que contiene los datos del fabricante y del dispositivo, la versión del actual del software y las actualizaciones, es decir, actúa como un libro de contabilidad distribuido que emplea el *blockchain* para certificar, proteger y mejorar la compatibilidad de los dispositivos IoT.

Para la defensa de los dispositivos IoT, investigadores del Instituto de Tecnología de Massachusetts han desarrollado un chip de Circuito Integrado para Aplicaciones Específicas (ASIC —por sus siglas

en inglés— *Application-Specific Integrated Circuit*) (Zewe, 2022), que puede evitar la extracción de información oculta de un dispositivo inteligente, mediante ataques de canal lateral —ataques que se caracterizan por recopilar información a través de la explotación indirecta de un sistema o hardware—. Asimismo, se puede monitorear las fluctuaciones atribuidas al consumo de energía del dispositivo, mientras una red neuronal especialmente diseñada, funciona para extraer información protegida filtrándose fuera del dispositivo.

El chip antes mencionado, puede ser incorporado en cualquier dispositivo IoT para realizar cálculos de forma segura, utilizando algoritmos de aprendizaje automático perimetral en los datos del sensor y con un bajo consumo de energía. Además, con este chip —en materia de costo computacional y energético— se superan otros métodos de procesamiento seguros como el cifrado homomórfico (Acar et ál., 2018; Martins et ál., 2017) que limita su uso.

Las empresas están anticipando las posibilidades infinitas que trae consigo el AIoT, sin embargo, la integración de dispositivos bajo esta tecnología es desafiante, no solo en lo concerniente al desarrollo, sino a la implementación y a la seguridad. Uno de los principales desafíos de implementar AIoT es la falta de estandarización e interoperabilidad entre dispositivos, dificultando que las empresas integren sistemas y plataformas IoT inteligentes con los *end-*

*points*. Además, la integración de las tecnologías de IA e IoT también trae consigo nuevos riesgos de seguridad, como la posibilidad de filtraciones de datos, el acceso no autorizado y la manipulación de algoritmos de IA.

La falta de segmentación de una red también puede convertirse en un problema de seguridad, ya que permite que los ciberdelincuentes se desplacen fácil y lateralmente por la red, para acceder a los datos confidenciales. Además, las empresas pueden tener dificultades para proteger y administrar la gran cantidad de datos de los dispositivos IoT y los algoritmos de IA, que puede generar problemas de privacidad y de cumplimiento normativo, por lo que puede ser un proceso complejo y desafiante, pero con las medidas de seguridad adecuadas las empresas pueden aprovechar los beneficios de esta tecnología y minimizar los riesgos.

## Estándares de sensores

Los sensores "se han utilizado tradicionalmente para obtener imágenes de la cámara, así como para comunicar información sobre la humedad, la temperatura, el movimiento, la velocidad, la proximidad y otros aspectos del entorno" (Chandrasekaran y Subramaniam, 2022); es así, que el desarrollo de estándares es clave, tanto para los fabricantes, la industria y los usuarios finales, de ahí que se trabaje en los siguientes estándares:

- IEEE 2700-2017: establece las definiciones relacionadas con parámetros de rendimiento y condiciones de los sensores más comunes en el mercado. Incluye las unidades de medida, terminología y especificaciones de rendimiento. "El estándar aborda acelerómetros, magnetómetros, giró metros/giroscopios, sensores combinados de acelerómetro/magnetómetro/giroscopio, barómetro/sensores de presión, higrómetro/sensores de humedad, sensores de temperatura, sensores de luz y sensores de proximidad". (The IEEE standards association, 2022)
- IEEE P2020: este estándar toma en cuenta la calidad de la imagen de las cámaras de un sistema automotriz —relacionado con los Sistemas Avanzados de Ayuda a la Conducción (ADAS —por sus sigla en inglés— Advanced Driver Assistance Systems) (Ziebinski et al, 2017; Jiménez et ál., 2016)— tales como la identificación de métricas e información de variables de calibración, como se muestra en la Figura 12; y la definición estandarizada de métodos de prueba —objetivos y subjetivos— relacionados con la comunicación e integración de sistemas y proveedores de componentes.

**Figura 12.** *ADAS actúa como sistema de apoyo al conductor en situaciones específicas de conducción*
Fuente: elaboración propia.

- ISO 21434: se considera la primera norma internacional para la ciberseguridad de los vehículos. Proporciona pautas para el diseño, desarrollo y producción de vehículos, con el objetivo de protegerlos de las ciberamenazas y garantizar su seguridad. Esta norma cubre el ciclo de vida del vehículo, desde el concepto inicial hasta el final de su vida útil. Incluye requisitos para la gestión de la ciberseguridad, proceso de desarrollo, validación y verificación de los sistemas relacionados con la ciberseguridad.

  Esta norma está diseñada para que los fabricantes de vehículos, proveedores y otras

partes involucradas en el desarrollo y producción automotriz —como los reguladores y autoridades que evalúan la ciberseguridad de los vehículos—, los clientes y usuarios finales la puedan usar. El estándar se divide en varias partes, en los que se aborda diferentes aspectos de la ciberseguridad. Las partes principales incluyen:

Parte 1. Requisitos generales: proporciona una descripción general del estándar y define los requisitos para la gestión de la ciberseguridad.

Parte 2. Gestión de la ciberseguridad: describe los requisitos para la gestión de la ciberseguridad, incluidos los de evaluación y gestión de riesgos, la gestión de incidentes y actualizaciones de seguridad.

Parte 3. Desarrollo y producción: define los requisitos para el desarrollo y producción de sistemas relacionados con la ciberseguridad, incluidos los requisitos para el diseño, implementación y validación de los controles de ciberseguridad.

Parte 4. Soporte y mantenimiento: brinda orientación sobre los métodos y técnicas a utilizar para respaldar y mantener la ciberseguridad en los vehículos a lo largo de su ciclo de vida.

- IEEE P1451.99: busca armonizar la compatibilidad entre ciertos dispositivos con los sistemas de IoT. Este estándar resulta ser importante dado a que, entre los dispositivos electrónicos y los sistemas IoT no se comparten datos de manera segura, por lo que, con este estándar se pretende establecer un puente de metadatos que facilite el transporte del protocolo IoT para diversos dispositivos, como sensores y actuadores, entre otros. La seguridad, escalabilidad e interoperabilidad juegan un rol crucial para el ahorro de costos y la reducción de la complejidad de ciertos sistemas.
- IEEE P2520: este estándar tiene como objetivo proporcionar pautas para el diseño e implementación de seguros en los Sistemas de Control Industrial (ICS—por sus siglas en inglés— *Industrial Control Systems*) y dispositivos IoT, utilizados en entornos de infraestructura crítica, incluidas las pautas para la evaluación de riesgos, el modelado de amenazas y las pruebas de seguridad. Se relaciona con los dispositivos y sistemas bioinspirados, estableciendo los métodos de medición y evaluación conforme a las respuestas quimiosensoriales humanas.

  El estándar aborda la seguridad en los sistemas de control industrial y los disposi-

tivos IoT, que a menudo están diseñados para operar en entornos hostiles y tienen requisitos diferentes a los de los sistemas de TI tradicionales. También incluye recomendaciones para el uso de protocolos de comunicación segura, el desarrollo seguro de *firmware* y software, y una posible respuesta y recuperación ante incidentes.

Este estándar está dirigido a organizaciones que operan infraestructura crítica —como empresas de servicios públicos, compañías de petróleo y gas, el sector de la salud y proveedores y fabricantes de dispositivos ICS e IoT—, así como a integradores de sistemas y profesionales de seguridad que trabajan en esos entornos.

- IEEE 2661: es un estándar para la evaluación de la seguridad del software para ICS y otros sistemas ciberfísicos. Proporciona un marco y una metodología comunes para evaluar la seguridad del software y los sistemas de ICS, ayudando a las organizaciones a identificar y abordar posibles vulnerabilidades de seguridad. Puede ser utilizado por desarrolladores de software, integradores de sistemas e interesados en la mejora de la seguridad de los sistemas y software de los ICS, para garantizar el cumplimiento de las normas y estándares pertinentes, como sucede en la

garantía de seguridad cibernética aplicada a dispositivos inalámbricos, empleados en telemedicina.

El estándar cubre todo el ciclo de vida de un sistema ICS, desde la fase inicial de diseño y desarrollo hasta el final de la vida del sistema. Incluye pautas para la evaluación de riesgos, el modelado de amenazas y el análisis de vulnerabilidades, así como los requisitos para prácticas, pruebas y validación de codificación segura. Este estándar se divide en varias secciones que abordan diferentes aspectos de la seguridad del software. Las secciones principales incluyen:

a. Introducción: proporciona una descripción general del estándar y su alcance.
b. Proceso de evaluación de la seguridad: describe el proceso general para evaluar la seguridad del software y los sistemas de ICS, incluidos los requisitos para la evaluación de riesgos, el modelado de amenazas y el análisis de vulnerabilidades.
c. Prácticas de codificación seguras: proporciona pautas para las prácticas de codificación seguras, incluidos los requisitos para la validación de entrada, el manejo de errores y el manejo seguro de datos.

d. Pruebas y validación: describe los requisitos para probar y validar el software y los sistemas de ICS, incluidos los requisitos para las pruebas de penetración, el análisis de vulnerabilidades y las pruebas de *fuzz*. Estas pruebas de fuzz son una técnica automatizada que envía datos aleatorios a una aplicación o sistema para detectar errores o fallos. Su objetivo es descubrir problemas de seguridad o estabilidad en el software, ayudando a encontrar entradas maliciosas o que causen errores en el sistema.

e. Seguridad de los componentes de terceros: brinda orientación sobre la seguridad de los componentes y bibliotecas de terceros utilizados en el software y los sistemas de ICS.

- IEEE P2888: proporciona un marco metodológico para evaluar la seguridad del software de dispositivos médicos; ayuda a las organizaciones a identificar y a abordar posibles vulnerabilidades de seguridad. El estándar cubre el ciclo de vida útil del software, incluyendo la fase de diseño y desarrollo. También relaciona diversos proyectos de estándares relacionados con áreas tecnológicas como la realidad aumentada, la realidad virtual, la realidad mixta, al igual

que las interfaces de sensores. El estándar se divide en varias secciones en las que aborda diferentes aspectos de la seguridad del software. Las secciones principales incluyen:

a. Introducción: proporciona una descripción general del estándar y su alcance.
b. Proceso de evaluación de la seguridad: describe el proceso general para evaluar la seguridad del software de dispositivos médicos, incluidos los requisitos para la evaluación de riesgos, modelado de amenazas y análisis de vulnerabilidades.
c. Prácticas de codificación seguras: proporciona pautas para prácticas de codificación seguras, incluidos los requisitos para la validación de entrada, manejo de errores y manejo seguro de datos.
d. Pruebas y validación: describe los requisitos para probar y validar el software de dispositivos médicos, incluidos los requisitos para las pruebas de penetración, análisis de vulnerabilidades y pruebas de fuzz.
e. Seguridad de componentes de terceros: brinda orientación sobre la seguridad de los componentes y bibliotecas de terceros utilizados en el software de dispositivos médicos.

f. Es importante tener en cuenta que la seguridad del software de un dispositivo médico es fundamental para la seguridad del paciente, garantizando que las medidas tomadas son las adecuadas para protegerlo de posibles ataques cibernéticos.

- IEEE P2846: este estándar tiene relación con los sistemas de seguridad automatizados e incorporados en vehículos, como el ADAS. Contempla las normas de tránsito —teniendo en cuenta las respectivas dependencias regionales— relacionadas directamente con el impacto del comportamiento del sistema ADAS en un entorno real.

Las tecnologías ADAS, como el recurso de advertencia de cambio de carril, el frenado automático y el control de crucero adaptativo, son cada vez más frecuentes en los vehículos; por lo que se espera que desempeñen un papel fundamental en el desarrollo de vehículos autónomos a gran escala. Sin embargo, estos sistemas también presentan nuevos riesgos y desafíos de seguridad, ya que dependen de redes de comunicaciones y software complejos que pueden ser vulnerables a ciberataques.

El estándar aborda estos desafíos de seguridad al proporcionar pautas para el diseño, implementación y pruebas de los sistemas ADAS. Abarca

también los protocolos de comunicación segura, el desarrollo de software, así como la respuesta y recuperación ante incidentes. El estándar también incluye recomendaciones para el uso de hardware y *firmware* seguros, la implementación de funciones de seguridad como el cifrado, la autenticación y el control de acceso.

- ISO 26262: es una norma internacional para la seguridad funcional de los sistemas eléctricos y electrónicos en la producción de automóviles. Esta norma proporciona pautas para el desarrollo y producción de sistemas relacionados con la seguridad en los vehículos, con el objetivo de reducir riesgos de accidente. Cubre el ciclo de vida de un sistema relacionado con la seguridad e incluye los requisitos para la gestión de la seguridad funcional, desarrollo, validación y verificación. La norma se divide en varias partes, en las que aborda diferentes aspectos de la seguridad funcional. Las partes principales incluyen:

  Parte 1. Introducción y requisitos generales: proporciona una descripción de la norma definiendo los requisitos generales para la gestión de la seguridad funcional.

  Parte 2. Glosario: proporciona definiciones de los términos utilizados en la norma.

Parte 3. Conceptos y modelos para la seguridad funcional: describe los conceptos y modelos para la seguridad funcional, incluido el ciclo de vida y los objetivos de seguridad.

Parte 4. Requisitos para el desarrollo y la producción: se establecen los requisitos para los sistemas relacionados con la seguridad como la gestión; el análisis de peligros y riesgos; la validación y verificación de los sistemas.

Parte 5. Métodos y técnicas de apoyo: se emplean para proporcionar apoyo a la implementación de la norma.

- ISO 26262: ete estándar es ampliamente adoptado por la industria automotriz y se considera clave para la seguridad funcional en dicho sector. El estándar también es relevante para otras industrias que utilizan sistemas relacionados con la seguridad funcional, como los dispositivos médicos, aeroespaciales y ferroviarios, proporcionando un marco para el desarrollo y la validación de los sistemas electrónicos y eléctricos utilizados en los vehículos y dispositivos, con el objetivo de garantizar que estos sistemas no causen daños no intencionados a los pasajeros u otros usuarios de la vía.

Es importante señalar que este estándar es diferente al de la seguridad de la información, porque atañe a la seguridad funcional, que se refiere a la capacidad de un sistema para realizar su función prevista sin causar daño, mientras que la seguridad de la información se refiere a la confidencialidad, integridad y disponibilidad de los datos.

La norma se divide en varias partes, cada una de las cuales aborda un aspecto diferente de la seguridad funcional. Las partes principales incluyen:

Parte 1. Requisitos generales: proporciona una descripción general del estándar y su alcance, así como las definiciones y conceptos utilizados en el estándar.

Parte 2. Conceptos, principios y métodos: describe los conceptos, principios y métodos utilizados para garantizar la seguridad funcional, incluidos los requisitos para el análisis de peligros, evaluación de riesgos y gestión de la seguridad.

Parte 3. Desarrollo de productos del sistema: proporciona pautas para el desarrollo y validación de sistemas electrónicos y eléctricos, incluidos los requisitos para la integración, prueba y validación.

Parte 4. Desarrollo de productos de hardware: proporciona pautas para el desarrollo y validación de sistemas electrónicos y eléctricos, incluidos los requisitos para el diseño, prueba y validación.

Parte 5. Desarrollo de productos de software: proporciona pautas para el desarrollo y validación de sistemas electrónicos y eléctricos, incluidos los requisitos para el diseño, prueba y validación.

Conforme los protocolos y estándares se establecen en los diversos campos de la industria y mercado del IoT, se hace evidente que en materia de construcción de sistemas seguros "deberá abordar el hardware, el software y los protocolos y su interacción. Los problemas de seguridad del hardware deben proteger contra ataques en los que un pirata informático puede actualizar físicamente un sistema para comprometer la seguridad o causar daños." (Institute of Innoavation Tecnhnological, 2022, s.p.).

## Ciberseguridad en IIoT

El uso de los sensores en diversos dispositivos IIoT se ha incrementado en los últimos años, debido a su progresiva funcionalidad, tamaño reducido y bajo consumo energético, maximizando las capacidades operativas e infraestructura en red sobre las que operan (Márquez, 2017). La adopción de los

sensores en diversos campos de la industria y servicios demanda una estandarización en materia de ciberseguridad, que garantice su uso en un entorno ubicuo. Cabe señalar, que un ciberataque no solo compromete la información, sino que lleva a la organización a fuertes sanciones legales y financieras por no cumplir con sus obligaciones contractuales.

Al comprometer la información ante un ciberataque, la imagen corporativa se afecta notoriamente ante sus clientes, a lo que se suma la desconfianza de los usuarios afectados. Reparar estos daños resulta ser costoso, con el riesgo de que la empresa desaparezca del mercado. En este orden de ideas, la ciberseguridad en el IIoT es una preocupación importante porque los sistemas industriales a menudo controlan la infraestructura crítica y tienen el potencial de causar un daño significativo si se ven comprometidos. Algunas de las consecuencias de las brechas de seguridad cibernética en el IIoT incluyen:

- *Pérdida de control:* los ataques cibernéticos pueden interrumpir o desactivar los procesos industriales, provocando accidentes o daños en los equipos, que llevan a la pérdida de control sobre estos.
- *Pérdida de datos:* los ataques cibernéticos también pueden provocar la pérdida de datos confidenciales —como propiedad in-

telectual o información financiera—, que puede tener graves consecuencias para las empresas y las personas involucradas.

- *Pérdida de reputación:* una brecha de seguridad cibernética puede dañar la reputación de una empresa o institución, que deriva en la pérdida de confianza del cliente y, potencialmente, en pérdidas financieras.
- *Daño físico:* en algunos casos, los ataques cibernéticos a los sistemas IIoT pueden provocar daños físicos a las personas o al medio ambiente. Por ejemplo, un ataque cibernético a un sistema de control industrial podría provocar un derrame químico, activación de válvulas de control de gas o petróleo, etc.

Hay muchas maneras en que los atacantes pueden manipular los dispositivos IoT. Algunos métodos de ataque comunes incluyen:

1. *Ataques de fuerza bruta:* es un tipo de ataque cibernético donde un actor malicioso usa software automatizado para probar repetidamente diferentes combinaciones de credenciales de inicio de sesión (por ejemplo, nombre de usuario y contraseña) en un intento de obtener acceso al dispositivo. Esto se hace mediante el envío repetido de solicitudes de inicio de sesión del dispositivo o al extremo de la API (*Application Programming Interface*), hasta que se descubren las credenciales correctas.

Este tipo de ataque puede ser especialmente peligroso para los dispositivos IoT, porque a menudo tienen medidas de seguridad débiles, como credenciales de inicio de sesión predeterminadas o contraseñas fáciles de adivinar. Además, muchos dispositivos IoT tienen memoria y potencia de procesamiento limitadas, que puede hacerlos más vulnerables a un ataque de fuerza bruta. Para protegerse contra estos ataques es importante implementar métodos de autenticación sólidos, actualizar y parchear regularmente el *firmware* del dispositivo y usar soluciones de seguridad como *firewalls* o sistemas de detección de intrusos.

2. *Acceso no autorizado:* consiste en intentar obtener acceso a un dispositivo IoT, sin las credenciales o permisos adecuados, probando repetidamente diferentes combinaciones de credenciales de inicio de sesión hasta que pueda obtener acceso. Esto se puede hacer mediante el uso de un software automatizado que prueba rápidamente miles de combinaciones diferentes, de nombre de usuario y contraseña, hasta encontrar la correcta. Una vez vulnerado el acceso, el atacante puede hacerse pasar por un sensor, enviando información corrupta, con el fin de alterar algún proceso industrial o servicio en la cadena de suministro.

   Una vez que el atacante ha obtenido acceso al dispositivo puede usarlo con fines maliciosos,

como robar información confidencial, interrumpir operaciones o usar el dispositivo como punto de lanzamiento para nuevos ataques. Para evitar el acceso no autorizado es importante implementar medidas de seguridad sólidas, como actualizar periódicamente el software y usar contraseñas complejas y únicas, así como monitorear el dispositivo para detectar actividades sospechosas.

3. *Ataques Man-in-the-middle (MitM):* este ataque conocido en español como "hombre en el medio", consiste en que un atacante intercepta las comunicaciones entre un dispositivo IoT y un servidor, luego, manipula o roba los datos que se transmiten sin que ninguna de las partes sea consciente del ataque. Esto puede suceder, por ejemplo, si el atacante está conectado a la misma red Wi-Fi que el dispositivo objetivo.

   Una vez que el atacante está en medio de la comunicación puede usar una variedad de técnicas para manipular los datos que se intercambian. Por ejemplo, pueden interceptar y modificar los comandos enviados al dispositivo, haciendo que realice acciones no deseadas. También pueden robar información confidencial, como credenciales de inicio de sesión o datos personales.

   Los ataques MitM pueden ser difíciles de detectar, ya que la comunicación entre las dos partes parece ser normal. Para protegerse contra

estos ataques es importante utilizar protocolos de comunicación seguros, como HTTPS o SSL, y mantener todos los dispositivos y software actualizados con los parches de seguridad más recientes. Además, el uso de una Red Privada Virtual (VPN —por sus siglas en inglés— *Virtual Private Network*) puede ayudar a cifrar la comunicación y protegerla de estos ataques.

4. *Ataques de malware:* el *malware* se diseña específicamente para interrumpir, estropear u obtener acceso no autorizado a un sistema informático. Los dispositivos IoT a menudo son objeto de este tipo de *malware*, que se puede entregar a través de una variedad de métodos como: correos electrónicos de *phishing*, sitios web infectados, una actualización de software o explotando una vulnerabilidad en el software del dispositivo. Una vez que el *malware* está en el dispositivo puede realizar una variedad de acciones como:
    - Recopilación de información confidencial del dispositivo: esto podría incluir información personal, credenciales de inicio de sesión u otros datos confidenciales.
    - Controlar el dispositivo: el *malware* puede tomar el control de un dispositivo, haciendo que realice acciones sin conocimiento del usuario.
    - Creación de una *botnet*: el *malware* puede usar el dispositivo infectado para crear una

*botnet*, caracterizada por estar compuesta por una red de dispositivos infectados que el atacante puede controlar de forma remota para escalar un ataque.

- Difundir *malware*: el *malware* puede propagarse a otros dispositivos en la misma red, infectándolos también.
- Denegación de servicio: el *malware* puede sobrecargar los recursos del dispositivo, haciendo que se bloquee o deje de responder, denegando el servicio al usuario, comprometiendo además la información de la organización secuestrándola.
- Creación de puertas traseras: el *malware* puede crear una puerta trasera en el dispositivo, que permite al atacante acceder en cualquier momento y robar información confidencial.

  Es importante mantener el dispositivo y su software actualizados y usar contraseñas seguras y encriptación para protegerse de los ciberataques. Además, es recomendable utilizar un buen software antivirus, habilitar *firewalls* de red y monitorear el tráfico de red regularmente para detectar y eliminar cualquier amenaza potencial.

5. *Ataques de DoS:* se intenta hacer que los dispositivos *endpoint* no estén disponibles en una red, saturándolos con tráfico de múltiples fuentes.

