ACORTANDO DISTANCIAS

UCOMPENSAR EN MISIÓN COLOMBIA-MÉXICO HACIA LA ERA DIGITAL E INDUSTRIAS 4.0

compensar
fundación universitaria

Fundación Universitaria Compensar
Facultad de Ingeniería

Barbosa Castro, Neider Duan - Bareño Gutiérrez, Raúl
Acortando distancias. U Compensar en la misión Colombia - México de la era digital e industria 4.0 / Neider Duan Barbosa Castro, Raúl Bareño Gutiérrez, Yesica Andrea Martín, Amaya Lilian Minottas, José Luis Mora Feo, Carlos Alfredo Sapuyes Ortega, Wilson Alexander Cruz Mesa, Michael Armando Escudero Ávila, Harold David Quiñones Ciprián, Andrés Felipe Velasco Romero, Pablo Emilio Ospina Rodríguez, Jeimy Adriana Linares Vergara, Sergio Ernesto Mesa Bernal, Blanca Nidia Prieto Alfonso, José Luis Cabra López, David Orlando Bernal Bohorquez, Wendy Vanessa Moreno Ramírez, Emily Tatiana Ricardo Mena, Andrés Felipe Robayo Perdomo, Anyela Andrea Tuso Saldaña, Jhon Alexander Hernández Martín, Santiago Bellaizan Chaparro, William Andrés González Neuta, Angie Paola Rique, Edgard Mauricio Gómez Gómez, Jhon Devisson Luna Prieto, Sara Ximena Ortiz Reyes, Brandon Sneyder Quintero Mancilla, Esteban Alejandro Cardenas Lancheros, Wilson Alexander Cruz Mesa, Michael Armando Escudero Ávila, Harold David Quiñones Ciprián, Andrés Felipe Velasco Romero, José De Los Santos Solorzano Suárez, Jhojan David Chaparro Calderón, Andrés Felipe Contreras Gómez, Faiver Leguizamo Rojas, Ángela María Suescun Padilla. -- Bogotá: Fundación Universitaria Compensar, 1a.ed. 2024
220; 24 cm.
ISBN 978-958- e-ISBN 978-958-
1. Tecnología I. Tít.
607 cd

Primera edición: Bogotá, Colombia, julio de 2024
ISBN 978-958-

Esta obra de divulgación, realizado conforme a los criterios de Minciencia, presenta capítulos desarrollados por sus autores. Estos capítulos resultan de la articulación de proyectos integradores por competencias de los estudiantes de la Facultad de Ingeniería, quienes participaron en la inmersión internacional a México en el año 2023. Los planteamientos y argumentos presentados en los capítulos del libro son responsabilidad única y exclusiva de sus autores, por lo tanto, los compiladores y la Universidad que respalda esta obra actúan como un tercero de buena fe.

Compiladores: Neider Duan Barbosa Castro y Raúl Bareño Gutiérrez
Diagramación de interiores: Oscar Javier Avendaño Yossa

Los costos editoriales fueron asumidos por la Fundación Universitaria Compensar.

Impreso y hecho en Colombia
Printed and made in Colombia

Contenido

Índice de figuras

Índice de tablas

Prefacio

Es para mí un honor presentar este libro titulado "UCompensar: La academia motor en la Transformación Digital y automatización de la Industria 4.0". Esta obra es el resultado de una cuidadosa recopilación de artículos de investigación, escritos por destacados académicos y profesionales comprometidos con el estudio y análisis de los desafíos y oportunidades que emergen en el contexto de la Transformación Digital y la Industria 4.0. En la actualidad, estamos inmersos en una era de rápidos avances tecnológicos, donde la digitalización y la interconexión están transformando radicalmente la forma en que operan las organizaciones. La Transformación Digital se ha convertido en una prioridad para las empresas, y la Industria 4.0 se ha erigido como el paradigma que redefine la manera en que se gestionan y automatizan los procesos industriales. El avance de las tecnologías que impulsan esta transformación juega un papel fundamental en la mejora de los procesos empresariales y en el desarrollo y fortalecimiento de las estrategias corporativas. Estas innovaciones abren oportunidades para satisfacer las demandas de los clientes, mejorar los procesos logísticos y facilitar la gestión de las cadenas de suministro.

La Industria 4.0, ampliamente abordada en la literatura académica, se refiere a la cuarta revolución industrial impulsada por la integración tecnológica en el desarrollo de los procesos de fabricación y la transformación digital en general. La adopción de estas tecnologías es fundamental para la implementación de procesos de "fabricación inteligente", donde dispositivos, máquinas, módulos de producción y productos pueden intercambiar información de manera autónoma, desencadenar acciones y controlarse mutuamente. Aunque el término Industria 4.0 fue acuñado originalmente para abarcar la integración y adaptación generalizada de tecnologías de la información en las industrias manufactureras, también puede ser definido en función de las tendencias tecnológicas que lo conforman. En este sentido, la Industria 4.0 es una manifestación clave de la transformación digital en el ámbito industrial.

Con este enfoque, es crucial que la academia desempeñe un papel activo en comprender, analizar y difundir estos cambios. La relevancia de abordar la transformación digital desde la academia se encuentra en la preparación de futuros profesionales, la investigación y generación de ideas innovadoras, la formación de expertos cualificados y la promoción de la colaboración con la industria. Al abordar la transformación digital, la academia contribuye al desarrollo de soluciones innovadoras y prepara a las generaciones futuras para enfrentar desafíos y aprovechar oportunidades en el entorno digital en constante cambio.

Este libro se enfoca en el papel fundamental que desempeña la academia como motor impulsor de la Transformación Digital y la adopción de la Industria 4.0. Los artículos presentados abordan no solo la generación de conocimiento y la formación de profesionales capacitados en estas áreas, sino también la colaboración entre la academia y las pequeñas y medianas empresas (pymes) en Colombia, con el objetivo de fomentar la adopción de tecnologías digitales en el sector industrial. A través de diferentes perspectivas disciplinarias y enfoques metodológicos, los autores de este libro exploran una amplia gama de temas relevantes. Estos incluyen la implementación de tecnologías disruptivas, los retos de la toma de decisiones en entornos digitales, la gestión de TI en las organizaciones, así como el impacto de la analítica de datos y la migración a la nube en las pymes colombianas.

Cada artículo presenta rigurosas investigaciones que proporcionan valiosas perspectivas y recomendaciones prácticas para enfrentar los desafíos y aprovechar las oportunidades que la Transformación Digital ofrece. Los lectores encontrarán análisis profundos, casos de estudio, buenas prácticas y reflexiones críticas sobre cómo impulsar la adopción de tecnologías digitales en el entorno empresarial.

Deseo expresar mi más profundo agradecimiento a todos los autores y colaboradores que han contribuido a este libro. Su experiencia, conocimientos y dedicación han enriquecido enormemente esta recopilación. Asimismo, quiero reconocer y agradecer a la Fundación Universitaria Compensar que siempre ha respaldado y apoyado este tipo de proyectos. Esta institución se ha caracterizado siempre por su fuerte vínculo con las empresas en la generación de conocimiento. Cabe resaltar, que esta relación entre la universidad y la empresa es fundamental para el desarrollo económico, la innovación y la formación de profesionales capacitados. A través de esta colaboración, se comparten conocimientos, recursos y se

promueve la transferencia de tecnología, lo que impulsa el crecimiento empresarial y la creación de empleo en el país.

Espero sinceramente que este libro sea una fuente de inspiración y conocimiento para académicos, profesionales y líderes empresariales interesados en la Transformación Digital y la automatización de la Industria 4.0. Que los hallazgos y las reflexiones presentadas en estas páginas fomenten el diálogo, la colaboración y la acción para impulsar una industria más eficiente, competitiva y sostenible en Colombia.

PhD. Omar León
Docente Investigador
Grupo de investigación GIO
Universidad de Oviedo
Gijón, España, junio de 2023

Prólogo

En un mundo cada vez más interconectado y digitalizado, la necesidad de comprender y adaptarse a los rápidos avances tecnológicos es más imperativa que nunca. Con este objetivo en mente, el presente libro recopila las experiencias y aprendizajes de un grupo selecto de estudiantes de Ingeniería de Sistemas, Software y Telecomunicaciones que, optando por una modalidad de inmersión internacional como parte de su proceso de graduación, emprendieron un viaje de exploración y descubrimiento a México, acompañados por el decano de la Facultad de Ingeniería y Tecnología y los directores de los programas de Ingeniería de Sistemas y Telecomunicaciones.

Esta inmersión en México no fue solo un viaje físico, también un profundo viaje académico y profesional. Los estudiantes se enfrentaron al reto de observar, analizar y comparar los desarrollos tecnológicos y las prácticas de la industria 4.0 en México, con el fin de contrastarlos con la realidad de su país, Colombia. Este intercambio cultural y educativo se convirtió en una oportunidad única para que los estudiantes aplicaran y ampliaran su conocimiento, viéndolo a través de una mirada transnacional.

El presente libro es el resultado de esta enriquecedora experiencia. Cada capítulo refleja un área específica de conocimiento en la que los estudiantes se sumergieron, desglosando sus observaciones y análisis en un formato estructurado que comprende el contexto, el marco metodológico y un análisis comparativo entre Colombia y México. A través de este formato, los estudiantes no solo presentan sus hallazgos, sino que también demuestran su habilidad para llevar a cabo investigaciones profundas y articuladas con alto análisis y pensamiento crítico.

Los temas tratados en este libro abarcan desde la ciberseguridad hasta las últimas tendencias en tecnologías de la información y comunicaciones, pasando por análisis detallados de la computación en la nube, IoT y prácticas de *ethical hacking*. Cada tema ha sido seleccionado y desarrollado no solo por su relevancia en el campo de la ingeniería, sino también por su

importancia estratégica en el marco de la industria 4.0, un área que continúa remodelando el panorama industrial y empresarial a nivel global.

Este compilado es, por tanto, un testimonio del empeño y la capacidad de estos nuevos ingenieros para interpretar y contribuir al mundo de la tecnología y la innovación. Es también un reflejo del compromiso de la Facultad de Ingeniería y Tecnología de la Fundación Universitaria Compensar con la formación de profesionales capaces de navegar y sobresalir en un entorno globalizado y tecnológicamente avanzado.

Con estos argumentos, invitamos a los lectores a sumergirse en un viaje de conocimiento y descubrimiento, explorando los desafíos y oportunidades que la industria 4.0 presenta en América Latina a través de los ojos y las experiencias de estos estudiantes, para que este trabajo no solo sirva como una fuente valiosa de información y análisis, sino también como una inspiración para futuros profesionales que busquen dejar su huella en el mundo de la ingeniería y la tecnología.

Contrastando proveedores *cloud*. Una mirada hacia la ciberseguridad. Un análisis comparativo

Contrasting cloud providers. A look at cybersecurity. A comparative analysis

Martín, Yesica Andrea
Candidato a ingeniero de sistemas

Minottas, Amaya Lilian
Candidato a ingeniero de telecomunicaciones

Mora Feo, José Luis
Candidato a ingeniero de telecomunicaciones

Sapuyes Ortega, Carlos Alfredo
Candidato a ingeniero de telecomunicaciones

Bareño Gutiérrez, Raúl
Docente del programa de ingeniería de sistemas

Resumen

El crecimiento exponencial de los ciberataques en la región presenta desafíos a la hora de tomar decisiones para implementar servicios en la nube. Los proveedores de servicios de *cloud computing* gestionan los problemas y riesgos de seguridad de la nube como una responsabilidad compartida. Generalmente, cubren la seguridad de la nube misma y los clientes cubren la seguridad de lo que ponen en ella.

La facilidad al acceso de estos servicios *cloud*, al estar expuestos a internet sin la capacitación adecuada para contratar e implementar en las empresas, suele dejarla vulnerable, presentando deficiencias en sus sistemas y procesos internos de ciberseguridad, ocasionando riesgos y amenazas de manera frecuente. Por ello, las empresas buscan reducir costos y salvaguardar la información, para lo cual se deben diseñar soluciones de ciberseguridad más rigurosas cuando se trata de migrar servicios hacia entornos *cloud*.

Basados en la metodología de Barbara Kitchenham, se efectuó una revisión en diferentes fuentes bibliográficas relacionadas con casos de estudio a empresas que tienen contratados estos servicios y autores que han investigado sobre los riesgos del *cloud computing*. Finalmente, en los principales proveedores de *cloud computing*, como Amazon Web Services (AWS), Microsoft Azure y Google Cloud, se contrastaron sus fortalezas y debilidades en ciberseguridad a nivel de Plataforma como Servicio (PaaS), Infraestructura como Servicio (IaaS) y Software como Servicio (SaaS), determinando las características distintivas a nivel de seguridad y cumplimiento de cada proveedor, que permitan a interesados tomar decisiones alineadas a sus necesidades y al *core* de sus negocios.

Palabras claves: *servicios cloud, ciberseguridad, confidencialidad, integridad, disponibilidad, proveedores***.**

Abstract

The exponential growth of cyberattacks in the region presents challenges when making decisions to implement cloud services. Cloud Computing service providers manage cloud security issues and risks as a shared responsibility.

Generally, they cover the security of the cloud itself and customers cover the security of what they put in it.

The ease of access to these Cloud services, being exposed to the Internet without adequate training to hire and implement in companies, usually leaves them vulnerable, presenting deficiencies in their internal cybersecurity systems and processes, frequently causing risks and threats. For this reason, companies seek to reduce costs and safeguard information, to which more rigorous cybersecurity solutions must be designed when migrating services to Cloud environments.

Based on Barbara Kitchenham's methodology, a review was carried out in different bibliographic sources related to case studies of companies that have contracted these services and authors who have investigated the risks of Cloud Computing. Finally, the main Cloud Computing providers such as: Amazon Web Service (AWS), Microsoft Azure and Google Cloud, their strengths and weaknesses in cybersecurity were contrasted at the level of Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS), determining the distinctive characteristics at the level of security and compliance of each provider, which allow interested parties to make decisions aligned with their needs and the core of their businesses.

Keywords: *cloud services, cybersecurity, confidentiality, integrity, availability, providers.*

Cursos articulados

Para llevar a cabo el proyecto "CONTRASTANDO PROVEEDORES *CLOUD*: UNA MIRADA HACIA LA CIBERSEGURIDAD, UN ANÁLISIS COMPARATIVO", se requiere una combinación de cursos que aborden aspectos esenciales de seguridad de la información, legislación de telecomunicaciones, auditoría de sistemas, economía para ingenieros, gestión de proyectos y tecnologías de la información. Estos cursos proporcionarán la base necesaria para evaluar y comparar de manera integral los proveedores de servicios en la nube desde perspectivas técnicas, legales y económicas, asegurando la seguridad y eficiencia del proyecto.

Introducción

Los entorno *cloud computing* son un modelo de entrega de servicios de computación a través de internet que permite a las organizaciones y personas acceder a recursos de computación como servidores, almacenamiento y redes sin tener que invertir en su propia infraestructura.

Los primeros servicios en la nube aparecieron en la década de 1990, pero no fue hasta la década de los 2000 que la nube se convirtió en una tecnología generalizada (Survu, 2023). En el 2000, la empresa de Amazon Web Services lanzó el servicio de infraestructura (IaaS) en la nube llamado Amazon Elastic Compute Cloud (Survu, 2023). Este servicio fue un momento de cambio en la historia de la nube, ya que hizo que la computación en la nube fuera más accesible para las organizaciones.

Los servicios en la nube se ofrecen en tres modelos principales:

- **Infraestructura como servicio (IaaS):** este modelo proporciona a los usuarios acceso a recursos de infraestructura, como servidores, almacenamiento y redes.

  Los usuarios son responsables de instalar y administrar su propio *software* y aplicaciones, brindando flexibilidad y control sobre sus recursos de TI de manera rentable (Amazon Web Services, s. f.-c).

- **Plataforma como servicio (PaaS):** es un entorno en la nube que incluye todo lo que los desarrolladores necesitan para crear, ejecutar y gestionar aplicaciones, desde servicios y sistemas operativos, incluyendo redes, herramientas y más dentro de una plataforma expuesta por un proveedor de servicio en la nube (Google Cloud, s. f.-b). Los usuarios son responsables de proporcionar su propio *software* y datos.

- **Software como servicio (SaaS):** este modelo proporciona a los usuarios acceso a *software* funcional, como lo son correos electrónicos, calendarios, herramientas ofimáticas como Office 365. Los usuarios no necesitan instalar ni administrar ningún *software*. SaaS ofrece una solución de *software* integral que se adquiere de un proveedor mediante un modelo de pago por uso, permitiendo una conexión mediante internet; el proveedor administra el *hardware* y el *software* garantizando la disponibilidad y la seguridad de la aplicación eliminando esta responsabilidad del usuario (Microsoft Azure, s. f.-b).

La flexibilidad y escalabilidad son las dos mayores ventajas competitivas que puede ofrecer la computación en la nube, dándonos agilidad en los procesos y una amplia disponibilidad siempre, sin depender de instalaciones propias y físicas que representan altos costos en instalación, implementación y mantenimiento (Flores, 2020).

La seguridad en la nube es un aspecto primordial en el proceso de adopción de tecnologías en la nube. Un estudio de Market Research Future señala que "… la seguridad es uno de los factores clave que influyen en la adopción de soluciones en la nube..." (Market Research Future, 2021), resaltando la necesidad de comprender y comparar las medidas de seguridad ofrecidas por diferentes proveedores de servicios en la nube. La realización de un comparativo permitirá identificar cuál de estas plataformas brinda un conjunto de herramientas y protocolos más sólidos para proteger los datos sensibles y mitigar posibles riesgos de ciberseguridad.

La integridad de los datos es otro aspecto importante en la adopción de soluciones en la nube. Un artículo en IEEE afirma que "… la integridad de los datos es esencial para garantizar la precisión, coherencia y confiabilidad de la información almacenada en la nube..." (Pena *et al.*, 2019); un análisis comparativo permitirá evaluar cómo cada plataforma aborda la verificación y el mantenimiento de la integridad de los datos, considerando factores como la detección de cambios no autorizados y la prevención de manipulación no deseada.

La disponibilidad de servicios en la nube es crucial para mantener la continuidad del negocio y la satisfacción del cliente; basados en el informe de Gartner, "… la disponib*ilidad de servicios es uno de los principales indicadores de rendimiento para la nube...*" (Gartner Inc., 2020). Realizar una comparativa exhaustiva entre Amazon Web Services, Google Cloud y Microsoft Azure, en términos de sus estrategias de disponibilidad y sus capacidades para gestionar cargas de trabajo en todo momento, permitirá a las organizaciones seleccionar la plataforma que mejor se adapte a sus necesidades y requerimientos de tiempo de actividad.

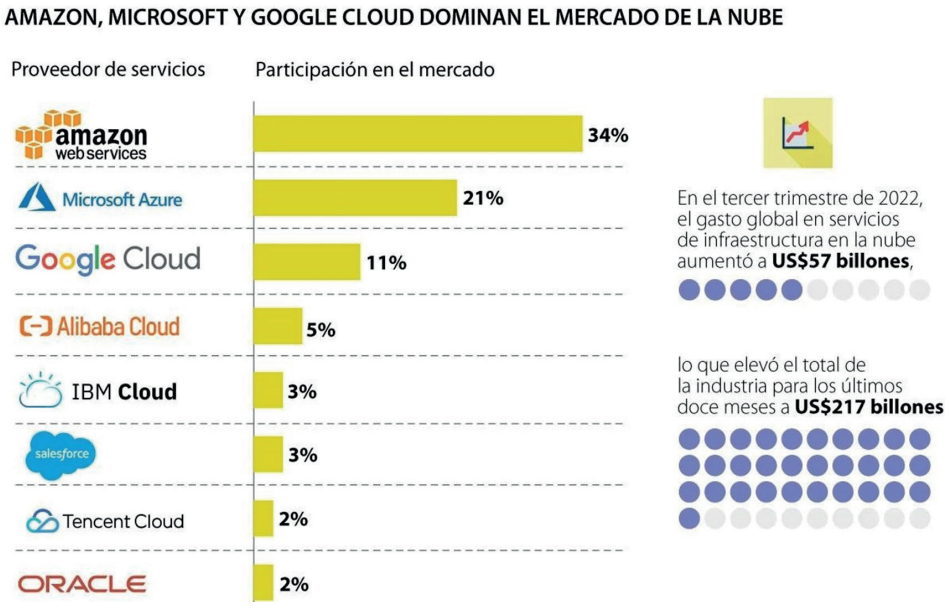
En primera instancia, los servicios en la nube pueden dar una sensación inferior de seguridad, ya que el cliente pierde el control de la seguridad de sus recursos físicos y este pasa a ser responsabilidad del proveedor contratado para la migración de los servicios en la nube (Aguilar, 2018). Sin embargo, las políticas del proveedor están bien definidas y las ejecutan fielmente, por lo que trabajar en la nube supondrá una mejor seguridad.

La seguridad proviene de la interacción entre el cliente y el proveedor, ya que, al momento de llevar los datos a la nube, se deben especificar las necesidades de seguridad y con estas el proveedor diseña un servicio específico para el cliente u organización (Aguilar, 2018; Amazon Web Services, s. f.-d).

El avance tecnológico ha impulsado a que más empresas migren sus servicios hacia entornos *cloud*, permitiendo una mayor competitividad en el mercado, al ofrecer servicios de alta calidad a un menor costo.

La digitalización de la sociedad y de la industria ha venido generando desafíos y oportunidades de mejora para el sector industrial, permitiendo adaptabilidad en los procesos, productos y modelos de negocio ayudando a generar un nuevo modelo industrial eficiente y con mejores beneficios económicos (Telefónica, s. f.). Como parte del gran reto en la industria, Google Cloud proporciona una de las mejores experiencias digitales para los consumidores, reduciendo costos y complejidad, generando nuevos flujos de ingresos digitales y ayudando a que sus clientes logren la transformación digital con las soluciones en la nube (Google Cloud, s. f.-d).

Figura 1. Participación en el mercado de servicios cloud para el año 2022



Nota. Por D. P. Rodríguez (2023). "Amazon Web, Microsoft y Google lideran el mercado de infraestructura en la nube". Diario La República.

Como parte principal de esta investigación, se toma como referencia a tres proveedores claves en la industria de servicios *cloud*, así como se evidencia en la imagen anterior:

Con base en la figura 1, se destaca que los proveedores de servicios *cloud* líderes en el mercado para el año 2022 eran Amazon Web Services, Microsoft Azure y Google Cloud, con la cuota de mercado principal en servicios IaaS y PaaS y en la parte de SaaS liderando Microsoft Azure; esta información es relevante para el desarrollo e investigación de casos de estudio relacionados con estos tres grandes tecnológicos y las soluciones que ofrecen mediante el uso de servicios y, principalmente, qué niveles de cumplimiento en seguridad brindan de cara a las organizaciones.

En los casos de estudio encontrados, podemos presentar a un grande de la industria automotriz como Volkswagen, que está utilizando el aprendizaje automático con el objetivo de diseñar automóviles más eficientes energéticamente (Menzel, 2022) por medio de los servicios de Google Cloud. Otro caso de estudio de Google Cloud en la industria es la ayuda tecnológica con la organización de grandes cantidades de información física de manera simplificada, como lo aplicó Toyota al manual del automóvil. El manual en papel ha sido reemplazado por una experiencia digital activada por voz que tiene una mejor accesibilidad y usabilidad (Wee, 2021).

Por parte del sector alimenticio, podemos destacar un caso de estudio del Grupo Bimbo y su implementación de una solución junto a Amazon Web Services para los problemas de atención al cliente, reduciendo en un 75 % los abandonos de llamadas, permitiendo mejorar la experiencia del cliente (Amazon Web Services, 2022).

También se encuentran casos de estudio de Coca-Cola Andina, que unificó el 95 % de sus datos adoptando inteligencia artificial, *machine learning* y otros servicios de análisis contratados con Amazon Web Services para mejorar la toma de decisiones, aumentando la productividad del equipo de análisis en un 80 % (Amazon Web Services, 2021).

Otro caso de estudio fue el que implementó Bosch en el sector de la seguridad vial, desarrollando un sistema que detectara cuándo un vehículo iba en sentido contrario en una carretera; este sistema requirió la solución de Azure Kubernetes Services para reducir los tiempos de procesamiento y notificación (Microsoft Azure, 2019). Bosch implementó un sistema que le permitía obtener información detallada en tiempo real sobre el clima y estado de las

carreteras usando Azure Data Explorer, aumentando la disponibilidad de las funciones de conducción automatizada (Microsoft Azure, 2020).

De acuerdo con los casos de estudio anteriormente nombrados, se presenta relación con los sectores que forman parte de nuestra investigación basada en una inmersión internacional a Ciudad de México, en el marco de una visita que permite contrastar aspectos de ciberseguridad en las organizaciones objeto de la visita, conocer los servicios en la nube que utilizan y los controles de seguridad implementados en comparación con los recomendados por los proveedores de servicios de *cloud computing*.

Todo ello enfocado en realizar un análisis comparativo detallado a nivel de seguridad, integridad y disponibilidad en tres de los principales proveedores de servicios en la nube: Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP).

La investigación se centrará exclusivamente en validar aspectos de ciberseguridad y su comparativa entre Amazon Web Services, Microsoft Azure y Google Cloud Platform.

Metodología

Para abordar el estudio sobre los proveedores de servicios *cloud* y contrastar aspectos de ciberseguridad específicamente basados en la confidencialidad, integridad y autenticación, se hace uso de la metodología propuesta por Barbara Kitchenham.

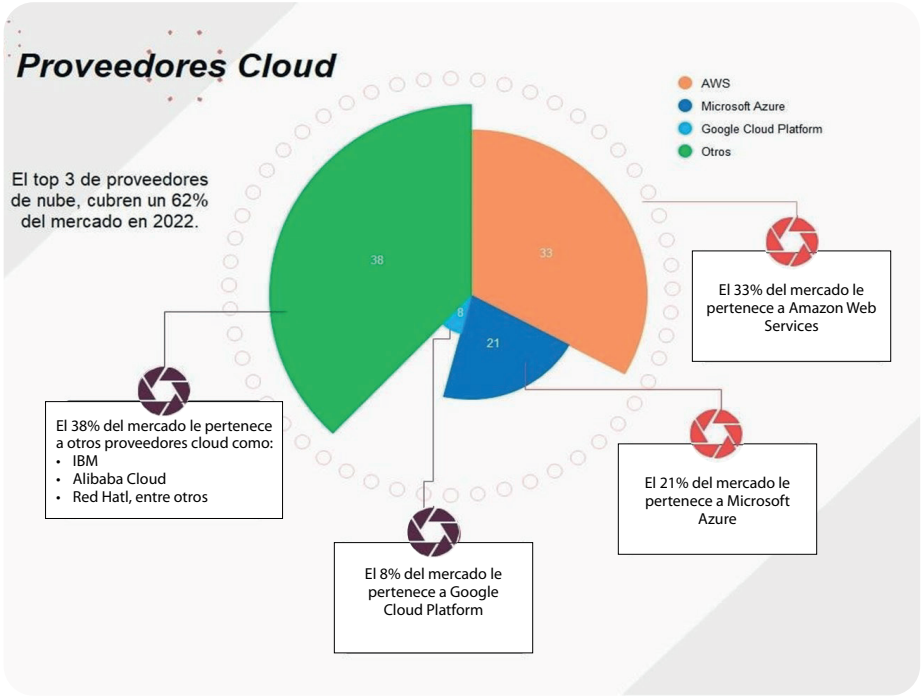
Se efectuó una serie de búsquedas de carácter tanto cualitativo como cuantitativo articulado con la selección de la literatura pertinente y científica, informes técnicos y documentación relacionada con la seguridad de los diferentes proveedores como Amazon Web Services (AWS), Microsoft Azure y Google Cloud, así como los estándares y marcos relevantes en la industria de la seguridad en la nube.

Se aplicaron criterios de inclusión y exclusión sobre bases de datos especializadas para seleccionar los estudios relevantes, con compuertas lógicas y otros parámetros de búsqueda que permitieron identificar fuentes relevantes relacionadas con la seguridad de forma coherente y comprensible basados en SaaS, IaaS y PaaS.

Resultados

El negocio de *cloud computing* crece cada año y, a su vez, los proveedores de servicios *cloud* se ven obligados a suplir las diferentes necesidades que surgen en el mercado (Rodríguez, 2019). Para el año 2022, uno de los proveedores más grandes como es Amazon Web Services (con el 33 % del mercado) se ha posicionado como el dominador del mercado en servicios *cloud*, seguido por Microsoft Azure (21 %) y Google Cloud (8 %).

Figura 2. Los proveedores cloud más grandes para el año 2022



Nota. Por Martínez (2023b). Evolución y futuro de los proveedores cloud.

Según Martínez (2023b), se evidencia el posicionamiento de los proveedores de servicios *cloud* más grandes para el 2022 y el porcentaje aproximado de cuota de mercado con respecto a los otros proveedores. Estos tres proveedores dominantes ofrecen una amplia gama de servicios en la nube que han transformado la forma en que las empresas operan. Sin embargo, a pesar de las ventajas significativas de la nube, como la escalabilidad y la flexibilidad, también existen desafíos como la seguridad. Considerando

que cada uno de los modelos de *cloud* cuenta con características únicas y demás (ver tabla 1), se puede tomar la información sobre las ventajas y desventajas que se deben tener en cuenta al momento de decidir aplicar la implementación del modelo en la empresa. Por medio del siguiente cuadro se visualiza al detalle:

Tabla 1. Comparativo de las ventajas y desventajas de SaaS, PaaS e IaaS

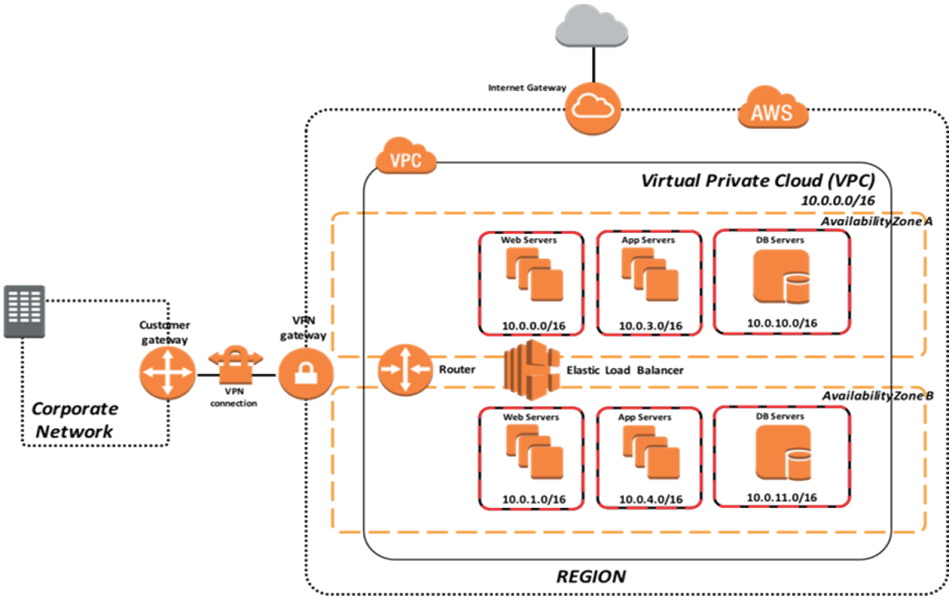
Servicio	Ventajas	Desventajas
Software como servicio	Cuenta con una buena y eficiente compatibilidad. Accesibilidad desde cualquier parte del mundo. Reduce la adquisición de licenciamiento. Depende de internet y capacidad para su conectividad.	No es posible aplicar cambios en el sistema. Si es masiva, afecta a todo personal del servicio. El proveedor del servicio es quien modifica el código fuente.
Plataforma como servicio	No requiere de infraestructura física. Pueden adquirirse solo los servicios que se requieren. El software construido es multitenant y escalable.	Dependencia del soporte del proveedor respecto a fallos. Puede tener un problema de seguridad en sus datos.
Infraestructura como servicio	No requiere de inversiones en hardware. Menos inconvenientes de seguridad de la información. El software construido es multitenant y escalable.	Depende del proveedor respecto a la disponibilidad y seguridad en el servicio. Menor control sobre la infraestructura. Posibles intermitencias de servicio que ocasionan que los usuarios no puedan acceder a sus datos.

Nota. Microsoft Azure (s. f.-b-c-d), Amazon Web Services (s. f.-f) y Virtasant (2022). Información recopilada de la documentación de los proveedores de servicios cloud.

Explorar las ventajas y desventajas de los servicios en la nube arroja luz sobre un panorama complejo. La flexibilidad y reducción de costos son atractivas, pero preocupaciones sobre seguridad y privacidad también están presentes. La topología de cómo funcionan las máquinas virtuales

en este contexto es esencial; revela la infraestructura que respalda estas ventajas y desventajas, destacando la importancia de comprender su funcionamiento para tomar decisiones informadas en la gestión de servicios en la nube.

Figura 3. Entorno virtual del proveedor Amazon Web Services



Nota. Amazon Web Services (s. f.-b). Topología de cómo funcionan las máquinas virtuales de una manera remota a través de cloud en AWS.

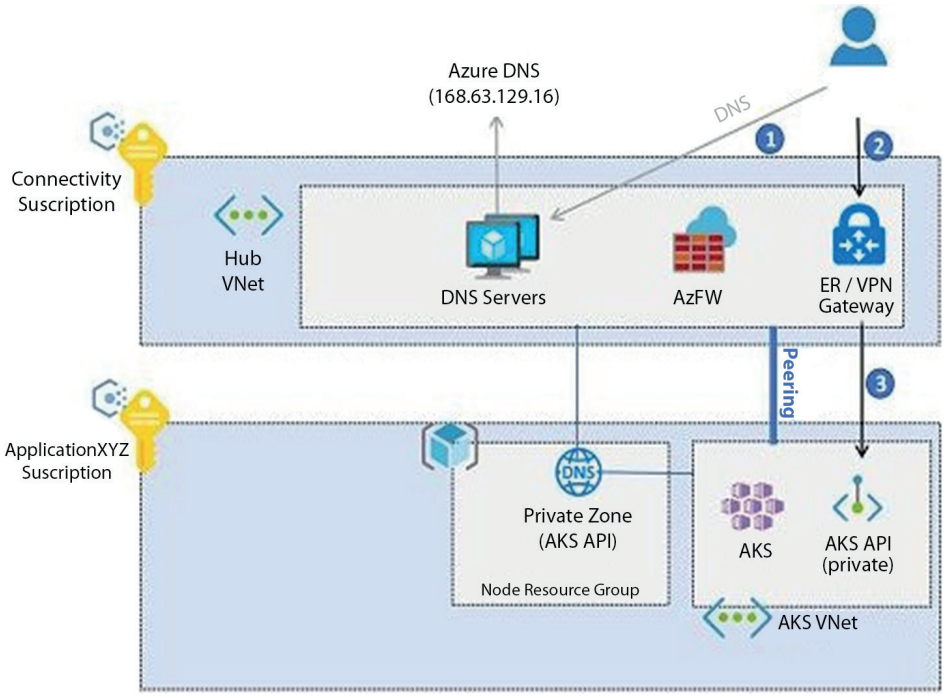
En la figura 3, se visualiza una réplica de la red que tiene el cliente, cuyo acceso el proveedor lo realiza por medio de una conexión VPN cifrada, que permite a un administrador por parte del cliente acceder a entornos virtuales (VPC). Ofrece control sobre los recursos virtuales incluyendo la red, el almacenamiento y la ubicación donde van a quedar alojados los recursos.

A nivel de seguridad, esta topología divide cada uno de los recursos de los servidores en entornos seguros del proveedor, utilizando grupos de seguridad sobre el acceso de la red. Se pueden establecer listas de control de acceso (ACL), para permitir o denegar tráfico entrante o saliente.

Según la figura 4, se muestra una solución basada en un Azure Kubernetes Service (AKS) de un *clúster* privado; al ser un *clúster* privado, lo que se hace es exponer una API de Kubernetes mediante una IP privada, por medio

de la cual solo se tendrá acceso por medio de su dominio completo "*Fully Qualified Domain Name*" (FQDN); la IP que se resuelve sobre dicho dominio y es configurada en la zona de DNS privado de Azure (Balunywa, 2023).

Figura 4. Topología *clúster* de Azure Kubernetes Services (AKS)



Nota. Balunywa (2023). Configuración de los clústeres a través de Azure Kubernetes Services.

Además, se observa cómo configurar una red virtual por medio de servidores DNS; adicional, brinda un acceso de administrador vía API sobre los Kubernetes de AKS; es un modelo de conectividad en estrella de red.

Según la tabla 2, se muestra un comparativo detallado sobre la triada de seguridad en las plataformas de servicios en la nube Amazon Web Services, Microsoft Azure y Google Cloud, lo cual es esencial para tomar decisiones informadas en la elección de una plataforma adecuada.

Dada la importancia crítica de estos aspectos en la adopción de la nube, un análisis completo y basado en evidencia resulta fundamental para garantizar la protección de los datos, la integridad de la información y la continuidad de los servicios empresariales.

Tabla 2. Comparativo detallado sobre la triada de seguridad en las plataformas de servicios en la nube

Amazon Web Services	Ventajas	Desventajas
Autenticación	Se confirma su identidad mediante el uso de algún tipo de credencial.	Los servicios en la nube son seguros por defecto.
Confidencialidad	Los estándares están protegidos por seguridad 2/3.	Riesgos de las amenazas online.
Integridad	Usan los metadatos disponibles: almacenamiento de origen. Sumas de verificación. Tamaños de archivos.	Complejidad de su integración con los sistemas actuales.
Disponibilidad	Establece el 99,9 % de disponibilidad para la interconexión dedicada.	Control sobre la infraestructura subyacente.

Nota. Amazon (web propia) (s. f-f), Microsoft Azure (s. f.-a) y Google Cloud (s. f.-d). Recopilado de documentación de cada proveedor cloud.

De acuerdo con la información encontrada en la documentación de cada uno de los proveedores de servicio como Amazon Web Services, Google Cloud y Microsoft Azure con relación a las ventajas y desventajas de cada proveedor, estas se resumen en la tabla 3.

Tabla 3. Ventajas y desventajas de proveedores cloud

Proveedor	Ventajas	Desventajas
Amazon Web Services	Seguridad, escalabilidad, flexibilidad, rendimiento, fiabilidad, respaldo y recuperación, seguridad y actualizaciones constantes.	Soporte deficiente, complejo de usar, gran dependencia del proveedor, reducción del tiempo necesario para despliegue y distribución entre servidores
Google Cloud	Seguridad, escalabilidad, rendimiento, respaldo y recuperación.	Sin soporte directo, documentación, curva de aprendizaje.
Microsoft Azure	Seguridad, adaptabilidad y escalabilidad	Costos, soporte, curva de aprendizaje

Nota. Google Cloud (s. f.-d) y Espin (2023). Descripción resumida de las ventajas y desventajas de servicios cloud.

De acuerdo con la información de la tabla 3, se destaca que Amazon Web Services es uno de los proveedores principales de servicios *cloud* en el mundo. Ofrece una amplia variedad de servicios que permiten a las organizaciones migrar hacia entornos *cloud* y a los desarrolladores les ofrece poder ejecutar aplicaciones y almacenar datos de manera rentable, segura y escalable (Amazon Web Services). Sin embargo, como cualquier plataforma tecnológica, AWS tiene sus ventajas y desventajas:

- **Ventajas de Amazon Web Services:**

  - ✓ Flexibilidad: permite seleccionar el sistema operativo y recursos que se requieran implementar a la solución de la organización, facilitando el proceso de migración de las aplicaciones (Amazon Web Services).

  - ✓ Escalabilidad y alto desempeño: permite escalar recursos de manera dinámica según la necesidad de la organización, posibilitando el aumento o reducción de la capacidad informática de manera rápida y eficiente (Amazon Web Services). También se adapta a los picos de alto tráfico o demanda.

  - ✓ Seguridad: AWS mantiene una innovación e inversión constante en seguridad para sus servicios (Amazon Web Services).

  - ✓ Respaldo y recuperación: AWS administra soluciones de respaldo y recuperación escalable. Como parte de su estrategia de protección de datos, encontramos que los datos puede estar replicados en al menos tres zonas de disponibilidad a nivel geográfico (Nizami, 2023).

- **Desventajas de Amazon Web Service:**

  - ✓ Costos variables: debido a que el portafolio de servicios por AWS no tiene ninguna restricción en su uso, es poco conveniente para un usuario inexperto, dada la dificultad de ver los gastos mensuales porque la tarifa de uso es variable (Gartner, 2023). Sin una gestión adecuada, los gastos pueden aumentar.

En los proveedores de servicios *cloud*, un grande tecnológico como Google Cloud se destaca por el uso de *big data*, herramientas de analíticas o *machine learning* (Rodríguez, 2019). A continuación, detallaremos sus ventajas y desventajas en el mercado:

- **Ventajas de Google Cloud:**

  - ✓ Seguridad: provee alto nivel de seguridad y protección de datos. Ofrece una plataforma de seguridad moderna para detectar amenazas, así como investigarlas y responder a ellas (Google Cloud).

  - ✓ Escalabilidad: la plataforma ofrecida por Google como lo es Google Cloud Platform (GCP) está dedicada a la expansión y escalabilidad (Espin, 2023).

  - ✓ Respaldo y recuperación: ofrece copias de seguridad automáticas con estándares de seguridad para las organizaciones.

- **Desventajas de Google Cloud:**

  - ✓ Documentación: para los usuarios puede llegar a ser confusa, con carencias en referencias y ejemplos (Gartner, 2023).

  - ✓ Soporte: no se cuenta con una línea directa de soporte (Gartner, 2023).

Por otro lado, en otro gran proveedor de servicios como Microsoft Azure, podemos encontrar una diferenciación notable en comparación con los servicios ofrecidos por Amazon Web Services. Sin embargo, también podemos abordar las siguientes ventajas y desventajas de este grande tecnológico:

- **Ventajas de Microsoft Azure:**

  - ✓ Seguridad: Azure cuenta con varias capas de seguridad para proteger los datos y sistemas por medio de encriptación y autenticación avanzada (Espin, 2023).

  - ✓ Adaptabilidad y escalabilidad: permite aumentar o disminuir los recursos de computación y almacenamiento de acuerdo con las necesidades de la organización (Espin, 2023).

- **Desventajas de Microsoft Azure:**

  - ✓ Soporte: debido a la lenta respuesta por parte del soporte de Azure a sus clientes, se han provocado pérdidas de dinero e inconformidad con el servicio contratado (Gartner, 2022).

La nube es una herramienta poderosa que puede ayudar a las organizaciones a ahorrar dinero, mejorar la eficiencia y mejorar la flexibilidad (Kaspersky). Sin embargo, también puede ser un objetivo atractivo para los ciberdelincuentes. La seguridad en la nube está dedicada a proteger los sistemas informáticos en la nube, incluyendo el mantenimiento de los datos privados y seguros en la infraestructura, las aplicaciones y las plataformas en línea (Kaspersky). En la tabla 4 se observan los aspectos más relevantes en cuanto a servicios se seguridad y autenticación de cada proveedor:

Tabla 4. Aspectos de seguridad, autenticación y cumplimiento de cada proveedor cloud

Aspectos	Amazon Web Services	Google Cloud	Microsoft Azure
Servicios destacados en seguridad	IAM, WAF, Security Hub.	Security Command Center.	Azure Security Center.
Servicios destacados de autenticación	Amazon Cognito, Amazon Identity and Access Management (IAM), AWS Secret Manager.	Google Cloud, Identity and Access Management (IAM), Cloud Key Management Services (KMS).	Azure Active Directory, B2C, Azure Key Vault, Azure ActiveDirectory Connect.
Ciberseguridad	Alta puntuación en seguridad.	Destacado en detección y mitigación de amenazas.	Fuerte en seguridad de infraestructura.
Estrategias de cumplimiento	Certificaciones: ISO 27001, Service Organization Control Type 2 (SOC 2).	Certificaciones: ISO 27001. Cumplimiento: Health Insurance Portability and Accountability Act (HIPAA), Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS).	Certificaciones ISO 27001, Service Organization Control Type 2 (SOC 2) Cumplimiento: reglamento general de protección de datos GDPR.

Nota. Google Cloud (s. f.-c), Microsoft Azure (s. f.-a) y Amazon Web Services (s. f.-d, e). Recopilado de documentación propia de cada proveedor cloud.

Se evidencia en la tabla 4 que los proveedores ofrecen una variedad de servicios y características relacionadas con el cumplimiento y la seguridad; significa que estos proveedores cumplen con los estándares de seguridad, privacidad de datos y aplicaciones de clientes.

También cuentan con información de cumplimiento de manera pública en sus páginas web. Finalmente, respecto a la seguridad, se puede contar con múltiples certificaciones que permiten a un cliente tener la confianza de poder entregar sus datos en la nube.

Cabe resaltar que la responsabilidad en la nube es compartida entre los proveedores y los clientes (Kaspersky). Los proveedores tienen la responsabilidad de implementar medidas de seguridad para proteger los datos y los sistemas y los clientes tienen la responsabilidad de tomar medidas para proteger sus datos y sistemas internos.

Con base en la información recopilada en la inmersión internacional, se obtienen los siguientes resultados; por un lado, tenemos industrias que en sí mismas son diferentes, pero que en medio de sus procesos a nivel tecnológico y de crecimiento se han apoyado en la tecnología e incluso, como lo son Bosch y KIO, proveen su propia tecnología y sistemas de almacenamiento en *cloud*.

Bosch en Colombia, en el año 2023, ha tomado fuerza liderando soluciones en movilidad en la feria de autopartes más grande de Latinoamérica (Bosch, 2023), presentando un amplio portafolio de componentes Bosch para vehículos pesados y livianos. Esta innovación ha sido impulsada gracias a su estructura cada vez más digitalizada, lo que ofrece a los clientes un sistema de gestión único e integrado (Bosch, 2023).

Bosch, como uno de los pioneros en los vehículos autónomos, ha desarrollado sistemas propios como Odín para la gestión interna y expuesta a sus clientes, pero también ha recurrido a proveedores de terceros como AWS con el reto de identificar de manera temprana las posibles causas de los problemas en las nuevas series de vehículos (Amazon Web Services, 2021).

En la experiencia de inmersión internacional en el país de México, quedó claro que la implementación en empresas y universidades se basa en la industria 4.0, especialmente en el KIO Data Center, que se enfoca en la automatización, el aprendizaje automático de *big data* como servicio en la nube y utiliza como centro de almacenamiento Amazon Web Services al 80 %.

Esto garantiza al centro de datos la máxima disponibilidad, seguridad contra desastres naturales y alta redundancia en todos sus componentes, como: conexiones de datos, almacenamiento, aire acondicionado, energía eléctrica, etc. En el Centro de Operaciones de Seguridad (SOC) manejan *firewall*, protección antivirus de sitios web, *antispam*, análisis forense, VPN; el dominio es kio.tech; además, los dispositivos Fortinet se utilizan como dispositivos de seguridad que permiten construir redes seguras y brindar atención integral e implementación integrada de protección contra amenazas.

Discusión

Considerando cada uno de los puntos expuestos sobre el documento bajo el cual se puede asegurar que los servicios *cloud* cuentan con varias características dentro de la seguridad, se destaca en la tabla 5 el punto de vista desde otros países y la manera en la que mantienen su cumplimiento de reglas y mejores prácticas bajo cada servicio.

Tabla 5. Revisión documental de uso de servicios cloud y seguridad en Europa, África y América

Autor	Título	Palabras clave	País	Conclusiones
Justus Haucap, Daniel Fritz y Susanne Thorwarth	The economic impact of cloud computing in europe. A research report commissioned by the European Cloud Alliance	Hyperscalers, pymes, servicios	Europa	La industria europea de la nube (IaaS e hyperscalers, PaaS) está dominada por tres grandes operadores ("hyperscalers"): Amazon Web Services ("Amazon"), Microsoft Azure ("Microsoft") y Google Cloud Platform ("Google"). Los servicios PaaS representan el segmento más pequeño de servicios de computación en la nube en Europa.
International	An interactive view of cloud computing in Africa	Africa, cloud computing, data center, Microsoft, Silicon Valley, technology	África	Tienen como proveedor de servicios cloud principal a Microsoft Azure, gracias a la instalación de un centro de datos en el continente.

Autor	Título	Palabras clave	País	Conclusiones
Davin Olën	South Africa: Cloud regulation and POPIA – What remote computing services need to know	Vendor management, data transfers	Sudáfrica	Para julio de 2022, la Ley de Protección de Información Personal 4 de 2013 ("POPIA") acoge a los proveedores de servicios cloud dentro del cumplimiento.
J. M. Martínez Corona, O. G. Delgado Cansino, R. Aragón Paulín y M. Arriaga Flores	Arquitectura de servidores en la nube IaaS	Instancia VM, instancia SKU, SLA, CSP	México	Obligatorio para organizaciones que contraten los servicios y para proveedores, por medio de una responsabilidad compartida que garantice la disponibilidad y seguridad de la información. Teniendo en cuenta el uso de la infraestructura como servicio, se puede bridar al usuario un entorno capaz de administrar sus propios recursos y por medio de los supuestos de Gowin establecer los puntos necesarios para establecer conexiones, orientar planificaciones y, finalmente, comprender el IaaS como servicio.

Nota. Martínez Corona et al. (2020), International Finance (2021), South Africa: Cloud regulation and POPIA - What remote computing (2022) y Copenhagen Economics (2019). Fuentes consultadas para la revisión de uso de servicios cloud.

La computación en la nube, en la parte de América del Norte, según lo mencionado por Martínez Corona *et al.* (2020) sobre la arquitectura en la nube de los servicios de infraestructura como servicio, cuenta con un control de seguridad por medio de *cloud-trust* el cual permite a un administrador tomar decisiones de cuál sería la mejor alternativa para poder contar con un factor de autenticación, los cuales se cifran por medio de llaves cifradas; cada uno de los fabricantes cuenta con un sistema único bajo el cual permite reforzar el sistema de logueo dentro de la infraestructura.

De manera adicional, en el continente africano se encuentra un gran apoyo por parte de Microsoft aportando a la computación en la nube con la instalación de centros de datos, lo que ha impulsado un crecimiento tecnológico, tal y como lo expresan en la revista *International Finance* (2021):

"Desde que Microsoft abrió sus oficinas en África, hemos sido testigos de un crecimiento increíble en el continente: más conectividad a internet, más capacidad digital y más innovación". Además, exponen cuatro pilares que permitirían al continente avanzar en el desarrollo tecnológico, proporcionando seguridad en los datos y garantizando la privacidad y confiabilidad con acceso a internet.

Según el marco regulatorio sobre el procesamiento de información bajo la Ley de Protección de Información Personal 4 de 2013 ("POPIA") en Sudáfrica, se reconoce el impacto directo sobre los servicios en la nube y las regulaciones que deben seguir las organizaciones que usan estos servicios, al igual que los proveedores, promoviendo las medidas de seguridad necesarias para garantizar la integridad y confidencialidad de la información.

También dan claridad sobre: "… las Partes Responsables deben tomar medidas técnicas y organizativas apropiadas y razonables para evitar el procesamiento, acceso o alteración ilícita de los datos" (*South Africa: Cloud regulation and POPIA - What remote computing*, 2022), lo que garantiza que la responsabilidad sea compartida entre el cliente y el proveedor.

Google ha invertido mucho en centros de datos y de infraestructura relacionada en Europa en los últimos años. Por ejemplo, se han construido enormes centros de datos a hiperescala en Dublín, Irlanda o en Eemshaven-Groningen (Países Bajos). En total, Google invirtió 6.900 millones de euros entre 2007 y 2018 (Copenhagen Economics, 2019).

Conclusiones

Google Cloud fue el de más rápido crecimiento, encontrándose dentro de los tres principales proveedores de servicios *cloud* en el mundo, representando el 8 % del mercado. Continúa centrándose en la soberanía digital, el análisis, la IA y la ciberseguridad como diferenciadores clave para Google Cloud, avanzando en su práctica de ciberseguridad en la nube.

Google Cloud tiene ventaja respecto al pago de consumo a largo plazo porque tiene descuentos provechosos que, con ayuda del rendimiento mejorado, permite asegurar un punto clave sobre el aprovechamiento de la capacidad de las máquinas virtuales y cuenta con seguridad de extremo a extremo que permitirá respaldar la información óptima, cifrada y dispo-

nible cuando el usuario la requiera, considerando también cada capa con nivel de seguridad que, al tener una amplia conexión de red a nivel mundial, le asegura al cliente usar una nube ubicada en la región.

La operatividad del servicio a nivel de red es muy importante; sin la información actualizada, se tarda más en los procesos para las mejoras a nivel de calidad del servicio. De igual forma, se requiere de una base de datos con el almacenamiento en la nube; este es un servicio de análisis y almacenamiento de datos orientado a proporcionar visualizaciones interactivas y capacidades de inteligencia empresarial con una interfaz lo suficientemente simple para que los usuarios finales a nivel empresarial. No es una infraestructura costosa. Es accesible, pero con la cuenta correspondiente empresarial. Permite la recuperación de datos. Garantiza la seguridad, no se usan recursos físicos, ya que se pueden reutilizar los mismos que brinda la compañía.

Ejecutando cada uno de los análisis sobre los modelos que se indagaron en el documento (IaaS, SaaS, PaaS), es relevante concluir que se cuenta con características únicas bajo cada uno de los servicios que ofrece Google Cloud Platform. Luego de generar el estudio comparativo, se observó una gran ventaja que ofrece el fabricante sobre las soluciones: costos y beneficios. Además, mediante cada certificación del fabricante, se puede determinar la confiabilidad sobre cada servicio en los modelos soportados que permiten administrar, desplegar y desarrollar de manera más efectiva y segura, cumpliendo con los estándares necesarios para mantenerse en un entorno confiable que garantice un esquema de ciberseguridad para proteger datos.

A pesar de su entrada tardía al mercado de servicios *cloud*, Google ha logrado predominar entre los servicios preferidos por los usuarios, gracias también a la cantidad de documentación y entrenamientos que brinda de manera gratuita a la comunidad, lo que ha permitido posicionar a Google Cloud Platform como el preferido en diferentes industrias, como logramos ver en los casos de uso, siendo predominante en el desarrollo de inteligencia artificial y soluciones de automatización.

Referencias

Aguilar, L. J. (2018, 14 de noviembre). *Computación en la nube: notas para una estrategia española en cloud computing*. https://revista.ieee.es/article/view/406

Amazon Web Services (s. f.-a). *Cloud Security – Amazon Web Services (AWS)*. Amazon Web Services, Inc. https://aws.amazon.com/security/

Amazon Web Services (s. f.-b). *Componentes de arquitectura – AWS. Guía prescriptiva*. https://docs.aws.amazon.com/es_es/prescriptive-guidance/latest/data-storage-decoupling-sas-fsx/architecture- components.html

Amazon Web Services (s. f.-c). *¿Qué es la IAAS? Explicación de la infraestructura como servicio - AWS*. Amazon Web Services, Inc. https://aws.amazon.com/es/what- is/iaas/#:~:text=Plataforma%20como%20servicio%20(PaaS)%2 0proporciona, en%20su%20centro%20de%20datos

Amazon Web Services (s. f.-d). *Seguridad en la nube - Amazon Web Services (AWS)*. Amazon Web Services, Inc. https://aws.amazon.com/es/security/

Amazon Web Services (s. f.-e). *Visión general de los beneficios*. Amazon Web Services, Inc. https://aws.amazon.com/es/application-hosting/benefits/

Amazon Web Services (s. f.-f). *What is SAAS? - Software as a service explained - AWS*. Amazon Web Services, Inc. https://aws.amazon.com/what- is/saas/#:~:text=Software%20as%20a%20Service%20(SaaS,customers%20t o%20access%20on%2Ddemand

Amazon Web Services (2021). "Coca-Cola Andina crea lagos de datos en AWS y aumenta la productividad de análisis en un 80 % para mejorar la toma de decisiones basada en datos". https://aws.amazon.com/es/solutions/case-studies-coca-cola-andina-case-study/

Amazon Web Services (2022). "Grupo Bimbo reduce en un 75 % los abandonos de llamadas y mejora la experiencia del cliente". https://aws.amazon.com/es/solutions/case-studies/grupobimbo

Balunywa (2023, 25 de mayo). *Topología de red y conectividad para Azure Kubernetes Service (AKS) - Cloud Adoption Framework*. Microsoft Learn. https://learn.microsoft.com/es-es/azure/cloud-adoption- framework/scenarios/app-platform/aks/network-topology-and-connectivity

Carleo, G., Cirac, I., Cranmer, K., Daudet, L., Schuld, M., Tishby, N. ... & Zdeborová, L. (2019). "Machine learning and the physical sciences". *Reviews of Modern Physics*, 91(4), 045002.

Celma, M. E. S., Cruz, F. A. & Bussière, Y. D. (2020). "El impacto de la instalación de Audi México en la Economía de Puebla-Tlaxcala". *TRANSITARE*, 5(1), 22-49.

Copenhagen Economics (2019). "Google's hyperscale data centres and infrastructure ecosystem in Europe". https://copenhageneconomics.com/wp-content/uploads/2021/12/copenhagen-economics-google-european[1]dcsinfrastructures-impact-study_september2019.pdf

Espin, A. S. (2023). *Análisis comparativo de las plataformas Amazon Cloud, Google Cloud, Azure Cloud*. https://www.dspace.utb.edu.ec/handle/49000/14184

Flores, J. M. (2020). *Arquitectura de servicios en la nube IaaS*. https://www.eumed.net/uploads/articulos/79219e032d3c4652cde034fe3d-dd33d4.pdf

Gartner Inc. (2020). *Magic Quadrant for Cloud Infrastructure and Platform Services*. Gartner. https://www.gartner.com/en/documents/3985595/ma gic-quadrant-for-cloud-infrastructure-and-platform-ser

Gartner, Inc. (2022, 1 de septiembre). *Support service is not up to the mark*. Gartner. https://www.gartner.com/reviews/market/cloud-infrastructure-and-platform-services/vendor/microsoft/product/azure/review/view/4385388

Gartner, Inc. (2023a, 31 de marzo). *Worst web services on the market. AWS*. Gartner. https://www.gartner.com/reviews/market/cloud-infrastructure-and-platform-services/vendor/amazon-web-services/product/amazon-web- services/review/view/4669100

Gartner, Inc. (2023b, 19 de abril). *Great public cloud with some specific quirks*. Gartner. https://www.gartner.com/reviews/market/cloud-infrastructure-and-platform-services/vendor/google/product/google-cloud-platform/review/view/4703314

Gartner, Inc. (2023c, 19 de abril). *The ultimate cloud computing service*. Gartner. https://www.gartner.com/reviews/market/cloud-infrastructure-and-platform-services/vendor/amazon-web-services/product/amazon-web-services/review/view/4703360

Gartner, Inc. (2023d, 27 de abril). *A scalable cloud platform*. Gartner. https://www.gartner.com/reviews/market/cloud-infrastructure-and-platform-services/vendor/microsoft/product/azure/review/view/4427120

Gartner, Inc. (2023e, 7 de junio). *Google cloud the standard platform for small business and many larger organizations*. Gartner. https://www.gartner.com/reviews/market/cloud-infrastructure-and-platform-services/vendor/google/product/google-cloud-platform/review/view/4791432

Gartner, Inc. (2023f, 7 de julio). *A tool that does job advertised*. Gartner. https://www.gartner.com/reviews/market/cloud-infrastructure-and-platform- services/vendor/amazon-web-services/product/amazon-web- services/review/vew/4862086

Gartner, Inc. (2023g, 24 de julio). *Powerfull and versatile cloud provider*. Gartner. https://www.gartner.com/reviews/market/cloud-infrastructure-and-platform- services/vendor/google/product/google-cloud-platform/review/view/4887412

Gartner, Inc. (2023h, 18 de agosto). *Amazon Web Services review in cloud infrastructure and platform services*. Gartner. https://www.gartner.com/reviews/market/cloud-infrastructure-and-platform-services/vendor/amazon-web-services/product/amazon-web-services/review/view/4935600

Google Cloud (s. f.-a). *Industria automotriz*. Google Cloud. https://cloud.google.com/solutions/automotive?hl=es- 419#:~:text=el%20siguiente%20paso-Google%20Cloud%20para%20la%20industria%20automotriz,las%20solucion es%20de%20Google%20Cloud

Google Cloud (s. f.-b). *¿Qué es una PAAS?* Google Cloud. https://cloud.google.com/learn/what-is- paas?hl=es#:~:text=Plataforma%20como%20servicio %20(PaaS)%20es,%2C%20middleware%2C%20herramientas%20y%20m%C3%A1s

Google Cloud (s. f.-c). *Security, privacy, and Cloud Compliance*. Google Cloud. https://cloud.google.com/security

Google Cloud (s. f.-d). *Ventajas de Google Cloud*. Google Cloud. https://cloud.google.com/why-google-cloud?hl=es-419

International Finance (2021, 18 de febrero). "An Interactive view of cloud computing in Africa". https://internationalfinance.com/magazine/technology-magazine/an- interactive-view-of-cloud-computing-in-africa/

Kaspersky (2023, 19 de abril). *¿Qué es la seguridad en la nube?* latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/what-is -cloud-security

Market Research Future (2021). *Smart Appliances Market Report Size, Share and Trends 2030*. https://www.marketresearchfuture.com/reports/cloud -security- market-1049

Martínez Corona, J. M., Delgado Cansino, O. G., Aragón Paulín, R. & Arriaga Flores, M. (2020). "Arquitectura de servidores en la nube IAAS". *Revista Académico-Científica Tectzapic*. https://www.eumed.net/uploads/articulos/79219e032d3c4652cde034fe3ddd33 d4.pdf

Martínez, J. (2023b, 3 de abril). *Evolución y futuro de los proveedores cloud*.

OpenWebinars.net. https://openwebinars.net/blog/evolucion-y-futuro-de-los -proveedores-cloud/

Menzel, A. A. (2022, 27 de septiembre). "Cómo Volkswagen y Google Cloud están utilizando el aprendizaje automático para diseñar automóviles más eficientes energéticamente". https://cloud.google.com/blog/products/ai-machine- learning/volkswagen/uses-google-cloud-ai-for-more-efficient-cards?hl=en

Microsoft Azure (s. f.-a). *Azure Security*. https://azure.microsoft.com/en-us/trust- center/security/

Microsoft Azure (s. f.-b). *¿Qué es SaaS?* https://azure.microsoft.com/en- us/resources/cloud-computing-dictionary/what-is-saas

Microsoft Azure (s. f.-c). *What is IaaS?* https://azure.microsoft.com/en- us/resources/cloud-computing-dictionary/what-is-iaas

Microsoft Azure (s. f.-d). *What is PaaS?* https://azure.microsoft.com/en- us/resources/cloud-computing-dictionary/what-is-paas/

Microsoft Azure (2019, 31 de octubre). *Microsoft Customer Stories*. https://customers.microsoft.com/en-us/story-765209-bosch-increases-vehicle-safety-using-map-matching-algorithms-and-azure-kubernetes-service

Microsoft Azure (2020, 19 de mayo). *Better forecasting, safer driving with Bosch*.

Microsoft Customers Stories. https://customers.microsoft.com/en- us/story/816933-bosch-automotive-azure-germany

Nizami, K. (2023, abril). *Enfoques de respaldo y recuperación en AWS - AWS Guía Prescriptiva*. https://docs.aws.amazon.com/es_es/prescriptive-guidance/latest/backup-recovery/welcome.html

Pena, R. G., Rivera, D., Gani, A. & Yeo, C. S. (2019). "Data Integrity Protection in Cloud Storage: Challenges, Techniques, and Future Trends". *IEEE Access*, 7, 178031-178043.

Rodríguez, D. P. (2023, 14 de enero). "Amazon Web, Microsoft y Google lideran el mercado de infraestructura en la nube". *Diario La República*. https://www.larepublica.co/internet-economy/amazon-web-microsoft-y-google-lideran-el-mercado-de-infraestructura-en-la-nube-3522658

Rodríguez, T. (2019). "La otra guerra entre Microsoft, Google y Amazon: la batalla por controlar los servicios en la nube para…". Xataka. https://www.xataka.com/servicios/otra-guerra-microsoft-google-amazon-batalla-controlar-servicios-nube-para-desarrolladores

Rosete, N. L. R. *Impacto socioterritorial ante la instalación de Audi en Puebla*.

South Africa: Cloud regulation and POPIA - What remote computing (2022, 20 de diciembre). DataGuidance. https://www.dataguidance.com/opinion/south-africa-cloud-regulation-and-popia-what-remote

Survu, M. S. (2023). *Cloud Computing Concept to Reality: A Historical perspective*. www.linkedin.com. https://www.linkedin.com/pulse/cloud-compu ting-concept-reality-historical-manohar-survi-l-i-o-n-

Telefónica (s. f.). *Transformación digital para el sector automotriz*. https://www.ane.gov.co/Sliders/archivos/gestionConocimiento/SectoresProductivos/2021/8%20JULIO%20TALLER%20AUTOMOTRIZ/Transformaci%C3%B3n%20Digital%20-%20Automotriz%20(1).pdf

Virtasant (2022, 27 de enero). *IAAS vs. PAAS vs. SAAS: A complete overview*. Virtasant. https://www.virtasant.com/blog/iaas-vs-paas-vs-saas-a-complete-overview

Wee, D. (2021, 22 de julio). *Google Cloud Blog*. https://cloud.google.com/blog/topics/manufacturing/toyota-modernizes-the-card-manual-with-google- cloud?hl=en

Ciberseguridad en industrias 4.0: Análisis comparativo para industrias manufactureras en Colombia y México

Cybersecurity in industries 4.0: Comparative analysis for manufacturing industries in Colombia and Mexico

Cruz Mesa, Wilson Alexander
Canditado a ingeniero de software

Escudero Ávila, Michael Armando
Candidato a ingeniero de software

Quiñones Ciprián, Harold David
Candidato a ingeniero de software

Velasco Romero, Andrés Felipe
Candidato a ingeniero de software

Ospina Rodríguez, Pablo Emilio
Docente del programa de ingeniería de telecomunicaciones

Resumen

Este documento busca aportar una perspectiva comparativa alrededor de la temática de ciberseguridad, considerando el estado actual, a partir de visitas presenciales y remotas mediadas por tecnología, realizadas específicamente para este fin en algunas de las industrias de Colombia y México. La recopilación realizada abarca una serie de aspectos críticos que incluyen: la adopción de tecnologías asociadas a la industria 4.0, estado actual de ciberseguridad, capacitación del personal de las compañías en materia de seguridad digital, consideración de amenazas de ataques cibernéticos y normativas vigentes que aplican tanto a nivel local como internacional. Este análisis se focaliza en la ciberseguridad dentro del sector manufacturero, con el propósito de comprender la situación actual en ambos países. Asimismo, se plantean recomendaciones como fruto de la comparativa en las visitas realizadas, que buscan concientizar sobre algunos aspectos sensibles de implementación para fortalecer las buenas prácticas en ciberseguridad de las empresas manufactureras de ambos países.