Los dispositivos IoT se pueden usar para lanzar ataques DoS, enviando grandes cantidades de tráfico a un objetivo. Esto se puede lograr mediante el uso de una red de dispositivos comprometidos, conocida como *botnet*, para lanzar el ataque o mediante el uso de técnicas de amplificación que aumentan la cantidad de tráfico enviado al dispositivo de destino.

Algunos tipos comunes de ataques DoS en dispositivos *endpoint* o IoT incluyen inundaciones UDP, inundaciones SYN e inundaciones HTTP (Márquez, 2020). Dado que los dispositivos IoT a menudo tienen recursos limitados, no están bien protegidos y son particularmente vulnerables a este tipo de ataques.

6. *Ataques de ransomware:* en el caso de los dispositivos IoT, los ataques de *ransomware* obtienen acceso no autorizado al dispositivo y luego cifran los datos almacenados en él. Una vez bloqueado el acceso, se pide rescate para restablecer el sistema, cuyo pago son criptomonedas, claro está, sin garantía alguna de que la información ya no se haya filtrado o comprometido en la darknet.

   Los dispositivos IoT son vulnerables a los ataques de *ransomware* porque pueden tener medidas de seguridad débiles, facilitando que los atacantes accedan a ellos. Además, muchos dispositivos IoT almacenan datos valiosos que un

atacante puede usar para extorsionar al propietario del dispositivo.

Los ataques de *ransomware* son cada vez más frecuentes en la industria a través de los dispositivos IoT, debido en parte a la falta de implementación de políticas de seguridad o no respetar las mismas. Al estar expuestos, estos dispositivos facilitan a los ciberatacantes acceder a la red e iniciar movimientos laterales para ampliar el control y posterior secuestro del sistema por medio de *exploits* especialmente diseñados.

Al utilizar los dispositivos IoT como puntos de entrada a una red, se procede a escalarla mapeando los diversos dispositivos como *routers*, cámaras, computadores, *tablets*, impresoras y servidores NAS, entre otros, infectándolos. El ataque busca desactivar el *firewall* y otros sistemas de protección para poder ejecutar programas maliciosos, que permitan lanzar ataques de denegación de servicio estándar o distribuido (DoS o DDoS) (Márquez, 2019), que conducen a la exfiltración de archivos y encriptación de estos, bajo los privilegios de administrador.

Este tipo de ataque está encaminado al software y al hardware, es decir, a los sistemas SCADA o PLCs sobre los que tendría un efecto inmediato y destructivo, ya que podría detener el funcionamiento de la maquinaria y del equipo crítico de una empresa.

7. *Ataques físicos:* estos ataques implican la manipulación física de un dispositivo —como sacarlo de su ubicación o acceder a él a través de un puerto físico desprotegido—, lo cual se puede hacer de varias maneras, como obtener acceso al dispositivo a través de una ubicación física insegura, usar herramientas físicas para eludir las medidas de seguridad o explotar vulnerabilidades en el hardware o *firmware* del dispositivo.

   Algunos ejemplos de ataques físicos en dispositivos IoT incluyen:

   - Manipular el *firmware* o el hardware de dispositivos para cambiar su comportamiento o funcionalidad.
   - Usar un dispositivo físico para eludir las medidas de seguridad, como un registrador de teclas o un *malware* basado en hardware.
   - Quitar el dispositivo de su ubicación segura y obtener acceso a los datos almacenados.
   - Usar herramientas físicas, como un soldador, para acceder a los componentes internos del dispositivo y extraer información confidencial como el *firmware* o chips específicos.
   - Explotar vulnerabilidades de hardware en el dispositivo, como protocolos de seguridad débiles o cifrado débil, para obtener acceso no autorizado al dispositivo o sus datos.

- Es importante que las organizaciones minimicen el riesgo en los *endpoint* e IoT evitando almacenar información confidencial, usando servicios basados en la nube.

La importancia de proteger los dispositivos IoT de ciberataques radica en mantenerlos actualizados con los parches de seguridad más recientes, utilizando contraseñas seguras y únicas, teniendo cuidado con las redes y los dispositivos a los que se conectan (Reddy y Rashmi, 2023). La protección subyace en el hecho que las empresas implementen medidas sólidas de ciberseguridad, incluida la actualización regular del software y el *firmware*, la capacitación de los empleados sobre las mejores prácticas en ciberseguridad y la implementación de contraseñas y controles de acceso seguros. La ciberseguridad es un asunto de gran importancia para la industria y los servicios, donde las interrupciones y peligros que conllevan a que los ciberataques pueden comprometer las infraestructuras críticas de una ciudad o país.

Un problema que no se ha podido solucionar actualmente, está relacionado con la implementación de los dispositivos de IoT con un nivel de ciberseguridad superfluo o inexistente, aunque hay directrices y protocolos encaminados a establecer y extender la raíz de confianza de la tecnología del IoT, que incluyen arranque seguro, detección de

anomalías mediante funciones de tipo NXP i.MX 8, cifrado de datos y gestión de claves, interfaces seguras de depuración de E/S, actualizaciones por aire (OTA), comunicaciones seguras, entre otras, es un problemas que no se ha podido solucionar en su totalidad, a pesar de las diversas herramientas de automatización, al igual que software de código abierto y funciones habilitadas de seguridad en hardware estándar y basado en IA.

Un estudio del Laboratorio de Epidemiología de Orange Cyberdefense proporcionó que "en 2019, un dispositivo IoT vulnerable podría infectarse en menos de 3 minutos, y en 2021, un dispositivo de IoT fue atacado en un promedio de 2814 veces cada día por más de 100 *botnets* diferentes que intentan secuestrarlo" (Fontaine y Charette, 2021, p. 3). Por lo tanto, no es de sorprender que este panorama vaya a cambiar para bien de no tomarse cartas sobre este asunto.

De lo anterior, se infiere que las fallas recurrentes de los dispositivos IoT están centradas en que muchos de ellos —por salir rápido al mercado— presentan problemas de seguridad relacionada con vulnerabilidades de ejecución remota de código en la IP, el control de acceso mal configurado o inexistente e incluso, problemas en el hardware. No es de extrañar que las posibilidades de ataque estén encaminadas a explotar estas fallas, para extraer

credenciales de seguridad, entre otros datos, con el objetivo de escalar el sistema para llegar a los servidores y vender dichas credenciales en la *darknet* para perpetuar otros ataques o extorsionar a la víctima.

Dentro de las posibles soluciones se plantea el uso de tarjetas SIM integradas o removibles, que actúen como receptáculo de claves y administrador con servicios criptográficos. Esto hace que no sea necesario ceder información secreta a los proveedores y tampoco agregar recursos dedicados, ni elementos costosos para salvaguardar los datos que captura un sistema IOT en la industria.

La razón del uso de las SIM radica en el hecho de que están protegidas contra ataques físicos —al igual que los chips con las que cuenta, que se encuentran estandarizados y cuya manufactura es de confianza—. Los dispositivos IOT industriales conectados a una red 5G cuentan con tarjetas SIM y se ha demostrado que son fiables, de bajo costo y no requieren chips especializados. Un ejemplo de implementación del uso de la SIM integrada con otros protocolos de comunicación seguros son AZURE y AWS, que se implementan bajo la iniciativa IOT SAFE (GSMA, 2021), los cuales proveen el código fuente para ser implementados en los dispositivos IOT además, de brindar almacenamiento de datos críticos y autenticación de software antes de su ejecución.

## Seguridad autónoma

La seguridad autónoma se refiere al uso de técnicas de IA y ML para monitorear y proteger sistemas y redes informáticas. Esto puede incluir tareas como identificar y bloquear amenazas cibernéticas, detectar y responder a violaciones de seguridad, automatizar operaciones y tareas de cumplimiento de un sistema. El objetivo de la seguridad autónoma es mejorar la eficiencia y la eficacia de la seguridad física y lógica, al reducir la necesidad de intervención manual, permitiendo que los sistemas respondan a las amenazas en tiempo real.

Las capacidades autónomas de diversos dispositivos se incorporan a la infraestructura física —desde el sistema de frenado automáticos en automóviles, como se muestra en la Figura 13, hasta la gestión y administración de energía en las redes

**Figura 13.** *Representación de vehículos autónomos en vía pública, realizando acciones propias de un conductor humano, tales como cambiar de carril, frenar y corregir el trayecto*
Fuente: elaboración propia.

eléctricas—, demostrando su valía en diversos sectores industriales, de construcción y de servicios. Esto ha dado lugar a que la industria se tome muy en serio la ciberseguridad de los diversos dispositivos IIoT, convergentes a detectar y bloquear cualquier actividad maliciosa que en cualquier dispositivo industrial o del hogar.

Existen incontables vulnerabilidades en los dispositivos autónomos (Algarni y Thayananthan, 2022; Moukahal et ál., 2021) —corregidos constantemente—, donde el problema subyace en el hecho de que muchas industrias que trabajan con el IoT están aprendiendo sobre la marcha y muchos de sus dispositivos se han implementado sin las respectivas pruebas de ciberseguridad, exhibiendo vulnerabilidades de software, facilitando que los piratas informáticos lo empleen para espiar o tomar el control sobre ellos.

¿Qué pueden hacer las industrias al respecto? Es imprescindible que quienes están a cargo de las TI y TO implementen el modelo de seguridad *Zero Trust*, para verificar siempre la procedencia de las solicitudes, sin excepción alguna. Quienes están a cargo de las TI y TO deben tener en cuenta que este modelo de seguridad está relacionado con los servidores, las bases de datos, el software de terceros —incluyendo los sistemas operativos, la virtualización de sistemas y protocolos TCP/IP—. Las TI en el entorno industrial se relacionan con las TO y con los sistemas

SCADA, PLC, controladores, protocolos de comunicación industriales, controles de acceso, sistemas biométricos, etc., que pueden ser monitoreadas e incluso, gestionadas por el IIoT y el AIoT.

Es fundamental para cualquier organización asumir que se ha producido una brecha de seguridad y establecer las pautas para limitar el daño en los sistemas de la periferia. Para el caso de los servicios en la nube, el asunto no es tan claro y por ello, la seguridad de confianza literalmente obliga la autenticación y verificación en cada acceso.

> El paradigma Zero Trust permite a los equipos de seguridad planificar la posibilidad de que existan vulnerabilidades a lo largo de una cadena de interacciones entre múltiples sistemas, como a través de varios servicios en la nube, procesos de datos, servicios de almacenamiento y redes. (Technology Innovation Institute, 2022, s. p.)

Por otra parte, debido a su diversificación de los sistemas autónomos —que abarcan la automatización física del hardware y software, los protocolos de comunicación y sistemas de control—, implican una superficie propia de ataque. Recientemente la industria de dispositivos IoT ha propuesto el modelo *Zero Trust* en el diseño de chips para mitigar los riesgos y amenazas potenciales como: ingeniería inversa, espionaje industrial, piratería, superproducción, manipulación e inserción de puertas traseras o troyanos en los chips, por parte de organizaciones

patrocinadas por el Estado. Para abordar estos problemas, se han propuesto varias técnicas como:

- Autenticación disruptiva de chip a chip: esta técnica se utiliza para extender la confianza cero aplicada a la comunicación de chip a chip y así mitigar el impacto de los ataques en la cadena de suministro física o de las actualizaciones de *firmware* maliciosas.
- Bloqueo lógico: esta técnica devuelve el control a la industria propietaria del diseño en la cadena de suministro del chip, mediante la introducción de un mecanismo de que requiere una clave de desbloqueo secreta, representada por un vector binario conocido solo por el fabricante principal.
- Pruebas cónicas ("concretas" más "simbólicas"): esta técnica se utiliza en el análisis de seguridad del software y podría extenderse al diseño de circuitos de chips para detectar problemas en el ciclo de diseño.

Además, el modelo de seguridad *Zero Trust* se puede aplicar en el contexto de TO y TI corporativa al verificar cada solicitud de acceso a los dispositivos IoT y *endpoints*. De esta forma, los usuarios, dispositivos, aplicaciones y datos que se conectan a la red están protegidos bajo las políticas de seguridad corporativas definidas. La tarea de los administradores de TI es asegurar los dispositivos bajo la estrategia

*Zero Trust*, registrándolos y monitoreando cada acción para asegurar el cumplimiento de las políticas.

## Discusión

Debido a la naturaleza de los dispositivos IoT y su relación con los *endpoints* —acoplados a TO y a las TI en un entorno industrial—, los cuales constantemente recopilan y envían información, se utilizan mensajes encriptados, sin embargo, puede suceder que la encriptación se utilice de forma incorrecta, lo que conlleva a revelar información crítica a terceros o peor aún, que no se utilice en absoluto.

Otra debilidad de IoT y de algunos *endpoints* es la violación de datos a través de sistemas heredados —que se refiere al "acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada" (CCNA, 2023) de información confidencial o sensible que se almacena en sistemas tecnológicos obsoletos—, que son aquellos que ya no son desarrollados o respaldados activamente por el proveedor y pueden tener vulnerabilidades conocidas o carecer de características de seguridad actuales. Estos sistemas también pueden tener controles de seguridad débiles o desactualizados que los hace vulnerables a ataques.

Las violaciones de datos pueden ocurrir a través de diversos medios, como la piratería informática, el *phishing*, la ingeniería social u otras formas de ci-

berataque, con graves consecuencias para las organizaciones, incluyendo pérdidas financieras, daños a la reputación y repercusiones legales.

> El Internet de las cosas es un tema emergente de importancia técnica, social y económica. Los objetos cotidianos, los productos de consumo, los bienes duraderos, los automóviles y camiones, los componentes industriales y de servicios públicos, los sensores y otros objetos cotidianos se combinan con la conectividad a Internet y las potentes capacidades de análisis de datos que prometen transformar la forma en que trabajamos, vivimos y jugamos. (Rose et ál., 2015, p.4)

El problema generalizado de los dispositivos IoT surge a partir de sus fabricantes que, por sacarlos rápido al mercado, vienen con las características mínimas necesarias para su funcionamiento, la inversión en el desarrollo de hardware y software seguros es reducida, lo que deriva en que el consumidor, sin saberlo, adquiera una tecnología que pone en riesgo su seguridad a través de algún tipo de dispositivo IoT, como parlantes inteligentes, timbres, dispositivos de *fitness* o bienestar, relojes inteligentes, rastreadores de actividad física, dispositivos de seguridad (cámaras en las puertas y cerraduras inteligentes), etc.

Según un estudio realizado por Dallon (2021), las medidas más comunes para proteger estos dispositivos son "agregar antivirus o VPN a teléfonos inteligentes, computadoras portátiles y tabletas en

la misma red que los dispositivos IoT, cambiar la contraseña predeterminada de enrutadores Wi-Fi y dispositivos inteligentes, y agregar un enrutador Wi-Fi VPN" (p. 15). Otro aspecto por considerar en materia de ciberseguridad, en la industria y en el sector de los servicios, está dirigida a implementar mejores prácticas para la protección de *endpoints* para bloquear el *ransomware* (Mott et ál., 2023; Razaulla et ál., 2023), como las que se enuncian a continuación:

- Mantener el software y el sistema operativo actualizados: asegurarse de instalar actualizaciones y parches tan pronto como estén disponibles, ya que a menudo incluyen correcciones para vulnerabilidades que podrían ser explotadas por ataques de tipo *ransomware*.
- Implementar tecnologías de solución: estas tecnologías permiten la EDR que mitigan riesgos ante potenciales incidentes de ciberseguridad, como la detección de *exploits* y *malware*.
- Usar contraseñas seguras y únicas: esto para todas las cuentas y dispositivos; es pertinente usar un administrador de contraseñas que ayude a generarlas y almacenarlas de manera segura.
- Habilitar la autenticación de dos factores (2FA): se requiere que los usuarios propor-

cionen una forma adicional de autenticación, como un código enviado al celular. Una vez validado el código, el usuario podrá acceder a sus cuentas personales y corporativas. Esta acción ayuda a evitar el acceso no autorizado por parte de piratas informáticos.

- Instalar software antivirus: este software ayuda a detectar y prevenir ataques como los *ransomware*, al escanear el computador en busca de *malware* y otras amenazas.
- Implementar soluciones anti-*spam* y anti-*phishing* para el e-mail: proteger el correo electrónico es crucial, ya que la mayoría de los ciberataques se valen de este medio.
- Implementar controles de seguridad de la red: usar *firewalls* de red y de aplicaciones web, sistemas de prevención de intrusiones y otros controles de seguridad para protegerse contra amenazas externas.
- Realizar una copia de seguridad: hacer una copia cifrada con regularidad puede ayudar a recuperarse en caso de un ataque de *ransomware*. Asegúrese de almacenar las copias en una ubicación segura, fuera del sitio, de la red y sin conexión. Asimismo, se requiere diseñar un plan de recuperación ante desastres que garantice restaurar los datos.

- Implementar herramientas de respuesta a EDR y de detección y respuesta ampliadas. De esta manera, se puedeN realizar búsquedas en todo el sistema para detectar indicadores de peligro e indicadores de ataque. "Las herramientas de EDR ayudan a los analistas a identificar los recursos que se han visto comprometidos, lo que a su vez ayuda a determinar el impacto y el alcance de un ataque" (Sophos, 2022, p. 4).
- Educar a los empleados: sobre los riesgos del *ransomware*, *phishing* e ingeniería social estándar e inversa para que sepan cómo reconocer y evitar correos electrónicos y sitios web sospechosos.
- Usar una VPN: puede ayudar a asegurar la conexión a internet y a proteger contra ataques de *ransomware* al cifrar el tráfico en línea. Sin embargo, no es recomendable su uso masivo como VPN de acceso remoto, sobre todo para aquellos empleados que trabajan fuera de la organización —donde las redes a las que están conectados pueden no estar protegidas—, dejando vulnerabilidades para un ciberataque.
- Reemplazar las VPN de acceso remoto por una *Zero Trust Network Access* (ZTNA). Una ZTNA (Rose et ál., 2020) ofrece mejor seguridad, presentando una administración sen-

cilla y experiencia al usuario. Se caracteriza porque utiliza autenticación multifactor y valida el estado del dispositivo conectado, controlando el acceso y conexión a una red específica.

- Usar la lista blanca de aplicaciones: que permite especificar qué aplicaciones pueden ejecutarse en el computador, lo que ayuda a prevenir la ejecución de software malicioso, incluido el *ransomware*.
- Eliminar los sistemas de escritorio y gestión remota, empleadas para acceder y administrar dispositivos IoT, computadores y servidores clave dentro de la organización. Sin las medidas de seguridad adecuadas, estas herramientas se convierten en un blanco ideal para ataques de *ransomware*.
- Implementar tecnologías de inspección profunda de paquetes en el *firewall*, incluido el descifrado TLS 1.3 de próxima generación para inspección de paquetes encriptados. Esto incluye sistemas de análisis de aprendizaje automático (Singh et ál., 2023) para la detección de amenazas de día cero y *sandboxing*.
- Limitar el movimiento lateral: durante un ataque, se limita la capacidad de moverse por la red libremente haciendo que el atacante circule en el perímetro alrededor de

los recursos de la red. Esto se logra empleando una VPN que proporcione el acceso solo a los usuarios autorizados, sumado a crear pequeñas VLAN conectadas a conmutadores y *firewall* que permitan emplear protección *antimalware* e IPS entre segmentos.

- Implementar sistemas automáticos que respondan a los ataques cibernéticos.
- Verificar las cuentas de correo corporativas, ya que pueden crearse de manera fraudulenta para luego venderlas al mejor postor en la *darkweb*.

Al seguir las prácticas anteriores, una organización se puede proteger de los ataques de *ransomware* y minimizar el riesgo de pérdida e interrupción de datos. Adicional a ello, se deben tener en cuenta algunas consecuencias de las brechas de seguridad cibernética en el IIoT que no se pueden pasar por alto, como, por ejemplo:

- Pérdida de confidencialidad: los ataques cibernéticos pueden dar lugar a la divulgación no autorizada de información confidencial, como secretos comerciales o datos personales.
- Pérdida de integridad: en la modificación no autorizada de datos lleva a la difusión de información errónea o engañosa.

- Pérdida de disponibilidad: la denegación de acceso a sistemas o servicios esenciales interrumpen las operaciones, lo que causa pérdidas financieras.
- Daño físico: en algunos casos, los ataques cibernéticos pueden provocar daños físicos en el equipo o la infraestructura, lo que genera reparaciones costosas y tiempo de inactividad.
- Daño a la reputación: provoca la pérdida de confianza de los clientes y las partes interesadas.

Los ataques a *endpoints* suelen implicar múltiples fases y técnicas. Los adversarios activos emplean distintas tácticas —como la escalada de privilegios para obtener más acceso en el sistema, el robo de credenciales de usuario e inyección de código malicioso en aplicaciones legítimas— que buscan comprometer los *endpoints* para ejecutar acciones malintencionadas, aprovechando las vulnerabilidades y debilidades de seguridad como las señaladas.

Si bien la seguridad en las TO es similar a la seguridad de las TI —en términos de las amenazas cibernéticas enfrentadas, las limitaciones técnicas de los *endpoints*—, las TO hacen que la seguridad sea desafiante, porque a medida que la fabricación cambia a un modelo de la industria 4.0, es probable que aumenten las amenazas hacia las redes de TO.

Sin embargo, los dispositivos de seguridad industrial modernos proporcionarán una forma efectiva y asequible para que las empresas se defiendan. En los próximos años, por ejemplo, los fabricantes tendrán acceso a equipos de seguridad diseñados especialmente para asegurar sus redes (Leon, 2023).

## Conclusiones

El internet de las cosas hace referencia a una red interconectada de dispositivos físicos integrados con sensores y actuadores, que les permite recopilar e intercambiar datos. En el caso del IIoT —que se refiere al uso del IoT integrado con la fabricación, monitoreo, energía y transporte de productos y servicios—, tiene el potencial de traer beneficios significativos para la industria y la sociedad, aunque también trae consigo nuevos riesgos de ciberseguridad.

Los dispositivos IoT y *endpoints* son fundamentales para la seguridad de la información de una organización, pero pueden ser interceptados mediante ataques de espionaje para obtener acceso a información protegida. Este tipo de riesgo puede tener consecuencias devastadoras para las organizaciones —que transmiten datos confidenciales a través de sus terminales—, particularmente, para las industrias de los sectores de la salud, la tecnología, la educación, la seguridad militar y gubernamen-

tal, y aeroespacial. Para minimizar estos riesgos se deben implementar políticas de seguridad e incluir el cifrado adecuado para los datos críticos, al igual que emplear estrategias de mitigación de riesgo, mediante software y hardware especializados y sistemas de protección que garanticen todo el tiempo la funcionalidad de las redes y los dispositivos.

Otro problema de seguridad se debe a la falta de segmentación de la red —entendida como la práctica de dividir una red más grande en subredes o segmentos más pequeños, cada uno con su conjunto de controles y protocolos de seguridad— por parte del personal encargado de las TO y las TI. Esta segmentación ayuda a limitar el alcance de una posible brecha de seguridad, dificultando que un atacante se mueva lateralmente dentro de la red y acceda a información confidencial. Si una red no está correctamente segmentada, un atacante que obtenga acceso podrá moverse libremente por esta, comprometiendo los datos o sistemas confidenciales. La falta de segmentación también puede dificultar la identificación y contención de un incidente de seguridad, provocando daños más extensos. La segmentación de la red se convierte en un factor de seguridad relevante y debe considerarse como parte de una estrategia de seguridad general, de ahí la importancia de proteger los dispositivos con tecnologías VPN, basadas en hardware y solu-

ciones de monitoreo inteligente que analice la red permanentemente.