Palabras clave: *ciberseguridad, vulnerabilidades, industria 4.0, capacitación.*

Abstract

This document seeks to provide a comparative perspective on the topic of cybersecurity, considering the current state, based on in-person and remote visits mediated by technology, conducted specifically for this purpose, in some of the industries in Colombia and Mexico. The Compilation conducted covers a series of critical aspects that include: the adoption of technologies associated with Industry 4.0, the current state of cybersecurity, training of company personnel in digital security, consideration of threats of cyber-attacks, and current regulations that apply both locally and internationally. This analysis focuses on cybersecurity within the manufacturing sector, with the purpose of understanding the current situation in both countries. Likewise, recommendations are made because of the comparison in the visits conducted, which seek to raise awareness about some sensitive aspects of implementation to strengthen good practices in cybersecurity of manufacturing companies in both countries.

Keywords: *cybersecurity, vulnerabilities, industry 4.0, training.*

Cursos articulados

Para el desarrollo de este documento, se aprovecharon los conocimientos y formación ingenieril obtenida al cursar y aprobar diferentes materias durante la carrera de las cuales se destacan las siguientes por su aplicabilidad: Introducción a las Telecomunicaciones, Metodología para el Manejo de la Información, Introducción a Redes de Datos, *Switching and Routing*, Instalación de Antenas y Telefonía, Sistemas Digitales, Administración y Gestión de Redes, Comunicaciones Análogas y Digitales, Administración y Servicios de Servidores, Estadística y Probabilidades, Interconexión de Redes WAN, Aplicaciones en Sistemas Embebidos, Seguridad en Redes de Telecomunicaciones, Electiva 2 (*Cloud Computing*), Seguridad de la Información, Ondas y Campos Electromagnéticos, Servicios en Sistemas de Telecomunicaciones, Diseño de Redes de Banda Ancha, Teoría de la Información y las Comunicaciones, Diseño de Proyectos, Gestión de Proyectos e Inglés I, II, III, que permitieron organizar y analizar en profundidad la información recopilada en función de las técnicas adquiridas.

Introducción

La creciente importancia de la seguridad informática en el ámbito global es innegable; la interconexión de sistemas y la adopción de tecnologías de vanguardia, como las asociadas a las industrias 4.0, son aspectos clave. En América Latina, las pequeñas y medianas empresas (pymes) representan más del 95 % de las empresas registradas (Mendoza & Cuellar, 2020).

A pesar de esto, muchas de estas pymes aún no han integrado en sus procesos y cultura empresarial este tipo de tecnologías que, lejos de ser innovaciones futuristas, son elementos esenciales que están transformando significativamente los procesos operativos a nivel global, implementando sistemas de automatización en la mayoría de las operaciones empresariales. En este escenario, se busca realizar una evaluación comparativa del estado de implementación y adopción de la seguridad informática en las industrias manufactureras en dos países clave de América Latina: Colombia y México. El objetivo es identificar áreas de mejora y detectar puntos de interés que faciliten un avance progresivo y continuo, adaptado a las necesidades específicas del entorno empresarial y su influencia sobre la economía, la sociedad y, en general, los diferentes *stakeholders* implicados.

El análisis actual surge de la necesidad de comprender y abordar las amenazas y desafíos que enfrentan las empresas manufactureras en Latinoamérica en cuanto a seguridad industrial y ciberseguridad. A medida que las industrias evolucionan hacia la digitalización y la automatización, su exposición a ataques cibernéticos se intensifica, lo que pone en riesgo la integridad de los datos, considerados el activo más crítico para cualquier empresa (Cisco Systems, Inc., 2020). Estos datos no solo respaldan la continuidad operativa, sino que garantizan la seguridad, confiabilidad e integridad en la información de estas y, por ende, en la de sus empleados.

Metodología

Siguiendo la estructura de análisis propuesta por la autora Barbara Kitchenham, se llevó a cabo una evaluación comparativa del estado de seguridad en las industrias 4.0 de México y Colombia. En este proceso, se examinaron varios aspectos clave, como las convergencias tecnológicas para optimizar procesos.

En primer lugar, se evaluó el nivel de adopción de las tecnologías asociadas a la industria 4.0 en ambas naciones. Esto permitió comprender el grado de implementación de innovaciones tecnológicas en sus respectivas industrias. Luego, se analizaron las medidas de ciberseguridad que estas implementan hoy en día. Se indagó cómo están protegiendo sus sistemas y datos contra posibles amenazas cibernéticas, reconociendo la importancia de salvaguardar la información crítica; además se llevó a cabo un análisis del nivel de capacitación del personal en materia de seguridad informática digital, evaluando la preparación y el conocimiento de los empleados en la prevención y mitigación de riesgos cibernéticos. Se ha destacado la importancia significativa de la seguridad informática en el contexto de esta investigación, reconociendo su papel central en la protección de datos y la continuidad de las operaciones empresariales. En esta etapa, se llevó a cabo una exploración en bases de datos académicas y otras fuentes relevantes de información. Esto incluyó consultar bases de datos académicas reconocidas como Google Academic, IEEE Xplore, Web of Science, Scopus, ProQuest y ACM Digital Library. También se examinaron recursos locales, como bases de datos universitarias, con el fin de abarcar tanto investigaciones globales como locales relacionadas con la ciberseguridad. Es importante resaltar que la búsqueda se limita a partir del año 2019, toda vez que cuenten con palabras claves como: "ciberseguridad", "vulnerabilidades", "industria 4.0", "capacitación de seguridad", "*cybersecurity*".

Se seleccionaron estudios que abordaron aspectos críticos de seguridad de la información y ciberseguridad en Colombia y México, tales como la adopción de tecnologías de la industria 4.0, cuestiones de ciberseguridad, capacitación del personal en seguridad digital y la consideración de amenazas de ataques cibernéticos a nivel global. Se dio prioridad a los estudios que presentaban propuestas concretas de soluciones o estrategias relacionadas con la ciberseguridad en estos dos países. Se incluyeron estudios en español e inglés, los idiomas pertinentes para Colombia y México.

Se realiza un proceso ordenado para obtener información importante de cada artículo encontrado. Esta información puede abarcar eventos relevantes, resultados específicos, datos estadísticos y detalles sobre cómo se llevaron a cabo, información demográfica y cualquier otro dato que tenga relevancia en el contexto del presente documento. Esta extracción de datos de manera sistemática es crucial en el desarrollo de revisiones, ya que permite reunir datos de diversas fuentes de manera coherente y organizada.

Se realiza una evaluación de la calidad metodológica de los estudios incluidos gracias al modelo de metodología adoptado. Esta evaluación es importante para determinar la calidad y la validez de los estudios que se utilizan en el presente documento. Una vez validadas las fuentes de información consultadas, se logra verificar que los artículos y fuentes citadas en este documento cumplen con las características tanto de la temática planteada como del tiempo mínimo requerido de cinco años para la autenticidad de la información.

Se realiza un análisis cuidadoso de la información recopilada de los artículos y estudios encontrados y posterior a ello se elabora un resumen coherente que proporciona una visión general de la comparativa realizada entre los países mencionados.

Resultados

Contextualización y estado del arte

Al referirnos al índice global de ciberseguridad del 2020 publicado por la Unión Internacional de Telecomunicaciones (UIT), observamos que “Más de la mitad de los países del mundo cuentan ahora con un equipo de

respuesta a incidentes informáticos (CIRT) y casi dos tercios tienen algún tipo de estrategia nacional de ciberseguridad que orienta su postura general en este ámbito" (International Telecommunication Union, 2020, pág. 4). Sin embargo, es evidente que existe una marcada disparidad en el ámbito de la ciberseguridad entre estos.

De todos los países de América Latina, los que ostentan las calificaciones más altas en este dominio, según las evaluaciones efectuadas por la Unión Internacional de Telecomunicaciones (UIT) bajo el nombre de Índice de Ciberseguridad Global (GCI, por sus siglas en inglés), son los siguientes: Brasil, el cual ocupa la posición más destacada situándose en el puesto número 18, México en la posición 52 y Colombia en la posición 81, ubicándose por debajo de naciones como Chile y Uruguay en el referido índice (International Telecommunication Union, 2020).

Aunado a ello, los ciberataques que más ocurrieron en la última década corresponden a *ransomware*, instalación de *malware* o *software* dañino, *spyware*, alteración de componentes e inestabilidad en los equipos, el *phishing*, los ataques de intermediario, los ataques de denegación del servicio, inyección de SQL, ataques de día cero y tunelización de DNS. Se debe tener en cuenta que la mayoría de este tipo de ataques proviene de un error humano por desconocimiento u omisión, entre otros, que abren la puerta a que el atacante pueda realizar su labor. De la misma forma, es imperioso mencionar que el 53 % de los ciberataques exitosos dan como resultado daños que sobrepasan los USD 500.000 (Cisco Systems, Inc., 2020).

Normatividad

La importancia de la normatividad en el ámbito de la ciberseguridad no puede ser subestimada, ya que es una pieza fundamental para garantizar la protección de la información sensible y la continuidad de las operaciones en un mundo cada vez más digitalizado. Entrando en este contexto, en Colombia, algunas de las normas clave incluyen la Ley 1273 de 2009 (Congreso de la República de Colombia, 2009), que aborda los delitos informáticos y la ciberseguridad, y la Norma Técnica Colombiana NTC-ISO/IEC 27001, que se enfoca en la gestión de la seguridad de la información (ICONTEC, 2022). En México, algunas de las normativas que aplican son: la Ley de Protección de Datos Personales en Posesión de Particulares, junto con la norma mexicana NMX-I-27018-NYCE-2021, la cual establece un conjunto de reglas que brinda directrices sobre cómo proteger los datos personales cuando se almacenan

en servicios de nube pública, especialmente cuando estos servicios son responsables del manejo de esos datos (Secretaría de Economía, 2022).

Estos estándares se basan en la norma internacional ISO/IEC 27018:2019, que fue desarrollada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) (International Organization for Standardization, 2019). Estas normativas proporcionan un marco legal y técnico que las organizaciones deben seguir para proteger la información y responder a incidentes de ciberseguridad de manera adecuada.

Por otra parte, se establece la norma ISO/IEC 27032:2023, la cual es un estándar a nivel global que ofrece directrices para garantizar la seguridad en el uso de internet. Esta norma se aplica a todas las organizaciones, sin importar su tamaño, sector o ubicación. En resumen, aborda una amplia gama de temas relacionados con la seguridad en línea, como la identificación y evaluación de riesgos, la implementación de medidas de seguridad, la gestión de incidentes de seguridad y la capacitación en ciberseguridad.

Al adoptar esta norma, las organizaciones pueden beneficiarse de una mayor protección de la información y los datos, una reducción en el riesgo de ataques cibernéticos, un aumento en la confianza de los clientes y socios comerciales, así como el cumplimiento de regulaciones y normativas (International Organization for Standardization, 2023).

Conferencias y visitas a campo

Durante la reciente visita realizada por el equipo que ha elaborado el presente documento al país de México, se tuvo acceso a visitar la fábrica más grande y moderna de ensamblaje de vehículos en toda América Latina y, de hecho, la única de su tipo en el continente que representa a uno de los principales exponentes de la industria automotriz con tecnología de vanguardia: Audi.

La mencionada fábrica se destaca por su nivel de automatización, que supera el 70 % en varios de sus procesos, gracias al empleo de tecnologías robóticas, *machine learning*, *cobots*, realidad virtual para el diseño e interacción con sus vehículos y conceptos de industria 4.0, donde lo describen como "La labor del área de Montaje se ve apoyada por la TI más moderna. Con «*pick by light*» y «*pick by voice*», la industria 4.0 se hace un hueco en la planta mexicana" (Audi de México, 2021).

Esta fábrica se posiciona como la única con la capacidad de fabricar el Audi Q5 a nivel mundial. Además de su impresionante eficiencia en la producción, esta instalación sobresale por sus rigurosos estándares de seguridad industrial, que han garantizado un récord impresionante: desde su inicio hace más de siete años, no se ha registrado un solo accidente grave. Durante este tiempo, la fábrica ha alcanzado la asombrosa cifra de más de un millón de vehículos fabricados.

Este logro no es solo testimonio de la excelencia en la ingeniería y producción automotriz, sino también de un enfoque hacia las industrias 5.0 que buscan la plena sostenibilidad a través de la innovación y el diseño. Audi México se ha comprometido a gestionar de manera responsable los residuos de sus productos y en abordar la obsolescencia postventa como parte de una estrategia de economía circular.

Este compromiso se ve en esta fábrica, que recicla el 95 % de sus residuos y la energía de las más de 460 hectáreas de esta, la cual es totalmente producida por ellos mediante celdas fotovoltaicas. Gran parte de lo visto durante esta vista puede ser consultado mediante la página web de la planta, en la que se evidencian algunos de sus procesos y estándares, además de fotografías de sus colosales naves de ensamblaje.

En lo que respecta a la seguridad informática, aunque la mayoría de información es confidencial, la empresa comparte detalles notables. Proporciona capacitaciones certificadas anuales para todos sus empleados que son obligatorias, en temas críticos como *phishing*, *smishing*, *malware* y seguridad de la información. Además, se prohíbe el uso de teléfonos móviles dentro de las instalaciones y cada usuario tiene asignados niveles de permisos específicos. Todos los datos se almacenan inmediatamente en el centro de datos principal de Audi en Alemania, con una copia local adicional.

Esto asegura que, en caso de un ataque, la empresa pueda continuar sus operaciones reduciendo el margen de afectación y garantizando la continuidad del negocio. Se mencionó un incidente reciente en el que la compañía enfrentó un ataque en su servidor principal en Alemania que duró aproximadamente 16 horas, siendo mitigado por sus ingenieros expertos. La fábrica en México se vio afectada por cinco horas, pero logró reanudar sus procesos industriales gracias a la robustez de su infraestructura y procedimientos de contingencia, dado el enfoque en la seguridad cibernética y la resiliencia demostrada por Audi México.

Otra de las visitas realizadas por el equipo fue al *data center* de KIO México a las afueras de Santiago de Querétaro, un centro de datos que se distingue por su enfoque en la seguridad, la redundancia y la continuidad de operaciones. Esta compañía cuenta con una infraestructura tecnológica de aproximadamente 5.000 m^2, dando un nivel de seguridad para que empresas mundiales de renombre como Google contraten sus servicios, teniendo presencia en más de 6 países, contando con más de 2.000 clientes *enterprise*, más de 20 centros de datos en el mundo y 20 años de experiencia en el sector.

Como dice la compañía:

> Proveemos servicios de Infraestructura de Tecnologías de Información de Misión Crítica que opera Centros de Datos en la región para administrar servicios en la Nube pública, privada e híbrida […] con presencia en México, Panamá, Guatemala, Colombia, República Dominicana y España (KIO, 2021).

Alguno de los aspectos destacables que se observaron en la visita fue el conjunto de rigurosos filtros de seguridad implementados tanto a nivel de red como en términos físicos y de acceso al *data center*. Uno de los pilares fundamentales en el funcionamiento de este es su enfoque en la redundancia; se pudo constatar que todos sus procesos están respaldados por sistemas duplicados, como la planta eléctrica, que cuenta con 10 generadores diésel que pueden respaldarse mutuamente y garantizar la alimentación de toda la infraestructura durante un período de 72 horas sin necesidad de rellenar los tanques de combustible, incluso en caso de fallo en la provisión de energía eléctrica principal.

Además, el proveedor de energía tiene múltiples puntos de acceso a la red y sistemas eléctricos independientes para asegurar la continuidad operativa. Adicional a ello, el cambio entre la energía convencional y la producida por los generadores se respalda mediante bancos de baterías de litio, los cuales, en caso necesario, inician el funcionamiento de los generadores mediante un motor de arranque alimentado por baterías, en su defecto, mediante un mecanismo similar a un arranque de motor.

El sistema de aire acondicionado del *data center* también está diseñado con redundancia en caso de una falla; si esta sucede, se activa de inmediato un sistema de respaldo para mantener las condiciones óptimas. Cuentan con una amplia gama de sensores que monitorean constantemente la temperatura, la humedad y la presencia de partículas en el aire generadas por el calentamiento de materiales aislantes y/o cualquier componente que esté dentro de las diferentes áreas del centro de datos.

En cuanto al control de acceso, se aplica un protocolo riguroso, con una seguridad sellada tanto a nivel del suelo como del aire. Las instalaciones cuentan con un avanzado sistema de cámaras de vigilancia de alta calidad y eficiencia que operan las 24 horas del día, supervisando tanto las áreas del *data center* como su topología de red interna, la cual está completamente aislada de internet, lo que proporciona una capa adicional de seguridad para mitigar posibles ataques cibernéticos y garantizar la integridad y confidencialidad de la información que alberga este centro de datos.

Contrastando las visitas realizadas en México, el equipo tuvo la oportunidad de asistir a una conferencia impartida por Carlos Sarmiento, un ejecutivo de negocios de Bosch en Colombia. Durante este encuentro, se abordaron aspectos relacionados con las industrias 4.0, poniendo énfasis en la percepción de que el país se encuentra rezagado en el proceso de transición hacia la Cuarta Revolución Industrial. Sarmiento destacó que este atraso se debe, en gran medida, al desconocimiento y temor al cambio.

El conferencista también ilustró su argumento con un ejemplo elocuente: la implementación de la industria 4.0 en un torno mecánico del siglo XIX a través de la incorporación de sensores para medir velocidad, aceleración y curvas de rendimiento logró determinar cuándo un operador alcanzaba su máxima operatividad, el momento en que empezaba a disminuir y cuándo se volvía improductivo debido al agotamiento. Estos datos permitieron definir horarios de trabajo y determinar la cantidad óptima de empleados necesarios para alcanzar objetivos específicos de producción.

Este caso ejemplifica que el proceso de industrialización se basa en capturar información y la optimización del proceso gracias al manejo de esta, implicando que no necesariamente conlleva una inversión significativa de capital. Otro punto relevante de esta charla fue la ausencia de información en cuanto a la gestión de la ciberseguridad de la compañía en Colombia, ya que no pudo proporcionar detalles sobre posibles programas de capacitación existentes en este campo, a diferencia de lo observado durante las visitas a las empresas en México.

También se toma en cuenta lo expuesto en la charla virtual dada por el docente perteneciente a la Universidad Compensar Omar León desde España referente a industrias 4.0, una revolución que no solo afecta al ámbito industrial, sino que también tiene un impacto significativo en la sociedad. Desde el control de la conducción de energía a través de materiales como el silicio hasta la evolución de la informática desde los años 70, especialmente en Colombia en los 90, se han sentado las bases de esta transformación.

La integración de computadores en organizaciones y hogares marcó el comienzo de cambios sociales, económicos y políticos, un fenómeno al que se le atribuye inicialmente el nombre de industria 4.0. La visión de la industria 4.0, originada en Alemania, no solo involucra avances tecnológicos, sino que también implica a las personas y cada elemento que la compone; la clave en este concepto es la interconexión industrial, permitiendo decisiones ágiles y soluciones rápidas, alentando a las máquinas a tomar decisiones y evolucionando el rol de las personas para estar a la vanguardia en estos procesos.

Los aspectos esenciales en esta industria incluyen la digitalización y flexibilidad, la simulación y procesamiento de datos y la eficiencia en el uso de energía y recursos. En términos de ciberseguridad, se reconoce la necesidad de un sólido trabajo a nivel cultural y social para abordar los cuidados y responsabilidades asociadas al manejo de datos en la era digital.

Antecedentes

Se evidencia que los incidentes de seguridad pueden tener consecuencias devastadoras, tanto en términos económicos como en la confianza de los consumidores y la reputación de las organizaciones. Un ejemplo reciente de esto ocurrió en México alrededor de enero del 2022, donde se llevó a cabo un ataque dirigido contra la Secretaría de la Defensa Nacional. En esta brecha de seguridad, se expuso información delicada que revelaba la creciente influencia de las fuerzas armadas en el gobierno civil, así como sus intentos de evitar cooperar en investigaciones de derechos humanos.

El ataque fue perpetrado por un grupo de piratas informáticos llamado Guacamaya y resultó en la filtración de millones de correos electrónicos y aproximadamente seis *terabytes* de datos. Estos datos expusieron detalles sobre cómo el ejército está adquiriendo un mayor control sobre las instituciones civiles y su estrecha relación con el presidente de esta época,

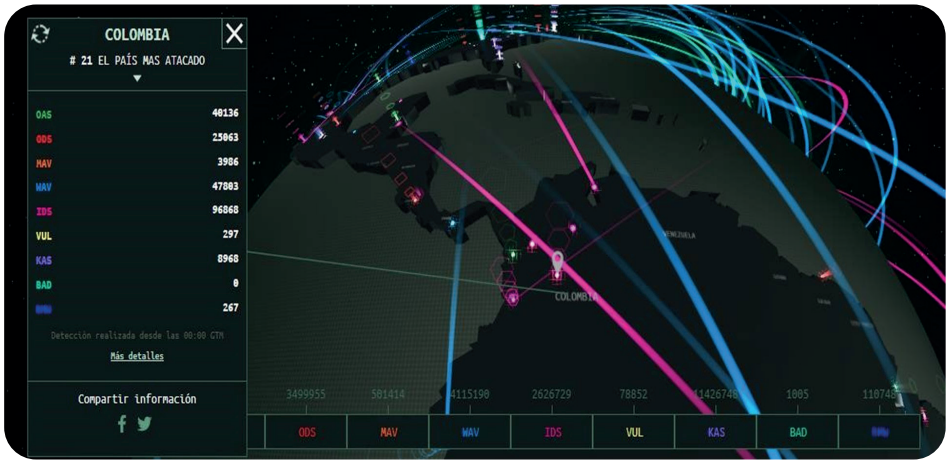
Andrés Manuel López Obrador. Además, se descubrió que el ejército estaba utilizando *software* espía, como Pegasus, para obtener información de periodistas y activistas, a pesar de las promesas previas del gobierno de no utilizar dicho programa en contra de los ciudadanos mexicanos. Este incidente resalta la importancia de la ciberseguridad y sus implicaciones en términos de seguridad nacional y derechos humanos (Abi-Hbib, 2022).

Por otra parte, se presentó un ataque cibernético el 12 de septiembre de 2023 dirigido a la compañía IFX Networks (IFX Networks, 2023), una empresa que ofrece servicios en la nube. Es importante resaltar que este ciberataque impactó negativamente sobre al menos 50 instituciones del Estado colombiano, incluyendo el Ministerio de Salud y Protección Social y el Consejo Superior de la Judicatura. Para este hecho, el ataque fue del tipo *ransomware*, en el cual los delincuentes cifraron los archivos y sistemas informáticos de la empresa y luego solicitaron un rescate para proporcionar la clave o herramienta necesaria para desbloquearlos, aunque, según la *Revista Semana* (2023), no se trató de un secuestro de datos, sino de un bloqueo para acceder a la información; también se afectó el acceso a las páginas gubernamentales y a más de 150 aplicaciones, por ejemplo, del Ministerio de Salud.

Esta situación colocó en jaque no solo a una empresa, sino a todo un Estado al tener tantas instituciones gubernamentales asociadas a esta compañía sin tener redundancia de dichos enlaces y de la información que se almacenó en los servidores del proveedor. El incidente puso de manifiesto la vulnerabilidad de la centralización de operaciones y la necesidad de abordar seriamente la seguridad en el entorno digital, lo que nos lleva a analizar "la implementación de planes de resiliencia que vienen desde la época de las Torres Gemelas, porque muchas empresas tenían sus oficinas principales en un edificio y el respaldo en otro, pero como tumbaron las dos torres, se quedaron sin nada" (Botero, 2023).

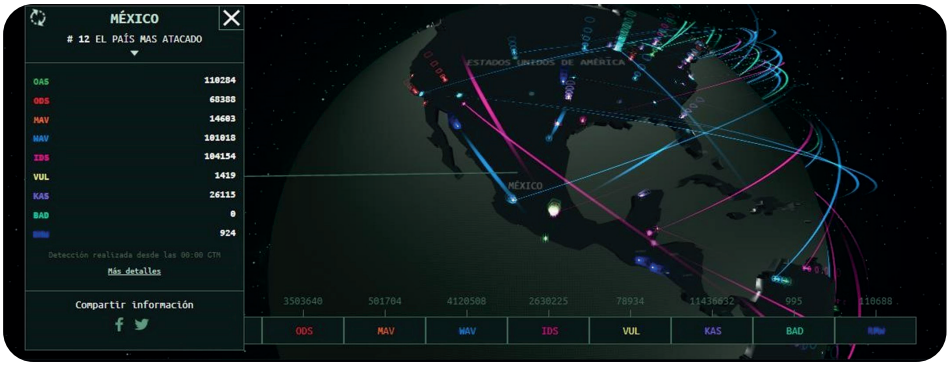
Es importante resaltar que los dos países que se están analizando (México y Colombia), a fecha de este estudio, ostentan lugares altos en la *ranking* mundial (posiciones 12 y 21 respectivamente), como se observa en la figura 5.

Figura 5. Posición de Colombia en el ranking de ataques de Kaspersky



Nota. Esta figura muestra la herramienta de Cybermap de Kaspersky donde se pueden ver en tiempo real los ataques por país de origen y destino y el ranking de Colombia. Recuperado de "Cybermap de Kaspersky" (Kaspersky Lab, 2023), (https://cybermap.kaspersky.com/es).

Figura 6. Posición de México en el ranking de ataques de Kaspersky

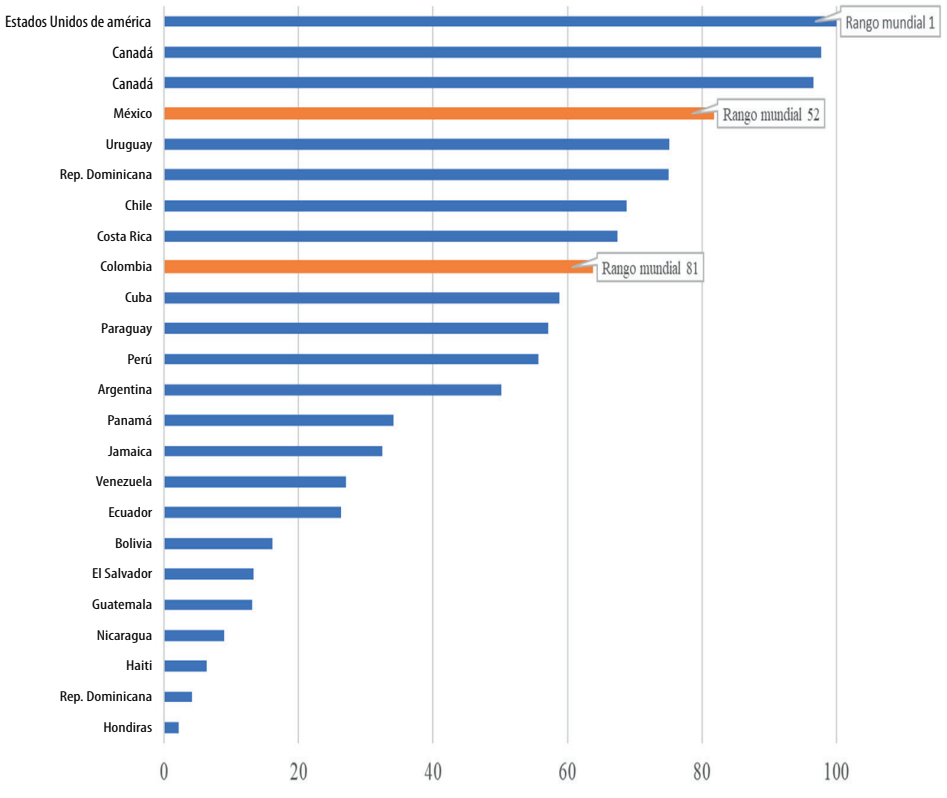


Nota. Esta figura muestra la herramienta de Cybermap de Kaspersky donde se pueden ver en tiempo real los ataques por país de origen y destino y el ranking de México. Recuperado de "Cybermap de Kaspersky" (Kaspersky Lab, 2023), (https://cybermap.kaspersky.com/es).

Además de la información proporcionada por Kaspersky, también se puede observar en la figura 7 la posición de estos dos países en un análisis realizado por la ITU en el año 2020 respecto a la fortaleza en seguridad de la información. En este análisis, México ocupó el puesto 52 y Colombia el puesto 81, haciendo notar la necesidad de implementar mejoras a nivel

de organización, capacitación y políticas que impulsen el avance en la ciberseguridad, para estar a la vanguardia en este ámbito.

Figura 7. Resultados del índice global de ciberseguridad para la región de las Américas



Nota. Esta figura muestra el ranking de ciberseguridad en las Américas, donde se valida la posición de Colombia y México. Adaptado de "Global Cybersecurity Index 2020" (International Telecommunication Union, 2020, págs. 26-28), (https://www.itu.int/epublications/publication/DSTR-GCI.01-2021-HTM-E/).

Contexto del proyecto

La importancia de esta investigación radica en la necesidad de comprender la situación actual de la seguridad en el entorno industrial de ambos países, identificando las brechas de seguridad existentes y proponiendo soluciones que puedan alertar a las compañías a una mejora en sus procedimientos

y políticas, teniendo en cuenta el giro que tomó el mundo después de la pandemia de COVID-19 volcando las empresas a la digitalización y generando un reto para las mismas al necesitar tener acceso constante a servicios en la nube desde cualquier ubicación para sus clientes y empleados, pero sin perder seguridad, mediante dispositivos confiables y protegiendo los activos empresariales contra accesos no autorizados (Tayouri, Hassidim, Smirnov & Shabtai, 2022). De la misma forma, se busca sensibilizar a las empresas de la importancia de la migración a industrias 4.0 que automaticen procesos y le den un manejo a la información que conlleve a la mejora continua sin necesidad de invertir grandes cantidades de dinero, contemplando siempre que de la mano de todo crecimiento industrial debe contemplarse un crecimiento a nivel de seguridad informática y de la red. Además, la comparativa entre Colombia y México permitirá destacar las mejores prácticas y lecciones aprendidas de ambas naciones, fomentando el intercambio de conocimientos y la mejora continua en el ámbito de la seguridad industrial.

En un mundo empresarial en constante evolución y en el marco de la Cuarta Revolución Industrial, la información y los sistemas de seguridad se han convertido en pilares fundamentales para la competitividad y la resiliencia de las organizaciones. Por lo tanto, los resultados y conclusiones de esta investigación no solo serán de gran valor para las empresas de ambos países, sino que también contribuirán al avance de la seguridad industrial en un contexto global caracterizado por las persistentes amenazas cibernéticas y la necesidad de adaptación a los cambios tecnológicos.

Discusión

Empleando el enfoque metodológico previamente explicado, se abordó el análisis de la ciberseguridad en el contexto de la industria 4.0 en Colombia y México. Durante este proceso, se reunieron datos esenciales sobre las estrategias que adoptan las grandes industrias en el ámbito de la ciberseguridad. Este análisis permite contrastar cómo las regulaciones y factores económicos influyen en las perspectivas de seguridad de la información de estas empresas.

También se destacan las diferencias clave en estos enfoques y, finalmente, los resultados fueron comparados con informes sobre ciberseguridad producidos por diversas entidades especializadas en la evaluación de países y sectores industriales en varios aspectos relacionados con la ciber-

seguridad. Por lo tanto, es imperativo evaluar de manera precisa y detallada el estado de seguridad en las industrias de estos dos países y proporcionar recomendaciones concretas para fortalecer sus sistemas y prácticas de seguridad basadas en los acontecimientos recientes y el atraso en ciberseguridad en Latinoamérica respecto a países del primer mundo desde los que provienen la gran mayoría de ataques globales.

Análisis

A continuación, se expone la comparativa a nivel de ciberseguridad entre Colombia y México permitiendo tener una visión más amplia sobre el contraste entre ambos países a la luz de las cifras recopiladas.

Tabla 6. Comparación de indicadores de ciberseguridad entre Colombia y México

Indicador	Colombia	México
Habitantes (2021)	51.049.000	126.705.138
Índice Global de Ciberseguridad (GCI)	81	52
Número de ataques cibernéticos	5.000 millones	14.000 millones
Porcentaje incidentes en organizaciones	44 %	56 %
Porcentaje recuperación incidente (horas)	25 %	20 %
Porcentaje recuperación incidente (minutos)	25 %	40 %
Porcentaje recuperación incidente (S.I./Confidencial)	50 %	40 %

Nota. Esta tabla muestra la comparación de algunos indicadores de seguridad entre Colombia y México en cuanto a incidentes de ciberseguridad en función de la población de cada país. Adaptado de International Telecommunication Union (2020), Datos Macro (2022), Lesmes Díaz (2023) y Díaz (2021).

A pesar de las expectativas iniciales, es evidente que tanto Colombia como México presentan una brecha considerable en la adopción de tecnologías de industria 4.0. Aunque México se destaca como uno de los líderes en este ámbito en el continente, en lo que respecta a la ciberseguridad, ambos

países se encuentran en una situación muy similar. Se observa una carencia significativa de cultura y concientización en materia de seguridad en las empresas, junto con políticas internas que no concuerdan con la protección adecuada de la información sensible. Además, se evidencian implementaciones inadecuadas, muchas veces a causa de personal no debidamente capacitado en seguridad cibernética.

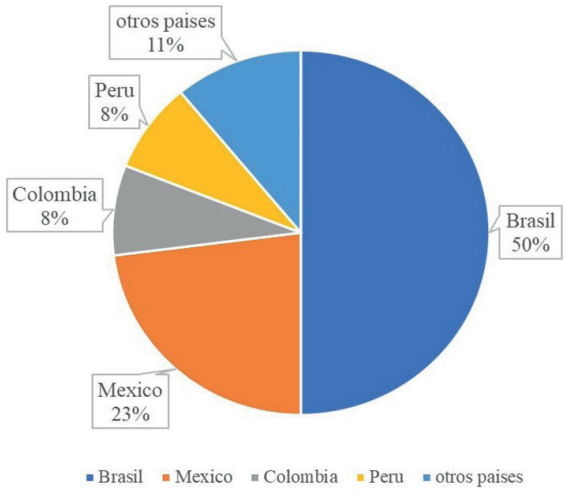
La ausencia de enlaces de redundancia y copias de seguridad de la información en ubicaciones geográficas distintas al canal principal, actualizaciones y/o cambio de *software* son fallas recurrentes en la mayoría de las empresas, ya que al implementarlas no se tienen en cuenta las comprobaciones de restricciones, buscando observar el flujo de datos y así evitar que a raíz de ellas se tengan brechas de seguridad (Ilhan & Karakose, 2019). Esta situación ha llevado a un aumento progresivo de ataques en los últimos años en los países latinoamericanos, dejando a las organizaciones cada vez más vulnerables.

Esta realidad obliga a implementar mejoras a nivel organizacional para mantenerse al día con los avances que los *hackers* han logrado en diversas formas de ataque; entre estas, el *ransomware* destaca como una de las amenazas principales y más perjudiciales para las organizaciones. Es fundamental que las empresas en Colombia y México prioricen estrategias de ciberseguridad efectivas para contrarrestar estas amenazas y proteger su información de manera integral.

Las estadísticas son alarmantes al considerar que, entre el período de 2021 y 2022, los ciberataques a países como Colombia experimentaron un aumento cercano al 25 %. Hasta el 15 de agosto de 2023, se habían registrado más de 5 millones de ataques dirigidos a la nación. Este dato es especialmente preocupante dado que aún quedaban 4 meses para finalizar el año, lo que sugiere un ritmo que indica un posible incremento continuo de ataques. A pesar de los esfuerzos realizados para implementar mejoras a nivel organizacional con el fin de prevenir y mitigar estos ataques, la tendencia al alza parece persistir.

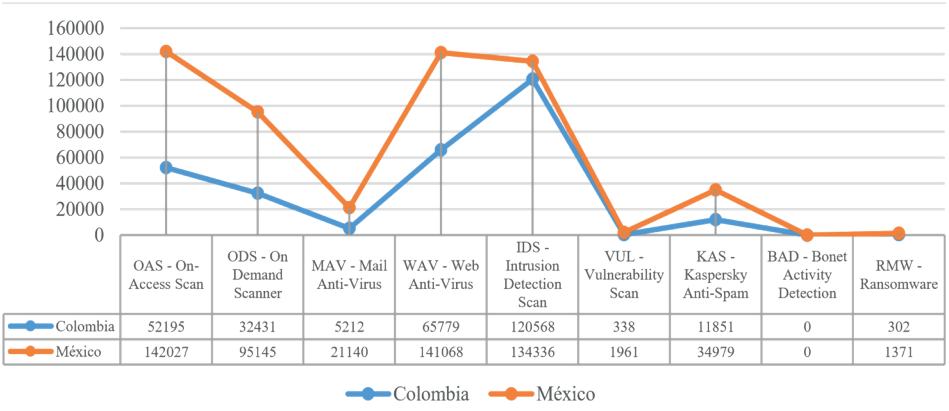
Esto resalta la necesidad apremiante de que las compañías centren una atención aún mayor en la salvaguardia de su información. Es importante que se refuercen las medidas de seguridad cibernética para proteger los activos de las empresas ante este constante aumento de ataques. Observando cómo se comportan las detecciones en un período de 24 horas, se pueden identificar similitudes en el comportamiento en ambos países.

Figura 8. Porcentaje de ciberataques en Hispanoamérica para el año 2022



Nota. Esta figura muestra el porcentaje de ataques cibernéticos a los países mayormente atacados para el año 2022, donde se puede observar que México fue el segundo país más atacado después de Brasil. Adaptado de "México es el primer país de Hispanoamérica en ciberataques, informa Lenovo" (De León, 2023), (https://es.wired.com/articulos/mexico-es-el-segundo-pais-delatinoamerica-en-ciberataques-informa-lenovo).

Figura 9. Detecciones de ataques promedio en un día



	OAS - On-Access Scan	ODS - On Demand Scanner	MAV - Mail Anti-Virus	WAV - Web Anti-Virus	IDS - Intrusion Detection Scan	VUL - Vulnerability Scan	KAS - Kaspersky Anti-Spam	BAD - Bonet Activity Detection	RMW - Ransomware
Colombia	52195	32431	5212	65779	120568	338	11851	0	302
México	142027	95145	21140	141068	134336	1961	34979	0	1371

Nota. Esta figura muestra las detecciones promedio de ataques de diferentes tipos en un día para Colombia y México. Adaptado de "Ciberamenaza, mapa en tiempo real" (Kaspersky Lab, 2023), (https://cybermap.kaspersky.com/es).

Durante el desarrollo de este documento en el aspecto de ciberseguridad aplicada a la industria 4.0 tanto en Colombia como en México y gracias a los resultados obtenidos a partir de la recopilación de información y datos recientes, se identificaron los siguientes puntos clave:

Conclusiones:

- A medida que surgen nuevas tecnologías, las amenazas cibernéticas evolucionan de manera sofisticada en busca de nuevas vulnerabilidades que buscan afectar de manera significativa la industria en sus diferentes etapas. Debido a que no existen sistemas 100 % seguros, se resalta la importancia de adoptar una mejora continua en las estrategias a nivel físico y lógico en ciberseguridad en las industrias 4.0.

- Los usuarios con privilegios restringidos, así como los que tienen un alto nivel de acceso a amplios recursos de información digital, deben ser concientizados sobre las diferentes tácticas, estrategias o modalidades de ataque que usan los ciberdelincuentes. Durante la misión académica internacional y la visita a Audi México, se resaltan las estrategias que esta industria adopta para enseñarle al usuario, mediante campañas de simulación de ataques de *phishing*, a identificar este tipo de correos, así como la detección de sitios web maliciosos, confirmando que la comprensión y las medidas que los usuarios puedan tomar frente a diferentes amenazas finalmente abarcan el mayor porcentaje de prevención ante incidentes de seguridad.

- En el ámbito de la industria 4.0, se evidencia la importancia de proteger la propiedad intelectual como activo crítico, ya que es importante evitar a toda costa la divulgación de tecnologías exclusivas que pudieran dar como resultado una competencia desleal y la afectación económica y reputacional de las industrias. Una de las estrategias comúnmente vistas durante la misión académica internacional tanto en la visita a Audi México como en el Datacenter KIO es la protección de su propiedad intelectual prohibiendo el registro fotográfico de las instalaciones internas y activos críticos de fabricación, así como de tecnologías adoptadas, ratificando que con medidas de seguridad simples pero efectivas se evita la divulgación de información confidencial de alto impacto para las industrias.

- Debido a la creciente adopción de la industria 4.0 en los procesos de fabricación y manufactura a nivel global, se observa que, en México, al adoptar tecnologías para la cuantificación de sus procesos de mayor complejidad, se posee una ventaja en términos de eficiencia y productividad, pero al mismo tiempo esto hace que, al tener esa dependencia e interconectividad tecnológica, se tengan que destinar recursos para garantizar que los procesos de digitalización y automatización se mantengan seguros, destacando la importancia de implementar tecnología de vanguardia en el aspecto de ciberseguridad.

- Se debe aplicar el concepto de resiliencia cibernética en las industrias adoptando medidas preventivas que permitan responder efectivamente a eventos de ciberseguridad. Teniendo en cuenta que ningún sistema es seguro y tomando como referencia los incidentes de ciberseguridad ocurridos en Colombia, se enfatiza la importancia de contar con sistemas efectivos de contingencia, siguiendo las buenas prácticas en seguridad de la información, que permitan a las organizaciones recuperarse en el menor tiempo posible después de un eventual ataque cibernético.

Recomendaciones

Según las diferentes fuentes de investigación consultadas, se encuentra que la industria 4.0, al traer un aumento significativo del uso de tecnologías y a la vez aumentar la cantidad de información y datos en tránsito a través de la red, trae consigo desafíos importantes en el aspecto de ciberseguridad que no solo involucra a la infraestructura tecnológica, sino también al usuario que interactúa con la información. A continuación, se exponen algunas recomendaciones que, a criterio de los autores, son de alta relevancia, no solo para la industria de fábrica y manufactura, sino para cualquier corporación en general:

- La educación constante dirigida a todos los usuarios en las organizaciones donde se promueva la formación y concientización en temas comunes de ciberseguridad, ya que, en muchas compañías, los usuarios no saben cómo reaccionar ante un mensaje, enlace, imagen o cualquier contenido sospechoso.

- La adopción de la norma ISO 27001, la cual establece diferentes criterios, especificaciones y controles que las organizaciones deben adoptar para mantener y gestionar de manera efectiva la seguridad de los activos críticos de la organización, ya que muchas compañías no la adoptan completamente y otras ni siquiera la aplican.

- Complementado a lo anterior, cada sistema informático puede administrase de manera que se puedan aplicar políticas de seguridad que restrinjan al usuario de realizar actividades no autorizadas, como la conexión de dispositivos de almacenamiento removibles, acceso limitado a funciones del sistema o cualquier acción que pueda considerarse de riesgo según las políticas internas de las organizaciones.

- Implementación de tecnologías de ciberseguridad que permitan detectar y reaccionar ante amenazas cibernéticas de manera efectiva, incluyendo, pero sin limitarse, a *firewalls* de nueva generación (NGFW), sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS), sistemas de gestión de identidades (IDM), sistemas antivirus, sistemas de administración de dispositivos móviles (MDM), sistemas de doble o múltiple factor de autenticación (2FA, MFA), entre otros.

- De cara a las organizaciones, es importante la gestión de actualizaciones de *software* y parches de seguridad, ya que los ciberdelincuentes aprovechan brechas presentes en *software* desactualizado que son fácilmente explotables. Debe implementarse una política donde se especifique la frecuencia de las actualizaciones y el ámbito de equipos a las cuales se les aplica. Adicionalmente, debe definirse una política para actualizaciones y parches de seguridad que corrijan vulnerabilidades *zero-day* (día cero) que tengan un impacto alto y crítico.

Referencias

Abi-Hbib, M. (6 de octubre de 2022). "El hackeo del ejército mexicano expone secretos de la institución más poderosa del país". Obtenido de https://www.nytimes.com/es/2022/10/06/espanol/mexico-sedena-guacamaya- hackeo.html

Audi de México (10 de agosto de 2021). *El montaje en México: industria 4.0*. Obtenido de https://www.audi.com.mx/mx/web/es/audi-en-mexico/planta-de-audi-en-mexico/elmontaje-en-mexico.html

Botero, M. C. (19 de septiembre de 2023). *El ataque cibernético que sacude a Colombia*. Obtenido de https://www.javeriana.edu.co/pesquisa/ciberataque-ifx-networks-colombia/

Cisco Systems, Inc. (20 de mayo de 2020). *¿Cuáles son los ciberataques más comunes?* Obtenido de https://www.cisco.com/c/es_mx/products/securi ty/commoncyberattacks.html

Congreso de la República de Colombia (5 de enero de 2009). Ley 1273 de 2009. Obtenido de https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1676699

Datos Macro (mayo de 2022). Colombia - Población. Obtenido de https://datosmacro.expansion.com/demografia/poblacion/colombia

Datos Macro (septiembre de 2022). México - Población. Obtenido de https://datosmacro.expansion.com/demografia/poblacion/mexico

De León, M. (10 de agosto de 2023). "México es el primer país de Hispanoamérica en ciberataques, informa Lenovo". Obtenido de https://es.wired.com/articulos/mexico-es-elsegundo-pais-de-latinoamerica-en-ciberataques-informa-lenovo

Díaz, R. M. (2021). *Estado de la ciberseguridad en la logística de América Latina y el Caribe*. Santiago de Chile: CEPAL Comisión Económica para América Latina y el Caribe.

ICONTEC (11 de noviembre de 2022). Norma Técnica Colombiana NTC-ISO-IEC 27001:2022. Obtenido de https://tienda.icontec.org/gp-ntc-iso-iec-seguridad-de-lainformacion-ciberseguridad-y-proteccion-de-la-privacidad-sistemas-de-gestion-deseguridad-de-la-informacion-requisitos-ntc-iso-iec27001-2022.html

IFX Networks (18 de septiembre de 2018). *Actualizaciones de Estado*. Obtenido de https://ifxnetworks.com/updates/#comunicado

Ilhan, I. & Karakose, M. (7 de noviembre de 2019). *Cybersecurity Framework for Requirements of Repair, Update, and Renovation in Industry 4.0*. Obtenido de https://ieeexplore.ieee.org/document/8965488

International Organization for Standardization (enero de 2019). ISO/IEC 27018:2019. Obtenido de https://www.iso.org/standard/76559.html

International Organization for Standardization (junio de 2023). ISO/IEC 27032:2023. Obtenido de https://www.iso.org/standard/76070.html

International Telecommunication Union (2020). *Global Cibersecurity Index*. Ginebra: International Telecommunication Union.

Kaspersky Lab. (28 de octubre de 2023). *Ciberamenaza mapa en tiempo real*. Obtenido de https://cybermap.kaspersky.com/es

KIO (28 de septiembre de 2021). *Acerca de KIO*. Obtenido de https://www.kio.tech/esmx/acerca-de

Lesmes Díaz, L. (15 de agosto de 2023). "Ciberseguridad: Colombia tuvo 5.000 millones de intentos de ataques el primer semestre". Obtenido de https://www.eltiempo.com/tecnosfera/novedades-tecnologia/colombia-tuvo-masn-de-5-000-intentos-de-ciberataques-al-inicio-del-2023-796252#:~:text=De%20acuerdo%20con%20cifras%20de,cuarto%20lugar%20a%20nivel %20regional

Mendoza P., M. A. & Cuellar, S. (30 de septiembre de 2020). *Industry 4.0: Latin America SMEs Challenges*. Obtenido de https://ieeexplore.ieee.org/document/9240428

Revista Semana (16 de septiembre de 2023). "Hackeo sin precedentes", págs. 32-33.

Secretaría de Economía (5 de enero de 2022). *Declaratoria de vigencia de la Norma Mexicana NMX-I-27018-NYCE-2021*. Obtenido de https://www.dof.gob.mx/nota_detalle.php?codigo=5642452&fecha=10/02/2022#gsc.tab= 0

Tayouri, D., Hassidim, S., Smirnov, A. & Shabtai, A. (28 de septiembre de 2022). *White Paper - Cybersecurity in Agile Cloud Computing-Cybersecurity Guidelines for Cloud Access*. Obtenido de https://ieeexplore.ieee.org/document/9904636

Características clave para elegir entre LORAWAN y Z-WAVE para una solución IOT

Key features to choose between LORAWAN and Z-WAVE for an IOT solution

Linares Vergara, Jeimy Adriana
Candidato a ingeniero de sistemas

Mesa Bernal, Sergio Ernesto
Candidato a ingeniero de sistemas

Prieto Alfonso, Blanca Nidia
Candidato a ingeniero de sistemas

Cabra López, José Luis
Docente del programa de ingeniería de telecomunicaciones

Resumen

Este artículo presenta los resultados de una investigación realizada durante el segundo semestre de 2023 sobre los protocolos de comunicación LoRaWAN y Z-Wave en el contexto de la Internet de las Cosas (IoT). Mediante una metodología de revisión de literatura, se analizan en detalle las características de cada tecnología con el objetivo de identificar los aspectos clave a considerar al elegir entre LoRaWAN y Z-Wave para la implementación de soluciones IoT. Ambos protocolos ofrecen interoperabilidad, robustas medidas de seguridad, eficiencia energética y amplia cobertura global. Sin embargo, sus aplicaciones varían: LoRaWAN se destaca en aplicaciones que requieren un alcance extenso, como la monitorización ambiental, Smart City o el seguimiento de activos, mientras que Z-Wave se posiciona como una excelente elección para aplicaciones de automatización del hogar y domótica. Esta investigación proporciona una guía útil para tomar decisiones informadas en la selección de protocolos de comunicación IoT.

Palabras clave: *IoT, LoRa, LoRaWAN, Z-Wave, elección, protocolo, comunicación.*

Abstract

This article presents the results of research conducted during the second half of 2023 on LoRaWAN and Z-Wave communication protocols in the context of the Internet of Things (IoT). Using a literature review methodology, the characteristics of each technology are analyzed in detail with the aim of identifying the key aspects to consider when choosing between LoRaWAN and Z-Wave for the implementation of IoT solutions. Both protocols offer interoperability, robust security measures, energy efficiency, and broad global coverage. However, its applications vary: LoRaWAN excels in applications that require extensive scope, such as environmental monitoring, Smart City, or asset tracking, while Z-Wave is positioned as an excellent choice for home automation and home automation applications. This research provides useful guidance for making informed decisions in the selection of IoT communication protocols.

Keywords: *IoT, LoRa, LoRaWAN, Z-Wave, election, protocol, communication.*

Cursos articulados

La estructura curricular del programa Ingeniería de Sistemas ofrece una serie de materias que hacen sinergia con el proyecto. Esta conexión es fundamental para aplicar y ampliar el conocimiento teórico a través de la experiencia práctica. En este contexto, las materias como: Algoritmos, Arquitectura de Hardware, Extracción Transformación y Carga de Datos, Sistemas Digitales, Gestión y Calidad de la Información, Análisis y Diseño de Sistemas de Información, Desarrollo Web, Arquitectura de Datos, Cloud Computing, Seguridad de la Información, Sistemas Distribuidos, Auditoría de Sistemas, contribuyeron en este trabajo para su desarrollo y éxito, para que se apliquen los conocimientos efectivamente.

Introducción

El IoT (Internet de las Cosas) permite conectar cualquier objeto o "cosa" a una red de internet, posibilitando la transmisión de datos para su posterior análisis y la ejecución de acciones basadas en estos datos (Cruz Vega y otros, 2015). El Internet de las Cosas (IoT) ha revolucionado nuestra interacción con objetos cotidianos y ha transformado la prestación de servicios en diversos sectores, abarcando desde la agricultura y la salud hasta la logística y la industria, entre otros.

Para implementar un sistema IoT, es fundamental considerar cuatro elementos importantes para la conexión y comunicación entre los dispositivos físicos a través de internet, tales como: sensores que capturan datos, el procesamiento y transmisión de los datos, un sistema de red (almacenamiento *cloud* o local) y, por último, la ejecución de acciones basadas en la información recopilada para la toma de decisiones (SAP, s. f.) Una red IoT se sustenta en protocolos de comunicación que facilitan la transferencia eficiente de datos entre dispositivos, Los protocolos de comunicación IoT se pueden clasificar en dos categorías principales: protocolos de corto alcance (9.144 metros aprox. en recintos cerrados) y protocolos de largo alcance (entre 5 y 15 kilómetros). Los primeros son apropiados para aplicaciones en las que los dispositivos están situados a poca distancia, mientras que los segundos son adecuados para aplicaciones en las que los dispositivos están situados a distancias más grandes (Quiñonez Muñoz, 2019).

La selección de un protocolo de comunicación adecuado se convierte en un aspecto crucial para lograr un rendimiento óptimo en cualquier implementación IoT. Los protocolos de comunicación ofrecen características que se adaptan a diferentes escenarios de aplicación. En este trabajo, se exploran dos de estos protocolos: LoRa y Z-Wave. LoRa se distingue por su capacidad de comunicación de largo alcance con un bajo consumo de energía, mientras que Z-Wave es un protocolo de corto alcance, ampliamente utilizado en la domótica debido a su enfoque en la interoperabilidad y la seguridad.

Metodología

Este estudio se enfocó en analizar la documentación relacionada con la implementación de IoT y la selección de protocolos inalámbricos, específicamente LoRaWAN y Z-Wave, debido a sus ventajas en cuanto a potencia, aplicaciones IoT, costos, seguridad, confiabilidad y facilidad de instalación. El objetivo era establecer un criterio para la elección entre estos protocolos, considerando las necesidades específicas de cada caso y evaluando sus similitudes.

Para llevar a cabo este trabajo, se aplicaron ciertos criterios de búsqueda y selección. En primer lugar, se consideró la documentación de los últimos 6 años, con el fin de asegurar la relevancia y actualidad de los datos. Las fuentes utilizadas incluyeron Google Académico, una fuente de información especializada en textos científicos y académicos, así como bibliotecas virtuales de universidades y el banco de publicaciones IEEE Explore, con contenido específico relacionado con la temática.

Con preferencia de búsqueda, se utilizaron términos clave como: IoT, IIoT, LoRaWAN y Z-Wave, protocolos estandarizados, cobertura a nivel mundial y popularidad en el mercado con el propósito de identificar de manera precisa los documentos que abordaran los aspectos relevantes para la elección de protocolos en soluciones IoT.

Como segundo criterio para el análisis de la información, se plantearon las siguientes preguntas:

- **P1.** ¿Cuáles son las principales características de los protocolos LoRaWAN y Z-Wave en términos de alcance, consumo de energía y capacidad de carga útil?

- **P2.** ¿En qué contextos o aplicaciones específicas se ha implementado con éxito LoRaWAN y Z-Wave en soluciones IoT?

- **P3.** ¿Existen diferencias significativas en la disponibilidad de *hardware* y soporte de la comunidad para LoRaWAN y Z-Wave?

- **P4.** ¿Cuáles son las tendencias y avances recientes en la implementación de LoRaWAN y Z-Wave en el contexto de IoT y cómo impactan en la elección del protocolo?

Discusión

Tanto Z-Wave como LoRaWAN presentan sus propias ventajas y desventajas, por lo que la elección entre uno u otro dependerá de las necesidades específicas de la solución a implementar.

Características clave

- **Frecuencia:** establece el alcance de la señal. Las frecuencias más bajas, como las que utiliza Z-Wave, pueden penetrar mejor los objetos sólidos; esto lo hace ideal para aplicaciones interiores. Las frecuencias más altas, como las utilizadas por LoRaWAN, pueden viajar más lejos, lo que lo hace ideal para aplicaciones exteriores.

- **Alcance:** determina la distancia máxima a la que un dispositivo puede estar del concentrador o *gateway*. Z-Wave tiene un alcance relativamente corto, mientras que LoRaWAN tiene un alcance mucho más largo.

- **Velocidad de transmisión:** define la cantidad de datos que se pueden transferir por segundo. Z-Wave tiene una velocidad de transmisión más alta que LoRaWAN.

- **Potencia de transmisión:** es el factor que fija hasta dónde llega la señal. Z-Wave tiene una potencia de transmisión más baja que LoRaWAN.

- **Consumo de energía:** establece el período de tiempo en el que las baterías de los dispositivos durarán. Tanto Z-Wave como LoRaWAN permiten hasta 10 años de funcionamiento continuo con una única batería tipo botón gracias a la gestión dinámica de energía.

- **Costo:** es el precio de los dispositivos, la infraestructura, la implementación y el mantenimiento necesarios para el montaje de la red. Independientemente del protocolo seleccionado, ya sea LoRaWAN o Z-Wave, el valor del proyecto se determina por su complejidad y alcance.

- **Disponibilidad:** es la facilidad con la que se pueden encontrar dispositivos y componentes compatibles. Z-Wave y LoRaWAN están ampliamente disponibles, pero hay algunos países en los que estos dos protocolos no están disponibles o tienen restricciones:

  ✓ Z-Wave:
    - China: está disponible, pero se requiere una licencia para operar.
    - Irán y Corea del Norte: está prohibido.

  ✓ LoRaWAN:
    - China: está disponible, pero se requiere una licencia para operar.
    - Irán, Corea del Norte, Cuba y Venezuela: está prohibido.

Desventajas

En el apartado anterior, se detallaron las características clave que describen y resumen las ventajas de Z-Wave y LoRaWAN. Ahora, procederemos a exponer las desventajas de cada uno de estos protocolos:

- Z-Wave:
  ✓ **Alcance limitado:** lo hace inadecuado para aplicaciones exteriores de largo alcance.

  ✓ **Interferencia:** puede verse afectado por la interferencia de otras señales inalámbricas, como wifi y Bluetooth.

- LoRaWan:
  ✓ **Velocidad de transmisión baja:** es de hasta 50 kbps. No es adecuado para la transmisión rápida de datos, pero es una elección apropiada para el envío de telemetría.

Posibles limitaciones en la investigación

Esta comparación se basa en una revisión de la literatura y la experiencia práctica. Es posible que existan limitaciones en la investigación, como la falta de datos específicos de los diferentes escenarios e implementaciones de las soluciones IoT. También es posible que existan áreas en las que se necesita más investigación, como el rendimiento de los dos protocolos en entornos desafiantes.

Áreas en las que se necesita más investigación

Rendimiento en entornos desafiantes: es importante investigar el rendimiento de Z-Wave y LoRaWAN en entornos desafiantes, como entornos con mucho ruido o con obstáculos.

- **Eficiencia energética:** es importante investigar la eficiencia energética de Z-Wave y LoRaWAN en aplicaciones que requieren una larga duración de la batería.

- **Costo:** es importante investigar el costo total de propiedad de Z-Wave y LoRaWAN, incluidos los costos de *hardware*, *software*, servicio y mantenimiento.

Resultados

En este apartado, se tratan los temas más fundamentales de los protocolos LoRaWAN y Z-Wave.

Componentes físicos

Características y arquitectura

En la siguiente tabla, se encuentran las características más representativas de cada protocolo.

Tabla 7. Características de los protocolos LoRaWAN y Z-Wave

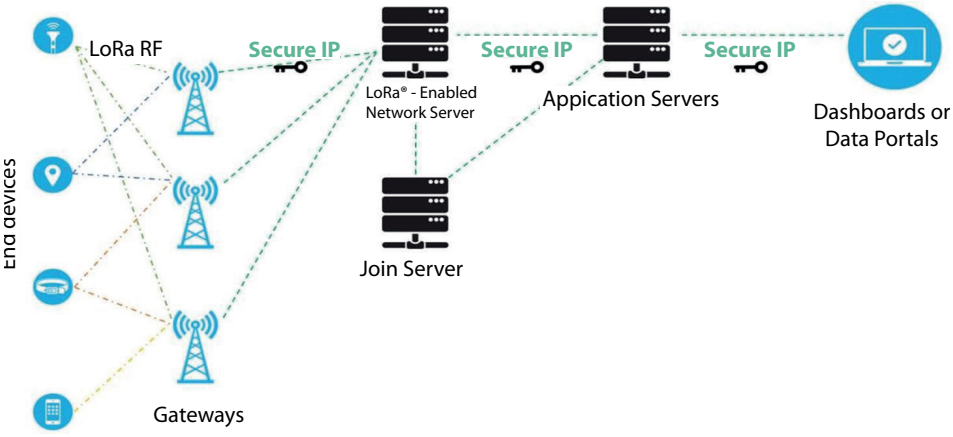
LoRaWAN	Z-Wave
• Largo alcance o amplia cobertura en interiores (incluidos edificios de varias plantas) • Diseño de red con topología en estrella, geolocalización o interior/exterior • Precisión sin necesidad de GPS o sin impacto en la duración de la batería • Batería de larga duración u optimizada para bajo consumo o hasta 10 años de vida útil o hasta 10 veces superior a M2M celular • Actualizaciones de *firmware* en el aire para aplicaciones y la pila LoRaWAN	• Tecnología de comunicaciones RF de baja potencia que admite redes de malla completas sin necesidad de un nodo coordinador. • Funciona en la banda sub-1GHz; impermeable a las interferencias de wifi y otras tecnologías inalámbricas en el rango de 2,4 GHz (Bluetooth, ZigBee, etc.). • Las capas PHY y MAC de Z-Wave están definidas por la recomendación ITU-T G.9959.
• Alta capacidad o millones de mensajes por estación base/*gateway* • Interoperabilidad multiusuario o despliegue en redes públicas o privadas • Itinerancia o *roaming*: traslados sin problemas de una red a otra • Bajo coste o infraestructura mínima o nodo final de bajo coste o *software* de código abierto • Seguridad o cifrado AES-128 integrado de extremo a extremo • Identificación única o aplicación o red	• Diseñado específicamente para aplicaciones de control y estado, admite velocidades de datos de hasta 100 kbps, con cifrado AES128, IPV6 y funcionamiento multicanal. • Interoperabilidad total hasta la capa 6 con compatibilidad con todas las versiones anteriores. • Se ha puenteado y probado con éxito con OpenADR, SEP 1, SEP 1.1 y otros protocolos de Smart Energy. Comparte la misma posición en el Catálogo de Normas NIST / SGIP que las familias IEEE 802.11 y 802.15 y 802.16.

Nota. Esta tabla reúne las principales características de LoRaWAN y Z-Wave (LoRa Alliance, s. f. y Z-Wave Alliance, s. f.).

Elementos de la red LoRaWAN:

A continuación, se examina la arquitectura de una red LoRaWAN.

Figura 10. Elementos de la red LoRaWAN



Nota. En este gráfico se visualizan los elementos importantes con que cuenta la red LoRaWAN (LoRa Alliance, s. f.).

- **Nodo o dispositivo final:** sensores o actuadores conectados de manera inalámbrica a través de puertas de enlace de radio que utilizan la modulación de RF LoRa. Los sensores se alimentan por batería, digitalizan condiciones físicas y eventos ambientales. Los actuadores se utilizan en aplicaciones como alumbrado público, cerraduras inalámbricas y control de válvulas de agua.

- ***Gateway*:** son dispositivos esenciales para la comunicación entre dispositivos finales y el servidor de red.

Las puertas de enlace LoRaWAN no están asociadas a un dispositivo final específico, es decir, pueden ser atendidos por la misma puerta de enlace.

Las puertas de enlace LoRaWAN verifican la integridad de los datos antes de reenviarlos al LNS. El LNS elimina los duplicados de los mensajes recibidos de las puertas de enlace.

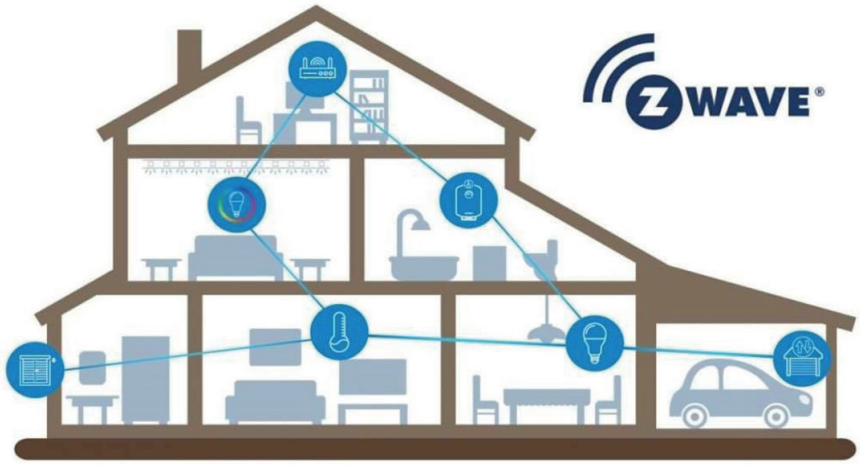
- **Servidor de red:** ajusta de manera dinámica los parámetros en respuesta a las condiciones cambiantes. Establece conexiones seguras de 128 bits AES para el transporte de datos entre los dispositivos y la nube del usuario final, controla el tráfico entre los dispositivos y el servidor de red, garantizando la autenticidad de los sensores y la integridad de los mensajes sin acceso a los datos de la aplicación.

- **Servidor de aplicación:** servidores encargados de procesar los datos transmitidos a través de la red. Aunque son independientes de la red LoRaWAN, mantienen comunicación con los servidores de red para recibir los datos y llevar a cabo su procesamiento (Instituto Nacional de Ciberseguridad, 2023).

Topología de red Z-Wave

Z-Wave utiliza una topología de red en malla, donde cada dispositivo (excepto los que usan batería) en la red actúa como repetidor de señal. En consecuencia, a medida que aumenta el número de dispositivos en su hogar, la red se fortalece. Aunque las señales Z-Wave atraviesan fácilmente la mayoría de las barreras físicas, como paredes, pisos y techos, los dispositivos también pueden tomar rutas inteligentes para sortear obstáculos, asegurando una cobertura sólida y continua en toda la casa (Z-Wave, s. f.).

Figura 11. Topología de red Z-Wave



Nota. En este gráfico se visualiza los elementos importantes con que cuenta la red Z-Wave (Z-Wave, s. f.).

Alcance y cobertura de transmisión

Alcance Z-Wave

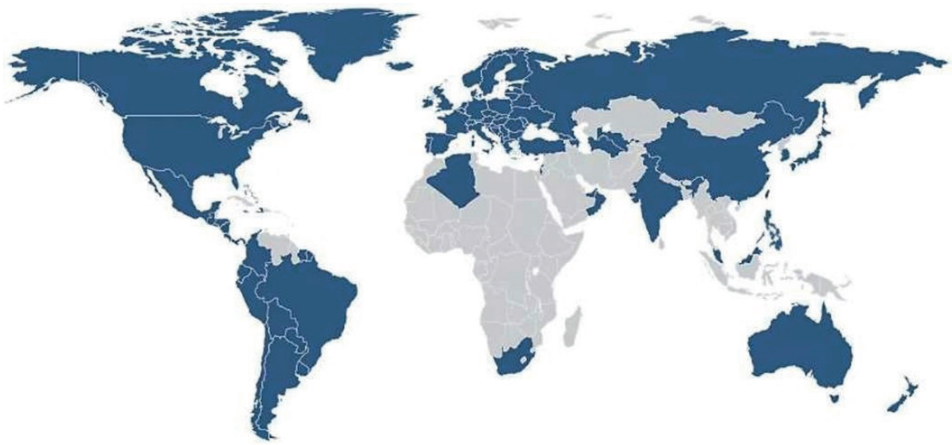
Resistente a interferencias inalámbricas debido a su uso de frecuencias de radio que se encuentran por debajo del rango de 1 gigahercio (GHz), en contraste con las redes inalámbricas, como wifi y Bluetooth, que operan en la banda de 2.4 GHz. Esto evita problemas de interferencia y congestión de tráfico y aporta eficiencia en términos de energía, mayor alcance y una menor interferencia de radiofrecuencia. (Z-Wave, s. f.).