Adicional a lo anterior, se encuentra la implementación de características de seguridad en los sistemas de red y los *firewalls* de próxima generación —como filtrado de URL avanzado, prevención de amenazas, seguridad de DNS y análisis de *malware*—, que convergen en el concepto de arquitectura única en paralelo de un solo paso (SP3), entendida como un sistema que permite la seguridad de una red, de alto rendimiento, con un solo escaneo y baja latencia, incluso, se incorporan características y tecnología avanzadas, eliminado funciones redundantes que obstruyen procesos críticos, sobre todo cuando el *firewall* realiza un solo procedimiento por carga en los dispositivos a los que está conectado (Kerravala, 2021).

La estandarización de la industria en los servicios de misión crítica, video y datos, así como de comunicaciones de baja latencia ultra confiables van a disparar el valor de las aplicaciones que ofrece el IOT —pues las empresas de telecomunicaciones ya están desplegando las redes 5G en todo el mundo, e involucran la fabricación, transporte, comunicación, entretenimiento y seguridad, cuyas aplicaciones pretenden aprovechar la velocidad, la capacidad y la baja latencia, que superan por mucho a las redes 4.5 G+ (OECD, 2021; Haidine y Hassani, 2016)—,

para las cuales el escalamiento al desarrollo de nuevas innovaciones como robots autónomos será posible gracias a las redes 5G, que garantizan un gran ancho de banda, baja latencia y alta seguridad. La infraestructura que se teje en torno a que las redes 5G impulsará el IoT y todas sus variantes, al igual que los servicios en la nube, en particular la computación en el borde.

## Capítulo 4

# Tecnología de drones LiDAR en la minería

*Luis G. Benavides R., Jairo E. Márquez D.,*
*Arles Prieto M.* y *Luz J. Castañeda R.*

La industria minera del carbón enfrenta desafíos por factores macroeconómicos, tales como la demanda global a la baja; los precios fluctuantes; la alta volatilidad de los mercados, el acceso complicado a los medios de transporte; entre otros. Frente a estas tendencias globales, industriales, laborales y regulatorias se debe recurrir a tecnologías disruptivas e innovadoras para ayudar a superar los desafíos que se avecinan, sin perder de vista las consideraciones ambientales. Estos desafíos requieren que las empresas exploten sus recursos de manera más inteligente. Es necesario repensar los modelos de minería tradicional para sobrevivir, abordando los impulsores financieros, de procesos comerciales y estratégicos (Saade, 2014).

Al capitalizar la automatización y la digitalización, la rentabilidad aumenta de manera proporcio-

nal a la productividad, lo que deriva en la reducción de costos y permite continuar con la competitividad. Es por esto que la disrupción digital está desafiando los modelos de los negocios globales actuales en la cadena productiva de valor. En la industria minera, por ejemplo, se experimenta una tendencia creciente en la implementación del IIoT, la automatización 4.0, la robótica colaborativa —incluidos los drones de última generación, el ML, el *Data Science*, la realidad aumentada, los metaversos, los *Digital Twins* y la gamificación—, sin embargo, los beneficio provienen de la combinación de estas tecnologías y no de uso de forma aislada.

La digitalización de las minas está ayudando a las empresas a funcionar de manera más eficientes y en muchos niveles —desde la gestión de las cadenas de suministro, los inventarios y los servicios—. En tal sentido, la tecnología está automatizando cada etapa del proceso de minería, ayudando que el negocio sea más rápido y genere un mayor retorno de la inversión (Saade, 2014). Además, se espera que en el proceso se generen menos desechos y emisiones, debido a prácticas operativas ambientalmente más eficientes. Por otra parte, la globalización implica que las empresas mineras deban innovar para sobrevivir, ya sea automatizando procesos repetitivos, reduciendo la cantidad de empleados necesarios para operar la mina o encontrar métodos de exploración más rentables y precisos, soportado en tecnologías

que ayudan a los mineros a optimizar los procesos de explotación (Herrera, 2017), teniendo en cuenta el cuidado del medioambiente.

En materia de fuerza laboral como administrativa, estas industrias pueden ser más productivas, gracias a procesos más estrictos y flujos de trabajo automatizados claramente definidos. La automatización de la recopilación de datos y los nuevos flujos de trabajo fotogramétricos —soportados por drones, el aprendizaje y la clasificación automáticos de escenas—, reducen la intervención humana y hacen que la información crítica esté disponible más rápido. La recopilación automatizada de datos a través de tecnologías basadas en imágenes, con drones y fotogrametría, puede entregar datos casi que de forma instantánea para decidir en los distintos niveles de la organización (Sánchez, 2017).

Por ejemplo, los procesos fotogramétricos producen modelos de pilas de almacenamiento en 3D, con mediciones de volumen más precisas, interpoladas a partir de formas simplificadas. Los cálculos automáticos de reservas, basados en datos geoespaciales, no solo son precisos, sino que también proporcionan una comunicación más rápida y en tiempo real sobre el progreso y las previsiones de producción, el tamaño de las reservas y la composición (Ramírez, 2021).

Por otra parte, los centros de comando central de las minas automatizadas y digitalizadas operan

la maquinaria y las herramientas mineras de forma remota, mediante sensores y robots controlados por IA, que en suma brindan entornos de trabajo más productivos y seguros. Esto significa que se podrán salvar miles de vidas cada año, sin mencionar la reducción significativa de lesionados.

En cuanto a la seguridad, el personal está protegido contra condiciones peligrosas, particularmente, en áreas de alta toxicidad, puesto que la tecnología portátil, los sensores conectados y los monitores alertan sobre problemas o condiciones peligrosas a los mineros que están operando en el lugar (Díaz, 2009). De hecho, la capacidad de pronosticar en tiempo real los peligros geotécnicos —tanto de forma cuantitativa y cualitativa—, tales como desprendimiento de rocas, bolsas de agua, estabilidad de taludes y concentración peligrosa de gases, proporciona estimaciones del peligro para comprenderlo mejor y así diseñar aplicaciones de monitoreo y gestión del riesgo.

Si bien la tecnología está eliminando los riesgos de la minería, en cada etapa de la cadena de valor, es particularmente beneficiosa en la exploración, en la que los drones y la fotogrametría brindan datos precisos y más rápidos para la toma de decisiones soportadas en la viabilidad operacional y comercial del sitio, habilitando lugares previamente insostenibles, como entornos submarinos y hostiles (Matías, 2020).

Con informes en tiempo real y análisis avanzados —respaldados por inteligencia artificial, aprendizaje automático y tecnología operativa conectada—, se puede comprender más rápidamente las situaciones complejas y así tomar mejores decisiones informadas. La fotogrametría y la IA aprovechan los algoritmos para procesar datos de fuentes de la cadena de valor tradicional, brindando soporte para decisiones en tiempo real y proyecciones futuras.

Los escenarios de simulación utilizan información geoespacial, aplicando análisis de estilo hipotético y generan informes cartográficos orientados, para que la ubicación sea un factor determinante en la predicción de las operaciones mineras. Los resultados también se pueden rastrear a lo largo del tiempo para cumplir con los estándares ambientales. Afortunadamente para la industria minera, el costo de la robótica, el software y otras tecnologías ha disminuido considerablemente, si se compara con la tecnología topográfica tradicional, la cual requiere de mucha mano de obra, habilidades especializadas y altos costos de operación.

Los ortomosaicos, las nubes de puntos, las Mezclas de Suelo Profundo (DSM —por sus siglas en inglés— *Deep Soil Mixing*) de las minas, producidos automáticamente aumentan la seguridad, la eficiencia y la precisión, al mismo tiempo que re-

ducen los costos y la mano de obra al mínimo, lo que hace que las actividades de extracción y gestión ambiental sean más fáciles de manejar y, por tanto, más rentables, reduciendo la exposición de los trabajadores a condiciones peligrosas.

Desde la automatización y la planificación en tiempo real, hasta la optimización de las operaciones mineras, se genera una mejor gestión en los ciclos de vida de los activos, pues las organizaciones mineras actuales tienen al alcance una mayor productividad y eficiencia operativa. Asimismo, las reconstrucciones precisas y digitalizadas de sitios en 3D, disponibles en servidores privados o en la nube, conectan las operaciones globales y pueden alinear los procesos corporativos y los informes a través de los ERP. El mapeo de drones y el flujo de trabajo integrado aprovecha la visión artificial, la fotogrametría, el aprendizaje automático y las técnicas de IA para agilizar los procesos mineros al conectarse directamente a los sistemas empresariales.

## Drones en ambientes no aptos para humanos

Los drones aportan una amplia gama de soluciones al campo minero, tanto en el control de movimientos de la tierra, como en el manejo de la acumulación de residuos (Matías, 2020). La aerofotogrametría de precisión soporta la etapa de in-

geniería conceptual durante los proyectos mineros, generando modelos digitales 3D del terreno, a partir de los datos obtenidos con el uso de drones, con lo cual se pueden determinar las curvas de nivel o volúmenes extraídos.

En zonas de alto riesgo, el sobrevuelo del área reduce al mínimo los recorridos a pie de las brigadas. Tanto el piloto, como los demás integrantes del equipo técnico pueden mantenerse resguardados mientras el dron realiza el recorrido, ya que su autonomía de vuelo permite llegar a cubrir grandes espacios en diferentes alturas. La calidad de inspección del aérea es un aspecto diferenciador, puesto que la data recolectada es fiable, precisa y permite exportarla a diferentes softwares de diseño y de geoposicionamiento (GIS) para su posprocesamiento. El uso de drones representa una ventaja competitiva, porque permiten:

- Reconocer el estado de las instalaciones, realizando mediciones de superficie más exactas, calculando los volúmenes y las distancias.
- Determinar la cantidad del material minero en stock.
- Calcular los volúmenes extraídos y comparar sus comportamientos con la inspección en dos periodos de tiempo diferentes.

- Hacer seguimiento de los diferentes trabajos productivos.
- Detectar zonas propensas a derrumbes por pendientes pronunciadas.
- Detectar zonas potencialmente inundables.
- Entrenar al personal menos técnico del proyecto, mediante modelados virtuales en 3D.

Otros beneficios incluyen:

- Mejorar la gestión de la seguridad de los trabajadores y del sitio.
- Reducir la variación en los cálculos de volumen de pilas de almacenamiento.
- Reemplazar las costosas aeronaves tripuladas, que además requieren pilotos altamente calificados.
- Permitir a los expertos concentrarse en el análisis y la interpretación los datos recopilados.

Además, facilita la implementación de sistemas de gestión como los riesgos operativos y de cumplimiento:

- Topografía del aérea y cartografía 3D.
- Planeación de actividades de perforación y voladura.
- Ingeniería topográfica.
- Inspecciones de activos, infraestructura, geotecnia y caracterización de estructuras.

Ciclo de vida de los activos:

- Mapeo base 0, para el diseño del sitio.
- Inspecciones durante la construcción del sitio.
- Comparación entre lo diseñado y lo finalmente construido.

Cadena de suministro:

- Gestión de inventarios de existencias.
- Inventario de la producción.
- Previsión de posibles pedidos de entrega.

Algunos casos de uso actuales de la tecnología de drones en operaciones mineras incluyen:

- *Estudios mineros:* un *Unmanned Aerial Vehicle* (UAV) equipado con una cámara RGB, orientada hacia abajo, toma imágenes de una mina o cantera a cielo abierto desde diferentes puntos. El software de fotogrametría utiliza estas imágenes para crear mapas 3D georreferenciados, líneas de contorno, modelos digitales de terreno o modelos digitales de superficie del lugar.

  La fotogrametría aérea realiza mediciones y mapeo de coordenadas 3D, a través de imágenes que contienen información geoespacial. Mediante la fotogrametría se pueden crear mapas topográficos tridimensionales asociados a las características del sitio minero, con los cuales se pueden producir

modelos digitales del terreno y mapas planimétricos (Carrillo, 2021). Esto significa que los modelos 3D son altamente realistas y se pueden usar para recorridos virtuales e información para evaluar los cambios visuales en un sitio a lo largo del tiempo. Los mapas e imágenes adicionales que puede crear este software incluyen ortofotos, nubes de puntos y malla con textura 3D.

- *Gestión de existencias:* las grandes pilas de materia agregada forman un cono, cuyo volumen en el suelo es difícil de estimar, por lo que los aviones tripulados tradicionalmente vuelan sobre estas pilas para tomar medidas minuciosas. Los drones que utilizan software de última generación ahora pueden identificar medidas, realizar cálculos y generar modelos aéreos del terreno con poco esfuerzo y sin personal altamente capacitado. Mediante estos cálculos frecuentes se puede aumentar la rentabilidad y minimizar el desperdicio.
- *Gestión de canteras y planificación de operaciones:* las imágenes aéreas de drones también se pueden usar para producir un modelo preciso del sitio, lo que permite que las operaciones del lugar se diseñen y administren de manera más eficiente y segura, al evaluar mejor el volumen del material que

se extraerá o moverá, optimizar los caminos de acarreo para reducir los costos de combustible y asegurarse de que cumplen con los estándares legales.

- *Perforación y voladura:* se pueden crear reconstrucciones en 3D y modelos de superficie de las zonas que se van a explotar. Después de la voladura, se utilizan imágenes térmicas y de fotometría para asegurarse de que no haya habido cambios potencialmente peligrosos en el material. Las comparaciones entre los estudios realizados previa y posteriormente a las voladuras permiten calcular los volúmenes de forma más precisa, mejorando la planificación de futuras explotaciones, reduciendo el costo de los explosivos y de tiempo de la perforación.
- *Represas de relaves:* son terraplenes de tierra que permiten el almacenamiento de subproductos químicos, potencialmente peligrosos del proceso minero. Los drones vigilan con mayor frecuencia las presas de relaves, para garantizar la integridad y control en los derrames o escorrentías que dañan el medioambiente.
- *Seguridad:* los drones pueden asegurar perímetros y proteger equipos, detectando actividades inusuales y alertando al personal. La perspectiva aérea es valiosa porque permiten

coordinar esfuerzos eficientes de respuesta ante emergencias, al guiar con seguridad a los vehículos de rescate a través de la zona minera en emergencia.

## Minas subterráneas

Las minas de socavón son los espacios más peligrosos de la industria minera, por lo tanto, requieren numerosas aplicaciones de drones para mejorar la seguridad, permitiendo el mapeo de rugosidad de superficies, análisis de estabilidad, modelado de ventilación y detección de fugas y acumulación de gases peligrosos. Sin embargo, las mismas razones por las que son peligrosas para los humanos, hacen que sea difícil operar drones en espacios confinados, con visibilidad reducida, polvo y obstáculos que obstruyen la propagación de la señal inalámbrica, lo que hace que su uso sea altamente especializado.

Los drones pueden monitorear minas abandonadas —de manera más eficiente y segura en comparación con las medidas tradicionales—, en busca de inundaciones, emisión y acumulación de gases, entre otras condiciones potencialmente peligrosas. Las listas de chequeo consignadas en las Tablas 4 y 5 permiten tener una mayor visión de las aplicaciones en minería:

**Tabla 4.** *Relación de objetivos de aplicaciones en una faena minera*

| Objetivo | Resultado |
|---|---|
| Aumentar distancia entre hombre máquina | ✓ |
| Mejorar la eficiencia en la inspección | ✓ |
| Disminuir los tiempos de inspección | ✓ |
| Mejorar la calidad de información proporcionada a los expertos encargados de realizar análisis | ✓ |
| Utilizar la información para realizar mantenimiento preventivo | ✓ |
| Aumentar la seguridad de los trabajadores | ✓ |
| Minimizar el riesgo de accidentes laborales originados en la inspección | ✓ |
| Realizar inspecciones sin generar interrupciones de la operación de explotación | ✓ |
| Inspección en lugares inaccesibles para el hombre | ✓ |
| Inspección de lugares peligrosos | ✓ |
| Disminución de costos | ✓ |

Fuente: Pinto, 2002.

**Tabla 5.** *Relación de actividades que se pueden realizar en una mina*

| Puntos | Cálculo de volúmenes | Registro de audio | Imagen térmica | Imagen HD |
|---|---|---|---|---|
| Concentrado en silos descubiertos | ✓ | | | ✓ |
| Volumen de pilas | ✓ | | | |
| Inventario de patios | ✓ | | | ✓ |
| Inspección de caminos | ✓ | | | ✓ |
| Humidificación de vías | ✓ | | | ✓ |
| Revisión de polines | | ✓ | ✓ | ✓ |
| Correas en mal estado | | ✓ | ✓ | ✓ |

Continúa tabla...

| Puntos | Cálculo de volúmenes | Registro de audio | Imagen térmica | Imagen HD |
|---|---|---|---|---|
| Maquinaria defectuosa | | ✓ | ✓ | ✓ |
| Chancadoras | | ✓ | ✓ | |
| Transformadores | | ✓ | ✓ | |
| Ventilación motores | | | ✓ | |
| Generadores eléctricos | | ✓ | ✓ | |

Fuente: Pinto, 2002.

## Fotogrametría

Si se observan las mismas características topológicas, desde tres o más posiciones referenciadas, se puede hacer la triangulación de la ubicación espacial (obteniendo las coordenadas X, Y, Z exactas). Una característica topológica se define como cualquier punto diferenciado visualmente en una imagen. Al tomar una imagen promedio de la captura, fácilmente se podrá seleccionar variadas características específicas entre las imágenes. Entre más funciones se combinen, se podrán relacionar las distintas imágenes entre sí, para reconstruir los objetos tridimensionales dentro de ellas. Esto es lo que hace el software de fotogrametría para mapear varias funciones en secuencia, hasta cubrir toda el área.

Cuando se tienen varias de estas características mapeadas, se puede generar la nube de puntos, donde cada uno de ellos tiene características coincidentes que describen el área capturada en esa ubicación.

Luego se convierte la nube de puntos en salidas, para ser utilizadas en algún software geoespacial, ya sea una malla 3D o un modelo de elevación digital.

## Medición de existencias e informes topográficos con drones

Los drones pueden mejorar la precisión de las mediciones y hacer que los informes de existencias sean más fáciles que nunca (Said et ál., 2020). La topografía con un dron no solo es más rápida y económica, que los métodos tradicionales, sino que también es significativamente más fácil de usar, porque no se necesita capacitación o educación especial, por lo que el personal puede realizar la captura por sí mismo.

Además, las plataformas de software de topografía con drones renderizan todo en 3D, para que se pueda ver virtualmente el sitio tal y como es en realidad, haciendo que la captura en 3D sea lo más cercana posible al mundo real. La medición de existencias y los informes representan los casos de uso más frecuentes de los drones en los lugares de trabajo minero. Se usa la topografía con drones y el software para obtener volumetría precisa, más que para cualquier otra cosa.

## Métodos de medición de pilas de acopio topográfica con drones

La "supervisión con drones" significa usar un dron para tomar fotos aéreas de un lugar, con alguna forma de Sistema de Posición Global (GPS —por sus siglas en inglés— *Global Positioning System*) y de control terrestre, vinculando las imágenes con el geoposicionamiento. Existen dos flujos de trabajo para esta supervisión: una es la topografía con drones basada en Puntos de Control Terrestre (GCP —por sus siglas en inglés— *Ground Control Points*) y la otra, se refeire a la topografía con drones de Postprocesado Cinemático (PPK—por sus siglas en inglés— *Kinematic postprocesado*).

## Topografía con drones y control terrestre tradicional

Se necesita una cantidad suficiente de puntos conocidos para verificar y fijar las imágenes de un dron al suelo, porque un dron sin capacidades de procesamiento correccional de GPS a bordo es solo un vehículo para capturar imágenes del sitio. Su posición en el cielo no está geoetiquetada con precisión, por lo que no obtiene datos de posición confiables solo de su hardware, de modo que esa precisión proviene del control de tierra.

Tener varios GCP en el sitio en el que se va al realizar el levantamiento, garantiza una precisión

de 1/10 o menos, pero pude llevar mucho tiempo configurarlos en un sitio de trabajo grande. Hay algunas formas de configurar el control de tierra que se enuncian a conitnuación:

- *Método del punto conocido:* un topógrafo tiene que recorrer físicamente el sitio, fotografiar los puntos con un *rover* y marcarlos para que sean visibles. Para ello se vale de los *AeroPoint* —que son GCP inteligentes que se colocan en una distribución óptima del área—. La topografía con drones con GPS diferencial integrado ha reducido la cantidad de control terrestre necesario. Los drones PPK pueden geoetiquetar con precisión y corregir los datos con GPS. Con la capacidad de PPK, el dron geoetiqueta las coordenadas X, Y y Z de cada imagen, en función de la unidad de GPS. Mientras esto sucede, una base (ya sea una estación base, un *AeroPoint* o la red CORS) en tierra también se registra la información de posicionamiento, pero con una triangulación mucho más precisa. Una vez que se completa el vuelo, esos dos conjuntos de datos de GPS se comparan mediante una marca de tiempo, que se registra cuando el dron toma una foto (Ramírez, 2021).

  Los datos iniciales del GPS a bordo, menos precisos, se sobrescriben, por lo que se pro-

porcionan etiquetas geográficas más precisas para las imágenes. Debido a su facilidad de uso y confiabilidad, se recomienda un flujo de trabajo de PPK para la topografía con drones en cualquier sitio, desde minas hasta vertederos y sitios de construcción intermedios.

- *Mediciones de volumen de acopio:* las reservas tienen una forma irregular, por lo que el dron debe capturar las irregularidades y representarlas para que la computadora calcule el volumen de la forma. Los drones pueden capturar y generar datos de mayor resolución, tan precisos como la topografía tradicional, razón por la que pueden producir levantamientos en 3D, con una precisión de 20 a 50 mm.

  Para medir una superficie o ver cuánto falta por recorrer, se comparan los volúmenes entre dos superficies de capturas diferentes y así se puede calcular la densidad del material, para obtener el tonelaje de la reserva. Más allá del modelo digital de las reservas, se debe asegurar que el software de procesamiento cuente con las herramientas que aumentan la eficiencia para extraer el análisis de datos para conocer cuánto dinero hay en la zona de acopio.

  Un software de posprocesamiento con detección automatizada de pilas de almacena-

miento reduce el tiempo en el que se tarda en calcular los volúmenes, por lo tanto, las demás mediciones se pueden procesar de una sola vez. Saber lo anterior permite gestionar los procesos de la cadena de suministro: conocer cuándo existe en stock y planificar cuándo se necesita comenzar a perforar y volar.

Por estas características, el dron se ha convertido en un generador de ganancias de alta rentabilidad. Hoy en día, medir e informar sobre las existencias disponibles con drones se ha convertido en el estándar industrial, debido a que se puede ajustar la previsión financiera y la gestión de la cadena de suministro.

## LiDAR

La tecnología con la que se miden las distancias de detección remota, mediante láseres de alta potencia y energía lumínica, se denomina LiDAR (*Light Detection and Ranging*), palabra que se acuñó de la combinación de *light* y *radar*. Los instrumentos LiDAR apuntan al objeto con el láser y miden tanto la velocidad como la intensidad de la señal reflejada, para calcular con exactitud la distancia entre dos puntos. Esta información de posicionamiento geoespacial se utiliza para crear modelos detallados en 3D (Vincent, 2010).

La tecnología LiDAR se utiliza en aplicaciones aéreas, terrestres y submarinas para diferentes industrias. La capacidad de colocar dispositivos LiDAR en un dron, hace que la tecnología de imágenes sea muy útil para realizar trabajos en los que los operarios humanos pueden estar bajo condiciones de riesgo. En tal sentido, estos dispositivos recopilan datos que permiten el modelado virtual en 3D, mediante el uso de láseres de alta potencia para medir un objeto desde lejos.

En la década de 1960 se desarrolló la tecnología LiDAR —montando los láseres y los escáneres en aviones— y se utilizó para hacer mapas de los cursos del agua. En la década de 1980, con la aparición del GPS, la tecnología LiDAR se convirtió en una herramienta integral para recopilar datos geoespaciales a gran escala y crear mapas topográficos. Sin embargo, los sensores LiDAR eran muy grandes y bastante inexactos, de modo que se montaban casi exclusivamente en grandes aviones y su operación era manual y muy costosa, no permitía un retorno costo-eficiente de la inversión.

Actualmente, la tecnología LiDAR es más barata, pequeña y accesible, lo que lleva a un mayor uso en diferentes industrias (Real, 2011). Los iPhones de última generación vienen equipados con escáneres LiDAR que permiten crear modelos 3D desde una distancia de 4.5 m a la redonda.

Como ya se mencionó, un sistema LiDAR calcula la distancia disparando un láser preciso y de alta potencia a un objetivo y mide el tiempo que demora la señal en retornar. Es por esto que la tecnología LiDAR funciona de forma similar al radar, excepto que usa ondas lumínicas en lugar de ondas de radio o de sonido. Al tener en cuenta la dirección en la que se envía la luz, la posición del escáner LiDAR y la distancia entre los dos puntos, las cargas útiles LiDAR pueden derivar las posiciones 3D exactas de cada punto, desde el cual las señales regresan o rebotan.

Para generar un modelo tridimensional de un objeto, los sensores LiDAR miden las siguientes variables:

- Tiempo: consumido por el retorno del pulso.
- Intensidad: fuerza de la señal de retorno del pulso láser.
- Ángulo de reflexión: las formas en las que se mide la superficie cambian según lo indicado por el ángulo de reflexión.

Después de recopilar estos puntos de datos, el software especializado de mapeo en 3D procesa esta información junto con los datos del GPS y los datos del Sistema de Navegación Inercial (INS —por sus siglas en inglés— *Inertial Navigation System*) para crear modelos 3D detallados y precisos de un área, objeto u objetivo.

Típicamente, un instrumento LiDAR tiene tres componentes principales:

1. Láser: si bien el color y la intensidad del láser varían según el tipo de datos que se recopilan, cada carga útil de LiDAR tiene un láser de alta potencia conectado. Los láseres emiten haces de luz concentrada hacia un objeto, el cual refleja la señal luminosa.
2. Escáner: estos pulsos reflejados son recibidos por el sistema LiDAR, que los mide con precisión; también llamado sensor o receptor. Dependiendo de lo que se mida, hay una variación de los tipos específicos de lentes y ópticas que se utilizan en un escáner LiDAR, por ejemplo, los divisores de haz o los espejos de orificio son dispositivos comunes que se utilizan para recopilar las señales reflejadas.
3. GPS: el sistema LiDAR requiere detectar con la mayor exactitud posible dónde está ubicado el objeto para medir la señal de retorno con alta precisión, por lo tanto, casi todos los equipos LiDAR tienen sistemas de geoposicionamiento y de navegación de última generación, que ayudan a determinar la posición y orientación absolutas del sensor (González y Angulo, 2005).

Hay otras consideraciones de hardware que se deben tener en cuenta al elegir o diseñar la carga útil

del LiDAR, si se va a montar en un dron, como el peso y dimensión de la batería; el sistema de captura de imágenes; el recolector de datos y la aeronave.

Todo el proceso de hacer rebotar un rayo de luz o láser en un objeto, recibir la señal devuelta y calcular su posición absoluta en el espacio se puede representar matemáticamente, usando el tiempo medido "t" (entre la emisión y recepción de la señal) y la velocidad conocida de la luz "c", la distancia "d" entre el sensor y el objetivo, usando la fórmula:

$$d = c * t / 2$$

## Beneficios de LiDAR

Hay una serie de beneficios que ofrece la tecnología LiDAR —y en casi todos los casos, es una mejor alternativa a otros sistemas de modelado 3D, como la fotogrametría—, como la precisión, pues es capaz de apuntar a objetos nebulosos como una nube o pequeños como moléculas individuales. La fotogrametría, que toma cientos de miles de fotografías y las sintetiza en un modelo, requiere de muchos más datos que LiDAR y rara vez es tan precisa.

Los sistemas de fotogrametría se vuelven inoperables en espacios oscuros como minas o cielos oscuros, pero la tecnología LiDAR no tiene problemas para trabajar en esos entornos, ya que funciona con láseres infrarrojos que permiten trabajar con poca luz o en áreas de poca visibilidad. Este es un bene-

ficio que brinda la tecnología LiDAR, ya que muchas industrias de servicios de seguridad o de emergencia la usan de forma intensiva (Fernández y Gutiérrez, 2017). También hay otros beneficios que ofrece la tecnología LiDAR:

- Capacidad de automatizar grandes porciones de trabajo.
- Capacidad de recopilar datos a partir de una amplia gama de fuentes.
- Costeo cada vez más bajo a medida que avanza la tecnología.

Los sistemas e instrumentos LiDAR se pueden clasificar según una serie de parámetros.

*Tipo de láser:* una distinción importante entre los diferentes tipos de LiDAR es el tipo de láser utilizado. Si bien hay cientos de láseres de diferente potencia y alcance, un diferenciador principal es si el láser LiDAR es topográfico o batimétrico.

- LiDAR topográfico: utiliza un láser infrarrojo para mapear los terrenos con sus diferentes características topográficas.
- LiDAR batimétrico: el tipo menos común, utiliza luz verde que penetra en el agua para medir cosas como la profundidad del fondo marino, la altura de la corriente y las elevaciones del lecho del río.

*Orientación:* otra forma en la que se pueden categorizar los diferentes tipos de sistemas LiDAR es

por su orientación: ¿dónde se ubican el láser y el sensor en relación con el objeto de que se está midiendo?

- Orientado al nadir, es decir, mirando hacia abajo, por ejemplo, altímetros LiDAR.
- Orientado al cenit, es decir, mirando hacia arriba, por ejemplo, instrumentos LiDAR atmosféricos.
- Orientado lateralmente, es decir, mirando lateralmente, por ejemplo, autos con conducción autónoma.

*Plataforma:* otra distinción útil entre los diferentes instrumentos LiDAR es ¿en qué plataforma está diseñado para montarse el sistema? (Vincent, 2010). Es decir, ¿la tecnología LiDAR se utilizará en una plataforma aérea o una terrestre? Los sistemas LiDAR aéreos se pueden dividir en drones LiDAR montados en helicópteros, aviones o satélites en órbita. Esta distinción es útil, ya que clasifica los tipos de LiDAR según el tipo de vehículo que maneja la carga útil.

## Dron LiDAR

Los drones LiDAR tienen como carga útil un sensor LiDAR. Se utilizan para recopilar datos desde una plataforma aérea, que se usan para hacer modelos 3D detallados, según requerimientos de la industria asociada (Fernández y Gutiérrez, 2017). Los sen-

sores LiDAR pueden proporcionar modelos 3D con mayor precisión y de alta resolución.

Hay tres formas típicas de usar LiDAR:

1. En la superficie, con un sensor LiDAR portable en un soporte de mano.
2. Aéreo, ya sea montado en un avión, helicóptero o dron equipado con un sensor LiDAR.
3. En el espacio, utilizando satélites en órbita.

Desde sus inicios, la tecnología LiDAR estuvo reservada para proyectos altamente especializados —por sus altos costos de adquisición, operación y mantenimiento—, sin embargo, a medida que los sensores están más disponibles por la reducción de costos y tamaño, las tecnologías de drones LiDAR (a diferencia de los aviones o helicópteros), se están volviendo cada vez más comunes para investigar reclamos de seguros o hacer descubrimientos arqueológicos ocultos por las densas capas vegetales.

La innovación en la tecnología LiDAR está reduciendo drásticamente el costo y el tamaño de los sensores, lo que hace que sea más factible instalar su carga útil en un dron. Asimismo, en la medida en la que los drones LiDAR se vuelven más costo-eficientes, la información que proporcionan es mucho más precisa y asequible.

Un sensor LiDAR conectado a un dron de ala fija puede cubrir alrededor de cuatro kilómetros cuadrados en un vuelo, con una precisión absoluta de

poco más de 10 cm en horizontal y 7 cm en vertical. Actualmente, se pueden lograr estos datos con cualquier método de topografía aérea.

Las diferentes combinaciones de sensores LiDAR y modelos de diseños de drones producirán diferentes tipos de resultados, en algunos casos, el sistema LiDAR no es el mejor método para usar en el modelado 3D. En entornos extensos y uniformes, por ejemplo, como túneles o tuberías de alcantarillado, los datos LiDAR pueden fallar en la creación de una representación 3D confiable, si no los maneja un piloto de drones profesional.

## Mejores drones LiDAR

Por ser una tecnología disruptiva, no existe un estándar mundial que determine cuál es el mejor dron LiDAR. La calificación de mejor dron depende de la configuración tecnológica adecuada para el uso previsto. Si bien existen drones todo en uno y paquetes LiDAR de servicio completo, la mejor inversión para aficionados, entusiastas o incluso empresas más pequeñas es un sensor LiDAR de alta calidad. Este sensor garantiza que se obtengan los datos que se necesitan, por lo tanto, la plataforma aérea que los transporta no es necesariamente lo más importante, por lo menos, no superior a los datos que puede capturar. Por eso, es recomendable determinar las aplicaciones que se le darán a esta tecnología antes de la adquisición y preguntarse lo siguiente:

¿Qué tan práctico y fácil es su manipulación?

Se deben tener en cuenta las condiciones de operación y mantenimiento de los diferentes componentes del dron con escáner LiDAR recomendadas por el fabricante. Se debe asegurar que todo el software y el hardware requerido está incluido y configurado de forma adecuada, con las funcionalidades óptimas de operación y recopilación de datos del sensor. Asimismo, hacer los mantenimientos y actualizaciones que brinda el fabricante, especialmente para las nuevas versiones de *firmware*.

¿Cuáles son sus aplicaciones de uso operativo?

Se pueden optimizar las características técnicas del dron para diferentes tipos de operaciones, lo mismo ocurre con los equipos de sensores LiDAR. El UAV LiDAR para la inspección de edificios puede no ser el mejor para la planificación del riego o fumigación para la agricultura, por lo que es importante conocer el uso previsto por el fabricante.

¿Cuánto pesa con carga operativa?

Si está comprando un sensor LiDAR para un dron que no lo tiene o lo va a remplazar, es de vital importancia saber el peso y volumen del sensor y si la sumatoria de su carga útil está dentro de la capacidad de carga del dron. Normalmente los sensores LiDAR superan el límite de carga máxima operativa de los drones tipo

"consumer", por lo que es pertinente asegurarse de hacer el cálculo de carga/capacidad antes de la inversión.

¿LiDAR es la mejor opción?

Si bien la tecnología disruptiva de sensores LiDAR es impresionante y de vanguardia, no siempre es la mejor opción cuando se trata de mapeo 3D. En algunos casos, los sistemas como la fotogrametría pueden ser una mejor solución costo-eficiente.

## Discusión

Ahora que se entiende qué es la tecnología LiDAR, cómo funciona y los diferentes tipos disponibles, se pueden observar las diferentes industrias que están implementando esta tecnología en la actualidad.

*Escenas de accidentes:* ya sea que se trate de una colisión a altas horas de la noche o de un choque en un camino rural, los sistemas LiDAR pueden recopilar grandes cantidades de detalles visuales en un solo paso y antes de que lleguen los médicos, lo que permite que los servicios de emergencia se concentren en salvar las vidas en lugar de evaluar la situación. Los sistemas LiDAR utilizan señales en el rango del ultravioleta o del infrarrojo cercano para mapear áreas, lo que permite hacer escaneos con poca o ninguna luz: en la noche, en situaciones

de accidentes automovilísticos, aéreos, derrumbes y otras catástrofes.

Con muy pocas pasadas los drones LiDAR pueden capturar los datos requeridos para producir mapas 3D, de cualquier tipo de accidentes que requieran servicios de emergencia. Por tanto, son una excelente herramienta tecnológica para crear informes precisos y detallados de cualquier situación de emergencia, incluso por su desplazamiento aéreo, porque pueden acceder a la zona del desastre antes de que lleguen los primeros socorristas. Los productos generados, tales como mapas, modelos 3D y otros datos recopilados por la tecnología LiDAR se usan en los tribunales como registros neutrales basados en datos reales, que ayudan a determinar causas y efectos de accidentes.

Dentro de los muchos beneficios que ofrece esta tecnología se encuentran:

- Asistencia en *triage*: con información precisa y un amplio conocimiento de los detalles visuales —que de otro modo podrían ser desconocidos—, los servicios de emergencia en la escena pueden dedicar esos primeros minutos críticos a rescatar a los ciudadanos y salvar vidas, en lugar de dedicar tiempo a evaluar la situación.
- Reconstrucción de accidentes: como los drones LiDAR tienen una cámara digital,

además del equipo sensor, capta datos visuales que se recopilan y se pueden presentar en las cortes como evidencia precisa y neutral que demuestran la causa de un accidente.

- Limpieza de los restos del desastre: los mapas que proporcionan los drones LiDAR pueden ayudar a los equipos de auxilio y de limpieza a manejar los desechos del accidente a un ritmo más rápido.
- Ahorro: los drones LiDAR suelen ser más costo-eficientes que los métodos alternativos para la reconstrucción de accidentes. Ayudan a reducir la cantidad de tiempo en la que pueden ocurrir accidentes secundarios. También, ahorran dinero al reducir la cantidad total de accidentes.
- Carreteras más seguras: los accidentes secundarios son comunes en las escenas de choques múltiple y cuanto más tiempo se tarda en despejar el área afectada, mayor es la ventana para nuevos accidentes. Al optimizar el proceso de limpieza, los drones LiDAR ayudan a mantener las carreteras más seguras.

*Agricultura:* la tecnología LiDAR ayuda a realizar la trazabilidad de todas las actividades de la granja. Permiten identificar las áreas que producen cultivos más rentables, miden las áreas de las inundaciones para ayudar a determinar la posición óptima de los

diques y rastrean las manadas de ganado errante. La aplicación convergente de sensores LiDAR en la agricultura son una gran combinación, pues pueden hacer configuraciones específicas de LiDAR para detectar insectos individuales en los cultivos de una granja.

El uso de drones y otras tecnologías robóticas para mejorar la agricultura suele denominarse agricultura de precisión y los datos LiDAR son un elemento clave en este nuevo enfoque productivo, brindando los siguientes beneficios:

- Producción de cultivos: la información proporcionada a través de los drones LiDAR se puede utilizar para hacer una serie de mapas para la toma de las decisiones agrícolas. Se incluyen mapas que muestran áreas de cultivos de alta, media y baja de producción, con información de dónde y cuándo usar fertilizantes —un recurso costoso, valioso y a menudo usado en exceso— e incluso, muestran áreas que reciben mayor cantidad de luz solar.
- Irrigación: en granjas de arroz —que requieren la construcción de diques intrincados y precisos para un riego adecuado—, los mapas generados por LiDAR pueden hacerse con los campos anegados, sin esperar a que se seque el suelo.

- Manejo de ganado: rastrear permanente al ganado que pasta es muy costoso a nivel del suelo, así como mantenerlo a salvo de depredadores o ladrones, especialmente de noche, cuando el control de tales amenazas se vuelve mucho más difícil y peligroso.
- Cartografía: en muy poco tiempo un dron con una carga útil LiDAR escanea y mapea la superficie total de la granja, con un alto grado de precisión y a bajo costo por hectárea.
- Ahorros: se pueden reducir los costos y el tiempo de las actividades de riego para la producción de cultivos sanos, así como la gestión eficiente de los rebaños pecuarios, al proporcionar datos precisos para informar sobre las estas actividades en tiempo real.

*Ambiente:* cuando se trata de asuntos de la atmósfera, los escáneres LiDAR, especialmente los que operan en el aire, tienen una serie de beneficios y casos de uso. Algunos de estos incluyen modelos de contaminación, perfiles de nubes, meteorología y asistencia para medir la densidad y distribución de varios gases y moléculas.

*Arqueología:* a mediados de la década pasada, los datos obtenidos por sensores LiDAR ayudaron a identificar un sistema de carreteras de los mayas en la cuenca del río El Mirador, en la selva de la Península de Yucatán. Este no es el único ejemplo en el que los escáneres LiDAR ayudaron en excavaciones

arqueológicas, pero es posible que estos caminos, utilizados por los mayas desde el año 600 a. C., nunca se hubieran descubierto si no fuera por la capacidad de penetración, no invasiva de LiDAR, para recopilar datos a través de las copas de los árboles densos y anchos.

Una historia similar ocurrió en 2019, en el Monumento Nacional "Canyons of the Ancients", en Colorado, USA, donde, los investigadores estaban mapeando el área de Sand Canyon, en lo que se intuía que era un sitio ancestral del Pueblo Anasazi. Usando LiDAR aéreo, el equipo de Sand Canyon pudo recopilar más de 3200 millones de puntos de datos en su mapeo del área. Algunos de los beneficios en esta área son:

- Capturas rápidas del sitio: los drones equipados con sensores LiDAR ayudan a los arqueólogos a inspeccionar posibles sitios de excavación sin siquiera levantar una pala.
- Sin daños: por sus características no invasivas, LiDAR permite a los arqueólogos examinar áreas de interés sin destruir lo que exista debajo de la superficie, lo cual preocupa en las exploraciones arqueológicas.
- Revela lo que está oculto: los investigadores pueden encontrar pruebas ocultas, cubiertas de maleza o casi enterradas, que pueden haber sido invisibles a simple vista. De hecho, los sensores LiDAR pueden detectar des-

de senderos para peatones hasta tumbas, sin alterar el suelo.

*Conservación:* la información proporcionada por los drones con sensores LiDAR son altamente eficaces para ayudar a mantener y conservar los recursos naturales de áreas de control medio ambiental.

Varios estados de USA están utilizando tecnología habilitada por LiDAR para mantener y conservar mejor los recursos naturales dentro de sus fronteras. Los drones LiDAR se utilizan para medir desde la altura de los bosques hasta la densidad de las dunas de arena, pero son especialmente útiles en la conservación del agua. Por ejemplo, en Iowa (USA), hay bases de datos con información recopilada mediante sensores LiDAR. El Sistema de Información Geográfica (SIG), implementado por el estado, contiene datos recopilados por los sistemas LiDAR bajo la dirección del Departamento de Recursos Naturales.

Utilizando modelos de alta fidelidad de llanuras aluviales y cuencas fluviales, obtenidos mediante capturas LiDAR, los gobiernos estatales y locales pueden prepararse mejor para los desastres naturales y predecir con mayor precisión su uso anual de recursos. Algunos de los beneficios pueden ser:

- Conservación de bosques: generar y mantener actualizados mapas 3D georeferenciados de los bosques para la conservación.
- Conservación del agua: los drones LiDAR mapean desde llanuras aluviales hasta cuen-

cas de aguas, generando mapas precisos y de alta fidelidad de estas áreas, que son usados por los gobiernos para preparar planes de reacción ante desastres naturales. Asimismo, para predecir con mayor precisión el consumo anual de los recursos disponibles, sin correr el peligro de extinguirlos.

*Inspecciones:* los drones o vehículos aéreos no tripulados, equipados con cargas útiles LiDAR pueden ingresar en áreas que son peligrosas o imposibles para los trabajadores humanos, esta capacidad puede ser de gran ayuda en el campo de la inspección y el mantenimiento. Desde medir la cantidad de vegetación que crece alrededor de una línea eléctrica hasta realizar estudios iniciales de sitios de construcción, el equipo que utiliza un escáner LiDAR puede reducir en gran medida el tiempo y el costo de un estudio o inspección manual y realizar planes de mantenimiento preventivo de rieles, tuberías y turbinas. Algunos beneficios se derivan de:

- Trazabilidad histórica: se pueden obtener mapas 3D, precisos y detallados, de la totalidad de un activo, que se puede comparar con las condiciones pasadas y predecir sus condiciones futuras del activo.
- Planificación: mediante una representación virtual 3D de un activo o área se puede planificar el trabajo futuro y asegurarse de que

no se pierda ningún detalle de requerimientos futuros.

- Seguridad: se evita la exposición riesgosa de seres humanos al ingresar físicamente a espacios confinados peligrosos o trabajar en altura, utilizando recolección de datos con drones en lugar de recopilar datos con inspectores humanos.
- Ahorro: al acelerar las inspecciones y reducir los tiempos de inactividad, los mapas 3D elaborados con datos aéreos LiDAR, se pueden generar grandes ahorros para las inspecciones industriales.

*Seguros:* la capacidad de inspeccionar grandes secciones de áreas urbanas, en cuestión de minutos, hace que la evaluación de siniestros —uno de los aspectos más costosos y que requiere más tiempo de la industria de seguros—, sea altamente eficiente. El uso de escáneres LiDAR para evaluar el daño de una inundación o comprender mejor la trayectoria de un tornado, permite, a nivel mundial, a las compañías de seguros brindar cotizaciones precisas y más económicas.

Los mapas que brindan los drones con sensor LiDAR ayudan a elaborar cotizaciones altamente personalizadas para eventos fortuitos, como inundaciones, terremotos o incendios, que permiten expedir seguros de propiedad e investigar reclamos por este tipo de incidentes. Algunos beneficios son:

- Prueba: cuando se trata de los reclamos de las pólizas de seguros, el récord que proporciona un sensor LiDAR se usa como evidencia de lo que realmente sucedió en un sitio determinado, afectado por condiciones climáticas extremas u otros incidentes.
- Seguridad: en el caso de las inspecciones de techos, el LiDAR aéreo puede reemplazar a una persona que tiene que subir físicamente a un techo, mejorando así la seguridad en el proceso de inspección.
- Velocidad: las investigaciones se pueden hacer de forma más rápida para soportar los reclamos de seguros.

*Silvicultura:* la tecnología LiDAR es especialmente buena para medir la altura y la ubicación de árboles individuales dentro de un bosque grande y denso. La capacidad de esta tecnología para moverse sobre las copas de los árboles la hace perfecta para recopilar información sobre el terreno.

Los métodos convencionales actuales de medición de bosques son ineficientes, puesto que requieren de mucho tiempo y de mucha luz, pero con los sensores LiDAR, los silvicultores pueden mapear amplias zonas de bosque de manera muy rápida y precisa. Los silvicultores usan drones LiDAR para medir la altura de un dosel arbóreo o el área de una sola hoja, y estos datos son utilizados para hacer clasificaciones de los terrenos y permiten gestionar

incendios forestales, analizar y reconocer ecosistemas complejos y hacer el inventario de los recursos comerciales de los bosques.