El alcance de Z-Wave es de 100 metros al aire libre, aunque puede verse reducido por materiales de construcción. Se sugiere tener un dispositivo Z-Wave aproximadamente cada 30 pies para una eficiencia óptima. La señal puede saltar unos 600 pies y las redes Z-Wave pueden conectarse para implementaciones más amplias. Cada red puede admitir hasta 232 dispositivos, según sus necesidades (Z-Wave, s. f.).

Cobertura Z-Wave

Z-Wave cuenta con cobertura en gran parte del mundo. Los siguientes datos son tomados del sitio oficial de Z-Wave.

Figura 12. Regiones globales de cobertura Z-Wave



Nota. Estos son los países en donde Z-Wave tiene cobertura (Silabs).

Alcance LoRaWAN

LoRaWAN opera en un canal de ancho de banda fijo de 125 KHz o 500 KHz (para canales de enlace ascendente) y 500 KHz (para canales de enlace descendente).

Tabla 8. Tabla de alcance LoRaWAN

Modulation	*Bandwidth [kHz]*	*Channel Frequency [MHz]*	*LoRa DR / Bitrate*	*Number of Channels*	*Duty Cycle*
LoRa	125	868,10 868,30 868,50	DR0 to DR5 / 0,3-5 kbps	3	< 1 %

Nota. Banda de canal de frecuencias; aplica a cualquier región en la que el uso del espectro radioeléctrico esté definido por la norma ETSI 544 [EN300.220-2] (LoRa Alliance, s. f.).

LoRaWAN se caracteriza por la capacidad para establecer conexiones de datos de largo alcance. Facilita comunicaciones de gran distancia, alcanzando hasta tres millas (cinco kilómetros) en entornos urbanos y más de 10 millas (15 kilómetros) en áreas rurales con línea de vista. Otra característica importante es su eficiencia energética, lo que permite la creación de dispositivos alimentados por baterías. Cuenta una topología en estrella, lo que permite comunicaciones a larga distancia o en espacios interiores entre una gran cantidad de dispositivos que consumen poca energía y transmiten pequeñas cantidades de datos (LoRa, s. f.).

Cobertura LoRaWAN

Los países con mayor cobertura de LoRaWAN son los siguientes (datos tomados de LoRa Alliance):

- **Europa:** Alemania, Francia, Italia, España, Reino Unido, Países Bajos, Bélgica, Suiza, Suecia, Dinamarca, Noruega, Finlandia, Polonia, Rusia, Ucrania, Turquía, Israel, Grecia, Portugal, Austria, República Checa, Eslovaquia, Hungría, Rumanía, Bulgaria, Letonia, Lituania, Estonia, Irlanda, Islandia, Malta, Chipre.

- **América:** Estados Unidos, Canadá, México, Brasil, Argentina, Chile, Colombia, Perú, Ecuador, Venezuela, Bolivia, Uruguay, Paraguay, Costa Rica, Panamá, Guatemala, El Salvador, Honduras, Nicaragua.

- **Asia:** China, India, Japón, Corea del Sur, Taiwán, Indonesia, Malasia, Tailandia, Vietnam, Filipinas, Singapur, Hong Kong, Macao, Pakistán, Sri Lanka, Bangladesh, Nepal, Bután, India, Afganistán, Irán, Irak, Siria, Líbano, Jordania, Israel, Arabia Saudita, Emiratos Árabes Unidos, Omán, Kuwait, Qatar, Bahrein, Yemen.

- **África:** Sudáfrica, Nigeria, Egipto, Kenia, Tanzania, Etiopía, Argelia, Marruecos, Túnez, Libia, Sudán, Sudán del Sur, Uganda, Ruanda, Burundi, Congo, Gabón, Camerún, Guinea Ecuatorial, Costa de Marfil, Ghana, Togo, Benín, Burkina Faso, Níger, Liberia, Sierra Leona, Guinea, Senegal, Gambia.

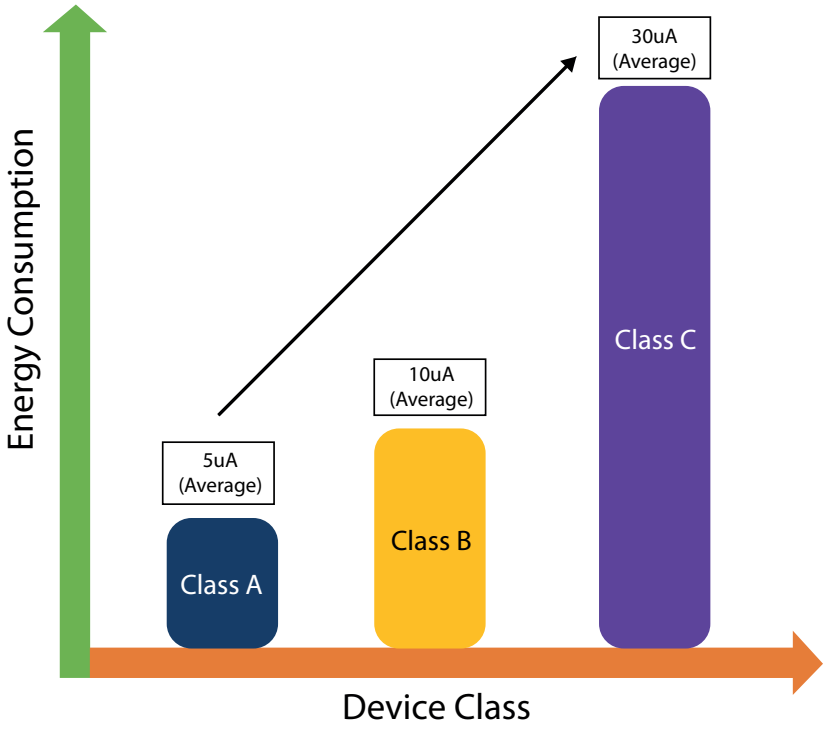
- **Oceanía:** Australia, Nueva Zelanda, Papúa Nueva Guinea, Islas Salomón, Vanuatu, Fiji, Tonga, Samoa, Islas Cook, Kiribati, Tuvalu, Nauru.

Consumo de energía

LoRaWAN

En una red LoRaWAN, los dispositivos finales se dividen en tres clases: Clase A, Clase B y Clase C, que determinan cuándo pueden recibir enlaces descendentes y su eficiencia energética. Los dispositivos de Clase A son los más básicos, solo pueden transmitir cuando están activos y tienen el menor consumo de energía. Los dispositivos de Clase B tienen intervalos de transmisión activa y pasiva, mejor rendimiento, pero mayor consumo. Los dispositivos de Clase C pueden transmitir en cualquier momento, siendo los de mayor rendimiento, pero con un alto consumo de energía.

Figura 13. Consumo de energía LoRaWAN



Nota. Diagrama de representación del consumo de energía en LoRaWan de acuerdo con las clases existentes en este protocolo (Semtech, s. f.)

Tabla 9. Consumo de energía de algunos sensores para LoRaWAN

Sensor	Consumo de energía	Sensor	Consumo de energía
Presión, nivel y temperatura en líquidos	≤ 0,4 mW (10 min intervalo)	Sensor humano	Modo activo: 22 uA Modo espera: 6 uA Modo suspensión: 1,75 uA
Temperatura de superficie + temperatura y humedad relativa	≤ 0,5 mW (10 min intervalo)	Hogar inteligente, transceptor LoRa de bajo consumo	Modo activo: 22 dBm Modo espera: 160 nA Modo suspensión: 160 nA

Sensor	Consumo de energía	Sensor	Consumo de energía
Temperatura y humedad relativa del subsuelo	≤ 0,95 mW (10 min intervalo)	Termómetro Infrarrojo/Sensor de temperatura de superficie	≤ 0,5 mW (10 min intervalo)
Radiación solar	≤ 0,5 mW (10 min intervalo)	Radiación fotosintéticamente activa	≤ 0,5 mW (10 min intervalo)

Nota. Consumo de energía de algunos sensores de marcas Catsensors y Semtech, tomados de las fichas técnicas de cada proveedor (Catsensors y Semtech, s. f.)

Z-Wave

El consumo de batería en Z-Wave depende de varios factores, entre ellos:

- Los dispositivos que transmiten datos con más frecuencia, como los sensores de movimiento, tienen un mayor consumo de batería que los dispositivos que transmiten datos con menos frecuencia, como los sensores de temperatura.
- Cuanto mayor sea la distancia, mayor será el consumo de batería.
- Cuanto más fuerte sea la señal, menor será el consumo de batería (Z-Wave, s. f.)

Tabla 10. Consumo de energía sensores para Z-Wave

Sensor	Consumo de energía	Sensor	Consumo de energía
Sensor de temperatura y humedad	Rango de voltaje 2,4-3,3 VDC	Luz, movimiento y temperatura	Batería 3V, 1.500 mAh
Multisensor *home smart*	Batería 3V, 1.500 mAh	Sensor de agua	Batería 3,6V, 5 mW
Sensor de puerta	Batería 3V, 800 mAh	Medidor de energía	20 mA

Nota. Consumo de energía sensores Aeotec Smart tomados de las fichas técnicas de cada proveedor (Aeotec).

Interoperabilidad

Z-Wave cuenta con una certificación de interoperabilidad en su capa de aplicación, permitiendo que más de 4.000 productos, que varían en marcas y generaciones de chips, funcionen conjuntamente. Estos productos incluyen bombillas inteligentes, cerraduras inteligentes, termostatos, sensores de movimiento, sensores de agua, sistemas de seguridad y una amplia gama de dispositivos (Z-Wave Alliance, s. f.).

En LoRaWAN, la interoperabilidad se logra mediante la adopción de estándares comunes entre los fabricantes de dispositivos y las redes LoRaWAN. Estos estándares abarcan el formato de los mensajes, protocolos de seguridad y gestión de la red. Como principales estándares de interoperabilidad se tienen los parámetros regionales de LoRaWAN, que definen aspectos como el ancho de banda y la frecuencia; las clases de LoRaWAN, que determinan características como el consumo de energía y el alcance; y las normativas de seguridad de LoRaWAN, que establecen protocolos de seguridad y cifrado para la transmisión de datos (LoRa Alliance, s. f.).

Seguridad

Cuando se trata de seleccionar una solución IoT, surge un desafío crítico al evaluar si LoRaWAN y Z-Wave cumplen con los requisitos de seguridad necesarios y al decidir cuál de los dos proporciona un nivel de seguridad más apropiado. Si bien ambos protocolos incorporan niveles de seguridad, aún subsisten diferencias significativas entre ellos.

LoRaWAN

Cada dispositivo cuenta con una llave privada que se utiliza para cifrar los datos que envía y recibe. La llave privada se almacena en el dispositivo y nunca se transmite por la red. Además de la llave privada, LoRaWAN también utiliza un mecanismo de autenticación para verificar la identidad de los dispositivos. Este mecanismo se basa en un servidor de autenticación que emite certificados a los diferentes nodos (LoRa Alliance, s. f.)

Los nodos que intervienen pueden unirse a la red utilizando dos métodos, de acuerdo a como se menciona en el blog web Digimodes (Casanova, 2017):

- ABP (*Activation by Personalization*). En este método de acceso a la red, tanto el nodo como el servidor conocen la clave de sesión y la dirección física del nodo (DevAddr). Esta es la forma más rápida de empezar a trabajar en la red, ya que el dispositivo se entrega preconfigurado; al no estar totalmente configurado, se pueden presentar riesgos, como lo son los ataques a la infraestructura física, lo que ocasionaría que un posible atacante podría registrar la actividad de un dispositivo a través de la interfaz aire (obteniendo información de su comportamiento) o cualquier persona podría desplegar un *gateway* y escuchar el tráfico aire-aire y capturar información como: DeviceID, Frame Counter, incluso se podría llegar a averiguar el tamaño del *payload*.

- OTAA (*Over-the-Air-Activation*). Para este método, el nodo y el servidor negocian las claves de cifrado mediante la interfaz aire-aire en el momento en el cual el nodo se conecta a la red. El dispositivo trata de activarse nada más encenderse enviando un "*join request*" a los demás equipos, esperando una respuesta del tipo "*join accept*".

  Para estos dos métodos las claves deben ser almacenadas para su posterior consumo:

  - ✓ En OTAA: AppKey.

  - ✓ En OTAA y ABP: DevAddr, NwkSkey, AppSkey.

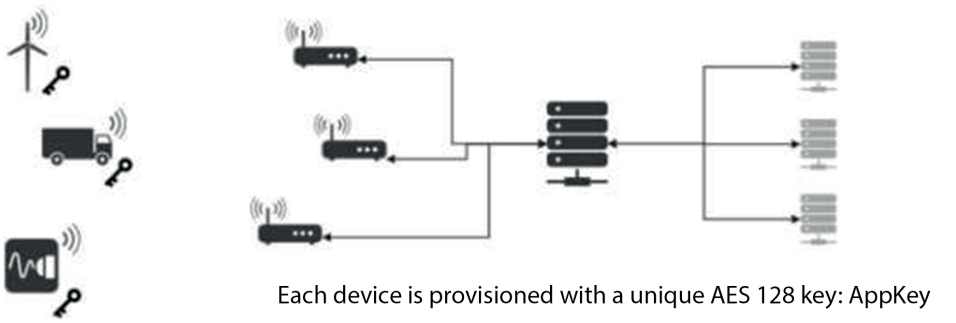
LoRaWAN facilita diferentes capas de cifrado, las cuales utilizan algoritmo de cifrado AES-128 (aunque OWASP recomienda en sus guías el uso de AES-256 para IoT) para proteger las comunicaciones de datos (Casanova, 2017):

- Network Session Key: clave de 128 bits que garantiza seguridad a nivel de red.

- Application Session Key: clave de 128 bits que garantiza seguridad extremo-extremo.

- Application Key: clave de 128 bits que se utiliza para despliegues OTAA.

Figura 14. Diagrama de seguridad LoRaWAN



Nota. En este diagrama se muestra la distribución de los equipos y cómo se aplica su sistema de seguridad.

Z-Wave

Según Lidia Fotia, Fabrizio Messina y otros (2023), el protocolo Z-Wave utiliza un esquema de seguridad llamado *Secure Neighbor Network* (SNN). SNN proporciona tres capas de seguridad:

- **Capa de red:** proporciona autenticación y cifrado para todos los mensajes enviados entre nodos de la red.
- **Capa de aplicación:** proporciona integridad y actualidad de los mensajes para todos los mensajes enviados entre nodos de la red.
- **Capa de dispositivo:** proporciona autenticación y autorización del dispositivo para todos los mensajes enviados hacia y desde un nodo de la red.

SNN utiliza una variedad de técnicas criptográficas para lograr estos objetivos de seguridad, que incluyen:

- **Cifrado AES-128:** todos los mensajes enviados entre nodos de la red se cifran mediante AES-128.
- **Autenticación de mensajes HMAC-SHA-1:** todos los mensajes enviados entre nodos de la red se autentican mediante HMAC-SHA-1.

- **Protección de reproducción no basada en tiempo:** todos los mensajes enviados entre nodos de la red utilizan un mecanismo basado en *nonce* para evitar ataques de reproducción.

Además de estas técnicas criptográficas, SNN también utiliza otras características de seguridad, como:

- **Inclusión segura de nodos:** cuando se agrega un nuevo nodo a la red, debe pasar por un proceso de autenticación segura.

- **Enrutamiento seguro:** los mensajes se enrutan a través de la red de manera segura, evitando que nodos no autorizados los intercepten.

- **Despertar seguro:** los nodos se pueden despertar de forma segura desde el modo de suspensión, evitando que nodos no autorizados los despierten.

SNN es un esquema de seguridad sólido que proporciona un alto nivel de protección para las redes Z-Wave (Fotia, 2023).

Ambos protocolos utilizan cifrado y autenticación para proteger los datos que se transmiten por la red. Sin embargo, existen algunas diferencias clave entre los dos protocolos: LoRaWAN es más resistente a los ataques de fuerza bruta, mientras que Z-Wave es más resistente a los ataques de intermediario (Z-Wave Alliance, *Security Overview*, 2023).

Costo de implementación

Los costos de implementación de los protocolos LoRaWAN y Z-Wave varían según las necesidades específicas del proyecto, como el tamaño, la complejidad de la red, el tipo de dispositivos a utilizar, el nivel de soporte requerido, entre otros.

Según Adrián I. Petrariu (2019), el costo de implementación depende de una serie de factores:

- **Tamaño de la red:** el costo de implementación aumenta con el tamaño de la red. Esto se debe a que se necesitan más *gateway* para cubrir un área más extensa. Las redes LoRaWAN y Z-Wave pueden cubrir varios kilómetros de diámetro. Sin embargo, el tamaño real depende de una serie de factores, como el tipo de red, el terreno, la densidad de dispositivos y la potencia de transmisión de los dispositivos.

- **Densidad de dispositivos:** el costo de implementación también aumenta con la densidad de dispositivos. Esto se debe a que se necesita ancho de banda para transmitir datos de más nodos. Las redes LoRaWAN se utilizan a menudo para aplicaciones que requieren una cobertura amplia, como el seguimiento de activos o la monitorización ambiental; estas aplicaciones generalmente tienen una densidad de dispositivos baja, de entre 1 y 10 dispositivos por kilómetro cuadrado. Sin embargo, las redes LoRaWAN también se pueden utilizar para aplicaciones que requieren una densidad de dispositivos alta, como la iluminación inteligente o el control de acceso. Estas aplicaciones pueden tener una densidad de dispositivos de hasta 100 dispositivos por kilómetro cuadrado.

En cuanto a las redes Z-Wave, se utilizan a menudo para aplicaciones que requieren una interacción cercana entre dispositivos, como los hogares inteligentes. Estas aplicaciones generalmente tienen una densidad de dispositivos alta, de entre 10 y 100 dispositivos por habitación.

Las redes Z-Wave también se pueden utilizar para aplicaciones que requieren una cobertura amplia, como el seguimiento de personas o animales. Estas aplicaciones pueden tener una densidad de dispositivos más baja, de entre 1 y 10 dispositivos por kilómetro cuadrado.

Tipo de gateway

El costo de los *gateways* varía según lo robustos que sean sus componentes. En LoRaWAN y Z-Wave se utilizan dos tipos principales de *gateway*:

- ***Gateways* de *hardware*:** estos *gateways* están formados por un dispositivo físico que se conecta a la red LoRaWAN o Z-Wave. Los *gateways* de *hardware* suelen ser más caros que los de *software*, pero son más fáciles de configurar y mantener.

- ***Gateways* de *software*:** estos *gateways* se ejecutan en un dispositivo informático, como un ordenador o una Raspberry Pi. Los *gateways* de *software* suelen ser más baratos que los de *hardware*, pero pueden ser más difíciles de configurar y mantener.

Gateways de LoRaWAN

Se conectan a la red LoRaWAN a través de una conexión Ethernet o wifi. Suelen tener una antena externa para mejorar la recepción de los dispositivos LoRaWAN.

Los *gateways* de LoRaWAN pueden ser de dos tipos:

- ***Gateways* de nivel de portadora:** estos *gateways* reciben las señales de los dispositivos LoRaWAN y las retransmiten a la red LoRaWAN.

- ***Gateways* de nivel de aplicación:** estos *gateways* reciben las señales de los dispositivos LoRaWAN y las procesan antes de retransmitirlas a la red LoRaWAN.

Gateways de Z-Wave

Se conectan a la red Z-Wave a través de un puerto USB o Ethernet. Los *gateways* de Z-Wave suelen tener una antena interna para mejorar la recepción de los dispositivos Z-Wave.

Los *gateways* de Z-Wave pueden ser de dos tipos:

- ***Gateways* de nivel de red:** estos *gateways* conectan los dispositivos Z-Wave a la red Z-Wave.

- ***Gateways* de nivel de aplicación:** estos *gateways* proporcionan una interfaz de usuario para controlar los dispositivos Z-Wave.

Elección del tipo de *gateway*

La elección del tipo de *gateway* adecuado depende de una serie de factores, como el presupuesto, las necesidades de la aplicación y la experiencia del usuario.

Si el presupuesto es limitado, los *gateways* de *software* pueden ser una buena opción. Sin embargo, si se necesita uno que sea fácil de configurar y mantener, los de *hardware* pueden ser una mejor opción.

Si la aplicación requiere una cobertura amplia, un *gateway* de nivel de portadora puede ser una buena opción. Si la aplicación requiere la capacidad de procesar datos, un *gateway* de nivel de aplicación puede ser una mejor opción.

Si el usuario tiene experiencia con redes inalámbricas, un *gateway* de *hardware* puede ser una buena opción. Si el usuario tiene poca experiencia con redes inalámbricas, un *gateway* de *software* puede ser una mejor opción.

Servicio de backend

Los servicios de *backend* proporcionan funciones como almacenamiento, análisis y procesamiento de datos.

Como análisis y comparación de costos de implementación de LoRaWAN y Z-Wave de una red se pueden generalizar los siguientes ítems:

- **Costo de *hardware*:** los *gateways* LoRaWAN presentan un valor elevado con respecto al precio de los concentradores Z-Wave, debido a que requieren una mayor robustez en las características de sus componentes.

- **Costo de *software*:** LoRaWAN requiere un *software* de administración de red para configurar y gestionarla. El *software* de administración de LoRaWAN es más caro que el *software* de administración de Z-Wave.

- **Costo de licencias:** en algunos países, se requieren licencias de espectro para operar una red LoRaWAN. Las licencias de espectro pueden ser costosas, especialmente para redes grandes.

- **Costo de mantenimiento:** el costo de mantenimiento de una red LoRaWAN también puede ser más alto que el costo de mantenimiento Z-Wave. Esto se debe a que LoRaWAN es una tecnología más compleja y requiere más conocimientos técnicos para mantenerla.

Estimación del costo

Para estimar el costo de implementación de una red IoT, se puede utilizar la siguiente fórmula:

Ecuación 1. *Estimación de costos de implementación de red IoT*

$$\text{Costos} = \text{Costo de Hardware} + \text{Costo de Software} + \text{Costo de servicios}$$

Por ejemplo, para implementar una red LoRaWAN con 100 *gateways*, 10.000 dispositivos LoRaWAN y un servicio de *backend*, el costo estimado sería el siguiente:

- Costo = $10.000 USD por *gateway* + $10 USD por dispositivo + $1.000 USD por mes por servicio de *backend*

- Costo = $1.000.000 USD + $100.000 USD + $12.000 USD
- Costo = $1.112.000 USD

Para implementar una red Z-Wave con 100 dispositivos Z-Wave, un concentrador Z-Wave y un servicio de *backend*, el costo estimado sería el siguiente:

- Costo = $50 USD por dispositivo + $100 USD por concentrador + $1.000 USD por mes por servicio de *backend*

- Costo = $5.000 USD + $100 USD + $12.000 USD

- Costo = $17.100 USD

Este es solo un estimado y el costo real puede variar según los factores mencionados anteriormente.

Factores adicionales que considerar

Además de los factores mencionados anteriormente, cuando los servicios están en la nube, el valor de dicho servicio puede ser calculado de diferentes maneras, pero una forma común es utilizar el costo por transacción. El costo por transacción es el costo total de realizar una transacción en un servicio en la nube.

Para AWS, Google y Azure, el costo por transacción puede variar según el tipo de servicio, el volumen de transacciones y el nivel de rendimiento. Sin embargo, en general, el costo por transacción es relativamente bajo.

Amazon Web Services (AWS):

- **EC2:** el costo por transacción de EC2 varía según el tipo de instancia, la región y el período de tiempo. Para una instancia t2.micro en la región us-east-1, el costo por transacción es de aproximadamente $0,0000025 USD.

- **S3:** el costo por transacción de S3 varía según el tipo de objeto, el tamaño del objeto y la región. Para un objeto de 1 KB en la región us-east-1, el costo por transacción es de aproximadamente $0,000001 USD (Amazon, s. f.).

Google Cloud Platform (GCP):

- **Compute Engine:** el costo por transacción de Compute Engine varía según el tipo de instancia, la región y el período de tiempo. Para una instancia n1-standard-1 en la región uscentral1, el costo por transacción es de aproximadamente $0,000002 USD.

- **Cloud Storage:** el costo por transacción de Cloud Storage varía según el tipo de objeto, el tamaño del objeto y la región. Para un objeto de 1 KB en la región us-central1, el costo por transacción es de aproximadamente $0,000001 USD (Google, s. f.).

Microsoft Azure:

Microsoft menciona unos ítems importantes para tener en cuenta:

- **Virtual Machines:** el costo por transacción de Virtual Machines varía según el tipo de instancia, la región y el período de tiempo. Para una instancia A1 v2 en la región central-us, el costo por transacción es de aproximadamente $0,000002 USD.

- **Azure Blob Storage:** el costo por transacción de Azure Blob Storage varía según el tipo de objeto, el tamaño del objeto y la región. Para un objeto de 1 KB en la región central-us, el costo por transacción es de aproximadamente $0,000001 USD.

El costo por transacción es una forma útil de comparar el valor de los servicios en la nube.

En general, el costo por transacción es relativamente bajo para AMS, Google y Azure.

Algunos ejemplos de transacciones que pueden ocurrir en un servicio en la nube incluyen:

- **Almacenamiento:** almacenar un archivo en un servicio de almacenamiento en la nube.
- **Procesamiento:** ejecutar un programa en un servidor en la nube.
- **Bases de datos:** consultar una base de datos en la nube.
- **Redes:** enviar un mensaje a través de una red en la nube.

Es importante considerar todos estos factores al estimar el costo de implementación de una red LoRaWAN o Z-Wave.

Ejemplo de costos:

- **Red LoRaWAN pequeña:** una red LoRaWAN pequeña con 10 dispositivos LoRaWAN, un *gateway* LoRaWAN y un servicio de *backend* puede costar alrededor de $10.000 USD.

- **Red LoRaWAN mediana:** una red LoRaWAN mediana con 100 dispositivos LoRaWAN, un *gateway* LoRaWAN y un servicio de *backend* puede costar alrededor de $100.000 USD.

- **Red LoRaWAN grande:** una red LoRaWAN grande con 1.000 dispositivos LoRaWAN, varios *gateways* LoRaWAN y un servicio de *backend* puede costar alrededor de $1.000.000 USD.

- **Red Z-Wave pequeña:** una red Z-Wave pequeña con 10 dispositivos Z-Wave, un concentrador Z-Wave y un servicio de *backend* puede costar alrededor de $500 USD.

- **Red Z-Wave mediana:** una red Z-Wave mediana con 100 dispositivos Z-Wave, un concentrador Z-Wave y un servicio de *backend* puede costar alrededor de $5.000 USD.

- **Red Z-Wave grande:** una red Z-Wave grande con 1.000 dispositivos Z-Wave, varios concentradores Z-Wave y un servicio de *backend* puede costar alrededor de $50.000 USD.

En general, LoRaWAN es más costoso de implementar que Z-Wave. Esto se debe a que LoRaWAN requiere más *hardware* y *software* y también requiere licencias de espectro en algunos países.

Escalabilidad

La escalabilidad en el contexto del IoT se refiere a la capacidad de operar de manera efectiva y eficiente en redes que pueden expandirse y adaptarse a medida que se incorporan más dispositivos.

Z-Wave emplea una estructura de red de estrella especial, en la que la información se transmite de un nodo a otro hasta alcanzar el concentrador. Esta

comunicación indirecta entre dispositivos permite expandir la red para incorporar hasta 4.000 nodos en una sola red, con 232 nodos para Z-Wave y 4.000 nodos para Z-Wave LR (Z-Wave Alliance, s. f.).

En una red LoRaWAN, cada dispositivo se comunica directamente con un *gateway*, lo que simplifica la expansión de la red. El número de dispositivos que una red puede manejar depende de la cantidad de mensajes que cada dispositivo envía diariamente. Por ejemplo, si cada dispositivo envía 10 mensajes al día, un solo *gateway* puede admitir alrededor de 10.000 dispositivos. Si la red incluye 10 *gateways*, podría manejar aproximadamente 100.000 dispositivos y hasta un millón de mensajes. Si se requiere más capacidad, todo lo que se necesita es agregar puertas de enlace adicionales a la red (Semtech, 2019).

Facilidad de implementación y mantenimiento

Comparando LoRaWAN y Z-Wave en términos de facilidad de implementación para soluciones IoT, se pueden identificar diferencias significativas. En lo que respecta a la infraestructura de red, LoRaWAN requiere la configuración de un *gateway* para garantizar una cobertura completa. Esto implica una inversión en *hardware* de *gateway* y conectividad a internet (Petrariu, Lavric & Coca, 2019). Por otro lado, Z-Wave permite que los dispositivos se comuniquen directamente en una red de malla, lo que puede requerir menos infraestructura en entornos más complejos.

En términos de conocimientos técnicos, la implementación de LoRaWAN puede resultar más compleja debido a factores como la ubicación, ya sea rural o urbana, lo que requiere conocimientos técnicos en infraestructura de redes, topología de red, enrutamiento de datos y comprensión de las especificaciones técnicas de los dispositivos seleccionados para conectar a la red LoRaWAN (Petrariu, Lavric & Coca, 2019). Por otro lado, Z-Wave ofrece una instalación y emparejamiento más sencillos, diseñados principalmente para permitir el uso de los dispositivos inmediatamente después de conectarlos y para emparejarlos fácilmente con otros dispositivos. Sin embargo, la configuración de redes extensas con más de cien dispositivos o con tipologías complejas, como redes con múltiples nodos interconectados y diversas rutas de comunicación, puede requerir experiencia técnica y conocimientos especializados en estos aspectos.

En lo que respecta a proveedores de productos y servicios, ambos protocolos cuentan con amplios ecosistemas de proveedores que ofrecen

productos y servicios compatibles (LoRa Alliance, 2021; Z-Wave Alliance, 2021). Esto proporciona opciones y flexibilidad a los usuarios al elegir dispositivos y soluciones que se adapten a sus necesidades específicas en sus aplicaciones IoT.

En cuanto al mantenimiento, Z-Wave utiliza redes de malla que son resistentes a fallos individuales. Si un dispositivo Z-Wave en la red experimenta un fallo, otros dispositivos pueden redirigir las señales a través de rutas alternativas, garantizando así la continuidad de la conectividad (Z-Wave Alliance, s. f.). Esta característica resulta especialmente beneficiosa en aplicaciones críticas donde la pérdida de comunicación podría tener un alto costo o representar un riesgo significativo. Además, esta capacidad facilita la expansión de la red sin necesidad de modificar la infraestructura existente, lo que simplifica en última instancia las tareas de mantenimiento.

En lo que respecta a los dispositivos finales, la sencilla instalación y emparejamiento de los dispositivos Z-Wave contribuye a reducir la complejidad asociada al mantenimiento de dispositivos individuales. Sin embargo, es importante destacar que la complejidad del mantenimiento dependerá de la infraestructura específica en uso.

En contraste, los dispositivos finales en una red LoRaWAN generalmente requieren un mantenimiento menos frecuente. Están diseñados para ser altamente eficientes en cuanto al consumo de energía y presentan una vida útil de la batería prolongada (LoRa Alliance, s. f.). Esto implica una menor necesidad de intervención y reemplazo, lo que puede simplificar aún más las tareas de mantenimiento en comparación con Z-Wave.

Conclusiones

Alcance y cobertura

LoRaWAN es ideal para aplicaciones que requieren una comunicación de largo alcance, especialmente en entornos rurales o áreas con poca infraestructura.

Z-Wave es más adecuado para aplicaciones de corto alcance en el hogar y la domótica. Su capacidad para atravesar obstáculos y penetrar paredes lo hace adecuado para aplicaciones en interiores.

Consumo de energía

LoRaWAN consume menos energía que Z-Wave y es más adecuado para dispositivos que deben funcionar con baterías durante períodos prolongados.

Z-Wave consume más energía, pero ofrece una respuesta más rápida y es adecuado para aplicaciones en las que la eficiencia energética es menos crítica.

Interoperabilidad y seguridad

Ambos protocolos son estándares abiertos y promueven la interoperabilidad entre dispositivos de diferentes fabricantes.

La seguridad es sólida en ambos protocolos, pero LoRaWAN es más resistente a los ataques de fuerza bruta, mientras que Z-Wave es más resistente a los ataques de intermediario.

Costos de implementación

Los costos de *hardware* y servidores de red tienden a ser más bajos en el caso de Z-Wave.

Los costos de implementación de LoRaWAN pueden ser más altos debido a la infraestructura de puertas de enlace y servidores de red.

Escalabilidad y mantenimiento

Ambos protocolos son escalables, pero LoRaWAN es más adecuado para implementaciones de mayor envergadura debido a su cobertura de largo alcance.

Z-Wave es más adecuado para aplicaciones de automatización del hogar y redes de menor escala.

Recomendaciones

Elección del protocolo

Seleccione el protocolo que mejor se ajuste a las necesidades de su aplicación. Si necesita una cobertura de largo alcance y una eficiencia energética, LoRaWAN es una excelente opción. Si su enfoque está en aplicaciones de hogar inteligente, Z-Wave podría ser más adecuado.

Seguridad

Independientemente del protocolo, asegúrese de configurar y mantener adecuadamente las medidas de seguridad, como la autenticación y el cifrado, para proteger sus datos y dispositivos.

Costos y escalabilidad

Considere su presupuesto y las necesidades de escalabilidad. Si planea una red grande, prepárese para una inversión inicial mayor en infraestructura LoRaWAN. Si está implementando una red más pequeña o una solución doméstica, Z-Wave podría ser más rentable.

Mantenimiento

Tenga en cuenta que, con el tiempo, todas las implementaciones IoT requieren mantenimiento. Evalúe la capacidad de su equipo para mantener y actualizar la red a medida que evolucionan las necesidades y las amenazas de seguridad.

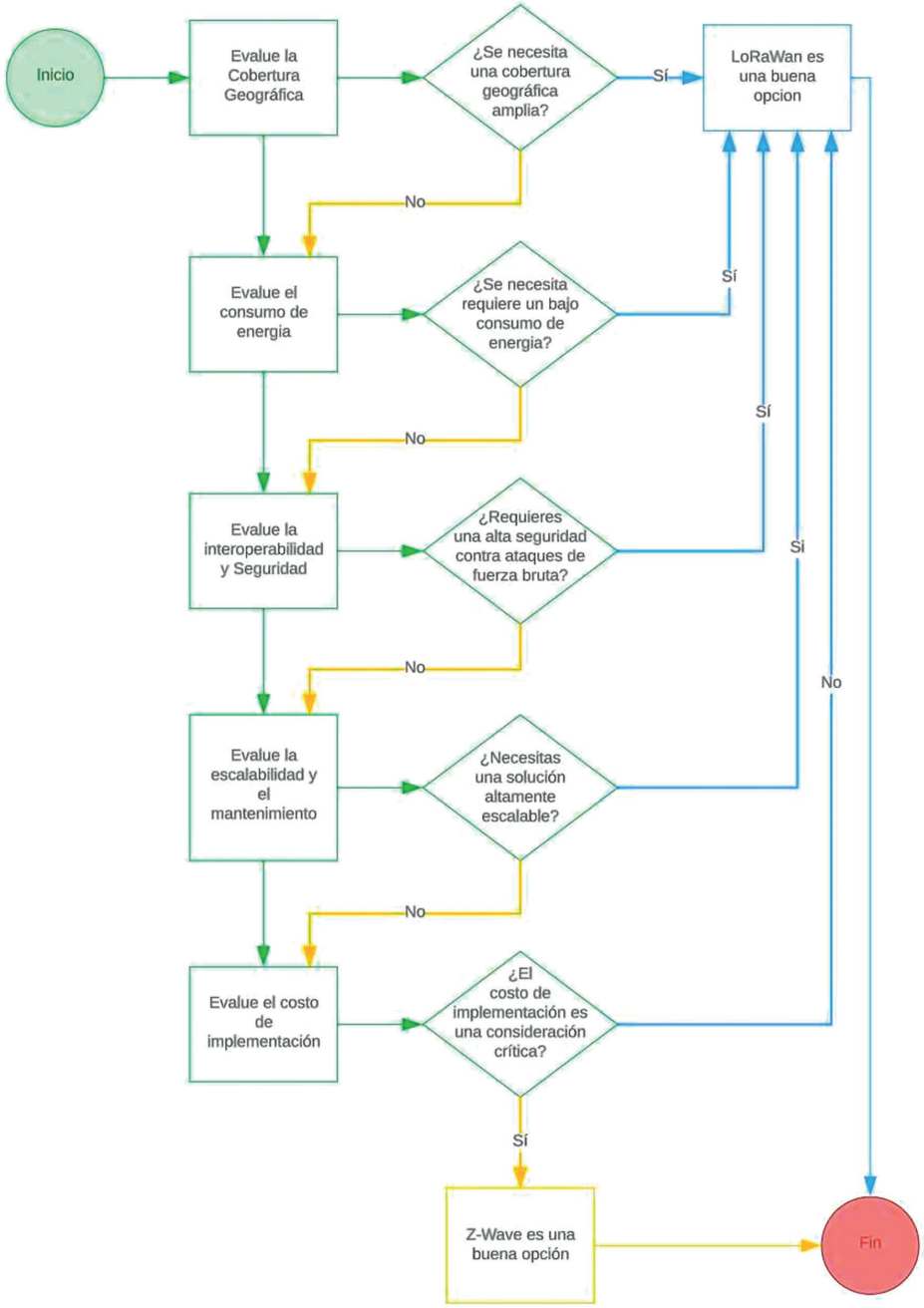
Pruebas piloto

Antes de realizar una implementación a gran escala, considere realizar pruebas piloto para evaluar el rendimiento y la eficacia del protocolo en su caso de uso específico.

Cuál escoger

Para ayudarlo en la toma de decisión entre LoRaWan y Z-Wave, hemos elaborado el siguiente diagrama de flujo:

Figura 15. Diagrama de flujo selección de protocolo



Nota. Diagrama de flujo principales características para tener en cuenta en la toma de decisión entre LoRaWan y Z-Wave.

Referencias

Adrián I. Petrariu, A. L. (23-26 de octubre de 2019). *Gateway LoRaWAN: diseño, implementación y pruebas en entorno real*. Obtenido de ieeexplore: https://ieeexplore.ieee.org/document/9823664

Aeotec (s. f.). *aërQ Temperature and Humidity Sensor*. Obtenido de https://aeotec.freshdesk.com/support/solutions/articles/6000227919-a%C3%ABrqtemperature-and-humidity-sensor-technical-specification-

Aeotec (s. f.). *Home Energy Meter Gen5*. Obtenido de https://aeotec.freshdesk.com/support/solutions/articles/6000168072-home-energy-meter-gen5-technical-specifications-

Aeotec (s. f.). *MultiSensor 7*. Obtenido de https://aeotec.freshdesk.com/support/solutions/articles/6000246153-multisensor-7technical-specifications

Aeotec (s. f.). *Recessed Door Sensor 7*. Obtenido de https://aeotec.freshdesk.com/support/solutions/articles/6000226851-recessed-door-sensor-gen7-technical-specifications-

Aeotec (s. f.). *TriSensor*. Obtenido de https://aeotec.freshdesk.com/support/solutions/articles/6000195461-trisensor-technicalspecification-

Aeotec (s. f.). *Water Sensor 7*. Obtenido de https://aeotec.freshdesk.com/support/solutions/articles/6000228223-water-sensor-7technical-specifications-

Amazon (s. f.). Obtenido de Amazon: https://aws.amazon.com/es/ec2/pricing/?p=pm&c=ec2&z=4

Calidad del aire (4 de enero de 2022). Obtenido de Universidad Distrital: https://geox.udistrital.edu.co/index.php/reving/article/view/17589

Casanova, A. (18 de febrero de 2017). *Seguridad en redes LoraWAN*. Obtenido de https://digimodes.wordpress.com/2017/02/18/seguridad -en-redes-lorawan-parte-i/

Catsensors (s. f.). *Sensor DL-PAR IoT LoRaWAN: radiación fotosintéticamente activa*. Obtenido de https://www.catsensors.com/media/Decentlab/Decentlab-DL-PAR-datasheet.pdf

Catsensors (s. f.). *Sensor DL-PR21 LoRaWAN: nivel, temperatura y presión (sonda digital I2C)*. Obtenido de https://www.catsensors.com/media/Decentlab/DL-PR21-datasheet_2019.pdf Catsensors

Catsensors (s f.). *Sensor DL-PYR IoT LoRaWAN: radiación solar*. Obtenido de https://www.catsensors.com/es/lorawan/sensores-lorawan-decentlab/dl-pyr-sensor-lorawanradiacion-solar

Catsensors (s. f.). Sensor DL-SMTP IoT LoRaWAN Agricultura: Perfil AquaCheck de Temperatura y Humedad Relativa del subsuelo. Obtenido de https://www.catsensors.com/media/Decentlab/Productos/Decentlab-DL-SMTPdatasheet.pdf

Catsensors (s. f.). *Sensor DL-WRM: sensor de temperatura de superficie + temperatura y humedad relativa*. Obtenido de https://www.catsensors.com/media/Decentlab/Decentlab-DL-WRM-datasheet-2022.pdf

Catsensors (s. f.). *Termómetro infrarrojo/sensor de temperatura de superficie*. Obtenido de https://www.catsensors.com/media/Decentlab/Decentlab- DL-ITST-datasheet-2022.pdf

Cruz Vega, M., Oliete Vivas, P., Morales Ríos, C., González Luis, C., Cendón Martín, B. & Hernández Seco, A. (2015). *Las tecnologías IOT dentro de la industria conectada*. España: EOI Escuela de Organización Industrial.

DHL (s. f.). Obtenido de DHL: https://www.dhl.com/mx-es/home/supply-chain/industrias/tecnologia.html

e-consulta (s. f.). Obtenido de e.consulta: https://www.e-consulta. ¿com/nota/2019-09-01/sociedad/en-puebla-el-control-del-servicio-de-agua-mas-moderno-del-pais-ap

embeddedcomputing (s. f.). Obtenido de Embedded Computing: https://embeddedcomputing.com/application/automotive/adas-autonomous-drive/antzertech-introduces-lorawan-and-nb-iot-vehicle-tracker

Fotia, L. (2023). *Security, Trust and Privacy Models, and Architectures in IoT Environments*. Alemania: Springer International Publishing.

Global Market Insights (febrero de 2022). Obtenido de "ZigBee Market by Application, Vertical, and Region - Global Forecast to 2027,": https://www.gminsights.com/

Google (s. f.). Obtenido de Google: https://cloud.google.com/pricing/list?hl=es

Homesecurity (s. f.). Obtenido de Homesecurity: https://www.homesecurity.com.co/

IADB (junio de 2016). Obtenido de IADB: https://publications.iadb.org/en/international-casestudies-smart-cities-medellin-colombia

Ingetes (s. f.). Obtenido de Ingetes: https://www.ingetes.com.co/en/home/

Instituto Nacional de Ciberseguridad (15 de junio de 2023). *LoRaWAN y su aportación a las tecnologías IIoT*. Obtenido de https://www.incibe.es/incibe-cert/blog/lorawan-y-suaportacion-las-tecnologias-iiot

Kobal, D. (11 de marzo de 2019). *Inceptum*. Obtenido de https://www.inceptum-oss.com/fieldservice-management-in-the-era-of-the-industrial-internet-of-things-iiot/

Lidia Fotia, F. M. (2023). *Security, Trust and Privacy Models, and Architectures in IoT Environments*. Springer.

LoRa (s. f.). *LoRa Developer portal*. Obtenido de https://loradevelopers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan/

LoRa Alliance (s. f.). *LoRaWAN*. Obtenido de https://lora-alliance.org/

Manrique Latorre, M., Buitrago Márquez, L. & Hernández Gutiérrez, J. (2019). *Redes LoRaWAN. Revisión de componentes funcionales en aplicaciones IoT*. Bogotá: Universidad Distrital Francisco José de Caldas.

Mario Cruz Vega, P. O. (2015). *Las tecnologías IOT dentro de la industria conectada*. España: EOI Escuela de Organización Industrial.

MarketsandMarkets (febrero de 2020). Obtenido de "LoRaWAN Market by Component, Deployment Type, Application, Vertical, and Region - Global Forecast to 2025": https://www.marketsandmarkets.com/

Medium (25 de septiembre de 2017). *Haciendo IoT con LoRa*: Capítulo 1.- "¿Qué es LoRa y LoRaWAN?". Obtenido de https://goo.su/6BFcUep

Microsoft (s. f.). Obtenido de Microsoft: https://azure.microsoft.com/es-es/solutions/cloudeconomics/

Oracle (3 de septiembre de 2023). *Oracle*. Obtenido de https://www.oracle.com/co/internet-of-things/what-is-iot/

Petrariu, A. I., Lavric, A. A. & Coca, E. E. (23-26 de octubre de 2019). *LoRaWAN Gateway: Design, Implementation and Testing in Real Environment*. Obtenido de IEEExplore: https://ieeexplore.ieee.org/document/8990791

Quiñonez Muñoz, O. (2019). *Internet de las Cosas (IoT)*. n.p.: Ibukku, LLC.

RF Wireless Word (2023). Obtenido de RF Wireless Word: https://www.rfwirelessworld.com/Tutorials/z-wave-security.html.

SAP (s. f.). *SAP*. Obtenido de https://www.sap.com/latinamerica/products/artificialintelligence/what-is-iot.html

Semtech (s. f.). Obtenido de Semtech: https://www.semtech.com/company/press/semtech-andwitrac-transform-asset-tracking-for-maritime-transport-utilizing-lorawan

Semtech (diciembre de 2019). *LoRa® and LoRaWAN®: A Technical Overview*. Obtenido de https://lora-developers.semtech.com/uploads/documents/files/LoRa_and_LoRaWANA_Tech_Overview-Downloadable.pdf

Semtech (s. f.). *Control PerSe, sensor humano de 3 canales de baja potencia SX9210*. Obtenido de https://semtech.my.salesforce.com/sfc/p/#E0000000JelG/a/2R000000UhVf/_oKgstKC7CCljWxbYQ.E48VQJTo9WvOwEEIlF0l5owk

Semtech (s. f.). *LoRa Connect™ para aplicaciones de hogar inteligente, transceptor LoRa de bajo consumo +22 dBm*. Obtenido de https://semtech.my.salesforce.com/sfc/p/#E0000000JelG/a/2R000000HTJR/Tem0gUxGfOZ2Qn3bUzmV2zKNQRYJ3bpobPfOQ7B.erE

Silabs (s. f.). *Z-Wave Global Regions - Where Z-Wave Works*. Obtenido de https://www.silabs.com/wireless/z-wave/global-regions

Smarthomecolombia (s. f.). Obtenido de Smarthomecolombia: https://www.smarthomecolombia.com.co/

SPC (s. f.). Obtenido de SPC: https://www.spc.es/products/spc-aura

Thingpark (s. f.). Obtenido de Thingpark: https://market.thingpark.com/lorawan-contact-tracingsensor-30.html

Tibco (septiembre de 2023). *Tibco*. Obtenido de https://www.tibco.com/es/reference-center/whatis-the-internet-of-things-iot

Z-Wave Alliance (2023). *Security Overview*. Obtenido de https://www.rfwireless-world.com/Tutorials/z-wave-security.html.

Z-Wave (s. f.). *Z-Wave*. Obtenido de https://www.z-wave.com/

Z-Wave Alliance (s. f.). *Descripción general de la tecnología*. Obtenido de https://zwavealliance.org/

Z-Wave Alliance (2022). *What is Z-Wave Long Range and How Does it Differ from Z-Wave?* Obtenido de https://z-wavealliance.org/what-is-z-wave-long-range-and-how-does-itdiffer-from-z-wave/

Ethical hacking: Una vista hacia la ciberseguridad en Colombia y México en sector industria 4.0 y educativo

Ethical hacking: a look at cybersecurity in Colombia and Mexico in the industry 4.0 and education sector

Bernal Bohorquez, David Orlando
Candidato a ingeniero de telecomunicaciones

Moreno Ramírez, Wendy Vanessa
Candidato a ingeniero de telecomunicaciones

Ricardo Mena, Emily Tatiana
Candidato a ingeniero de telecomunicaciones

Robayo Perdomo, Andrés Felipe
Candidato a ingeniero de telecomunicaciones

Tuso Saldaña, Anyela Andrea
Candidato a ingeniero de telecomunicaciones

Hernández Martín, Jhon Alexander
Docente del programa de ingeniería en telecomunicaciones

Resumen

Hoy en día, es común escuchar historias entre profesionales y trabajadores en las que se comentan experiencias relacionadas con ciberataques personales y empresariales. En este documento, se abordarán aspectos centrados en la consulta e investigación sobre la temática de ciberseguridad, puntualmente dirigido hacia el *hackeo* ético (*ethical hacking*). En el desarrollo de este documento se realizaron una serie de actividades en la Universidad UCompensar, así como también una salida internacional de investigación con el ánimo de realizar levantamiento de información sobre el *ethical hacking* y cómo lo abordan las instituciones visitadas, las cuales estarán mencionándose en la trazabilidad de este documento. El interés hacia la temática estuvo dado a que puede convertirse en una gran estrategia proactiva, haciendo uso de herramientas abiertamente disponibles a todo el público y que están diseñadas para el despliegue del *hackeo* ético a nivel empresarial. Así mismo, se buscará establecer algunas recomendaciones que puedan ser adoptadas por empresas de cualquier sector económico (industria, tecnología, educación, entre otras), que posteriormente puedan ser consideradas abiertamente como planes de acción, metodologías o soluciones.

Palabras clave: *hacking ético, ciberseguridad, nube, AIoT, SOC, pruebas de penetración, vulnerabilidades.*

Abstract

Nowadays, it is common to hear stories among professionals and workers, in which experiences related to personal and business cyberattacks are discussed. This document will address aspects focused on consultation and research on the topic of cybersecurity, specifically directed towards ethical hacking. In the development of this document, a series of activities were carried out at the UCompensar university as well as an international research outing with the aim of collecting information on ethical hacking and how the institutions visited address it, which will be mentioned in the traceability of this document. The interest in the topic was due to the fact that it can become a great proactive strategy, making the use of tools openly available to the public and that are designed for the deployment of ethical hacking at a business level. Likewise, we will seek to establish some recommendations that can be adopted by compa-

nies in any economic sector (industry, technology, education, among others), in which they can later be openly considered as action plans, methodologies or solutions.

Keywords: *ethical hacking, cybersecurity, cloud, IA, SOC, penetration test, vulnerabilities.*

Cursos articulados

Gracias a las asignaturas de Metodología para el Manejo de la Información, Seguridad en Redes de Telecomunicaciones, Seguridad de la Información, Servicios en Sistemas de Telecomunicaciones, Diseño de Proyectos y Gestión de Proyectos, estarán soportándose los conocimientos adquiridos, así como las investigaciones que forman parte integral de este documento.

Introducción

En la actualidad, existe una gran variedad de herramientas y sistemas informáticos diseñados para que las personas documenten o plasmen información, ya sea para uso propio, particular o para soportar trazabilidades de grado un poco más complejo como actividades productivas. Algunos escenarios son:

Office365 de Microsoft brinda un entorno colaborativo que ofrece un lugar para desarrollar sitios web compactos, equipos de trabajo, almacenamiento en la nube, conversaciones en tiempo real y modificación de documentos en línea, junto con una variedad de otras herramientas beneficiosas para fomentar la colaboración laboral (Quintero Barrizonte, 2020).

FreeNAS es un sistema operativo de código abierto basado en UNIX, específicamente en FreeBSD, diseñado para funcionar como un servidor de almacenamiento conectado a la red (NAS). Permite transformar una computadora en un dispositivo capaz de proporcionar soporte de almacenamiento en red, lo que posibilita tareas como el almacenamiento de archivos multimedia, imágenes, documentos, bases de datos, entre otros, accesibles desde cualquier ubicación en la red (Quintero Barrizonte, 2020).

La computación en la nube posee una variedad de ventajas y desventajas que no siempre se solapan. En líneas generales, OneDrive en la nube ofrece múltiples beneficios, aunque con ciertas precauciones, especialmente si se trata de un usuario novato. Puede requerir un cierto nivel de comprensión para utilizarlo eficientemente (Agus *et al.*, 2019).

Retomando un poco la historia, en la época de los 70 se produjo lo que se denominó la revolución telemática; en aquella época se desarrollaron los primeros sistemas de información que hacían uso de las telecomunicaciones y la informática como dúo dinámico, las bases de datos y los vídeos con texto fueron los primeros en marcar la información digital (Vargas, 2019). Ahora, ya hablando directamente a nivel empresarial, por lo general las compañías utilizan herramientas un poco más sofisticadas o de pago para guardar la información de sus colaboradores internos o externos, en sistemas desde los más simples hasta los más complejos que se pueda llegar a imaginar. La intención de enfocarse en los procedimientos internos es mejorar la eficiencia de la secuencia de actividades de la empresa. Siguiendo este razonamiento, de acuerdo con el estudio de Ávila *et al.*, el Cuadro de Mando Integral (CMI) contribuye con el 69 %, el Sistema de Información Ejecutiva (EIF) con el 8 %, la minería de datos con el 8 % y el modelo tradicional con el 15 % (Ávila *et al.*, 2020). Allí los autores hacen referencia al análisis sobre el manejo corporativo con recursos tanto humanos como tecnológicos, con enfoque al manejo de la información.

Ahora bien, vale la pena mencionar que la sociedad actualmente se encuentra en una era donde el crecimiento de los sistemas digitales es exponencial y ferozmente acelerado. En el año 2018, la seguridad de la información personal de más de 2 mil millones de individuos se vio amenazada debido a diversas vulnerabilidades en la protección de datos en línea (Páez *et al.*, 2019). Por esta razón, el *ethical hacking* o *hackeo* ético se ha convertido en una metodología primordial para la seguridad de los sistemas informáticos y la información contenida en ellos.

En este punto ya es necesario desglosar un poco la definición de *ethical hacking*. Es un término que se usa indistintamente con *hacktivismo* en los medios, pero que tiene un significado distinto en la disciplina de la informática; no encasilla al término explícitamente como un servicio, sino más bien como el uso no violento de una tecnología en pro de una causa, política o de otro tipo, que a menudo es jurídica y moralmente ambigua (Maurushat, 2019).

Entonces, la práctica de *hackeo* ético, cuando es permitido, resulta ser efectiva para identificar ciertas amenazas o vulnerabilidades en la red, proporcionando a las empresas una destreza a la hora de proteger eficazmente lo más importante, que es la información (González González, 2023). Ahora bien, un ataque a nivel de red como lo es la denegación de servicios consiste en saturar la red hasta que esta falle; este tipo de ataques puede venir desde cualquier parte del mundo, desde el momento en que se tenga una conexión a internet.

El *hackeo* ético tiene como propósito el estudio y las prácticas sobre el uso del *hacking* en todos los ámbitos informáticos (Ariza Bonces, 2019).

Otra perspectiva es la indicada por Sánchez, quien resalta más allá el término de *ethical hacking* al considerar dos categorías de *hackers*: aquellos que tienen buenas intenciones se les puede llegar a denominar como *hackers* éticos, dado que usan los principios de ética y hacen uso de sus habilidades y técnicas proporcionando seguridad a datos confidenciales de una organización. Por otra parte, menciona a los *cracker*, los cuales explica que son individuos que rompen la seguridad de alguien con el objetivo principal de robar o intenciones maliciosas considerando el daño a la información más relevante (Sánchez Ávila, 2019).

Acorde a lo mencionado previamente, no solamente es necesario considerar a qué se refiere el *hackeo* ético, sino también qué tipo de propósitos y perfiles de individuos son abordados por este tipo de práctica. Claramente, todas las perspectivas abordadas hablan desde algún punto de conocimiento en experiencias que lograron dar forma a una práctica que hoy en día es considerada casi que de manera exclusiva para las organizaciones, pero que si alguien desea realizarlo para uso investigativo o experimental, lo podrá hacer, dentro de los alcances y permitiendo garantizar el costo, la flexibilidad, la eficiencia y sobre todo la seguridad dentro de las políticas que maneje la empresa (Navarro *et al.*, 2022).

Remontando un poco a la historia, Jaquet-Chiffelle discrimina en su obra que por allá en los años 1960-1970 (que a fecha de hoy ya son varias décadas) los piratas informáticos que surgían en dicha época no estaban impulsados a ejecutar acciones malintencionadas o intenciones maliciosas, sino que frecuentemente apoyaban valores éticos más grandes que las cuestiones de seguridad informática, como la libertad de expresión e incluso la democracia. Menciona que así mismo las computadoras, por no charlar de las redes, se encontraban en plena fase de desarrollo; la grandeza

de la economía que era influenciada por la informática era realmente insignificante en comparación con la influencia actual y los estudiantes o exploradores de este ámbito (como los programadores) apenas lograban imaginar todo un ecosistema digital (Jaquet-Chiffelle & Loi, 2020).

A partir de este punto, dejando claro cuál es el tema central de la investigación, estará estableciéndose la metodología sobre la cual se realizaron las consultas, de manera directa, de algunas fuentes bibliográficas en la web que pueden llegar a soportar la información establecida en este documento, así como los hallazgos sobre charlas nacionales e internacionales obtenidas y algunas herramientas a utilizar en base al *ethical hacking* de tipo sombrero gris (*gray hat*), las cuales pueden ser utilizadas a nivel personal, profesional o laboral.

Los fundamentos esenciales del *hacking* ético se exponen para comprender los principios cruciales relacionados con la utilización de herramientas automatizadas de penetración remota. Además, se especifican los componentes necesarios para ejecutar con éxito un ataque empleando Metasploit o herramientas de Kali Linux (De la Cruz Gámez, 2022).

Metodología

Dentro del marco de investigación, se realizaron actividades relacionadas con la industria 4.0 y 5.0 por medio de charlas brindadas en la Universidad Fundación Universitaria Compensar, de manera virtual y presencial. La primera charla fue realizada por un especialista externo de la empresa Bosch con representación en Colombia. Allí, estudiantes y docentes de la institución recibieron información de gran interés con enfoque hacia la historia y los hitos referentes a la industria y automatización. Dado que no es un tema que se va a profundizar en este documento, se aprovecharon los espacios brindados para generar preguntas a la ciberseguridad y puntualmente hacia el tema de *ethical hacking*.

Infortunadamente no fueron fructíferas las consultas, ya que la charla estuvo enfocada hacia la evolución de la industria, aunque por parte del expositor comentó en su momento que dicho fabricante cuenta con el desarrollo de plataformas de ciberseguridad, pero no enfocadas hacia el servicio de *ethical hacking*, tema central de este documento. Dadas las circunstancias, se procedió a realizar la consulta en la internet, en donde se realiza el hallazgo

de temas relacionados con la ciberseguridad por parte de Bosch en Colombia y es allí donde ellos mismos recalcan la importancia de la seguridad de la información, donde garantizan y contribuyen en la industria por medio de los desarrollos de AIoT (Inteligencia Artificial de las Cosas).

Explican que en este tipo de soluciones se busca establecer una confiabilidad en los sistemas dando por entendido que es más que necesario tener un buen manejo de la seguridad y la privacidad de la información, siendo que la AIoT no se enfoca específicamente en conectar cosas, sino en hacer una participación para los negocios y la vida privada de las personas (Robert Bosch Ltda., 2021).

Por otro lado, luego de la charla mencionada, se realiza una conferencia por parte del hoy en día profesor de investigación Ing. Omar León, egresado de la Fundación Universitaria Compensar y que se encuentra actualmente en la Escuela Politécnica de Ingeniería en España trabajando en proyectos de investigación enfocados a la industria 4.0, en donde León menciona que no solamente se busca indagar el impacto industrial, sino también social. Al final de la charla, uno de los estudiantes invitados consultó sobre el tema de ciberseguridad y sobre el impacto que puede llegar a tener en la industria al expositor, pero realmente en este punto fue más una opinión que un argumento en firme, puesto que claramente la charla no era exclusiva o enfocada hacia ciberseguridad.

Es entendible en este punto, dado que el enfoque de la investigación estuvo dirigido hacia la industria, pero es aquí donde a los autores de este documento les es muy relevante el abarcar la investigación hacia el manejo de la información, dado que en la industria, si bien se cuenta con muchos desarrollos hacia nuevos sistemas o el mejoramiento de los mismos, no tanto hacia el cómo se trata la información, es decir, cómo se almacena, quién tiene acceso, quién puede influir en ella, protegerla, eliminarla, consultarla o cualquier acción sobre la misma. En estas actividades o acciones es donde cabe perfectamente el uso de estrategias de *hackeo* ético, en donde se puede llegar a hacer un estudio sobre los sistemas (sean sistemas de *big data* o desarrollo de aplicaciones o los mismos sistemas informáticos) que tienen que ver directamente con la automatización y digitalización de la información.

Dichas charlas son la base en la cual están realizándose las consultas y generación de inquietudes de ¿cómo llegar a realizar un *hackeo* ético hacia componentes del ecosistema de la industria 4.0? o ¿podrían llegar

a realizarse estudios de tipo *hackeo* ético hacia las compañías que se hayan involucrado de manera directa en el marco de investigación de este proceso? Pues bien, dado que la información no logró obtenerse de manera directa, en decisión unánime se procede a realizar actividades de *pentesting* sobre los dominios que pueden llegar a ser visitados de manera pública de las instituciones involucradas en las charlas, Bosch Colombia y la Universidad de Oviedo.

Se listan a continuación los siguientes dominios para ser estudiados con las herramientas disponibles de manera abierta de tipo Open Source (fuente abierta): 1) https://www.bosch.com.co/ y 2) https://www.uniovi.es/. Los hallazgos que llegasen a reportarse en las herramientas a utilizar estarán siendo compartidos a nivel de imágenes *printscreen* en la sección de resultados.

Retomando nuevamente la inmersión internacional, los autores, junto con los directores de programa, realizan una visita al país de México, en donde se tiene previamente un cronograma de trabajo; los autores tienen prevista la visita a las entidades Audi, KIO y Universidad Autónoma de México (sede Ecatepec) y la ciudad universitaria ubicada en la Ciudad de México CDMX.

Dentro de los resultados que estarán plasmándose más adelante, se realizarán algunos comentarios al respecto de las ventajas y desventajas que se tienen a nivel de industria en una comparación de opinión neutra entre los países de Colombia y México.

Tal como se realizaron las actividades de testeo de penetración (*pentesting*) a las entidades relacionadas previamente de Colombia, se ejecuta el mismo procedimiento con las entidades conocidas y visitadas en México en los dominios públicos: *https://www.audi.com.mx/; https://www.kio.tech/esmx/; https://www.unam.mx/*; *https://cuecatepec.uaemex.mx/*. Es de aclarar que las intenciones de dichas pruebas son netamente investigativas y no cuentan con un fin específico. En caso de encontrar vulnerabilidades o novedades en los resultados, se estará informando a los puntos de contacto de cada entidad, según aplique.

Con el fin de entender cómo se encuentra actualmente la ciberseguridad, se aclara y desglosa la ciberseguridad a nivel global. No es sorpresa mencionar que el ecosistema tecnológico de hoy se encuentra interconectado a una red informática mundial (Mirashi, 2023). A diario, las personas se conectan a través de las redes sociales, plataformas digitales y otros medios

de comunicación digital, en donde se almacenan inimaginables volúmenes de *bytes* de información que embeben datos sensibles y la privacidad de los usuarios, tanto compañías privadas, empresas públicas del sector gobierno, usuarios individuales y otros.

El departamento de tecnología de la información administra un servidor especializado en guardar una variedad de archivos. Este servidor está enlazado a una dirección IP y puede ser accesible por cualquier dispositivo dentro de la organización. En varios dispositivos, no se solicita identificación para acceder a este servidor, lo que podría permitir a usuarios no autorizados manipular los documentos almacenados a su voluntad (Damián Retamozo, 2020).

Ahora bien, se evidencia que se ha generado un aumento en la ciberdelincuencia, por el cual se ha visto un crecimiento en los diferentes métodos para extorsionar, robar o suplantar la identidad de los usuarios (Sánchez, 2019). Desde otra vista, a partir de la llegada del COVID-19, la humanidad se vio obligada a desplazarse al mundo digital, siendo ahora común entre las compañías contar con empleados en teletrabajo, lo cual permite que los usuarios se encuentren vulnerables en la red, por lo que se ha convertido en un reto para los gobiernos de cada país salvaguardar y crear políticas para proteger los datos, tal como se expresa a continuación:

> Con la COVID-19, las amenazas han ido en aumento al mismo ritmo que los ciberataques a organismos estatales, autonómicos, y, también, a las entidades locales, mucho más frágiles y vulnerables en el entorno digital en esta etapa de transición hacia una plena transformación en administración electrónica, más expuesta a fallos de seguridad (Ametller, 2021).

Con respecto a los blancos preferidos por los ciberdelincuentes, son aquellos que suministren con facilidad su información, como ubicación, dirección IP, metadatos, entre otros, y aquellos que proporcionen bases de datos relevantes, tales como hospitales, laboratorios, sistema bancario y aquellos sectores que mueven la economía del mundo, es decir, bases de datos que suministren información valiosa para la competencia, delincuentes, aseguradoras, etc. (Anaya Laime, 2022).

En el mundo, la noción de la ciudad inteligente, o *smart city*, implica el uso extensivo de datos, incluyendo su adquisición, recolección, almacenamiento y análisis, para así obtener valor que facilite la toma de decisiones

y la prestación de servicios ágiles y eficaces (Hueso & Signes, 2022), lo cual genera que información sensible sea más vulnerable a infiltraciones de personas no autorizadas.

Se deben aplicar políticas y regulaciones tanto para atenuar vulnerabilidades físicas como digitales con el objetivo de reducir fallos en la red y evitar el acceso no autorizado por parte de intrusos, lo que podría perjudicar la documentación empresarial (Durand More, 2019). El Gobierno estadounidense y chino están desarrollando planes para gestionar la seguridad de la información,

> Por lo tanto, la seguridad del espacio cibernético se convierte tanto en un ámbito de cooperación como de conflicto para ambos Estados, propiciado por el desarrollo de las nuevas tecnologías de información y comunicación (Patiño Orozco, 2021).