La tecnología LiDAR permite ignorar las sombras proyectadas por los árboles, sus láseres pueden ingresar hasta el suelo del bosque, a través de la capa vegetal, permitiendo la recolección de datos sobre el estado del terreno al nivel del suelo, lo que otros métodos tradicionales no pueden hacer. Dentro de los beneficios que puede brindar la tecnología LiDAR a la silvicultura, se encuentran:

- Ahorros: un sistema LiDAR aéreo recorre rápidamente un área para hacer un estudio arbóreo, por lo tanto, es menos costoso.
- Velocidad: los métodos convencionales de medición de bosques tienen ineficiencias inherentes a las tecnologías usadas, las cuales requieren mucho tiempo y son casi imposibles de usar sin buena iluminación.
- Investigación: los datos obtenidos con sensores LiDAR son cruciales para mejorar la comprensión del estado del bosque investigado, a partir de datos de los árboles y la arboleda.
- Administración de recursos: ayuda a realizar inventarios, catalogación y rastreo de diferentes puntos de recolección de datos relevantes para la silvicultura, incluida la

cantidad total de los árboles existentes en un área, sus tipos y características de especie, su distribución geográfica e incluso, el estado de salud de cada individuo.

- Incremento de los negocios y la conservación: mejorar la calidad y aumentar la cantidad de los datos forestales recolectados tiene grandes implicaciones para los optimizar los esfuerzos de conservación, como para las actividades industriales que dependen de los bosques del mundo, como los negocios de producción y comercialización de papel, jarabes y muebles, entre otros.

*Cumplimiento de la ley:* desde inicios del presente siglo los diferentes departamentos de policía del mundo están cambiando sus pistolas de radares convencionales por pistolas LiDAR, utilizando esta tecnología más exacta y precisa para medir mejor la velocidad de los autos que transitan por las vías. Sin embargo, el uso de LiDAR en la aplicación de los controles legales del tránsito, va mucho más allá de las multas por exceso de velocidad, así mismo, los militares pueden usar sensores LiDAR para aprender sobre otros combatientes, examinar áreas enemigas o incluso obtener una vista panorámica de una situación de rehenes. Algunos beneficios son:

- Información táctica: en situaciones de retención de rehenes, las fuerzas policiales usan drones LiDAR para obtener desde le-

jos imágenes completas de la amenaza. En cualquier momento los oficiales pueden usar drones para comprender y evaluar situaciones peligrosas y de alto riesgo.

- Búsqueda y rescate: buscar y rescatar personas perdidas en áreas remotas e inaccesibles, incluso de noche, es una actividad que requiere del uso de esta tecnología.
- Rescate acuático: usando sensores LiDAR batimétricos (un tipo de LiDAR que produce una luz verde que penetra en el agua en lugar del láser infrarrojo cercano del LiDAR topográfico), se puede identificar rápidamente los restos o incluso los sobrevivientes que pueden estar parcial o totalmente sumergidos en el agua.

*Minería:* en la industria minera y las ciencias geológicas aplicadas, la tecnología LiDAR está haciendo que la inspección, el levantamiento topográfico y el mapeo sean más eficientes y seguros. En las explotaciones mineras, los drones LiDAR se utilizan para inspeccionar las zonas después de las detonaciones planificadas, a fin de garantizar que el área sea segura antes de enviar trabajadores humanos. Estos equipos también se utilizan para medir volúmenes de mineral acopiado y los espacios subterráneos de extracción de mineral.

Los entornos de minería subterránea hacen que las operaciones de GPS sean imposibles para los

drones, por lo que LiDAR y los sensores visuales son cruciales para hacer posible que un dron opere bajo tierra sin GPS. Algunos beneficios uden ser:

- Extracción de minerales: los mapas 3D creados con datos LiDAR pueden ayudar a identificar el potencial del mineral restante, lo que puede generar grandes cantidades de ingresos adicionales para una empresa minera.
- Planificación: junto con los escáneres posicionados en el suelo, los drones LiDAR pueden comparar nuevos datos de superficie con escaneos anteriores, que permiten determinar las áreas de la mina que son ricas en recursos y así planear el próximo objetivo de explotación.
- Seguridad: mapeo de áreas inestables peligrosas para que puedan ser evaluadas en cuanto a su seguridad.
- Ahorros: una mejor comprensión de las excavaciones cruciales en una mina puede conducir a una mayor extracción de mineral y una mayor eficiencia en general, lo que genera enormes ahorros potenciales.

*Transporte:* en la industria del transporte los escáneres LiDAR ayudan a optimizar los diferentes procesos, desde la planificación de distribución de las áreas de los estacionamientos y de líneas de los fe-

rrocarriles, hasta los ajustes de ruta en tiempo real debido a la congestión del tráfico vehicular.

*Coches autónomos:* la conducción autónoma utiliza sistemas LiDAR laterales que detectan obstáculos y que pueden generar peligros de colisiones. También pueden ayudar en el control de navegación y atraque de cruceros.

## Conclusiones

Las minas a cielo abierto o subterráneas requieren de frecuentes inspecciones para monitorear las condiciones del terreno y garantizar la seguridad y productividad de sus trabajadores. Las minas subterráneas suelen ser lugares peligrosos, especialmente después de la excavación para la extracción del mineral, dejando una caverna abierta llamada rebaje abierto. Una vez que se ha extraído el mineral recuperable del rebaje, se debe reponer el material removido, proceso conocido como "relleno", para evitar derrumbes en el área circundante y garantizar la seguridad y continuidad en la mina.

Para dar solución a esta problemática, según la encuesta de Global Data de más de 200 sitios mineros (Davis y Bizo, 2022), la industria minera está adoptando Sistemas Aéreos No Tripulados (UAS —por sus siglas en inglés— *Unmanned Aerial Systems*), particularmente, en las regiones de Australasia y África. Estos equipos combinados con software de fotogrametría para topografía y mapeo brindan

una gran cantidad de datos avanzados y en tiempo real. Los drones LiDAR se usan para recopilar datos de manera más eficiente y precisa, lo que permite mejorar la seguridad de las operaciones mineras. De acuerdo con la encuesta de Global Data, reemplazar aviones convencionales por drones, puede ahorrar hasta el 90 % del costo de operación por hora (Davies y Fumega, 2022).

Los mapas y modelos de sitios digitales georreferenciados, accesibles para las partes interesadas en todos los niveles, conducen a una mejor toma de decisiones y una mayor participación en la cadena de suministro, creando una industria sostenible y más segura, con la oportunidad de obtener mayores ganancias (Cacheiro y Taboada, 1998). De hecho, se estima que para la próxima década habrá un valor agregado potencial para la industria minera, cuantificado en miles de millones de dólares, mediante de la automatización y la robótica.

El futuro de la minería beneficiará a aquellos que estén preparados para abrazar esta revolución tecnológica; aquellos que sobrevivan y prosperen, serán los que estén preparados para innovar, invertir y remodelar su modelo de negocio para adaptarse al entorno minero moderno, que exige la globalización de los mercados. Así las cosas, se estima que para la próxima década, la automatización y la robótica agregarán valor cuantificado en miles de millones para la industria minera.

## Capítulo 5

# Seguridad y salud ocupacional en la explotación minera de carbón en Colombia

*Luz J. Castañeda R., Jairo E. Márquez D., Arles Prieto M.* y *Luis G. Benavides R.*

La minería en Colombia, como parte del sector primario de la economía, reviste un alto grado de importancia gracias a su significativa contribución al desarrollo del país, con un notable crecimiento en América Latina desde inicios del siglo xxi (Cárdenas y Reina, 2008). Sin embargo, también ha generado preocupaciones debido al impacto ambiental y social que van en aumento. La minería ilegal y la explotación de recursos en zonas protegidas ha causado daños ambientales significativos y ha generado conflictos con las comunidades locales que se ven afectadas por la actividad minera, causando afectaciones a nivel micro y macroeconómico por evasión tributaria, así como las condiciones de inseguridad laboral (Juárez, 2016). La explotación

de los recursos minerales actualmente se encuentra ubicada en gran parte hacia las regiones Andina, Pacífica y Caribe.

La Iniciativa de Transparencia de las Industrias Extractivas (EITI —por sus siglas en inglés— *Extractive Industries Transparency Initiative)* señala que Colombia se caracteriza por ser un país rico en recursos naturales y cuenta con una gran variedad de minerales como oro, plata, aluminio, hierro, esmeraldas, cobre, níquel, carbón y petróleo (EITI Colombia, 2016, párr.1), donde la minería se lleva a cabo tanto a cielo abierto como subterránea. La minería ilegal, asociada en gran medida a la presencia de grupos al margen de la ley (Cubides, Suárez & Hoyos, 2018), agudiza la problemática relacionada con los riesgos para los mineros que trabajan en condiciones de inseguridad y por supuesto, no garantiza la salud y la seguridad de los trabajadores reglamentada en el país por el Decreto 1886 de 2015.

El gobierno colombiano ha implementado una serie de políticas de Estado para regular al sector minero a través de la creación de la Agencia Nacional de Minería (ANM), mediante el Decreto 4134 de 2011, y la implementación de leyes para proteger los derechos de las comunidades locales y los trabajadores con la creación de las leyes y decretos: Ley 1450 de 2011, Ley 1753 de 2015, Decreto 1886 de 2015, Decreto 1666 de 2016, Decreto 539 de 2022, Resolución 0206 de 2013. Sin embargo, la

efectividad en el cumplimiento de estas políticas sigue siendo un desafío, no solo por la falta de concienciación, sino por la corrupción en el sector. La ANM está implementando tecnologías basadas en IA para regular la explotación a través de la legalidad de los títulos mineros, lo que redunda en garantizar el desempeño laboral bajo las condiciones de seguridad y salud adecuadas.

Un desarrollo soportado en la detección de minas a cielo abierto a partir de imágenes satelitales adelantado por Santiago Saavedra, concluye que el eje problemático de su trabajo radica en que el 80 % de las minas en Colombia no cuentan con títulos de explotación y a partir de la implementación tecnológica, se hace un gran aporte en materia de regulación minera (Saavedra, 2020).

Aunque esta tecnología solo aplica para minería a cielo abierto, representa un gran salto hacia el control y prevención de diferentes situaciones de índole social y económico que afectan el sector. De otra parte, Chile es pionero en usar minas digitales, empleando la denominada "tecnología de gemelos digitales" que se está implementando en Colombia, donde se procesa una gran cantidad de datos que permite hacer una simulación de los riegos y peligros posibles, facilitando la exploración de una manera más segura en minas subterráneas (IAC, 2022).

Con respecto a la extracción de carbón (térmico, metalúrgico y antracitas), vale la pena resaltar

que "el sector minero representa el 2 % del PIB, el 20 % de las exportaciones y el 13 % de la inversión extranjera directa" (ANM, 2019, párr. 3), (aunque hubo un decaimiento, en un 0,7 % aproximadamente, entre 2020 y 2021 por la pandemia). De acuerdo con la expresidenta de la ANM, Silvana Habib, el carbón aporta en un 88 % a las regalías del sector en Colombia (ANM, 2019).

## Organización del sector minero en Colombia

En Colombia la ANM es la entidad del estado de la rama ejecutiva, suscrita al Ministerio de Minas y Energía (Minminas) como máxima autoridad del sector que, de acuerdo con el Artículo 1 del Decreto 4134 de 2011 es la encargada de "administrar integralmente los recursos minerales de propiedad del Estado" (Decreto 4134, 2011). Es también la autoridad en el país que otorga los títulos mineros que facultan la explotación de los recursos minerales, tanto a cielo abierto como subterráneo y regula las buenas prácticas de explotación, el uso de explosivos, entre otros aspectos.

La ANM trabaja con el apoyo de la Unidad de Planeación Minero-Energética (UPME) quien es la responsable de planear en el corto, mediano y largo plazo el aprovechamiento de los recursos minerales y energéticos, junto con el Servicio Geológico Co-

lombiano (SGC), quien principalmente desarrolla la investigación científica en ocho subcategorías, incluida la de los recursos minerales que se encuentran en el subsuelo colombiano (Minminas, 2019).

En la Figura 14 se observa el organigrama del subsector minero, mostrado en la *Guía para la Incorporación de la Dimensión Minero-Energética en el Ordenamiento Territorial Municipal* (Minminas, 2019).

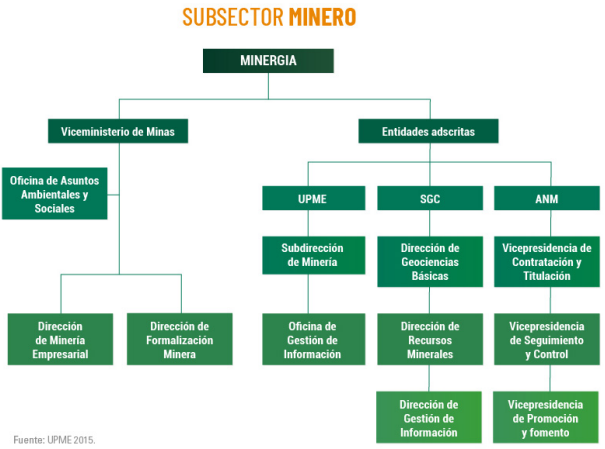



**Figura 14.** *Organigrama del subsector de minería en Colombia*
Fuente: Ministerio de Minas y Energía (Minminas), 2019.

Es importante tener en cuenta que de acuerdo con la "caracterización de la industria" definida en el Decreto 1666 de 2016, el sector minero se clasifica en minería de subsistencia (que aplica solo para minería a cielo abierto), de pequeña escala, mediana y

gran escala, en concordancia con las dimensiones del terreno a explotar y según el tipo de explotación, se clasifica en cielo abierto y subterránea (Decreto 1666 de 2016). En la Tabla 6, se presenta la consolidación de la organización del subsector minero en Colombia.

**Tabla 6.** *Organización del subsector minero en Colombia*

| Entidad | Funciones |
|---|---|
| **Ministerio de Minas y Energía (MME)** | Establece las políticas y regulaciones para el sector minero en Colombia. |
| **Agencia Nacional de Minería (ANM)** | Autoriza y regula la exploración y explotación de los recursos minerales en Colombia. También es responsable de la gestión del catastro minero y la promoción de la formalización minera. |
| **Instituto Colombiano de Geología y Minería (Ingeominas)** | Realiza investigaciones geológicas y mineras para el país y proporciona información y asesoramiento técnico al sector minero. |
| **Unidad de Planeación Minero-Energética (UPME)** | Es la encargada de planificar y coordinar el desarrollo del sector minero-energético en Colombia, en colaboración con otras entidades del gobierno y el sector privado. |
| **Consejo Nacional de Política Económica y Social (Conpes)** | Establece las políticas y estrategias para el desarrollo del sector minero en Colombia. |

Fuente: elaboración propia.

## Seguridad y salud en el trabajo

En el marco del proyecto "Prototipo electrónico para la evaluación del riesgo al interior de una mina

de carbón en la provincia de Ubaté", desarrollado por el grupo de investigadores de la Universidad de Cundinamarca, autores de este libro, se considera de alta importancia proteger la vida y la salud del trabajador minero desde el desarrollo tecnológico, basado en IoT para reducir el riesgo que se da en la explotación subterránea, mediante la lectura y procesamiento constante de un conjunto de variables químicas a las que están expuestos los mineros en un socavón.

La labor minera es considerada como una actividad de riesgo máximo (clase V según el Decreto 1295 de 1994, artículo 26) y en mayor medida la minería subterránea, sujeta a la incidencia de múltiples factores (Rivera y Echeverri, 2014). La Seguridad y Salud en el Trabajo (SST) para el trabajador minero en Colombia se rige por la Ley 1562 de 2012, la cual establece que todas las empresas deben implementar un Sistema de Gestión de SST que garantice la prevención de accidentes y enfermedades laborales. En Colombia, el Ministerio del Trabajo es el encargado de velar por el cumplimiento de las normas de SST en el sector minero. Entre las principales medidas de SST para el trabajador minero en Colombia se encuentran:

- Implementación de protocolos de seguridad para el manejo de explosivos.
- Capacitación constante en prevención de accidentes y enfermedades laborales.

- Uso de equipos de protección personal adecuados para cada tarea.
- Realización de exámenes médicos periódicos.
- Promoción de la cultura de prevención en el lugar de trabajo.

En este orden de ideas, el sector minero colombiano está sujeto a una serie de requisitos legales y reglamentarios destinados a proteger a los trabajadores. Estos incluyen regulaciones relacionadas con el Equipo de Protección Personal (PPE), la planificación de respuesta a emergencias, las sustancias peligrosas y la seguridad de las máquinas.

Los empleadores del sector minero están obligados a proporcionar a los trabajadores el equipo de protección personal adecuado, incluida la ropa de protección, el equipo de protección respiratoria y auditiva. Los empleadores también deben contar con planes de respuesta ante emergencias para abordar posibles accidentes en el lugar de trabajo y deben proporcionar a los trabajadores capacitaciones sobre los mismos.

El gobierno colombiano también ha establecido regulaciones relacionadas a las sustancias peligrosas que se encuentran comúnmente en la minería, como el mercurio, el plomo y el asbesto. Los empleadores deben tomar medidas para evitar la liberación de estas sustancias en el medioambiente y garantizar

que los trabajadores no estén expuestos a niveles inseguros de estas sustancias.

La seguridad de las máquinas es otro aspecto crítico para el sector minero. Los empleadores están obligados a garantizar que las máquinas se diseñen y mantengan de manera que se minimice el riesgo de accidentes. Los empleadores también deben proporcionar a los trabajadores capacitación sobre la operación segura de las máquinas y los procedimientos de mantenimiento.

En Colombia existen normas específicas para la minería, como el Decreto 1886 de 2015, en el que se establecen los requisitos técnicos para la gestión de la seguridad minera. Asimismo, la Resolución 2400 de 1979, establece las normas de higiene y seguridad industrial para las empresas del país.

Es necesario destacar que la SST en el sector minero es un tema de gran importancia debido a la alta tasa de accidentes y enfermedades laborales en la industria minera. Por esta razón es fundamental que las empresas cumplan con las normas y protocolos establecidos y promuevan una cultura de prevención en el lugar de trabajo, así como promover el uso de dispositivos y tecnologías emergentes que permitan medir y generar alertas tempranas, para prevenir situaciones que puedan atentar contra la vida de los trabajadores mineros.

## Normativas

Como ya se mencionó, se creó la ANM en Colombia, con el Decreto 4134 de 2011, además, se han implementado otras normas para proteger los derechos de las comunidades locales y los trabajadores con las leyes: Ley 685 de 2001, Ley 1562 de 2012, y los decretos: Decreto 1477 de 2014, Decreto 1886 de 2015, Decreto 1666 de 2016, Decreto 944 del 1 de junio de 2022, Resolución 0206 de 2013.

La Ley 685 de 2001 constituye el Código de Minas, en el que, el artículo 60, indica que son los poseedores del título minero los responsables del "cumplimiento de las normas de seguridad e higiene mineras". El artículo 361 de esta Ley derogó el Decreto 2655 de 1988, anterior Código Minero. La Ley 1562 de 2012 define y rige el sistema de riesgos laborales, en los artículos 3 y 4 definen el "accidente de trabajo" y la "enfermedad laboral" respectivamente.

El Decreto 1477 de 2014, *Anexo Técnico,* expone la "Tabla de enfermedades laborales", definiendo su relación con el tipo de agente o factor de riesgo y la actividad laboral asociada. Clasifica las enfermedades laborales por categorías para facilitar el diagnóstico médico.

El Decreto 1886 de 2015 "Por el cual se establece el Reglamento de Seguridad en las Labores Mineras Subterráneas", es uno de los más relevantes

en el tema que aquí se trata. Este decreto deroga al Decreto 1335 de 1987 y define los lineamientos para prevenir los riesgos en las labores de minería subterránea, además de definir los procedimientos relacionados con la inspección y vigilancia de estas actividades. También determina los valores estandarizados para algunas variables de control dentro de un socavón minero, como el oxígeno, la concentración de CO2 y CO, la temperatura, la identificación de gases y el ruido. El Decreto 1666 de 2016 es una adición al Decreto 1073 de 2015, donde se destaca la clasificación de la minería en Colombia y por ende, la capacidad de explotación según el título minero otorgado.

El Decreto 944 del 1 de junio de 2022 modifica el Título III del Decreto 1886 de 2015 y 25 artículos más. En esta actualización se responsabiliza al "empleador minero" de proyectar e implementar el SG-SST y de hacerse partícipe de las investigaciones de los accidentes laborales, reportando cada caso a las autoridades mineras correspondientes y contando con el personal capacitado "socorredores mineros" para atender las contingencias.

La ANM dispone del "Manual del socorredor minero", ya que es la entidad que dirige el Servicio Nacional de Salvamento Minero y cuenta con el apoyo de organismos nacionales e internacionales. Actualmente, Colombia hace parte de la red inter-

nacional de apoyo *International Mines Rescue Body* – IMRB (AMN y UPTC, 2020a).

Finalmente, la Resolución 0206 de 2013 de la ANM reglamenta al interior de la agencia las distintas dependencias que la conforman, dentro de ellas se encuentra la Vicepresidencia de Seguimiento, Control y Seguridad Minera, a la cual se encuentra suscrito el Grupo de Seguridad y Salvamento Minero, que rige el protocolo de atención de acuerdo con lo definido en el "Manual de Socorredor Minero" (AMN y UPTC, 2020b).

En la Tabla 7 se registran los aspectos generales de la normatividad vigente, relacionada con la SST de las actividades de minería subterránea. La ANM genera boletines, guías y documentos orientados a comunicar, a los involucrados en las labores mineras, la aplicación de las normas enunciadas en materia de SST.

**Tabla 7.** *Normas colombianas relacionadas con la SST del trabajador de minería subterránea*

| Norma | Tema | Contenido |
|---|---|---|
| **Ley 685/2001** | Código de minas y otras disposiciones | Establece disposiciones sobre la explotación de los recursos mineros del estado y privados, para cumplir con la demanda interna y externa. Expedida por el Congreso de la República de Colombia. |

Continúa tabla...

| Norma | Tema | Contenido |
|---|---|---|
| **Ley 1562/2012** | Modifica el sistema de riesgos laborales | Establece la afiliación por parte del empleador al Sistema General de Riesgos Laborales, define la naturaleza y líneas de acción del SG-SST. Expedida por el Congreso de la República de Colombia. |
| **Decreto 4134/2011** | Creación de la Agencia Nacional de Minería, ANM | Legaliza la naturaleza y líneas de acción de la ANM como agencia estatal colombiana asociada a la Rama Ejecutiva del poder público. Expedido por la presidencia de la República de Colombia. |
| **Decreto 1477/2014** | Tabla de Enfermedades Laborales | Bajo un concepto favorable del Consejo Nacional de Riesgos Laborales, se actualiza el listado de las que son consideradas enfermedades laborales. Expedido por la presidencia de la República de Colombia. |
| **Decreto 1886/2015** | Reglamento de seguridad en las labores mineras subterráneas | Establece las condiciones laborales requeridas para la explotación minera subterránea, incluyendo los límites permitidos de gases, temperatura, atmósfera, ventilación. Expedido por la presidencia de la República de Colombia. |
| **Decreto 1666/2016** | Adición al Decreto Único Reglamentario del Sector Administrativo de Minas y Energía de la clasificación minera. | Clasifica la actividad minera. Expedido por la presidencia de la República de Colombia. |
| **Decreto 944/2022** | Modificación al Decreto 1886 de 2015. | Por actualización tecnológica se modifican los artículos 2, 7, 11, 29, 31, 34, 40, 46, 47, 48, 51, 65, 77, 79, 88, 158, 159, 169, 170, 171, 179, 181, 182, 233, 234, y el Capítulo III del Título I. Expedido por la presidencia de la República de Colombia. |
| **Resolución 0206/2013** | Creación y funciones de Equipos Internos de Trabajo en la ANM. | Organización administrativa y puntos de atención regional de las dependencias de la ANM. |

Fuente: elaboración propia.