Para el Estado Federal, la ciberseguridad se ha convertido en el intento de salvaguardar los sistemas digitales e informáticos y así lograr garantizar la confidencialidad de la información, compartir datos de manera segura y garantizar la disponibilidad de la red. De igual manera, el Estado Federal pretende garantizar que la fiabilidad de la información no ha sido alterada ni modificada y es auténtica (Patiño Orozco, 2021)

A nivel de Latinoamérica, se han introducido numerosas herramientas informáticas que los ciudadanos de Ecuador utilizan en línea para una variedad de propósitos, como transacciones financieras, educación, interacciones sociales y actividades de ocio. Esto ha despertado el interés de los ciberdelincuentes, quienes han identificado fallos de seguridad en las tecnologías de la información y la comunicación (Villacís, 2022).

A través de este plan de aseguramiento se pretende realizar un esquema controlado de ataques al servidor web de la Universidad Técnica del Norte (UTN), en el cual se utilizó la metodología ofensiva de seguridad para la ejecución de un *pentesting* que establece mejoras en el rendimiento del servicio web (Cuzme-Rodríguez *et al.*, 2019).

Marco legal en México:

1. Ley Federal de Protección de Datos Personales en Posesión de los Particulares: esta legislación regula la protección de datos personales en México y establece las obligaciones de las organizaciones en cuanto al manejo adecuado de la información personal (Tenorio Cueto, 2019).

2. Conforme a la norma ISO 27001, la protección de la información se refiere a mantener su confidencialidad, integridad y disponibilidad, así como la salvaguarda de los sistemas relacionados con su manipulación dentro de una entidad u organización (Arias León & Ruiz Correa, 2019).

Marco legal en Colombia:

1. Regulación en materia de protección de datos: Colombia cuenta con regulaciones específicas en materia de protección de datos personales, como la Ley 1581 de 2012 y el Decreto 1377 de 2013. Estas leyes establecen los principios y requisitos para el manejo de datos personales y la seguridad de la información (Jiménez Reyes, 2023).

2. Guía de Seguridad de la Información (RISI): la Superintendencia de Industria y Comercio (SIC) de Colombia ha desarrollado la Guía de Seguridad de la Información (RISI), que proporciona orientación sobre cómo implementar medidas de seguridad de la información de acuerdo con la legislación colombiana (Ministerio de las Tecnologías de Información y Comunicaciones [MinTIC] de Colombia, 2020)

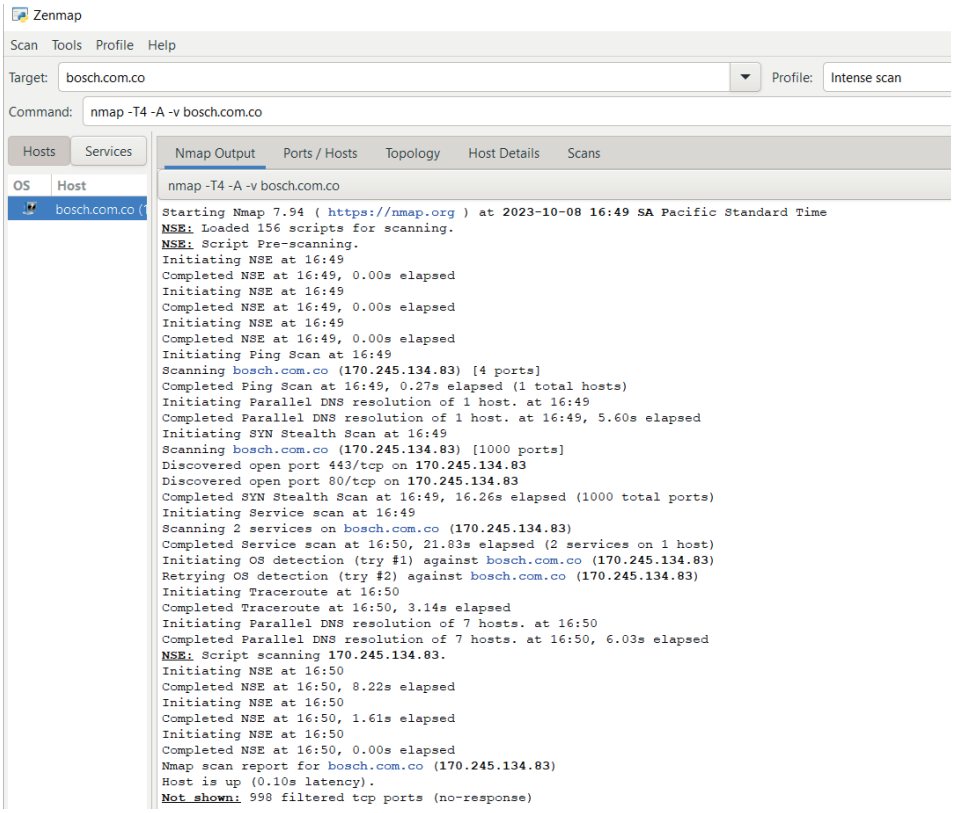
3. ISO 27001: al igual que en México, muchas organizaciones colombianas optan por implementar el estándar ISO 27001 para gestionar la seguridad de la información de manera más estructurada y basada en riesgos (Mendoza Gamboa, 2019).

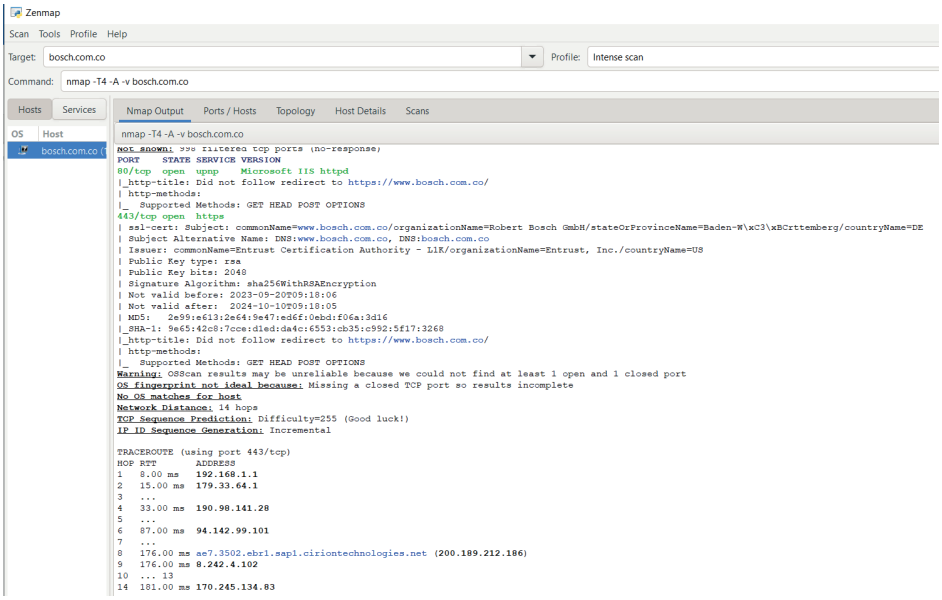
Resultados

Dentro del objetivo de *ethical hacking*, se realiza un *pentesting* por medio de la herramienta Nmap de Windows; entre una amplia gama de herramientas informáticas, ha sido adoptada para diversos fines en línea, como transacciones financieras, educación, interacciones sociales y entretenimiento. Esto ha despertado la atención de los delincuentes cibernéticos, quienes han descubierto vulnerabilidades en las tecnologías de la información y la comunicación (Monterroza Barrios, 2019).

Ahora bien, acorde a las actividades basadas en la herramienta Nmap en Windows se obtuvo:

Figura 16. Muestreo de resultados con herramienta Nmap en dominio

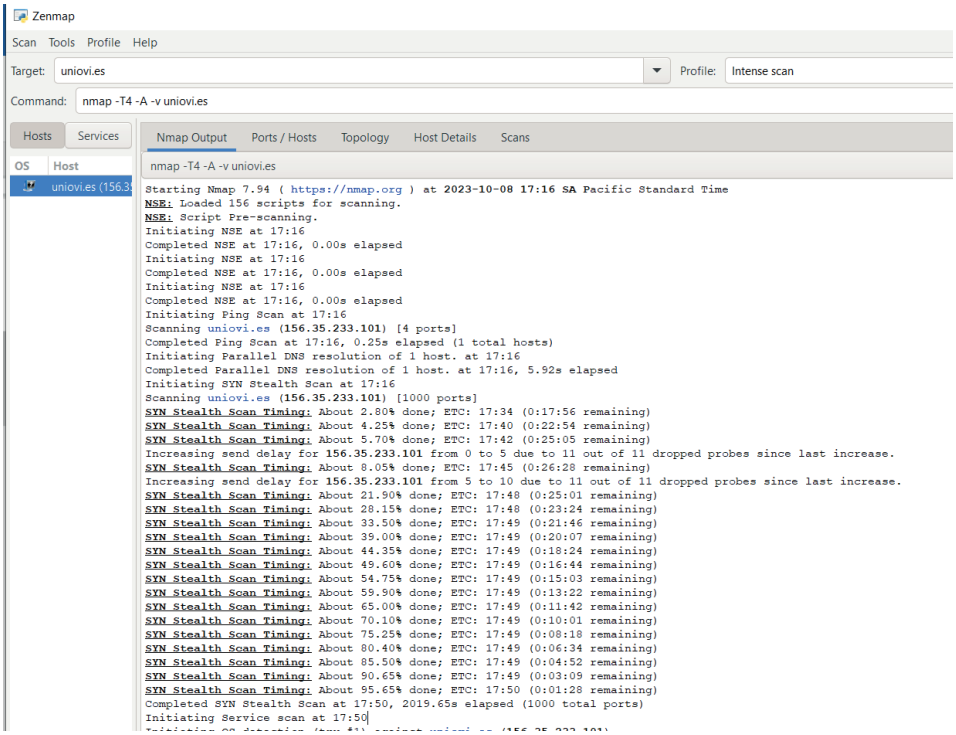


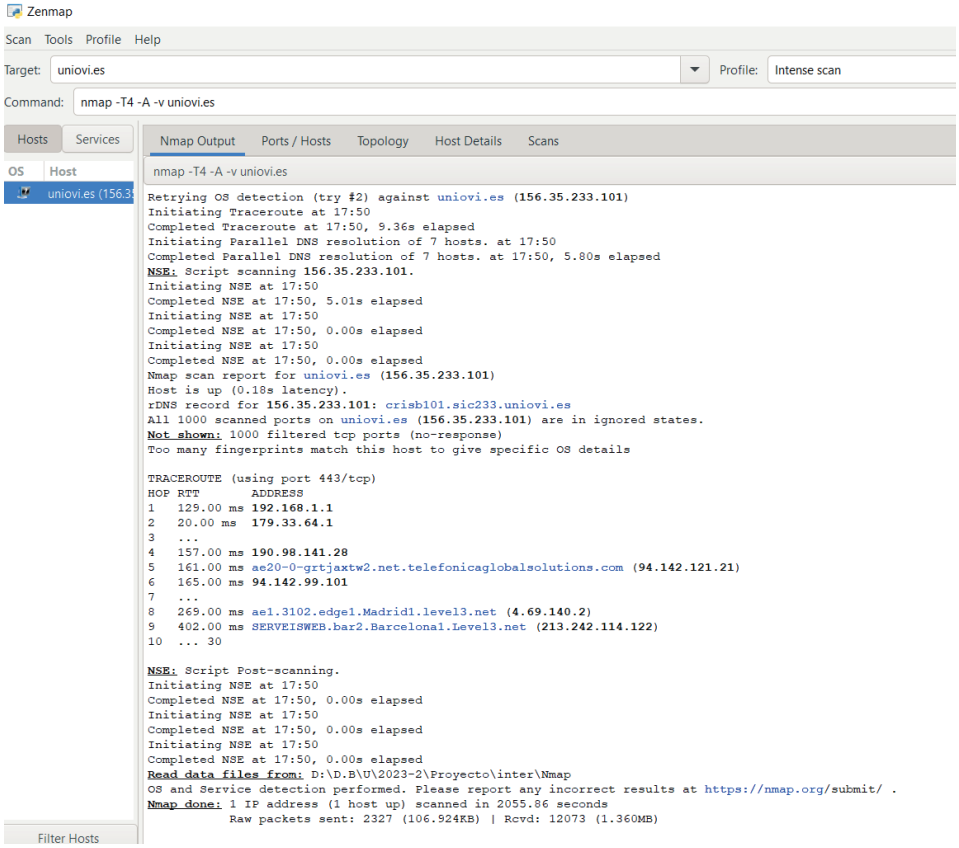


```
NSE: Script Post-scanning.
Initiating NSE at 16:50
Completed NSE at 16:50, 0.00s elapsed
Initiating NSE at 16:50
Completed NSE at 16:50, 0.00s elapsed
Initiating NSE at 16:50
Completed NSE at 16:50, 0.00s elapsed
Read data files from: D:\D.B\U\2023-2\Proyecto\inter\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 71.31 seconds
           Raw packets sent: 2130 (98.856KB) | Rcvd: 10842 (1.226MB)
```

Nota. Muestreo de resultados herramienta Nmap en dominio web https://www.bosch.com.co.

Figura 17. Muestreo de resultados con herramienta Nmap en dominio web

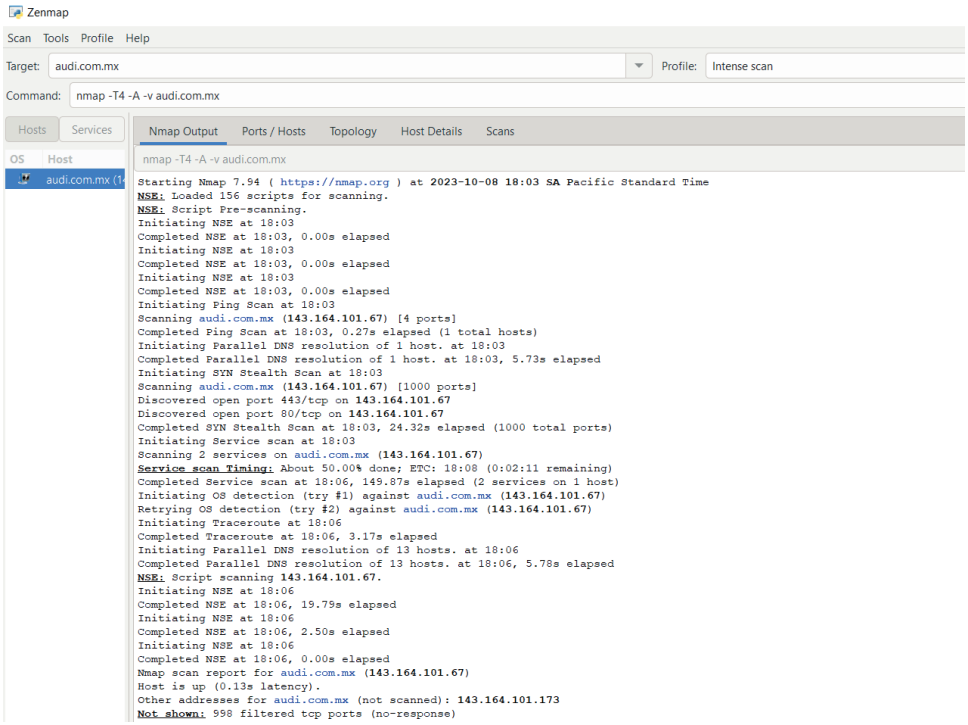


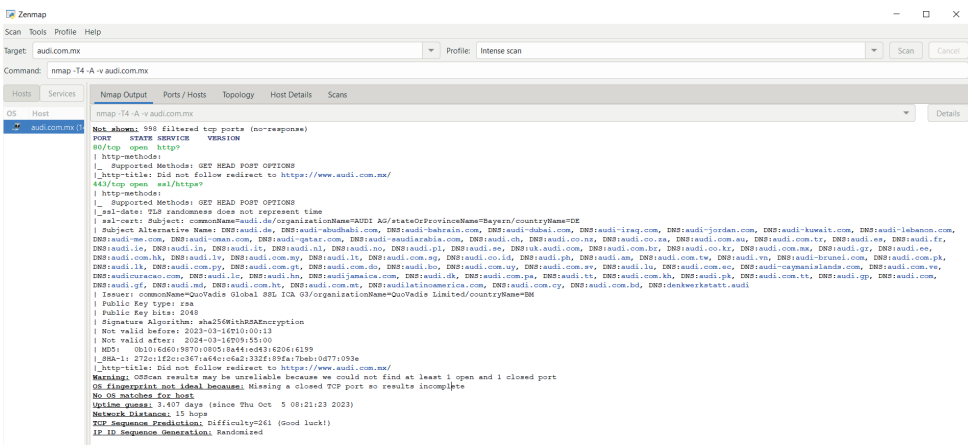


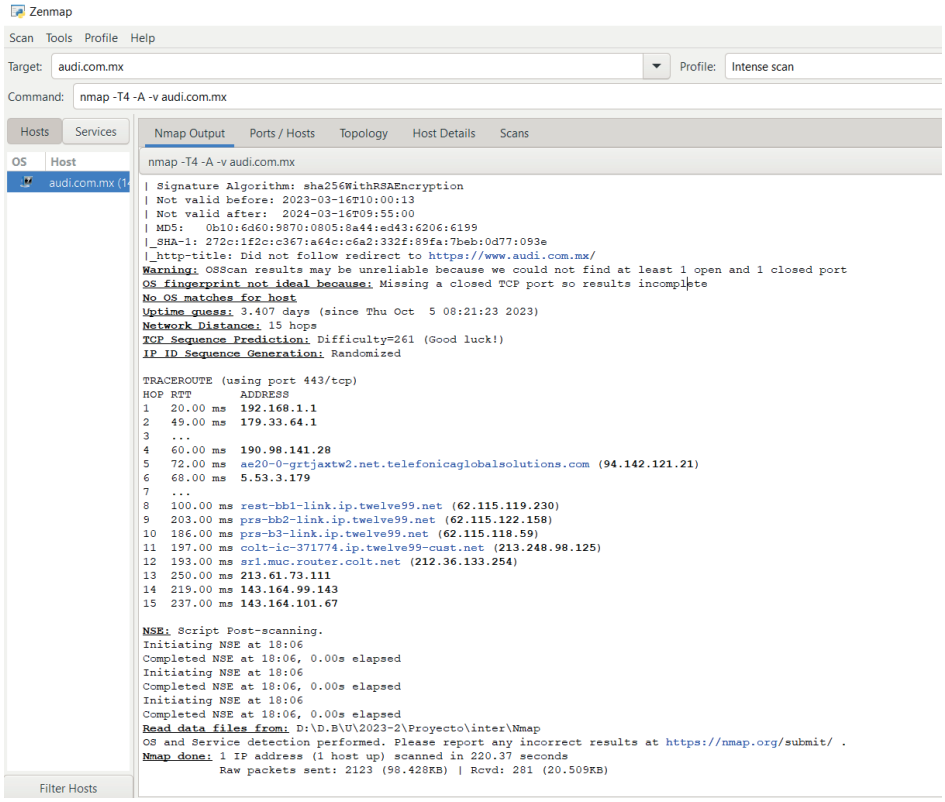
Nota. Muestreo de resultados con herramienta Nmap en dominio web https://www.uniovi.es/.

Respecto a las empresas visitadas en México, se obtuvieron los dominios previamente mencionados en la metodología de este documento, en donde se obtienen los siguientes resultados:

Figura 18. Muestro y resultados de herramienta Nmap en dominio web https://www.audi.com.mx/

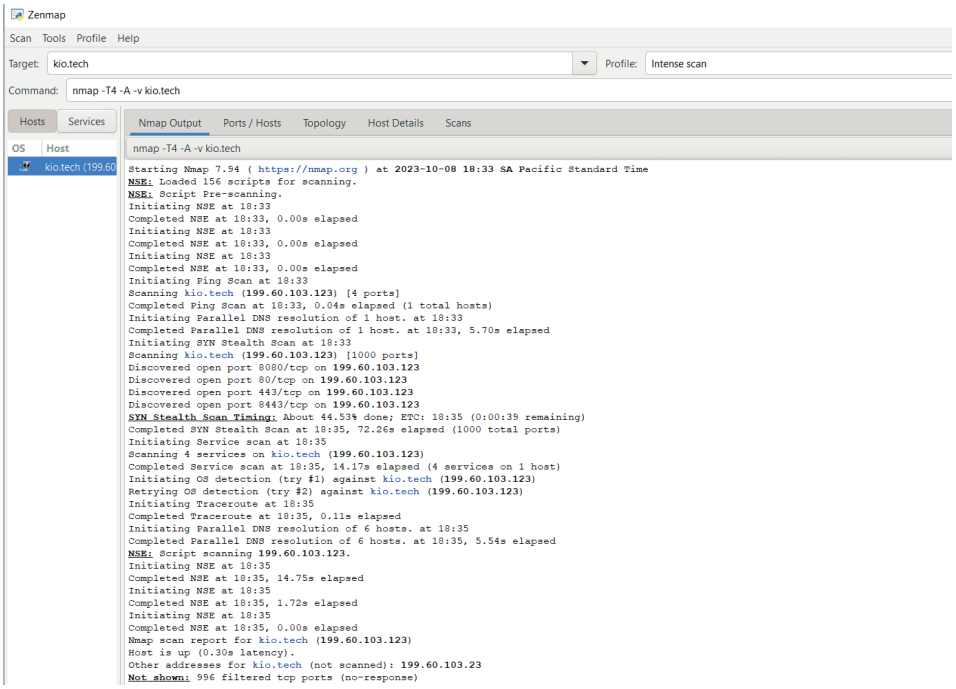


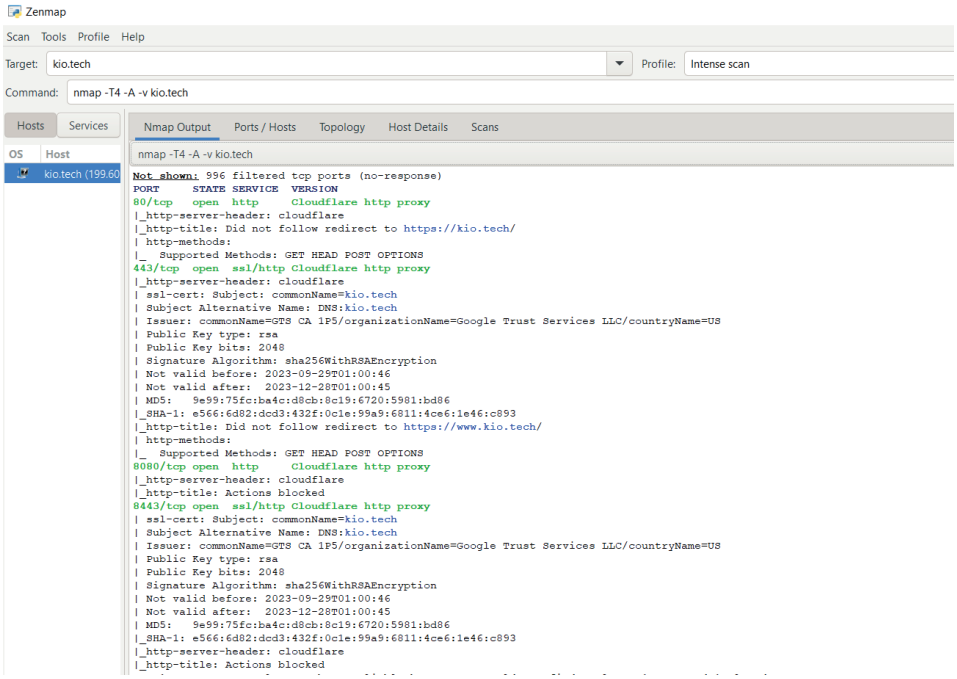


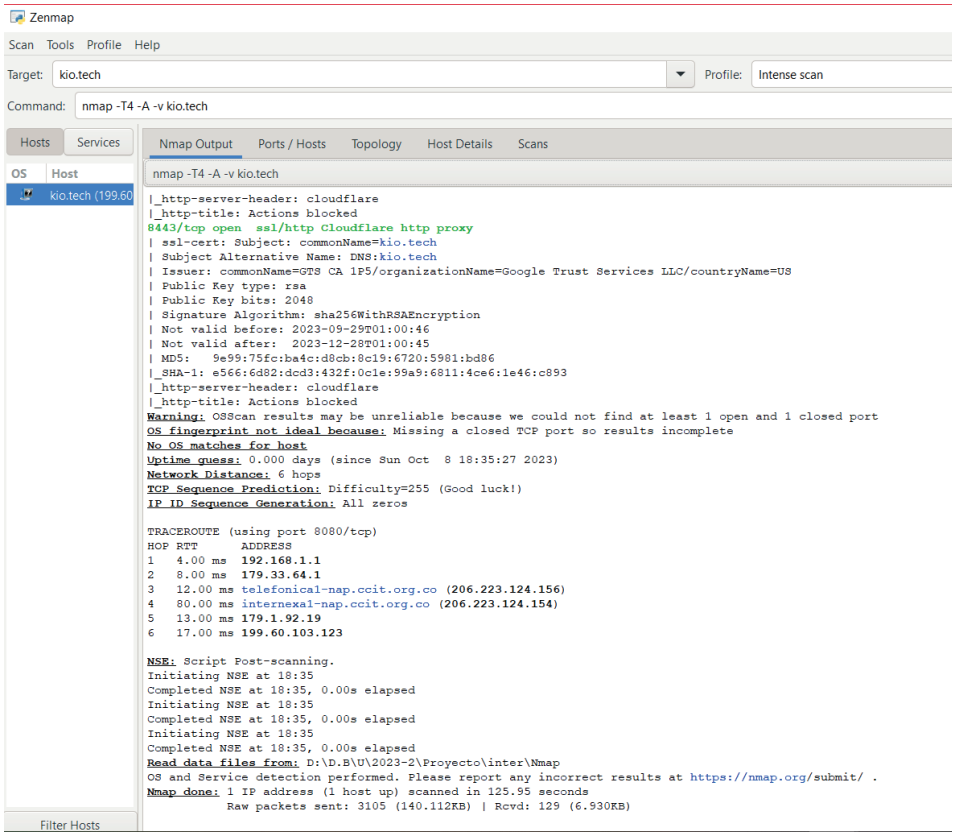


Nota. Muestro y resultados de herramienta Nmap en dominio web https://www.audi.com.mx/.

Figura 19. Muestreo y resultados de herramienta Nmap en dominio web https://www.kio.tech/es-mx/

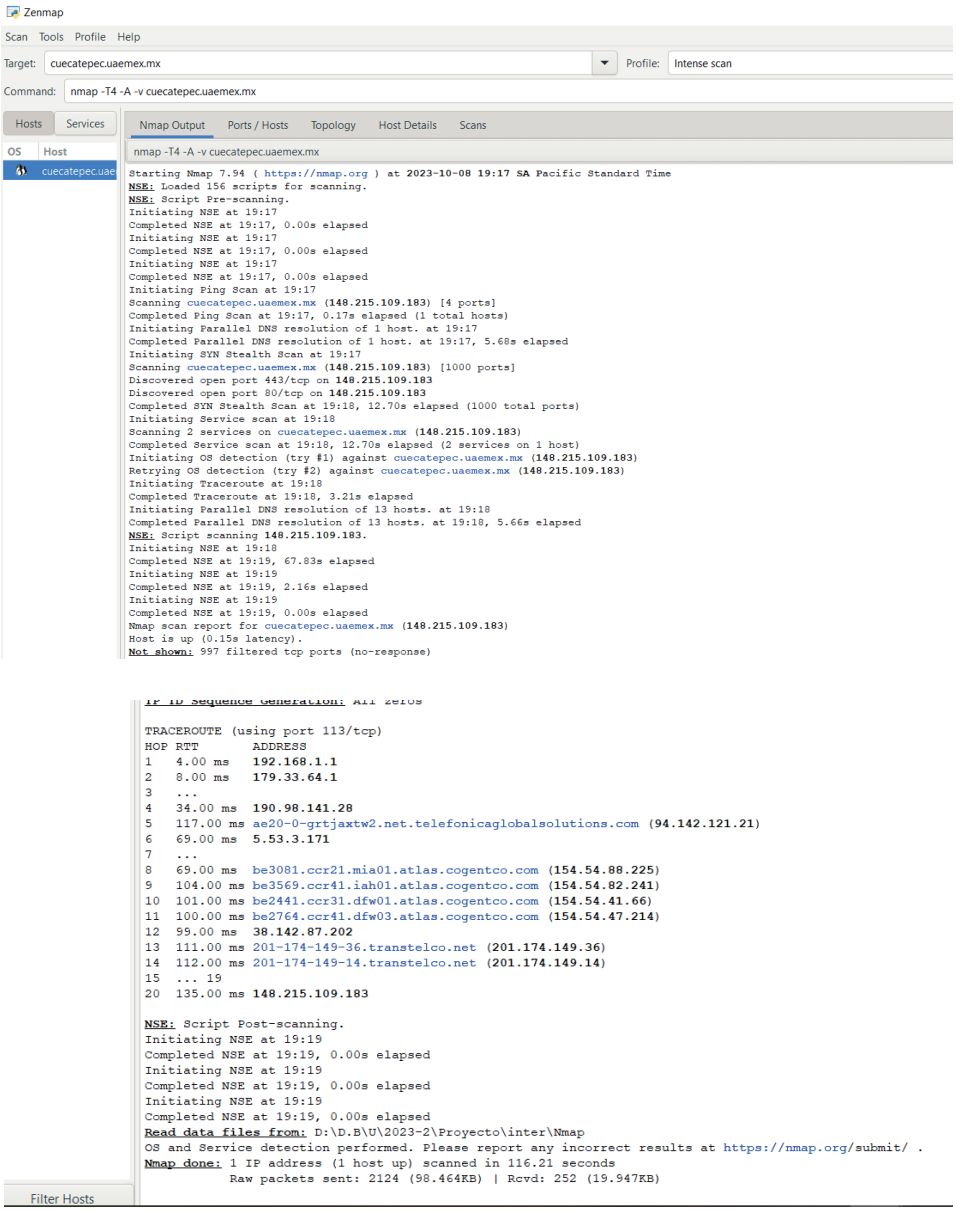






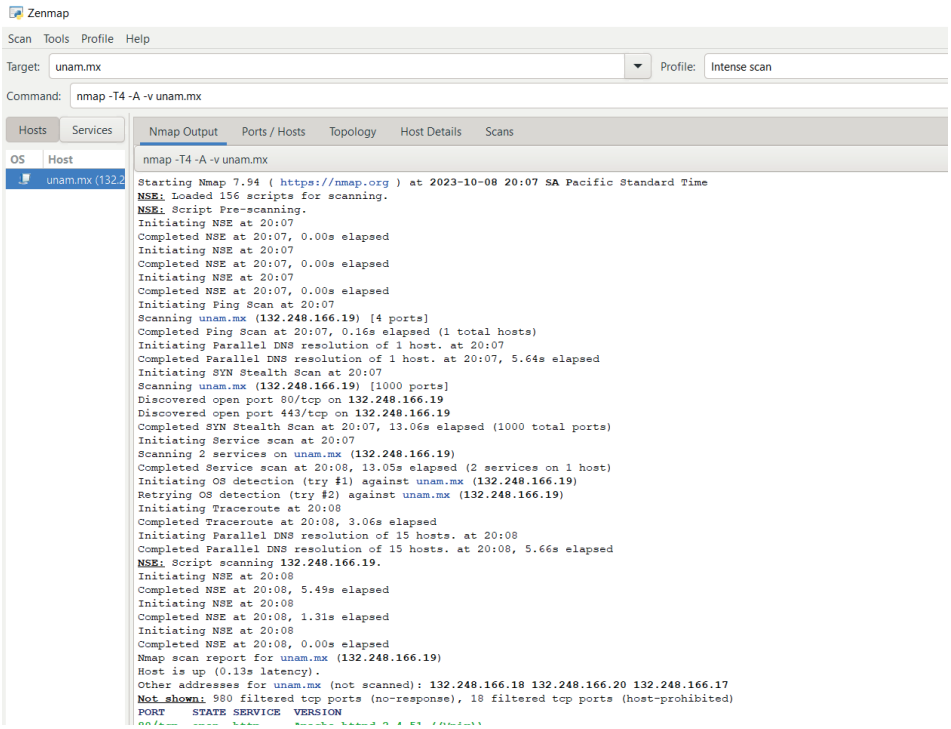
Nota. Muestreo y resultados de herramienta Nmap en dominio web https://www.kio.tech/es-mx/.

Figura 20. Muestreo y resultados de herramienta Nmap en dominio web https://cuecatepec.uaemex.mx/



Nota. Muestreo y resultados de herramienta Nmap en dominio web https://cuecatepec.uaemex.mx/.

Figura 21. Muestro y resultados de herramienta Nmap en dominio web https://www.unam.mx/




```
TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   9.00 ms   192.168.1.1
2   14.00 ms  179.33.64.1
3   ...
4   32.00 ms  190.98.141.28
5   81.00 ms  ae20-0-grtjaxtw2.net.telefonicaglobalsolutions.com (94.142.121.21)
6   72.00 ms  5.53.3.171
7   104.00 ms 213.140.37.158
8   ...
9   127.00 ms 245.189-204-203.bestelclientes.com.mx (189.204.203.245)
10  121.00 ms 106.200-57-8.bestelclientes.com.mx (200.57.8.106)
11  135.00 ms 104.200-57-8.bestelclientes.com.mx (200.57.8.104)
12  131.00 ms 141.189-202-244.bestelclientes.com.mx (189.202.244.141)
13  136.00 ms 177.201-148-69.bestelclientes.com.mx (201.148.69.177)
14  129.00 ms 192.100.200.81
15  127.00 ms 132.248.133.50
16  131.00 ms 1006-iimas.redunam.unam.mx (132.247.237.221)
17  132.00 ms 132.248.166.19

NSE: Script Post-scanning.
Initiating NSE at 20:08
Completed NSE at 20:08, 0.00s elapsed
Initiating NSE at 20:08
Completed NSE at 20:08, 0.00s elapsed
Initiating NSE at 20:08
Completed NSE at 20:08, 0.00s elapsed
Read data files from: D:\D.B\U\2023-2\Proyecto\inter\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.90 seconds
           Raw packets sent: 2090 (95.540KB) | Rcvd: 289 (22.230KB)
```

Discusión y experiencias obtenidas

Análisis sobre la charla presencial de ingeniero mecánico de la multinacional Bosch

Aquí se amplió la visión de la empresa que día a día innova con su gran grupo de investigadores, los cuales generan no solo herramientas de construcción, las más populares, sino un conglomerado de equipos que aportan en la industria 4.0, entre ellos: microchips que están en la estación espacial, gafas de realidad aumentada, sensores IoT en vehículos para mejorar la movilidad urbana, escáneres biométricos, lectores de retina, equipos de control y monitoreo, motores eléctricos a la vanguardia de este tipo de industria, electrodomésticos con diferentes prestaciones.