## Enfermedades laborales en el sector minero

La SST es un aspecto primordial en la industria minera, ya que los trabajadores están expuestos a diversos riesgos que pueden afectar su bienestar físico y psicológico. La exposición a contaminantes ambientales y físicos, el trabajo en altura, la manipulación de cargas pesadas, entre otros factores, son los principales riesgos a los que se enfrentan los trabajadores mineros, como se muestra en la Tabla 7. Los accidentes laborales más comunes en la industria minera son las lesiones musculoesqueléticas, las caídas y los traumatismos, causados, en mayor porcentaje, por derrumbes, los cuales pueden ser prevenidos mediante la implementación de medidas de seguridad y el uso de equipos de protección personal adecuados.

En cuanto a la salud de los trabajadores mineros, la exposición a sustancias químicas tóxicas presentes en el ambiente laboral puede generar enfermedades respiratorias, dermatológicas y neurológicas. La Organización Internacional del Trabajo (OIT), (2013) afirma que "millones de trabajadores siguen corriendo el riesgo de contraer neumoconiosis (en especial silicosis, neumoconiosis del trabajador del carbón). La neumoconiosis tiene períodos de latencia largos y en muchos casos ni se diagnostica ni se notifica" (p. 5).

Además de la neumoconiosis, reconocida como enfermedad profesional asociada a la exposición a partículas minerales por la OIT (2010a) también se encuentran casos de enfermedad obstructiva crónica por inhalación de polvo de carbón, tuberculosis por encontrarse expuesto a sílice (origen de la silicosis), enfermedades del sistema osteomuscular que pueden ser por higiene postural o por manejo de los instrumentos de trabajo, entre otras de origen psicológico.

En la Tabla 8 se presenta una extracción del conjunto de enfermedades laborales asociadas a la actividad minera subterránea, de acuerdo a lo estipulado en el Decreto 1477 de 2014, cada una asociada con el Código de Clasificación Internacional de Enfermedades (CEI). Algunas enfermedades son consideradas directas, de acuerdo con la labor desarrollada por el trabajador.

**Tabla 8.** *Extracto de la tabla de enfermedades laborales asociadas a la actividad minera subterránea - Decreto 1477 de 2014*

| Tipo de agente | Agentes etiológicos / factores de riesgo | Enfermedades |
|---|---|---|
| Agente químico | *Sustancias asfixiantes*: | Demencia en otras enfermedades especificas clasificadas en otra sección (F02:8) |
| | Monóxido de carbono<br>Sulfuro de hidrógeno (Ácido sulfhídrico) | Trastornos del nervio olfatorio (incluye anosmia) (G52.0)(Sulfuro de hidrógeno)<br>Encefalopatía tóxica crónica (G92.2)(Secuela)<br>Conjuntivitis (H10)(Sulfuro de hidrógeno)<br>Queratitis (H 16) y queratoconjuntivitis (H16.2)<br>Angina de pecho (120)(Monóxido de carbono)<br>Infarto agudo de miocardio (121)(Monóxido de carbono)<br>Paro cardiaco (146)(Monóxido de carbono)<br>Arritmias cardiacas (149)(Monóxido de carbono)<br>Bronquitis y neumonitis causada por productos químicos, gases, humos y vapores (Bronquitis química aguda)(J68.0)(Cianuro de hidrógeno)<br>Edema pulmonar agudo causado por productos químicos, gases, humos y vapores (Edema pulmonar químico)(J68.1)(Cianuro de hidrógeno)<br>Síndrome de disfunción reactiva de las vías aéreas (J68.3)(Cianuro de hidrógeno)<br>Bronquiolitis obliterante crónica, enfisema crónico difuso o fibrosis pulmonar crónica (J68.4) (Cianuro de hidrógeno)(Sulfuro de hidrógeno)<br>Efectos tóxicos agudos (TS7.3)(T58)(TS9.6) |
| | Sílice libre (Óxido de silicio Si 02) | Neoplasia maligna de bronquios y de pulmón (C34)<br>Enfermedad cardiaca pulmonar sin especificar (127,9)*(Cor Pulmonale)*<br>Otras enfermedades pulmonares obstructivas crónicas (Incluye asma obstructiva, bronquitis obstructiva crónica)(J44)<br>Silicosis (J62)<br>Neumoconiosis asociada con tuberculosis (Silicio Tuberculosis)(J63.8)<br>Síndrome de Captan (J99.1; M05.3) |

Continúa tabla...

| Tipo de agente | Agentes etiológicos / factores de riesgo | Enfermedades |
|---|---|---|
| Agente físico | Ruido | Pérdida de la audición provocada por el ruido, (H83.3)<br>Otras percepciones auditivas anormales: alteraciones temporales del umbral auditivo, compromiso de la discriminación auditiva e hipoacusia (H93.2)<br>Hipertensión arterial (110)<br>Síndrome por ruptura traumática del tímpano (por el ruido)(809.2) |
| | Vibraciones de no parte: cuerpo entero | Síndrome de Raynaud (173.0)<br>Acrocianosis y acroparestesias (173.8)<br>Otros trastornos articulares no clasificados en otra parte: Dolor articular (M25.5)<br>Síndrome cervicobraquial (M53.1)<br>Fibromatosis de la fascia palmar: Contractura de Dupuytren (M72.0)<br>Lesiones de hombro (M75): Capsulitis. adhesiva de hombro (hombro congelado, periartritis de hombro)(M75.0); Síndrome de manguito rotador o Síndrome de supraespinoso (M75.1); Tendinitis bicipital calcificante de hombro (M75.3); Bursitis de hombro (M75.5); Otras lesiones de hombro (M75.8); Lesiones de hombro no especificas (M75.9).<br>Otras enteropatías (M77): Epicondilitis medial (M77.0); Epicondilitis lateral (M77.1); Mialgia (M79.1).<br>Otros trastornos específicos de tejidos blandos (M79,8).<br>Osteonecrosis (M87)<br>Otras osteonecrosis; secundarias (M87.3).<br>Enfermedad de Kienbock del adulto (Osteocondrosis del adulto del semilunar del carpo)(M93.1) Y otras osteocondropatias específicas (M93.8) |
| | Temperaturas extremas<br><br>Calor - Frío | Golpe de calor e insolación (T67.0)<br>Síncope por calor (T67, 1)<br>Calambre por calor (T67.2)<br><br>Urticaria debida al calor o al frío (L50.2)<br>Leucodermía no clasificada en otra parte (1ncluye vitíligo ocupacional)(L81.5) |

Continúa tabla...

| Tipo de agente | Agentes etiológicos / factores de riesgo | Enfermedades |
|---|---|---|
| Agente biológico | Microorganismos y parásitos infecciosos vivos y sus productos tóxicos. | Tuberculosis (A15 A19)<br>Carbunco (A22)<br>Brucelosis (A23)<br>Leptospirosis (A27) Tétano (A35)<br>Psitacosis, ornitosis, enfermedad de los cuidadores y tratadores de aves (A70)<br>Dengue (A90)<br>Fiebre amarilla (A95)<br>Hepatitis virales (815- 819)<br>Enfermedad ocasionada por el virus de la inmunodeficiencia humana (VIH) (B20 – B24)<br>Dermatofitosis (B35) y otras micosis superficiales (B36)<br>Paracoccidioidomicosis (B41)<br>Malaria (850 – 854)<br>Leishmaniasis cutánea (855.1) o Leishmaniasis cutáneo-mucosa (855,2)<br>Neumonitis por hipersensibilidad a polvo orgánico (J67); Pulmón del granjero (J67.0); Bagazosis (J67.1); Pulmón de los criadores de pájaros (J67.2); Suberosis (J67.3); Pulmón de los trabajadores de malta (J67A); Pulmón de los que trabajan con hongos (J67.5); Enfermedad pulmonar debida a sistemas de aire acondicionado y de humidificación del aire (J67.7); Neumonitis de hipersensibilidad ocasionada por otros polvos orgánicos (J67.8); Neumonitis de hipersensibilidad ocasionada por polvos orgánicos no especificas (Alveolitis alérgica extrínseca; Neumonitis de hipersensibilidad) (J67.0).<br>Dermatosis pápulo – pustulosas complicaciones (L08.9) |
| Agente psicosocial | *Carga física:* (Esfuerzo fisiológico que demanda la ocupación, generalmente ... | Trastornos psicóticos agudos y transitorios (F23)<br>Depresión. (F32)<br>Episodios depresivos (F32.8).<br>Trastorno de pánico (F41.0)<br>Trastorno de ansiedad generalizada (F41.1)<br>Trastorno mixto ansioso-depresivo (F41.2) |

Continúa tabla...

| Tipo de agente | Agentes etiológicos / factores de riesgo | Enfermedades |
|---|---|---|
| Agente psicosocial | *Carga física:* ...en términos de postura corporal, fuerza, movimiento y traslado de cargas e implica el uso de los componentes del sistema osteomus-cular, cardiovascular y metabólico | Reacciones a estrés grave (F43).<br>Trastornos de adaptación (F43).<br>Trastornos adaptativos con humor ansioso, con humor depresivo, con humor mixto, con alteraciones del comportamiento o mixto con alteraciones de las emociones y del comportamiento (F43.2).<br>Hipertensión arterial secundaria. (115.9).<br>Angina de pecho (120) Cardiopatía isquémica (125).<br>Infarto agudo de miocardio (121).<br>Enfermedades cerebrovasculares (160 – 169).<br>Encefalopatía hipertensiva (167.4).<br>Ataque isquémico cerebral transitorio sin especificar (G45.9).<br>Úlcera gástrica (K25)<br>Úlcera duodenal (K26)<br>Ulcera péptica, de sitio no especificado (K27).<br>Úlcera gastroyeyunal (K28) |
| | *Condiciones del medio-ambiente de trabajo:* (Deficiencia en: aspectos físicos; químicos; biológicos; de diseño del puesto y de saneamiento, como agravantes o coadyuvantes de factores psicosociales. | |

Continúa tabla...

| Tipo de agente | Agentes etiológicos / factores de riesgo | Enfermedades |
|---|---|---|
| Agente ergonómico | Posiciones forzadas, manejo de cargas y movimientos repetitivos (Trabajos en los que se realizan presiones repetidas, como mineros (de las minas de carbón y manganeso). | Trastornos del plexo braquial (Síndrome de salida del tórax, síndrome del desfiladero torácico) (M.70)<br>Mononeuropatías de miembros superiores (G56)<br>Síndrome de túnel carpiano (G56.0)<br>Síndrome de pronador redondo (G56.1)<br>Síndrome de canal de Guyon. Lesión del nervio cubital (Ulnar) (G56.2)<br>Lesión del nervio radial (G56.3)<br>Compresión del nervio supraescapular (G56.8)<br>Otras mononeuropatías de miembros superiores (G56.8) |

Fuente: Ministerio del trabajo, 2014.

En general, de acuerdo con la OIT (2006, 2010b) y en concordancia con el Decreto 1886 de 2015, los factores que representan un riesgo para la salud del trabajador minero se pueden agrupar, como se muestra en la Tabla 9.

**Tabla 9.** *Posibles variables de riesgo en una mina de carbón*

| | | Tipo de variable | | Valor límite permisible | | Tipo de riesgo para el trabajador |
|---|---|---|---|---|---|---|
| | Decreto 1886 2015 | Agentes Químicos Gases | Fórmula química | % en volumen | ppm | |
| Gases tóxicos | | Dióxido de carbono | $CO_2$ | 0,5 | 5000 | Químico por posible intoxicación |
| | | Monóxido de carbono | $CO_2$ | 0,0025 | 2 | |
| | | Ácido sulfhídrico | $H_2S$ | 0,0015 | 15 | |
| | | Anhídrido sulfuroso | $SO_2$ | 0,001 | 10 | |
| | Gases nitrosos | Óxido Nítrico | NO | 0,0025 | 25 | |
| | | Dióxido de nitrógeno | $NO_2$ | 0,0005 | 5 | |
| Gases explosivos | | Metano | $CH_4$ | <4 causa ardor en la piel 5 a 15 (explosivo) >15 asfixiante | | |
| | | Nitrógeno | N | 78-88 | 25ppm | |
| | | Hidrógeno | H | | | |
| | | Oxígeno | O | | | |
| | | Material particulado | Fórmula química | | | |
| | | Sílice | $SiO_2$ | | | |
| | | Polvo de carbón | | | | |

Continúa tabla...

| | | Tipo de variable | | Valor límite permisible | | Tipo de riesgo para el trabajador |
|---|---|---|---|---|---|---|
| | Decreto 1886 2015 | Agentes Químicos Gases | Fórmula química | % en volumen | ppm | |
| | | Agentes geológicos | | | | Riesgo físico y biológico por presencia de virus o bacterias en el suelo |
| | | Deformaciones del terreno | | | | |
| | | Procesos geomorfológicos: inundaciones | | | | |
| | | Agentes ambientales - físicos | | | | Riesgo físico y biológico por presencia de virus o bacterias en el ambiente |
| | | Humedad | | | | |
| | | Temperatura | | | | |
| | | Presión | | | | |
| | | Agentes ergonómicos | | | | Riesgo ergonómico: posiciones forzadas y movimientos repetitivas |
| | | Postura | | | | |
| | | Manejo de la instrumentación | | | | |
| | | Trabajo repetitivo | | | | |
| | | Psicosociales | | | | |
| | | Jornada laboral | | | | Riesgo psicosocial |
| | | Condiciones laborales | | | | |

Fuente: elaboración propia con base en los factores de riesgo definidos en el Decreto 1477 de 2014.

## Métricas sobre incidentes y accidentes en el sector minero

Desafortunadamente, la industria minera del carbón en Colombia ha sido históricamente una de las más peligrosas del país, registrando un alto número de accidentes graves e incidentes en las minas de carbón a lo largo de los años. La ANM reporta que entre 2005 y 2021 se registraron 1582 accidentes, con cerca de 1800 fallecimientos de mineros en Colombia, en promedio 103 muertes por año (Dueñas, 2023).

En lo que va corrido del año 2023, se reportan 25 accidentes mineros y 24 fallecimientos. La última tragedia se vivió el 14 de marzo de 2023, en una mina subterránea de carbón de Sutatausa que dejó 11 mineros sin vida, cuya causa posible fue la acumulación de gases: metano y probablemente polvo de carbón (González, 2023).

En la Figura 15 se puede observar que durante los 17 años registrados, la tasa de emergencias como de fatalidades ha incrementado, particularmente en los últimos 5 años; en el 2010 la tasa de fallecidos fue del 9,7 % y en el 2020 fue del 8,5 %, años que reflejan los valores más altos. En este periodo la minería ilegal ha tenido un aumento precipitado, así como las tasas de accidentes y muertes.

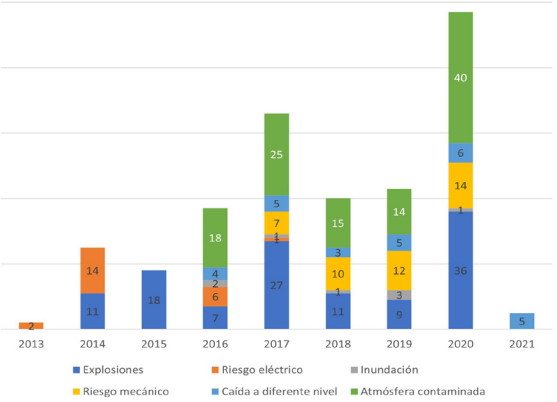
**Figura 15.** *Representación del número de emergencias y número de fatalidades en labores mineras entre 2005 y 2022*


Fuente: elaboración propia con base en las estadísticas de emergencias y mortalidades mineras de los boletines emitidos por la ANM, 2021.

Si se revisan los orígenes, las situaciones que aquejan a la labor minera son distintas —como se muestra en la Figura 16—, cuyos registros entre los años 2013 y 2021 dejan ver que las causas más recurrentes son las explosiones, las cuales generan derrumbes al interior de la mina y la atmósfera contaminada. Para el año 2020 se registró una de las tasas de accidentalidad y número de fatalidades más altas, pero también es uno de los años que cuenta con mayor número de reportes registrados.

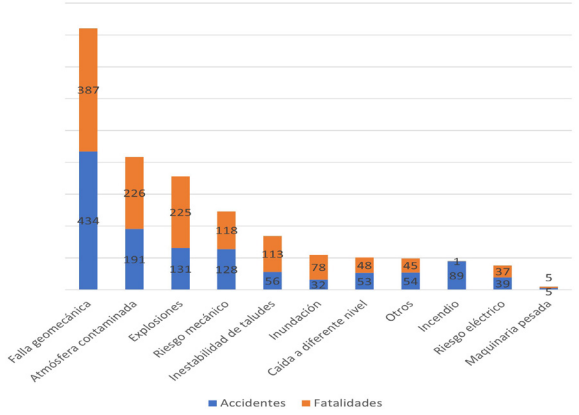
En la Figura 17 se observa la relación del número de accidentes y fatalidades, por tipo de emergencia, entre 2011 y 2022, con los "derrumbes" con el mayor indicador y por "fallas geológicas" con un 28,4 %, seguido de "atmósfera contaminada", es decir, la acumulación de gases, con un 23 %, seguido de "explosiones" e "incendios", con un 12,7 % y 11,2 % respectivamente.

**Figura 16.** *Causas de emergencias mineras durante los años 2013 a 2021*




Fuente: elaboración propia basado en las estadísticas de Lecciones Aprendidas de la ANM, 2021.

**Figura 17.** *Número de accidentes y de fatalidades según la causa de emergencia minera durante 2011 a 2022*




Fuente: elaboración propia basado en las estadísticas de Política de seguridad minera de la ANM, 2022.

La actualización de la "Política de Seguridad Minera de Colombia" muestra una situación preocupante frente a la seguridad actual en las labores mineras, que se consolida en la Tabla 10 (Minminas, 2022).

**Tabla 10.** *Breve análisis de las causales de la situación actual de la seguridad minera*

| Agente involucrado | Eje problémico (Política de seguridad minera, 2022) | Análisis |
|---|---|---|
| **Empleador, trabajador** | Reducida afiliación de los trabajadores vinculados al sector minero al sistema general de seguridad social integral. | Solo el 27 % de los trabajadores mineros se estima que estén afiliados al Sistema de Salud. |
| **Autoridad minera** | Deficiente análisis de la causalidad de la accidentalidad minera. | Falta un registro más detallado de la causa de la siniestralidad y se requiere una estandarización para los registros. |
| | Indicadores en materia de siniestralidad por tipo de minería y tipo de mineral. | |
| **Autoridad minera empleador trabajador** | Bajo conocimiento de los mineros de las políticas y reglamentación técnicas vigentes en seguridad minera. | Es evidente la necesidad de incentivar la cultura para una explotación segura y el conocimiento de las normas vigentes, así como de los derechos laborales de los trabajadores mineros. |
| | Escasa gestión de la prevención diaria en las actividades por parte de los mineros. | |
| | Baja formación en seguridad y escasa implementación de las competencias laborales de los mineros. | |

Continúa tabla...

| Agente involucrado | Eje problémico (Política de seguridad minera, 2022) | Análisis |
|---|---|---|
| **Autoridad minera empleador trabajador** | Escaso desarrollo e interiorización de una cultura efectiva de la seguridad en las actividades mineras en el territorio nacional. | Es evidente la necesidad de incentivar la cultura para una explotación segura y el conocimiento de las normas vigentes, así como de los derechos laborales de los trabajadores mineros. |
| | Desconocimiento, por parte de los mineros, de la enfermedad laboral, su tratamiento, la vigilancia epidemiológica y el control de esta. | |
| **Autoridad minera** | Fiscalización integral y desarrollo de visitas conjuntas entre entidades que toman decisiones en materia de seguridad minera. | Entre 2011 y 2022 el 33,3 % de las fatalidades ocurridas en ese periodo fueron causadas en minas que funcionan de forma ilícita (Minminas, 2022), razón por la cual la Política de Seguridad propone un mayor seguimiento y control por parte de la **ANM** invitando a la legalidad, pero también, a un mejoramiento en los instrumentos requeridos para este fin. |
| | Reducido control de títulos mineros con alta densidad de operadores mineros que aportan un número significativo de accidentalidad. | |
| | Instrumentos de verificación, control y seguimiento a la ejecución ycumplimiento de acciones enmarcadas en la política de seguridad. | |
| | Ilegalidad de las operaciones mineras. | |

Fuente: elaboración propia basada en la actualización de la Política de Seguridad Minera en Colombia, 2022.

Dados los altos índices de accidentalidad registrados durante los últimos tres años (2020-2022), donde las tasas de fatalidad oscilan entre el 7,6 % y

el 8,7 %, con referencia al número total de fatalidades ocurridas entre 2005 y 2022 (Figura 15), conscientes de que la SST para los mineros de carbón son fundamentales para proteger la vida y la salud, así como la capacitación en seguridad, la evaluación de riesgos, el uso del equipo de protección personal, la ventilación adecuada, la iluminación, las pruebas de salud regulares y las medidas de emergencia. En junio de 2022, en el municipio de Guachetá, Cundinamarca, el Ministerio de Trabajo ha iniciado una campaña de capacitación y sensibilización denominada "Minero seguro tiene futuro", cuyo propósito es reducir la tasa de accidentalidad y la prevención de enfermedades laborales, dirigida principalmente a los departamentos con un mayor índice de accidentalidad (Mintrabajo, 2022).

Hasta mayo de 2023 se han registrado 56 mineros fallecidos por explosión en las minas, razón por la cual, la actual ministra del trabajo comunicó las labores de inspección, vigilancia y control que se vienen adelantando, sumado al fortalecimiento de la campaña "Minero seguro tiene futuro" (Medina, 2023). Con una tasa de mortalidad tan alta en lo que va corrido del año 2023, Minminas llevará a cabo la visita de inspección sobre la aplicación de protocolos de seguridad a 300 minas de carbón (Medina, 2023).

## Futuro del sector minero del carbón en Colombia

El futuro de la extracción de carbón en Colombia es incierto, ya que el país enfrenta varios desafíos relacionados con la transición hacia fuentes de energía más limpias y renovables que propenden por la reducción de emisiones de carbono a nivel mundial, así como con los problemas ambientales y sociales relacionados con la minería del carbón.

El "Plan Nacional de Desarrollo 2022-2026", del actual gobierno de Colombia, que se apoya en la Ley 2099 de 2021, "Ley de Transición Energética", en el eje "Transición energética justa, segura, confiable y eficiente", promueve la exploración de otros minerales y recursos para diversificar la explotación minera, reduciendo los volúmenes de explotación del carbón y petróleo, mediante estudios que permitan identificar los recursos locales, aprovechables para la obtención de energía eléctrica.

La migración de las termoeléctricas hacia nuevas alternativas es una tendencia mundial y plausible en la "Hoja de Ruta del Hidrógeno" de Minminas, documento guía para la producción energética dentro de los próximos 30 años, en el que se pretende lograr bajas emisiones de efecto invernadero, porque se espera que el hidrógeno verde sea la vía hacia la descarbonización, incentivando tecnologías basadas en energía eólica, geotérmica, mareomotriz y solar

(Minminas, 2021). De igual manera, se busca que la exploración de minerales sea orientada a la identificación de aquellos que sean aprovechables para insumos agrícolas.

El 26 de mayo de 2023 se adelantó en la Universidad Nacional de Colombia la primera Cumbre Minera, que tenía como propósito principal analizar el sector para la construcción de la "Nueva Ley Minera para la Vida", cuyo proyecto de ley se espera que sea radicado en el congreso en la segunda mitad del 2023 (Minminas, 2023a). La Cumbre contó con la participación de aproximadamente 1500 actores de la minería en Colombia y con representantes de las comunidades dedicadas a esta labor. Los ejes principales del ordenamiento territorial minero consisten en: proteger la minería artesanal y de pequeña escala como sustento de las familias involucradas; la extracción sustentable y responsable de minerales; y principalmente, la transición hacia el uso de energías más amigables con el medioambiente. La metodología de la Cumbre Minera contempló cuatro ejes de discusión en 50 mesas de trabajo. El espacio buscó dar vigencia a las metas trazadas en el "Plan de Desarrollo actual, en el que se asumen grandes retos a nivel nacional e internacional en materia de política pública para el sector de las minas y la energía (Minminas, 2023b).

## Discusión

Se puede explicar la existencia de políticas y protocolos de atención de emergencias y su relación con la seguridad en las minas subterráneas, pero que aún no son suficientes para garantizar la protección de la SST mineros. Si bien existen políticas y protocolos destinados a garantizar la extracción segura de minerales y la SST de los trabajadores mineros, no parecen ser suficientes para evitar el aumento de la tasa de mortalidad. Este aumento podría estar relacionado con una mayor presión sobre los trabajadores mineros para que cumplan con los objetivos de producción, lo que a su vez conlleva a una mayor exposición a riesgos laborales.

Es necesario buscar nuevas soluciones para garantizar la SST de los trabajadores de minas subterráneas y reducir la tasa de mortalidad que ha aumentado en los últimos tres años. Gran parte de las situaciones de riesgo sugieren un control exhaustivo que permita verificar, de manera constante, la valoración de las variables que pueden representar un peligro, para salvaguardarlas dentro de los límites permitidos. Por ejemplo, los dos accidentes en minas de carbón presentados en los municipios de Sutatausa y Cucunubá, Cundinamarca, en 2023, fueron ocasionados por explosiones.

Rivera Ramírez y Echeverri Zapata (2014), concluyen que "el liderazgo y compromiso de la

alta dirección de las mineras […] se describe directamente relacionado con el control, la minimización y eliminación del riesgo, […] situación que no concuerda con el desempeño en la seguridad y salud ocupacional" (p. 32), pasados nueve años en la revisión realizada en el presente documento, la conclusión sigue siendo la misma: los indicadores de accidentalidad y fatalidad así lo confirman.

La implementación de tecnologías emergentes aporta en dos aspectos altamente relevantes para la minería: la regulación del sector y la seguridad del trabajador minero. Es de resaltar que, aunque se están orientando las políticas hacia la transición energética, es un proceso que se irá dando de manera paulatina por el nivel de desarrollo de la ciencia y la tecnología que se requiere, así como de inversiones económicas considerables. Por ello, aún son necesarios los desarrollos tecnológicos orientados a resolver situaciones relacionadas con los actuales modelos de minería.

China es uno de los países pioneros en la implementación de proyectos de hidrógeno verde y pondrá en funcionamiento una nueva planta el 30 de junio de 2023, a cargo de la empresa petrolera Sinopec. En el corto plazo esperan poner en funcionamiento una planta que supera a esta, en un tercio de su capacidad, con una inversión de casi tres millones de dólares, para producir cien mil to-

neladas de $H_2$, conducido a través del gasoducto de Mongolia Interior hasta Pekín (Sinopecgroup, 2023). Quizás, esta tecnología sea implementada en Colombia dentro de unos años. En el momento, los esfuerzos están orientados hacia la definición de las políticas alineadas con las tendencias y normas internacionales. La "Hoja de Ruta Hidrógeno" fue definida durante el gobierno del expresidente Duque.

## Conclusiones

Las políticas y protocolos existentes en Colombia no son suficientes para garantizar la protección de la SST de los trabajadores mineros. Esto se debe a que hay factores como la presión para cumplir con los objetivos de producción y la ilegalidad minera, que aumentan la exposición a riesgos laborales y la tasa de mortalidad en los últimos tres años. Es necesario buscar soluciones adicionales para reducir la tasa de mortalidad y garantizar la seguridad de los trabajadores mineros.

Una alternativa que se puede considerar es el uso del IoT para monitorear y controlar las variables que representan un peligro para la salud y seguridad de los trabajadores mineros. La implementación de esta tecnología permitiría un monitoreo permanente, generando alertas tempranas y minimizando el riesgo de accidentes en las minas subterráneas, en

concordancia con el análisis de Rodríguez et ál., (2020).

Los trabajadores de la minería en Colombia requieren un enfoque integral que incluya el cumplimiento normativo, programas de educación y capacitación, y una planificación eficaz de respuesta a emergencias. Al abordar estas áreas clave, es posible minimizar los accidentes laborales y promover un ambiente de trabajo seguro y saludable para los trabajadores mineros en Colombia.

En conclusión, para garantizar la SST de los trabajadores mineros, especialmente en las minas subterráneas, se deben buscar soluciones adicionales más allá de las políticas y protocolos existentes. Tecnologías como el IOT, la IA, la computación en el borde, el *Big Data*, entre otros, ofrecen una alternativa prometedora para el monitoreo y control constante de las variables de riesgo, lo que contribuiría a la reducción de la tasa de mortalidad en las minas subterráneas. Empero, se requiere también del compromiso de los actores de esta actividad del sector primario.

# Referencias bibliográficas


Acar, A., Aksu, H., Uluagac, A. & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys (CSUR), 51(4), 79.

Acharya, S. y Tiwari, N. (2016). Survey of ddos Attacks Based On TCP/IP Protocol Vulnerabilities. *Journal of Computer Engineering (IOSR-JCE),*18(3), 68-76. https://doi.org/10.9790/0661-1803046876

Ackerman, D. (2020). *System Brings Deep Learning to "Internet of Things" Devices. MIT News on campus and around the Word.* https://news.mit.edu/2020/iot-deep-learning-1113

Agencia Nacional de Minería (anm). (22 de mayo de 2019). *Avanza la diversificación minera con una mayor participación del oro en las regalías*. https://acortar.link/0XP2my

Agencia Nacional de Minería (anm) - Universidad Pedagógica y Tecnológica de Colombia (uptc). (2020). *Manual del socorredor minero.* https://www.anm.gov.co/sites/default/files/DocumentosAnm/manual-del-socorredor-minero-15-12-2020.pdf

Alemami, Y., Al-Ghonmein, A. M., Al-Moghrabi, K. G. & Mohamed, M. A. (2023). Cloud data security and various cryptographic algorithms. *International Journal of Electrical and Computer Engineering,* 13(2), 1867. https://doi.org/10.11591/ijece.v13i2.pp1867-1879

Algarni, A. & Thayananthan, V. (2022). Autonomous Vehicles: The Cybersecurity Vulnerabilities and Countermeasures for Big Data Communication. *Symmetry*, 14, 2494. https://doi.org/10.3390/sym14122494

Argaw, S., Troncoso, P., Lacey, D., Florin, M., Calcavecchia, F., Anderson, D., … Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, 20(1). https://doi.org/10.1186/s12911-020-01161-7

Ariza, Y. (2018). Estrategia de integración. *Yesidariza.blogspot.* http://yesidariza.blogspot.com/2018/02/estrategia-de-integracion.html

Ashfaq, Z., Rafay, A., Mumtaz, R., Zaidi, S. M. H., Saleem, H., Zaidi, S. A. R.,... Haque, A. (2022). A review of enabling technologies for Internet of Medical Things (IoMT) Ecosystem. *Ain Shams Engineering Journal*, *13*(4), 101660. https://doi.org/10.1016/j.asej.2021.101660

Associated Press. (2021). *Suspected Russian Hack Fuels New US Action on Cybersecurity*. https://www.voanews.com/usa/suspected-russian-hack-fuels-new-us-action-cybersecurity

Astudillo, B. (2019). *Hacking ético*. Madrid, España, tercera edición, Ed. Ra-ma.

Awasthi, A., Bär, F., Doetsch, J., Ehm, H., Erdmann, M., Hess, M., ... Yarkoni, S. (2023). Quantum Computing Techniques for Multi-Knapsack Problems. arXiv https://doi.org/10.48550/arXiv.2301.05750

Ayerbe, A. (2017). *La Ciberseguridad de la Industria 4.0: Un medio para la continuidad del negocio*. Tecnalia.

Azadi, M., Moghaddas, Z., Cheng, T. & Farzipoor, S. (2023). Assessing the sustainability of cloud computing service providers for Industry 4.0: a state-of-the-art analytical approach. *International Journal of Production Research*, 61(12), 4196-4213. https://doi.org/10.1080/00207543.2021.1959666

Baena, G. R., Mendoza, M. R. y Joel, C. E. (2019). Importancia de la norma ISO/EIC 27000 en la implementación de un sistema de gestión de la seguridad de la información. Revista contribuciones a la Economía, 1-13.

Banca electrónica. (2022). *¿Qué es la revolución industrial? – Definición de Revolución Industrial.* https://bancaelectronica.net/que-es-la-revolucion-industrial-definicion-de-revolucion-industrial/

Barea, M., Rovira, F., Quecedo, G., Gol, M. y del Llano, S. (2021). Oportunidades y retos de los macrodatos (Big data): en la toma de decisiones sanitarias. (1ra Edición). Fundación Gaspar Casal. https://fundaciongasparcasal.

org/wp-content/uploads/2021/01/oportunidades-y-retos-de-los-macrodatos.pdf

Barona, G. & Velasteguí, L (2021). Automatización de procesos industriales mediante Industria 4.0. *AlfaPublicaciones,* 3(1), 84-101. https://doi.org/10.33262/ap.v3i3.1.80

Bockholt, N. (2017). *Realidad virtual, realidad aumentada, realidad mixta y ¿qué significa "inmersión" realmente?* https://www.thinkwithgoogle.com/_qs/documents/2027/c922f_15_perspectivas_realidadvirtual_quesignificainmersion.pdf.

Bonafini, S, & Sacchi, C. (2019). An Analytical Study on Functional Split in Martian 3-D Networks, ieee *Transactions on Aerospace and Electronic Systems*, 59(1), 745-753. https://doi.org/10.48550/arXiv.2207.00153

Boneder, S. (2023). *Evaluation and comparison of the security offerings of the big three cloud service providers Amazon Web Services, Microsoft Azure and Google Cloud Platform.* [Doctoral dissertation]. Technische Hochschule Ingolstadt.

Branch, L., Eller, W., Bias, T.K., McCawley, M., Myers, D., Gerber, B. & Bassler, J. (2019). Trends in Malware Attacks against United States Healthcare Organizations, 2016-2017. *Global Biosecurity,* 1(1),15–27. https://doi.org/10.31646/gbio.7

Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. *Network Security,* (9), 5–9. https://doi.org/10.1016/s1353-4858(16)30086-1

Bullee, J., Montoya, L., Junger, M. & Hartel, P. (2017). Spear phishing in organisations explained. *Information and Computer Security,* 25(5), 593-613. https://doi.org/10.1108/ICS-03-2017-0009

Burke, B. (2020). *Automatización e inteligencia artificial: de aterrador, a encantador.* Softtek. https://blog.softtek.com/es/automatizaci%C3%B3n-e-inteligencia-artificial-de-aterrador-a-encantador

Cacheiro, M. y Taboada, M. (1998). Elaboración de modelos de elevación digital empleando técnicas geoestadísticas y sistemas de información geográfica. Facultad de Ciencias. Uni-

versidad de La Coruña. *Cadernos Lab. Xeolóxico de Laxe*, 23, 137-150.

Cárdenas, M. y Reina, M. (2008). La minería en Colombia: impacto socioeconómico y fiscal. Cuadernos de Fedesarrollo 25. https://www.repository.fedesarrollo.org.co/handle/11445/893

Carrillo, J. (2021). *El Dron Método de Levantamiento Topográfico más eficaz para el Municipio de Villanueva, Departamento del Casanare, Colombia*. [Tesis de especialización]. Universidad Militar Nueva Granada. http://hdl.handle.net/10654/40316.

ccna. (2023). *Características y Funciones de* ospf. https://ccnadesdecero.es/caracteristicas-funciones-ospf/

Chandrasekaran, S. & Subramaniam, R. (2022). *Why iot Sensors Need Standards They could improve performance and spur development of new applications*. ieee Spectrum. https://spectrum.ieee.org/why-iot-sensors-need-standards

Chaves, J. (2004) Desarrollo tecnológico en la primera revolución industrial. *Revista de Historia*, 17, 93-109.

Clifford, S., Quilty B., Russell, T., Liu, Y., Desmond, C., Pearson, C., Rosalind, M., Akira, E. y Stefan, F. (2020). Estrategias para reducir el riesgo de reintroducción del sars-cov-2 de viajeros internacionales. medRxiv. https://doi.org/10.1101/2020.07.24.20161281

Collier, R. (2017). nhs ransomware attack spreads worldwide. cmaj: Canadian Medical Association journal. *Journal de l'Association medicale canadienne*, 189(22), E786-E787. https://doi.org/10.1503/cmaj.1095434

Comer, D. & Stevens, D. (2020). Internetworking with tcp/ip: Principles, Protocols, and Architecture (Vol. 1, 6th ed.). Pearson Education.

Connolly, Y. & Wall, D. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security,* 87, 101568. https://doi.org/10.1016/j.cose.2019.101568

Cruz, M., Morales, C. y Ayala, R. (2006). Diseño de productos asistidos por realidad virtual inmersiva. Ingeniería Mecánica. *Tecnología y Desarrollo,* 2(3), 93-100.

Cubides, C., Suárez, P. y Hoyos, R. (2018). *Responsabilidad ambiental del Estado colombiano con ocasión del conflicto armado interno.* https://publicaciones.ucatolica.edu.co/pdf/responsabilidad-internacional-y-proteccionambiental.pdf

Dallon, A. (2021). *Cybersecurity lags behind as iot devices proliferate, according to a new report*. https://www.techrepublic.com/article/cybersecurity-lags-behind-as-iot-devices-proliferate-according-to-a-new-report/?ftag=TRE684d531&-bhid=29819942023096896100958364571180&mid=13445830&cid=2392697384

Dao, N. (2023). Internet of wearable things: Advancements and benefits from 6G technologies. *Future Generation Computer Systems*, *138*, 172-184. https://doi.org/10.1016/j.future.2022.07.006

Davies, T. y Fumega, S. (2022). Informe Barómetro Global de Datos (2022). Primera Edición. https://doi.org/10.5281/zenodo.6488349

Davis, J. y Bizo, D. (2022). Uptime Institute Global Data Center Survey 2022. *Planning & Strategy Ui Intelligence*. [Report 78]. https://uptimeinstitute.com

Decreto 1477 de 2014 [Ministerio del Trabajo de Colombia]. Por el cual se expide la Tabla de enfermedades laborales. 5 de agosto de 2014. https://www.mintrabajo.gov.co/documents/20147/36482/decreto_1477_del_5_de_agosto_de_2014.pdf/b526be63-28ee-8a0d-9014-8b5d7b299500

Decreto 1666 de 2016. [Presidencia de la república de Colombia]. (21 de octubre de 2016). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77883

Díaz, M. (2009). *Manual de salud y seguridad en trabajos de minería*. Fundación uocra.

Dueñas, C. M. (16 de marzo de 2023). Más de 1.262 accidentes mineros en Colombia durante los últimos 10 años. *Forbes Staff.* https://forbes.co/2023/03/16/actualidad/mas-de-1-

262-accidentes-mineros-en-colombia-durante-los-ultimos-10-anos

Enciclopedia Británica. (2022). Industrial Revolution. Encyclopedia Britannica.

European Telecommunications Standards Institute (etsi). (2020). CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements. etsi en 303 645. European Standard 2(1.1), 13-24 https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

Fernández, J. y Gutiérrez, G. (2017). Uso de lidar y Aeronaves No Tripuladas para la cartografía y registro de zonas de interés geominero: un ejemplo de la minería aurífera romana en el Valle del Eria (León, España). A*rqueología en el valle del Duero: Del Paleolítico a la Edad Media*, 520-536.

fips 140-3 (2019). *Federal information processing standards publication (Supersedes* fips PUB *140-2).* Security requirements for cryptographic modules. Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, md 20899-8900. https://doi.org/10.6028/NIST.FIPS.140-3.

Forouzan, B. (2020). tcp/ip Protocol Suite (5th ed.). McGraw-Hill Education.

Garrell, A, y Guilera, L. (2019). *La industria 4.0 en la sociedad digital* (1ra ed.). Marge Books.

Gittins, Z. & Soltys, M. (2020). Malware Persistence Mechanisms.24th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems. *Procedia Computer Science,* 176, 88–97. https://doi.org/10.1016/j.procs.2020.08.010

González, H. y Angulo, J. (2005). Teoría, diseño básico y señales recibidas por un sistema lidar para mediciones atmosféricas. *Ingeniería* 10(2), 67-78.

González, H., Armas, A., Coronel, L., Vergara, M., Maldonado, L. y Granillo, M. (2021). El desarrollo tecnológico en las revoluciones industriales. *Ingenio y Conciencia Boletín Cien-*

*tífico de la Escuela Superior Ciudad Sahagún* 8(16), 51-52. https://doi.org/10.29057/escs.v8i16.7118

González, L. (16 de marzo de 2023). ¿Qué tan peligrosa es la minería en Colombia?: desde el 2005 se han reportado más de 1.700 emergencias en el país. Infobae. https://www.infobae.com/colombia/2023/03/16/que-tan-peligrosa-es-la-mineria-en-colombia-desde-el-2005-se-han-reportado-mas-de-1700-emergencias-en-el-pais/

gsma. (2021). *iot SAFE: Robust iot security at scale. The why, what and how of securing iot applications and data.* gsma. https://www.gsma.com/iot/wp-content/uploads/2021/06/IoT-SAFE-Whitepaper-2021.pdf

Gupta, B., Mittal, P. & Mufti, T. (2021). A review on amazon web service (aws), microsoft azure & google cloud platform (gcp) services. Proceedings of the 2nd International Conference on ICT for Digital, Smart, and Sustainable Development, ICIDSSD 2020, 27-28, Jamia Hamdard, New Delhi, India. http://dx.doi.org/10.4108/eai.27-2-2020.2303255

Gutiérrez, N. (2023). *Oficina virtual de Sanitas, afectada por ciberataque, ya está habilitada para pedir citas*. La República. https://www.larepublica.co/empresas/oficina-virtual-de-sanitas-afectada-por-ciberataque-ya-esta-habilitada-para-pedir-citas-3523652

Haidine A. & Hassani, S. E. (2016). LTE-a pro (4.5G) as pre-phase for 5G deployment: Closing the gap between technical requirements and network performance. International Conference on Advanced Communication Systems and Information Security (ACOSIS), Marrakesh, Morocco, 2016, 1-7, https://doi.org/10.1109/ACOSIS.2016.7843933.

Han, H., Shiwakoti, R., Jarvis, R., Mordi, C. & Botchie, D. (2023). Accounting and auditing with blockchain technology and artificial Intelligence: A literature review. *International Journal of Accounting Information Systems*, 48, 100598. https://doi.org/10.1016/j.accinf.2022.100598

Handayani, I., Apriani, D., Mulyati, M., Yusuf, N. & Zahra, A. (2023). A Survey on User Experience of Blockchain Transactions: Security and Adaptability Issues. *Blockchain Frontier Technology,* 3(1), 160-168. https://doi.org/10.34306/bfront.v3i1.366

Harkins, M. & Freed, A. (2018). The Ransomware Assault on the Healthcare Sector. *Journal of Law & Cyber Warfare*, 6(2), 148-164.

Harth, N., Anagnostopoulos, C. & Pezaros, D. (2018). Predictive intelligence to the edge: impact on edge analytics. *Evolving Systems,* 9, 95–118. https://doi.org/10.1007/s12530-017-9190-z

Herrera, J. (2017) *Introducción a la Minería. (Vol. I) Conceptos, tecnologías y procesos.* Universidad Politécnica de Madrid. https://doi.org/10.20868/UPM.book.63396

Hussein, A. & ALRikabi, H. (2023). Secured Transfer and Storage Image Data for Cloud Communications. *International Journal of Online & Biomedical Engineering*, 19(6), 4-17. https://doi.org/10.3991/ijoe.v19i06.37587

ibm. (5 de agosto de 2023). *Cómo las tecnologías de la Industria 4.0 están cambiando la fabricación*. https://www.ibm.com/es-es/topics/industry-4-0

Iniciativa de Transparencia de las Industrias Extractivas (eiti). (2016). *Sector minería*. https://www.eiticolombia.gov.co/es/informes-eiti/informe-2016/marco-institucional/sector-mineria/#:~:text=El%20sector%20minero%20colombiano%20se,la%20industria%20y%20la%20construcci%C3%B3n

Inteligencia Artificial Colombia (iac). (2022). Gemelos digitales en la minería colombiana. https://ia-colombia.co/gemelos-digitales-en-la-mineria-colombiana/

International Labour Organization. (2020). An employers' guide on working from home in response to the outbreak of covid-19. Geneva: International Labour Office. www.ilo.org/publns

Jiménez, F., Naranjo, J. E., Anaya, J. J., García, F., Ponz, A. & Armingol, J. M. (2016). Advanced Driver Assistance System

for Road Environments to Improve Safety and Efficiency. *Transportation Research Procedia*, 14, 2245-2254. https://doi.org/10.1016/j.trpro.2016.05.240

Jiménez, P. (2021). Learning in autonomous and intelligent systems: Over-view and biases from data sources. *Arbor*, 197(802): a627. https://doi.org/10.3989/arbor.2021.802005

Johnson, D. (2020). *New ransomware campaign exploits weak MySQL credentials to lock thousands of databases*. https://www.scmagazine.com/home/security-news/ransomware/new-ransomware-campaign-exploits-weak-mysql-credentials-to-lock-thousands-of-databases/

Joyanes, L. (2017). *Industria 4.0: la cuarta revolución industrial.* Alfaomega.

Juárez, F. (2016). *La minería ilegal en Colombia: un conflicto de narrativas*. El Agora USB, 16(1), 135-146.

Kozierok, C. (2019). The tcp/ip Guide: A Comprehensive, Illustrated Internet Protocols Reference (6th ed.). No Starch Press.

lemo (2023). *This Startup Is Building the Internet of Underwater Things*. https://spectrum.ieee.org/wsense-internet-of-underwater-things

Leon, R. (2023). *OT Security: Protecting Industry 4.0 from Attack.* https://acortar.link/2lD8OP

Levich, B., Vdovin, I. & Miamlin, V. (2022). *Mecánica cuántica*. Reverté.

Lin, J., Chen, W., Lin, Y., Cohn, J., Gan C. & Han, S. (2020). mcunet: Tiny Deep Learning on iot Devices. 1-13. arXiv:2007.10319v2. https://arxiv.org/abs/2007.10319

Ling, P. (2021). *Data security in the iiot is only going one way.* https://www.avnet.com/wps/portal/us/resources/article/data-security-in-the-iiot-is-only-going-one-way/

Liñan, A., Vives, A., Bagula, A., Zennaro, M. y Pietrosemoli, E. (2015). *Internet de las Cosas.* http://wireless.ictp.it/Papers/InternetdelasCosas.pdf

Luo, C., Fei, Y., Ding, A. & Closas, P. (2019). Comprehensive Side-Channel Power Analysis of XTS-AES. ieee *Transactions on Computer-Aided Design of Integrated Circuits and Systems,* 38(12), 2191-2200. https://doi.org/10.1109/TCAD.2018.2878171.

Márquez, D. (2017). Armas cibernéticas. Inteligencia artificial para el desarrollo de virus informáticos letales. *Revista Ing. USB-Med,* 8(2), 48-57. https://doi.org/10.21500/20275846.2955

Márquez D. (2019). Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas. *Revista Bìotica i Dret.* Rev Bio y Der, 46, 85-100. https://doi.org/10.1344/rbd2019.0.27068

Márquez, D. (2020). Internet of Things and Distributed Denial of Service as Risk Factors in Information Security [Online First], *IntechOpen,* https://doi.org/10.5772/intechopen.94516.

Márquez, D. (2021). Internet de las cosas (iot) y grandes datos frente ataques de denegación de servicio distribuido (ddos). Nanoingeniería. Scientific Academic Research Activity, 189-235. https://www.researchgate.net/publication/344672925_Internet_de_las_cosas_y_Big_Data_frente_ataques_de_denegacion_de_servicio_distribuido_en_el_sector_sanitario

Márquez, J. (2022). Cybersecurity and Internet of Things. Outlook for this Decade. Computación y Sistemas, 26(3), 1191–1204. https://doi.org/10.13053/CyS-26-3-3925

Márquez, J. (2023a). Desarrollos tecnológicos e implicaciones de los drones autónomos militares: perspectivas en la geopolítica mundial. *Revista Tecnológica* - espol, 35(1), 137-151. https://doi.org/10.37815/rte.v35n1.1018

Márquez, D. (2023b). Modelos de lenguaje natural en la investigación científica: una descripción técnica. *Innovación y ciencia,* 33(1), 1-6. https://innovacionyciencia.com/articulos_cientificos/modelos-de-lenguaje-natural-en-la-investigacion-cientifica-una-descripcion-tecnica

Martins, P., Sousa, L. & Mariano, A. (2017). A survey on fully homomorphic encryption: An engineering perspective. acm *Computing Surveys (*csur*),* 50(6), 83.

Guardicore. (2020). Massive new botnet discovered. *Computer Fraud & Security,* 3(9). https://doi.org/10.1016/S1361-3723(20)30092-0

Matías, R. (2020). *Aplicación de un dron para mejorar los procesos productivos en Minera Chinalco Perú S. A., Morococha 2020*. [Trabajo de Investigación para optar el Grado Académico de Bachiller en Ingeniería de Minas]. Universidad Continental de Perú.

Maurya, A., Kumar, N., Agrawal, A. & Khan, R. (2018). Ransomware: Evolution, Target and Safety Measures. *International Journal of Computer Sciences and Engineering,* 6(1), 80-85. https://doi.org/10.26438/ijcse/v6i1.8085

Medina, C. (2023). La anm anunció un plan de choque en el país tras accidentes minero0073. *W Radio.* https://www.wradio.com.co/2023/05/02/la-anm-anuncio-un-plan-de-choque-en-el-pais-tras-accidentes-mineros/

Mekki, K., Bajic, E., Chaxel, F. & Meyer, F. (2018). A comparative study of lpwan technologies for large-scale iot deployment. ict Express, 5(1), 1-7. https://doi.org/10.1016/j.icte.2017.12.005

Ministerio del Trabajo de Colombia (Mintrabajo). (2022). Ministerio del Trabajo lanza la campaña "Minero seguro tiene futuro". Comunicados de prensa Mintrabajo. https://www.mintrabajo.gov.co/prensa/comunicados/2022/mayo/ministerio-del-trabajo-lanza-la-campa%C3%B1a-minero-seguro-tiene-futuro-

Ministerio de Minas y Energía de Colombia (Minminas). (2019). Guía para la incorporación de la dimensión minero-energética en los planes de ordenamiento municipal. https://repositoriobi.minenergia.gov.co/handle/123456789/2841

Ministerio de Minas y Energía de Colombia (Minminas). (2021). *Hoja de Ruta del Hidrógeno*. https://www.minener-

gia.gov.co/static/ruta-hidrogeno/src/document/Hoja%20Ruta%20Hidrogeno%20Colombia_2810.pdf

Ministerio de Minas y Energía de Colombia (Minminas). (2022). Política de seguridad minera. https://www.minenergia.gov.co/documents/6027/Pol%C3%ADtica_Nal.Seguridad_Minera_ajustada_vrs_MAL_29032022_2__01042022_comentario_9egb6kZ.pdf

Ministerio de Minas y Energía de Colombia (Minminas). (2023a). En segundo semestre de 2023, será radicado en el Congreso el proyecto de nueva Ley Minera. Sala de prensa. https://acortar.link/mPJmOf

Ministerio de Minas y Energía de Colombia (Minminas). (2023b). *Generalidades de la Cumbre Nacional Minera*. https://acmineria.com.co/sitio/wp-content/uploads/2023/05/CNM-Generalidades.pdf

Ministerio de de Tecnologías de la Información y Comunicaciones de Colombia (Minatic). (2016). *Guía para la Implementación de Seguridad de la Información en una MIPYME* (Norma núm. 1.2). https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

Mott, G., Turner, S., Nurse, J., MacColl, J., Sullivan, J., Cartwright, A. & Cartwright, E. (2023). Between a rock and a hard (ening) place: Cyber insurance in the ransomware era. *Computers & Security*, *128*, 103162. https://doi.org/10.1016/j.cose.2023.103162

Moukahal, L., Zulkernine, M. & Soukup, M. (2021). Vulnerability-Oriented Fuzz Testing for Connected Autonomous Vehicle Systems. IEEE Transactions on Reliability, 4(70), 1422-1437. https://doi.org/10.1109/TR.2021.3112538.

Newball, C. (2014). Configuración, programación e implementación de interfaz humana del prototipo de empacadora de galletas para la operación dentro de la línea de producción del Laboratorio de Automatización de la upb. [Trabajo de grado]. Universidad pontificia Bolivariana. http://hdl.handle.net/20.500.11912/10024.

Nikpour, M., Yousefi, P. B., Jafarzadeh, H., Danesh, K. & Ahmadi, M. (2023). Intelligent Energy Management with iot Framework in Smart Cities Using Intelligent Analysis: An Application of Machine Learning Methods for Complex Networks and Systems. 1-37. *arXiv preprint arXiv:2306.05567*. https://doi.org/10.48550/arXiv.2306.05567

Nuttah, M., Roma, P., Nigro, G. & Perrone, G. (2023). Understanding blockchain applications in Industry 4.0: From information technology to manufacturing and operations management. *Journal of Industrial Information Integration*, 33, 100456. https://doi.org/10.1016/j.jii.2023.100456

Organización para la Cooperación y el Desarrollo Económicos (oecd). (2021). Tax Challenges Arising from the Digitalisation of the Economy – Global Anti-Base Erosion Model Rules (Pillar Two): Inclusive Framework on beps, oecd, Paris https://www.oecd.org/tax/beps/tax-challenges-arising-from-the-digitalisation-of-theeconomy-global-anti-base-erosion-model-rules-pillar-two.htm.

Organización Internacional del Trabajo. (2006). Meeting of Experts on Safety and Health in Coal Mines. http://ilo.org/wcmsp5/groups/public/---ed_dialogue/---sector/documents/meetingdocument/wcms_162579.pdf

Organización Internacional del Trabajo. (2010). *Lista de enfermedades profesionales (revisada en 2010)*. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/publication/wcms_150327.pdf

Organización Internacional del Trabajo. (28 de abril de 2013). *La prevención de las enfermedades profesionales*. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/publication/wcms_209555.pdf

Ortiz, C. (2019). Normativa Legal sobre Delitos Informáticos en Ecuador. *Revista Científica Hallazgos21*, 4(1), 100- 111.

Ortiz, C., Fernández, L., Cadavid, N. y Gallego, D. (2018). Computación en la Nube: Estudio de Herramientas Orien-

tadas a la Industria 4.0 *Lámpsakos,* 1(20), 68-75. https://doi.org/10.21501/21454086.2560

Panda, M. & Tripathy, B. (2018). adaret of Things and Artificial Intelligence: A New Road to the Future Digital World. In B.K. Tripathy & J. Anuradha, (eds.). Internet of things (iot). Technologies, Applications, Challenges, and Solutions, (p. 41-58).. New York, crc Press.

Parisyan, S. (2023). *19 Cloud Computing Statistics You Need to.* https://egen.solutions/articles/19-cloud-computing-statistics-you-need-to-know-in-2023/

Pernet, C. (2023). *More phishing campaigns are using* ipfs *network protocol.* https://www.techrepublic.com/article/ipfs-phishing-attacks/

Perry, T. (2023). *Baterías de papel, puntos cuánticos azules y otras tecnologías habilitadoras de CES 2023*. https://spectrum.ieee.org/future-tech-ces-2023

Pinto, R. (2014). *Drones: La Tecnología, Ventajas y sus posibles aplicaciones. Sociedad Nacional de Minería de Chile*. https://www.sonami.cl/v2/

Portugal, P., Álvarez, F., Tejedor, M. y Rodríguez, B. (2023). La administración de la cadena de suministro y su importancia en las empresas, como parte de la estrategia en los nuevos modelos de negocios. *Ciencia Latina Revista Científica Multidisciplinar*, 7(3), 7203-7219. https://doi.org/10.37811/cl_rcm.v7i3.6709

Ramírez, M. (2021). Post-Procesamiento de Datos gps Cinemático Aerotransportado y Datos Inerciales. Instituto Geográfico Agustín Codazzi (igac).

Razaulla, S., Fachkha, C., Markarian, C., Gawanmeh, A., Mansoor, W., Fung, BC y Assi, C. (2023). *La era del ransomware: una encuesta sobre la evolución, la taxonomía y las direcciones de investigación. Acceso IEEE.* https://doi.org/10.1109/ACCESS.2023.3268535.

Real, E. (2011). *El Modelado Geomático del lidar: De la Fusión SVM a la Noción de Posdetección.* [Tesis de maestría en Geo-

mática]. Centro de Investigación en Geografía y Geomática Centro Público de Investigación conacyt.

Reddy, V. & Rashmi, S. (2023). Prevalent Cyber Attacks and Defense. In ieee *International Conference on Integrated Circuits and Communication Systems (*icicacs*)* (pp. 1-6). ieee.

Reinoso, R. (2013). Introducción a la Realidad Aumentada. https://www.educa.jcyl.es/crol/es/repositorio-global/introduccion-realidad-aumentada-37162.ficheros/511255-3711.pdf

Rincón, T. (2019). *Revolución industrial.* https://rincontarea.info/revolucion-industrial/

Ristov, R. & Koceski, S. (2023). Quantum Resilient Public Key Cryptography in Internet of Things. In 12th Mediterranean Conference on Embedded Computing (meco), (pp. 1-4). ieee. https://doi.org/10.1109/MECO58584.2023.10154994

Rivera Ramírez, L. V. & Echeverri Zapata, J. C. (2014). Estado del arte de la seguridad y salud en el trabajo en el sector minero en Colombia. [Trabajo de grado]. Universidad Corporación para Estudios en Salud ces. https://repository.ces.edu.co/handle/10946/2066

Rodríguez, R., Reyes, C. y Torres, V. (2020). Análisis técnico de los sistemas de gestión de seguridad y salud en el trabajo para el sector de minería subterránea en el Municipio de Muzo, Departamento de Boyacá-Colombia. https://repositorio.ecci.edu.co/handle/001/846

Rose S., Borchert, O., Mitchell, S. & Connelly, S. (2020). *NIST Special Publication 800-207 Zero Trust Architecture.* Computer security, National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Rose, K., Eldridge, S. & Chapin, L. (2015). *The internet of things: An overview. Understanding the Issues and Challenges of a More Connected World.* Geneva, The Internet society.

Saade, M. (2014). *Buenas prácticas que favorezcan una minería sustentable.* La problemática en torno a los pasivos ambientales mineros en Australia, el Canadá, Chile, Colombia, los Estados Unidos, México y el Perú Serie Macroeconomía del

Desarrollo. División de Desarrollo Económico de la Comisión Económica para América Latina y el Caribe (cepal), Naciones Unidas, Santiago de Chile.

Saavedra, S. (2020). Inteligencia artificial para frenar la minería ilegal en Colombia. *Semana.* https://www.semana.com/contenidos-editoriales/mineria/articulo/inteligencia-artificial-para-frenar-la-mineria-ilegal-en-colombia/202000/

Said, K. O., Onifade, M., Githiria, J. M., Abdulsalam, J., Bodunrin, M. O., Genc, B.,... & Akande, J. M. (2021). On the application of drones: a progress report in mining operations. *International Journal of Mining, Reclamation and Environment*, *35*(4), 235-267. https://doi.org/10.1080/17480930.2020.1804653

Sanger, D. & Perlroth, N. (2020). *U.S. to Accuse China of Trying to Hack Vaccine Data, as Virus Redirects Cyberattacks.* https://www.nytimes.com/2020/05/10/us/politics/coronavirus-china-cyber-hacking.html

Sección industrial (2023). *Proyectos industria 4.0 ejemplos*. https://seccionindustrial.com/suministros-industriales/proyectos-industria-4-0-ejemplos/

Serpanos, D. y Wolfm, M. (2018). *Internet-of-Things (iot) Systems. Architectures, Algorithms, Methodologies.* Switzerland, Springer.

Shapiro, S. (2023). *The strange story of the teens behind the mirai botnet. Their ddos malware threatened the entire Internet*. https://spectrum.ieee.org/mirai-botnet

Singh, J., Sharma, K., Wazid, M. & Das, A. K. (2023). sinnrd: Spline interpolation-envisioned neural network-based ransomware detection scheme. *Computers and Electrical Engineering*, *106*, 108-601. https://doi.org/10.1016/j.compeleceng.2023.108601

Sinopecgroup. (2023). Sinopec Launches the World's Largest Green Hydrogen-Coal Chemical Project in Inner Mongolia. News Sinopec. http://www.sinopecgroup.com/group/en/Sinopecnews/20230331/news_20230331_502557647316.shtml

Sistu, S., Liu, Q., Ozcelebi, T., Dijk, E. & Zotti, T. (2019). Performance Evaluation of Thread Protocol based Wireless Mesh Networks for Lighting Systems. International Symposium on Networks, Computers and Communications (isncc), Istanbul, Turkey, 1-8, https://doi.org/10.1109/ISNCC.2019.8909109.

Soltani, R., Zaman, M., Joshi, R. & Sampalli, S. (2022). Tecnologías de contabilidad distribuida y sus aplicaciones: una revisión. Ciencias Aplicadas, 12(15), 78-98. https://doi.org/10.3390/app12157898

Soori, M., Arezoo, B. & Dastres, R. (2023). Internet of things for smart factories in industry 4.0, a review. *Internet of Things and Cyber-Physical Systems.* https://doi.org/10.1016/j.iotcps.2023.04.006

Sophos. (2022). *Guía de respuesta a incidentes. Los 10 pasos para crear un plan de respuesta a ciberincidentes efectivo.* Sophos Cibersecurity delivered.

Suganya, M. & Sasipraba, T. (2023). Stochastic Gradient Descent long short-term memory based secure encryption algorithm for cloud data storage and retrieval in cloud computing environment. *Journal of Cloud Computing,* 12(1), 1-17. https://doi.org/10.1186/s13677-023-00442-6

Tanenbaum, A. & Wetherall, D. (2019). Computer Networks (5th ed.). Pearson Education.

Tascón, M. y Coullaut, A. (2016). *Big data y el internet de las cosas. Qué hay detrás y cómo nos va a cambiar.* Madrid, Ed. Catarata.

Technology Innovation Institute. (2022). *Building a Zero Trust Security Model for Autonomous Systems It's imperative to extend a Zero Trust architecture to protect autonomous systems like drones, industrial equipment, and smart cities.* The ieee Spectrum. https://spectrum.ieee.org/zero-trust-security-autonomous-systems

Thapa, S., Ghimire, A., Adhikari, S., Kumar B. & Barsocchi, P. (2022). Chapter 3 - Cognitive Internet of Things (iot) and computational intelligence for mental well-being. In A.

Kumar, V. Albuquerque, S. Naga & G. Marques, G. (eds.). Intelligent Data-Centric Systems, Cognitive and Soft Computing Techniques for the Analysis of Healthcare Data, (pp. 59-77). Academic Press. https://doi.org/10.1016/B978-0-323-85751-2.00004-9.

The ieee standards association. (21 de octubre de 2022). *Why Cybersecurity Is Key to iot Sensors The essential part of the iot is becoming a target for cyberattacks.* https://spectrum.ieee.org/sensor-cybersecurity-standards

Trend Micro (30 de abril de 2023). *6 Ransomware Trends & Evolutions For 2023.* https://www.trendmicro.com/en_us/ciso/23/b/ransomware-trends-evolutions-2023.html

Tyagi, A. K., Dananjayan, S., Agarwal, D. & Thariq Ahmed, H. F. (2023). Blockchain—Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0. *Sensors*, 23(2), 947. https://doi.org/10.3390/s23020947

Unterfingher, V. (2020). *Ryuk Ransomware – Untangling a Convoluted Malware Narrative.* Heimdal. https://heimdalsecurity.com/blog/ryuk-ransomware/

Valencia, A. y Portilla, P. (2019). Internet industrial de las cosas (iiot): 490, Nueva forma de fabricación inteligente. *Fundación Universitaria de Popayán*. http://unividafup.edu.co/repositorio/files/original/0cba2296f09e033fe6c-5c08e5a6a0119.pdf

Vilaplana, F. (2019). Digitalización y personas. *Empresa y humanismo*, 23(1), 113-137. https://doi.org/10.15581/015.XXIII.1.113-137

Villas, S. (2006). *La primera Revolución Industrial.* Boletín de la academia malagueña de ciencias.

Villegas, J. (2023). *Implementación del proceso de mantenimiento preventivo para vehículos, en la empresa "RC Motors Ingeniería Automotriz", basado en la Norma ISO 9001: 2015* [Tesis de pregrado]. Universidad Central de Ecuador. https://www.dspace.uce.edu.ec/entities/publication/779016d5-8b53-451b-b93c-f9dfc3a44d34

Vincent, R. (2010). Light Detection and Ranging (*lidar*) Technology Evaluation. [Final Organizational Results Research Report]. Missouri Department of Transportation.

Witorg, (2019). *Pirámide de la automatización e industria 4.0.* https://www.witorg.org/piramidede-la-automatizacion-e-industria-4-0/

Ynzunza, C., Izar, L., Bocarando, Ch., Aguilar, P. y Larios, O. (2017). El entorno de la Industria 4.0: Implicaciones y perspectivas futuras. *Conciencia Tecnológica*, 54, 1-19. https://www.redalyc.org/journal/944/94454631006/94454631006.pdf

Zahera, M. (2012). La fabricación aditiva, tecnología avanzada para el diseño y desarrollo de productos. XVI Congreso Internacional de Ingeniería de Proyectos. *Fundación Cotec,* 2088- 2098. http://dspace.aeipro.com/xmlui/bitstream/handle/123456789/1283/CIIP12_2088_20

Zewe, A. (2022). New Chip Can Prevent Hackers from Extracting Hidden Information from Smart Devices. SciTechDDaily. https://scitechdaily.com/new-chip-can-prevent-hackers-from-extracting-hidden-information-from-smart-devices/

Zhao, E, M. & Geng, Y. (2019). Homomorphic Encryption Technology for Cloud Computing. *Procedia Computer Science,* 154, 73–83. https://doi.org/10.1016/j.procs.2019.06.012

Zharovskikh, A. (2023). *The benefits of AI in Cloud Computing.* InData Labs. https://indatalabs.com/blog/ai-cloud-computing

Ziebinski, A., Cupek, R., Grzechca, D. & Chruszczyk, L. (2017). Review of Advanced Driver Assistance Systems (adas). *Proceedings of the International Conference of Computational Methods in Sciences and Engineering 2017* (ICCMSE-2017) aip Conf. Proc.120002-1–120002-4. https://doi.org/10.1063/1.5012394

*Industria 4.0. Internet de las Cosas: ciberseguridad y aplicaciones*
terminó su edición
el 30 de julio de 2024.

Se utilizaron las fuentes
Garamond Pro y Barlow.

# Industria 4.0.
## Internet de las Cosas:
### ciberseguridad y aplicaciones

La Industria 4.0 está transformando la forma en que las organizaciones operan y compiten a través de sistemas de automatización que utilizan tecnologías avanzadas. Esta industria ofrece numerosos beneficios gracias a la automatización, las tecnologías integrales —horizontales y verticales—, a la fabricación aditiva, la realidad aumentada, la computación en la nube, el Internet de las Cosas, la inteligencia artificial, el *blockchain*, entre otras. El Internet de las Cosas conlleva vulnerabilidades que pueden explotarse en ataques de *ransomware*, *botnet* y de Denegación de Servicio Distribuido (DDoS), razón por la que los estándares de seguridad son necesarios, a pesar de los desafíos que existen, como la brecha de habilidades, la falta de interoperabilidad, las preocupaciones sobre la privacidad, las consideraciones éticas y las amenazas a la seguridad cibernética.

En el caso específico de la industria minera y la tecnología que implica la Industria 4.0, los drones LiDAR son útiles para realizar fotogrametrías en las minas —las cuales miden los volúmenes de acopios y realizan topografías en 3D—, sumado a que en entornos inadecuados para humanos, como en la minería de carbón, se puede hacer uso de estos drones, especialmente cuando se desea cumplir con las normas y regulaciones de seguridad y salud ocupacional, así como reducir las enfermedades laborales y los incidentes en el sector minero en Colombia. En conclusión, la Industria 4.0 debe abordarse de manera reflexiva, responsable e inclusiva si se quiere que sus beneficios lleguen a todos.

Universidad de CUNDINAMARCA

ISBN: 978-628-7621-85-5