Análisis sobre charla virtual del docente investigador Omar León de la Universidad UCompensar, quien está realizando su estancia postdoctoral en la Universidad de Oviedo en España

La charla se basó en la industria 4.0, en donde abarcó en primera medida la historia de las industrias y su evolución, la importancia de conocer el término e irlo implementando a medida que se vaya conociendo la tecnología; además, expuso ejemplos con el videojuego Pokemon Go, el cual se basa en realidad aumentada, así como también dio una introducción de la industria 5.0, en donde la inteligencia artificial formaría parte del diario vivir, poniendo en tela de juicio si la humanidad cuenta con el control de ella, así como el miedo a posibles consecuencias.

La multinacional Audi en San José de Chiapa cerca de la ciudad de Puebla Mx.

Se indica como primera medida a los visitantes (incluyendo claramente a los autores de este documento) que se deben dejar equipos electrónicos y celulares en el bus, ya que por políticas de la compañía son prohibidos al interior de la planta por temas de confidencialidad; seguido, el ingreso fue bastante riguroso por temas relacionados con el sistema de registro de visitantes, el cual lo realizan tres funcionarios en un software que colocaban dato a dato en este; dentro de la planta, la visita fue guiada por tres pasantes de recursos humanos y estas colaboradoras brindan una introducción explicando que la planta produce exclusivamente vehículos de la línea Q5.

Retomando el tema principal, el cual es el estudio del *ethical hacking* y la ciberseguridad, se logra observar que las funcionarias en la explicación tenían equipos celulares, los cuales usaban para comunicarse con los demás empleados y que llevaban todo el tiempo generando un riesgo potencial, ya que dentro de la línea hay un sistema de códigos QR y lectores wifi para la personalización de los vehículos a petición del cliente.

Data center de KIO en la ciudad de Santiago de Querétaro (México)

Una de las visitas más enriquecedoras a nivel de sistemas informáticos fue el poder apreciar el *data center* de la empresa KIO, donde los estándares de seguridad se componen de 5 filtros que se observan desde el ingreso, donde nos registraban y escaneaban con detectores de metales; seguido, una charla introductoria en la cual se nos divide en dos grupos de 16 personas para empezar el recorrido, para lo primero dar a conocer que tienen redundancia en absolutamente todo, desde la parte eléctrica hasta la conexión por fibra óptica.

El concepto de KIO es traducido al español como "espejo" y es precisamente replicar el sistema para tener respaldo; en cuanto al inicio, se observa una conexión eléctrica la cual tiene dos ingresos de energía de diferentes sectores eléctricos según la distribución de la ciudad, por lo que, si falla, entra como primera medida una UPS de seis minutos, tiempo para encender plantas generadoras de corriente alterna que funcionan con ACPM; estas plantas tienen también un respaldo. Por parte del edificio principal, un bloque de concreto dividido horizontalmente en tres pisos tipo búnker, el cual maneja dos secciones verticales con respaldo el uno del otro, sistemas de CCTV a lo largo de todo el complejo, sala de SOC (Security Operations Center) con más de 30 personas verificando tráfico y posibles amenazas de intrusión.

Dentro de la infraestructura de los *rack*, hay pasillo de zonas frías y calientes con sensores de temperatura, sistema de aire acondicionado y todos los demás estándares a nivel global, que ofrecen alta disponibilidad, redundancia, seguridad y mantenimiento en todo lo que compone el término *data center*. Luego del recorrido, a los visitantes se les ingresa a una sala con los ingenieros encargados del SOC, los cuales ofrecen información limitada; entre esta indican que el NOC (Network Operations Center) no se encuentra en esa sede y se encargan de responder lo justo por temas de confidencialidad.

Es crucial que los países desarrollen un comité inclusivo para abordar las malas experiencias pasadas en la región, donde la falta de cooperación entre las autoridades y las partes interesadas ha sido un problema. Este comité permitirá la interacción entre el instituto, la industria, la academia, las entidades públicas y cualquier otra persona interesada para discutir las necesidades, estrategias y estudios actuales y futuros sobre la transformación digital y el impacto de 5G en el servicio público de telecomunicaciones (De León, 2022).

La Universidad Autónoma del Estado de México

Para esta visita, los directivos debían tener credenciales que permitieran la identificación de los visitantes (en este caso, los autores y otros estudiantes de la UCompensar). Dentro de las instalaciones, se organizaron grupos de seis personas con el ánimo de ejecutar un recorrido por las diferentes sedes indicando cómo implementan las tecnologías de la industria 4.0; adicional, se recorren las áreas donde se logró observar proyectos de realidad virtual y aumentada, recolección de datos (*big data*), *display* flexible donde imprimían el circuito y se podía observa la estructura electrónica con microscopio, *software* de identificación de perfiles educativos a través de herramientas propias. En cuanto al análisis de *ethical hacking*, se observó que no tienen una cultura de seguridad informática dentro de todo el personal que compone la universidad, esto evidenciándose que están enfocados principalmente en *big data* y realidad virtual; además, en forma incógnita, se abre el historial de búsqueda en uno de los equipos de cómputo evidenciando acceso libre a internet sin restricciones.

La Universidad Nacional Autónoma de México

Esta conceptualizada como ciudad universitaria debido a su gran extensión; la llegaron a comparar como 5 veces más grande que la Universidad Nacional en Bogotá, Colombia. Este complejo comprende las diferentes facultades dictadas según la estructura del Gobierno mexicano. La visita se concentró en conocer los diferentes laboratorios del área de ingeniería industrial; adicional, se conoció el edificio de investigación de todas las áreas de la robótica, en donde se observaron los diferentes proyectos realizados por estudiantes y profesores; también se vio el proceso de cómo se crea una impresión 3D.

Conclusiones

- Se determina que la ciberseguridad se encuentra en un alto crecimiento, ya que se hace importante para las compañías implementar dentro de su organización planes de seguridad informática para evitar el robo de su información.

- Se observa que a nivel latinoamericano no hay leyes establecidas que encaminen al cumplimiento de la ciberseguridad como escudo de protección hacia los ataques, lo cual es apenas entendible, dado que es tocar directamente el músculo financiero de las empresas e inversionistas; no es solo un requisito que debe cumplirse, sino una obligación de todos.

- Es claro que las metodologías de *ethical hacking* son parte fundamental del estudio de las aplicaciones y portales web que pertenecen al sector estudiado, en donde es posible evaluar ciertos riesgos que pueden ser mitigados y así evitar la propagación de ataques de cualquier rango.

- En la inmersión internacional se logró reflejar que el *hacking* ético en el contexto de la industria 4.0 revela la presencia de vulnerabilidades específicas, como la falta de actualizaciones de seguridad en dispositivos IoT, la exposición de interfaces de control industrial a internet y la falta de conciencia de seguridad en colaboradores de instituciones de educación e industria.

- Se identifica y establece que la seguridad cibernética en la industria 4.0 es un proceso continuo que debe resaltar la necesidad de evaluar periódicamente los sistemas de ciberseguridad, así como la ejecución de tipo *pentesting* y ejecutar las actualizaciones de políticas de seguridad para mantenerse al día con las amenazas en constante evolución y desarrollo.

- Se evidencia que, en la actualidad, el manejo de la información y el poseer bases de datos sensibles otorga una posición privilegiada, por lo cual es primordial salvaguardar esta data de los ciberdelincuentes.

Recomendaciones

Dentro del alcance investigativo y de la experiencia relacionada en este documento, se encontraron algunas características que valen la pena resaltar sobre las entidades visitadas, enfocado a la ciberseguridad y *ethical hacking*. En este punto, se logra identificar que en México hay muy poco enfoque e importancia sobre el tema de la ciberseguridad, las sedes universitarias y compañías visitadas no tenían mayor información con respecto al tema de la ciberseguridad. En la parte del SOC de KIO, sí es posible decir que tienen su propio departamento de *ethical hacking* tanto a nivel de cliente como a nivel de usuario interno. Dentro de su alcance, cuentan con capacitaciones internas sobre temas de ciberseguridad a todos los empleados de la compañía.

En cuanto a las entidades educativas, infortunadamente no se evidenció que cuenten con campañas o información sobre la ciberseguridad e incluso se evidenció que los equipos de salas visitadas estaban desbloqueados y con acceso, no existió algún tipo de restricción a la información (sea delicada o no), datos que no deberían poder consultarse. Ahora bien, respecto a Colombia, hay una escasa normativa según las consultas realizadas y están a nivel de sugerencias y modelos de recomendación, como lo son las guías de ciberseguridad publicadas por MinTIC, pero no hay una estrategia seria y de fondo sobre cómo se debe abordar el tema de la ciberseguridad y quizás un plan de trabajo que integre al *ethical hacking* como una estrategia idónea como escudo ante amenazas informáticas.

Referencias

Agus, I., Destiawati, F. & Dhika, H. (2019). "Perbandingan cloud computing Microsoft Onedrive, Dropbox, dan Google drive". *Faktor Exacta*, 12(1), 20-27.

Ametller, D. C. (2021). *Ciberseguridad: un nuevo reto para el Estado y los gobiernos locales*. El Consultor de los Ayuntamientos Wolters Kluwer España.

Anaya Laime, J. A. (2022). *La ciberdelincuencia y su influencia en el desarrollo económico-social en el distrito de Ayacucho, 2021*.

Arias León, J. A. & Ruiz Correa, J. G. (2019). *Definición de un modelo de evaluación de riesgos en seguridad de la información bajo los lineamientos de la norma ISO 27001, utilizando técnicas de redes neuronales*.

Ariza Bonces, D. M. (2019). *Ethical hacking: una estrategia de defensa proactiva*.

Ávila, E. M. B., Álvarez, J. C. E., Zurita, I. N. & Guzmán, D. M. C. (2020). "Soluciones corporativas de inteligencia de negocios en las pequeñas y medianas empresas". *Revista Arbitrada Interdisciplinaria Koinonía*, 5(10), 483-513.

Cuzme-Rodríguez, F., León-Gudiño, M., Suárez-Zambrano, L. & Domínguez-Limaico, M. (2019). "Offensive Security: Ethical Hacking Methodology on the Web". *Information and Communication Technologies of Ecuador* (TIC. EC), 6, 127-140.

Damián Retamozo, M. (2020). *Políticas de seguridad basadas en ethical hacking para mejorar los sistemas de intranet en la división de soporte informático del Hospital Ramiro Prialé Prialé-Huancayo*.

De la Cruz Gámez, E. (2022). *Ethical Hacking to remote systems using Metasploit and Kali Linux*. 2022 11th International Conference On Software Process Improvement (CIMPS), 224-226.

De León, O. (2022). *Redes 5G en América Latina: desarrollo y potencialidades*.

Durand More, A. D. (2019). *Evaluación de técnicas de ethical hacking para el diagnóstico de vulnerabilidades de la seguridad informática en una empresa prestadora de servicios*.

González González, J. M. (2023). *Uso de las técnicas del hacking ético para la reducción de amenazas de ciberseguridad*. Computer Engineering.

Hueso, L. C. & Signes, A. T. (2022). *Explotación y regulación del uso del big data e inteligencia artificial para los servicios públicos y la ciudad inteligente*. Tirant lo Blanch.

Jaquet-Chiffelle, D.-O. & Loi, M. (2020). "Ethical and unethical hacking". *The Ethics of Cybersecurity*, 179-204.

Jiménez Reyes, M. (2023). *El contenido y alcance de la imagen como derecho personal en la Ley 1581 de 2012 y su protección ante la Superintendencia de Industria y Comercio (SIC)*.

Maurushat, A. (2019). *Ethical hacking*. University of Ottawa Press.

Mendoza Gamboa, D. C. (2019). *Diseño de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001 para la Secretaría de Educación Departamental del Norte de Santander*.

Ministerio de las Tecnologías de Información y Comunicaciones (MinTIC) de Colombia. (2020, noviembre 11). *Guía 3 - Procedimiento de seguridad de la información*.

Mirashi, E. (2023). *Tratamiento procesal del cibercrimen y diligencias de investigación tecnológica: casuística y problemática*. Aranzadi/Civitas.

Monterroza Barrios, R. E. (2019). *Análisis, explotación y definición de estrategias de mitigación de vulnerabilidades en un sistema GNU/Linux*.

Navarro, C. G. C., Briones, V. F. V., Zambrano, J. L. V. & Felipe, M. del R. C. (2022). "Seguridad ofensiva mediante hacking ético para fortalecer infraestructuras en redes de telecomunicaciones". *Serie Científica de la Universidad de las Ciencias Informáticas*, 15(1), 40-53.

Páez, L. A. G., Arenas, J. E. T. & Moreno, A. N. B. (2019). *Ciberseguridad y ethical hacking: la importancia de proteger los datos del usuario*. Encuentro Internacional de Educación en Ingeniería.

Patiño Orozco, G. A. (2021). *Una comparativa de los esquemas de ciberseguridad de China y Estados Unidos* (*Chinese and American Cyber Security Models: A Comparative*).

Quintero Barrizonte, J. L. (2020). "Las tecnologías de la información y las comunicaciones como apoyo a las actividades internacionales y al aprendizaje a distancia en las universidades". *Revista Universidad y Sociedad*, 12(1), 366-373.

Robert Bosch Ltda. (2021, 9 de agosto). *Cyber Security: ¿cómo garantizar la seguridad y generar confianza en Internet?*

Sánchez Ávila, M. A. (2019). *Hacking ético: impacto en la sociedad*.

Sánchez, J. F. E. (2019). "Ciberdelincuencia. Aproximación criminológica de los delitos en la red". *La Razón Histórica: Revista Hispanoamericana de Historia de las Ideas Políticas y Sociales*, 44, 153-173.

Tenorio Cueto, G. A. (2019). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares, comentada*. Instituto Nacional de Transparencia, Acceso a la Información y Protección de…

Vargas, B. C. (2019). *Recursos y medios digitales de información: elementos teóricos y su uso desde la bibliotecología*. UNAM, Instituto de Investigaciones Bibliotecológicas y de la Información.

Villacís, R. P. C. (2022). "Ciberseguridad y ciberdefensa: perspectiva de la situación actual en el Ecuador". *Revista Tecnológica Ciencia y Educación Edwards Deming*, 6(1).

Comparativo de procesos operativos IOT entre México y Colombia

Comparison of IOT operational processes between Mexico and Colombia

Bellaizan Chaparro, Santiago
Candidato a ingeniero de sistemas

González Neuta, William Andrés
Candidato a ingeniero de sistemas

Rique, Angie Paola
Docente del programa de software

Resumen

La investigación hace un análisis comparativo de los procesos operativos relacionados con el Internet de las Cosas (IoT) entre México y Colombia. Se exploran aspectos que abarcan desde la regulación en términos legales y las instituciones nacionales encargadas de la misma en cada nación de América Latina hasta la adopción de industrias clave, desafíos, crecimiento y compatibilidad con estándares como NMX para el caso mexicano y las AID-ISO-IEC para Colombia. Los resultados muestran similitudes y diferencias en la normativa, aplicaciones en agricultura y manufactura y adopción de protocolos comunes. También se identifican retos compartidos en privacidad, ciberseguridad y conectividad en zonas alejadas. Adicionalmente, se presenta un análisis integral del estado actual y evolución de ambas naciones en relación con la preparación para la adopción de nuevas tecnologías, desde una perspectiva latinoamericana. El presente capítulo ofrece una visión integral del estado actual y tendencias de IoT en ambos países.

Palabras clave: *IoT, México, Colombia, industria, regulación, procesos, interoperabilidad.*

Abstract

This chapter addresses a comparative analysis of operational processes related to the Internet of Things (IoT) between Mexico and Colombia. It explores aspects ranging from legal regulation and the national institutions responsible for it in each Latin American nation to the adoption of key industries, challenges, growth, and compatibility with standards such as NMX for the Mexican case and AID-ISO-IEC for Colombia. The results reveal similarities and differences in regulations, applications in agriculture and manufacturing, and the adoption of common protocols. Shared challenges in privacy, cybersecurity, and connectivity in remote areas are also identified. Additionally, a comprehensive analysis of the current state and evolution of both nations in relation to preparedness for the adoption of new technologies is presented from a Latin American perspective. This chapter provides a comprehensive overview of the current status and trends of IoT in both countries.

Keywords: *IoT, México, Colombia, industry, regulation, processes, interoperability.*

Cursos articulados

El proyecto "Comparativo de procesos operativos IoT entre México y Colombia" ha sido completado satisfactoriamente. Se realizaron cursos clave, como "Internet de las Cosas" y "Sistemas Telemáticos", para comprender la tecnología subyacente. Además, "Análisis Numérico" y "Estadística y Probabilidad" ayudaron en el análisis de datos, mientras que "Teoría de la Información y las Telecomunicaciones" abordó las comunicaciones. "Inteligencia Artificial" exploró soluciones avanzadas. El proyecto permitió una evaluación en profundidad de los procesos operativos IoT en ambos países, brindando valiosas conclusiones para la investigación futura en este campo.

Introducción

El Internet de las Cosas (IoT) integra el mundo físico y digital mediante la interconexión de objetos cotidianos con identificación única, capacidades de comunicación, procesamiento y almacenamiento de datos (Bonilla *et al.*, 2016). IoT permite la recolección, intercambio y análisis de información en tiempo real para optimizar procesos en diversas industrias, pues permite la delegación de tareas repetitivas y la toma de decisiones complejas a sistemas automatizados (Gallardo *et al.*, 2023). La unión de estos aspectos genera un ecosistema en el cual los datos fluyen de forma constante, impulsando acciones inteligentes y toma de decisiones informadas.

En América Latina, la adopción de IoT para automatización de procesos crece en importancia, ante los beneficios potenciales en eficiencia operativa y competitividad (Campos *et al.*, 2020). Esta tendencia resalta la necesidad de comprender el panorama de internet de las cosas en países como México y Colombia, los cuales cuentan con industrias internacionales de gran reconocimiento y locales con posibilidades de expansión.

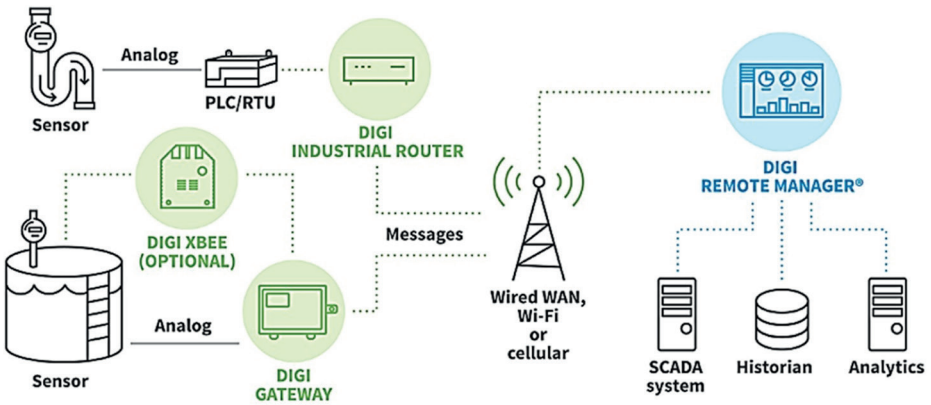
En este capítulo, se presenta un análisis comparativo de los procesos operativos relacionados con IoT entre México y Colombia, explorando diferentes perspectivas legales, estandarizadas y aplicadas, nacidas a partir de la visita física a entidades de diferentes índoles en México y el estudio de las industrias colombianas. El objetivo es identificar las similitudes y diferencias en el desarrollo IoT de ambos países.

Discusión

La evolución de los procesos en el Internet de las Cosas (IoT) ha sido significativa y sigue evolucionando rápidamente, pues la primera etapa se centró en la conexión de dispositivos a internet, lo que implicó la incorporación de sensores y conectividad a objetos cotidianos como electrodomésticos, vehículos y dispositivos industriales (Quiñonez Muñoz, 2019). A medida que más dispositivos se conectaron a internet, la recopilación de datos se convirtió en una parte central del IoT, los cuales se han utilizado para tomar decisiones más informadas en entornos relacionados con la gestión de activos, la monitorización ambiental y la automatización de procesos (Soori *et al.*, 2023).

La estructura del sistema IoT se presenta como un procedimiento de cuatro fases, en el cual la información se desplaza desde los sensores a los dispositivos a través de una red y, por último, se dirige hacia un centro de datos corporativo o a la nube para llevar a cabo su procesamiento, análisis y almacenamiento (Sethi & Sarangi, 2017). Lo anterior se encuentra estrechamente ligado al proceso de recolección de datos en tiempo real y su transmisión a través de comunicación inalámbrica como wifi, 4G/5G, LPWAN (Low Power Wide Area Network) o Bluetooth (Pons *et al.*, 2023). La elección de la tecnología depende directamente de la distancia, la velocidad y la cantidad de datos que se deben transmitir.

Figura 22. Las cuatro etapas de la arquitectura IoT



Nota. Las cuatro etapas de la arquitectura IoT. Fuente: Jahnke (2020).

En la figura 22 se establece el proceso general de IoT en sus 4 etapas, las cuales inician con la recopilación de información a través de dispositivos sensorios. Los datos captados son enviados a una plataforma IoT en la nube o en infraestructura local, donde son almacenados y procesados (Plana Casarrubios, 2023). Una vez procesados, los datos se utilizan para realizar análisis, frecuentemente mediante técnicas de aprendizaje automático e inteligencia artificial (Martín *et al.*, 2023). La automatización de procesos con IoT generalmente implica un ciclo de retroalimentación (López, 2021).A medida que se recaban más datos y se toman decisiones automatizadas, se pueden realizar ajustes para optimizar aún más el proceso y mejorar la eficiencia.

Adopción de IoT en América Latina

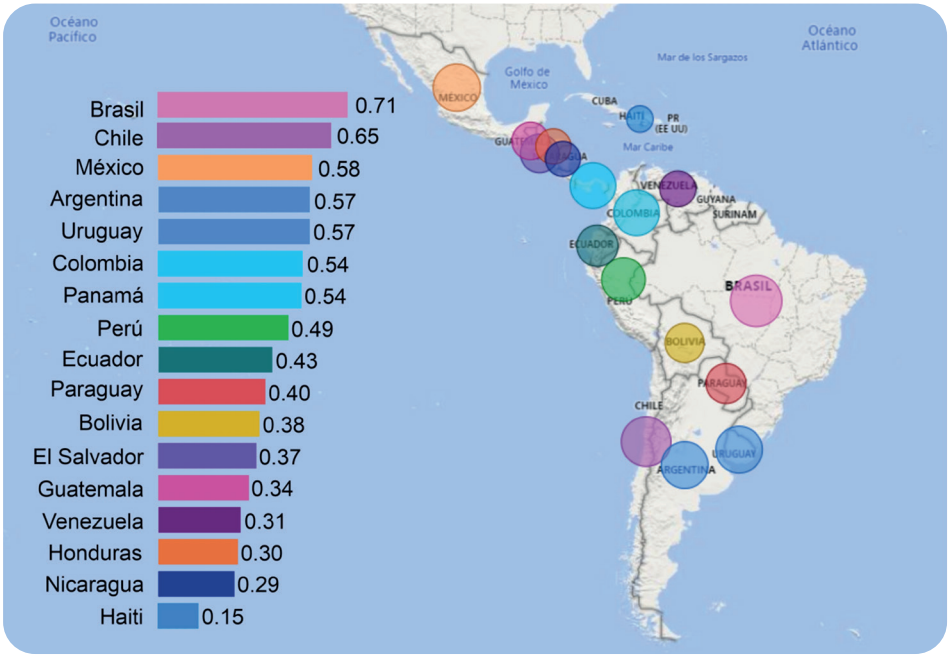
América Latina se encuentra en una fase de crecimiento en la adopción del internet de las cosas, impulsada por la necesidad de las empresas de mejorar procesos, reducir costos y volverse más competitivas a nivel global (ELAC, 2021). Según estimaciones de International Data Corporation (IDC), en la inversión de América Latina en proyectos IoT y tecnologías de negocios se espera un aumento del 15,5 % para 2026 y en telecomunicaciones del 4,9 % para el mismo año. De igual manera, se establece una inversión de América Latina en ciberseguridad de US$3.600 millones para 2023 y un crecimiento anual compuesto del 11,2 % hasta 2026 (International Data Corporation [IDC], 2023).

Lo anterior pone de manifiesto el interés del sector (Latinoamérica) en la adopción y apropiación tecnológica en los diferentes ámbitos de la vida cotidiana. Asimismo, se evidencia el continuo interés de la industria por mantener actualizados sus procesos, como se refleja en el estudio realizado por Deloitte sobre IoT para el sector empresarial en América Latina. En dicho estudio se observan los índices de inversión económica en IoT, con Brasil liderando con 1,8 billones de dólares, seguido por México, Argentina y Colombia (Deloitte, 2018).

De otra parte, es indiscutible que los países desarrollados y en vía de desarrollo invierten un porcentaje de entre el 3 % y el 5 % del PIB en I+D, mientras que, para el caso particular de México y Colombia, se invierte alrededor del 0,3 %, un promedio considerablemente bajo, más aún teniendo en cuenta que el promedio de inversión para países con ingresos medio-bajos es del 0,53 % (UNCTAD, 2023). En el Informe de Tecnología e Innovación 2023 de las Naciones Unidas, se obtuvo que los países con mayor índice de preparación para las tecnologías de vanguardia corres-

ponden a Estados Unidos, Suecia y Singapur, mientras que, para el caso de América Latina, Brasil cuenta con la mayor puntuación, seguido de Chile, Costa Rica y México (ver figura 23).

Figura 23. Índice de preparación para tecnologías de vanguardia



Nota. Índice de preparación para tecnologías de vanguardia. Fuente: autores.

Así mismo, se establece una relación directa cada vez más fuerte entre la convergencia del IoT y la tecnología 5G como una tendencia de impacto significativo en América Latina. A medida que se despliegan las redes 5G en la región, se abren nuevas oportunidades y desafíos para la implementación de IoT (GSMA, 2023). En este punto, es importante mencionar que la adopción de redes 5G en América Latina está en sus primeras etapas, pero se está acelerando en varios países de la región y se espera que la implementación de 5G permita velocidades de conexión mucho más rápidas, menor latencia y mayor capacidad de red, aspectos fundamentales para el soporte de aplicaciones de IoT que requieren conectividad confiable y de alto rendimiento (Pons *et al.*, 2023) .

Los sectores con mayor adopción de IoT en la región corresponden a la industria manufacturera, también conocida como industria 4.0 (Bonneau *et al.*, 2017); la agricultura, estableciendo una relación de tecnología de precisión, monitoreo de cultivos y automatización de riego (Peladarinos *et al.*, 2023); la logística, para el rastreo de vehículo, productos y gestión de rutas planificadas (Friha *et al.*, 2020); la energía, optando por la lectura remota de medidores, optimización de redes y ciudades inteligentes, y la salud, implementando la telemedicina y el monitoreo remoto de pacientes.

Los principales desafíos para la adopción del IoT en la región se encuentran ligados a la ausencia de estándares comunes, integración con sistemas heredados, preocupaciones de ciberseguridad y limitada infraestructura de conectividad en áreas rurales (Gómez-Carmona *et al.*, 2023; Tariq *et al.*, 2023). No obstante, con un marco regulatorio adecuado, modelos de financiación innovadores y la articulación de los sectores públicos y privados, América Latina puede convertir el IoT en un motor base de productividad y desarrollo sostenible.

Regulación del IoT

La regulación del IoT es clave para promover un desarrollo ordenado y ético de esta tecnología emergente. Es, por tanto, que los gobiernos buscan establecer marcos normativos integrales para el internet de las cosas abarcando aspectos de privacidad, seguridad, interoperabilidad y gestión en sus distintas aplicaciones a nivel industrial, público y privado. Teniendo en cuenta lo anterior, en la presente sección, se establecen los marcos regulatorios presentes en Latinoamérica, enfocando principalmente en las normativas internacionales; también se enuncian las normativas principales para la regulación de nuevas tecnologías e IoT en los países latinoamericanos.

Debido al auge del IoT a nivel global, surge la necesidad de establecer una normativa que establezca los límites y condiciones de su implementación respetando los derechos y libertades de las comunidades e industrias. Es por tal razón que en 2018 se da origen a la Norma Internacional ISO/IEC 30141 para la regulación del Internet de las Cosas (IoT) (ISO, 2018). Dicha norma proporciona un lenguaje común para el diseño y desarrollo de aplicaciones IoT apalancada en la ISO/IEC 20924 de 2018, la cual fue modificada en 2021 (ISO, 2021); esto permite el despliegue de sistemas seguros, confiables y con una alta capacidad de afrontar ataques cibernéticos.

Tabla 11. Generalidades de la Norma ISO/IEC 30141

Característica	Descripción
Nombre	ISO/IEC 30141: 2018 Internet de las Cosas (IoT) - Arquitectura de referencia.
Aplicación a IoT	Proporciona un lenguaje común para el diseño y desarrollo de aplicaciones de IoT.
Principios clave	Reforzamiento de la seguridad, mejoramiento en la protección, incremento en la fiabilidad y respeto por la privacidad.
Compatibilidad	Centraliza los símbolos y términos más utilizados en IoT, al igual que las características generales de los sistemas, componentes, uso y seguridad.
Roles	Establece de forma clara los roles involucrados en el IoT, relacionando los desarrolladores, los proveedores y los usuarios.
Beneficios	Fortalecimiento de la seguridad en los dispositivos. Mejoramiento en la calidad de los productos con una robustez mayor que permita soportar y contrarrestar los ciberataques. Establecimiento de normas técnicas que permiten una mayor protección de la información.

Nota. Generalidades de la norma ISO/IEC 30141. Fuente: autores.

Posteriormente, teniendo en cuenta las diferentes vertientes y complejidades sistemáticas de la aplicabilidad del IoT, se establecieron normativas adicionales relacionadas con la interoperabilidad de los sistemas IoT (ISO/IEC, 2022e), arquitectura de la internet relacionada a los medios (ISO/IEC, 2022f), directrices de seguridad y privacidad en IoT, confiabilidad de los sistemas y servicios IoT (ISO/IEC, 2021), marco de confianza de IoT (ISO/IEC, 2022h), entre algunas otras. Dichas normatividades surgieron posterior a la ISO/IEC 30141, a mediados de abril de 2019, y varias de estas se han ido actualizando año a año. A la fecha se cuenta con alrededor de 47 normas ISO relacionadas con el IoT.

Tabla 12. Algunas normas ISO para la reglamentación del IoT

Norma	Título	Generalidad
ISO/IEC 27400:2022	Cybersecurity – IoT security and privacy.	Proporciona pautas sobre riesgos, principios y controles para la seguridad y privacidad de las soluciones de Internet de las Cosas (IoT) (ISO/IEC, 2022g).

Norma	Título	Generalidad
ISO/IEC 30161-2:2023	Internet of Things (IoT) – Data exchange platform for IoT services – Part 2: Transport interoperability between nodal points.	Especifica los elementos para la interoperabilidad del transporte entre puntos nodales en la plataforma de intercambio de datos de IoT, como: requisitos, bloques funcionales y mecanismos de funcionamiento (ISO/IEC, 2023a).
ISO/IEC 30179:2023	Internet of Things (IoT) – Overview and general requirements of IoT systema for ecological environment monitoring	Especifica el sistema de IoT para el seguimiento del entorno ecológico en términos de la infraestructura del sistema para el seguimiento de recursos naturales como el aire, agua, suelo y los organismos vivos (ISO/IEC, 2023b).
ISO/IEC 30171-1:2022	Internet of Things (IoT) Base – station based underwater wireless acoustic network (B-UWAN) – Part 1: Overview and requirements	Proporciona una descripción general de las redes acústicas inalámbricas submarinas basadas en estaciones base (B-UWAN) y una descripción detallada de los componentes principales de B-UWAN y sus requisitos (ISO/IEC, 2022d).
ISO/IEC 30142-2:2022	Internet of Things (IoT) Underwater acoustic sensor network (UWASN) – Network management system – Part 2: Underwater management information base (u-MIB)	Establece la base de información de gestión submarina (u-MIB) del sistema de gestión de redes submarinas (U-NMS), dentro de la cual se especifican los requisitos generales para la construcción, diseño y la integración de objetos gestionados del gestor y agentes u-MIB (ISO/IEC, 2022a).
ISO/IEC 30162:2022	Internet of Things (IoT) Compatibility requirements and model for devices within industrial IoT systems	Especifica modelos de red para conectividad IoT y requisitos generales de compatibilidad para dispositivos y redes dentro de sistemas IoT en términos de interacción, interoperabilidad, marcos, red de conectividad, mejores prácticas y orientación para uso en el área de IoT (ISO/IEC, 2022b).
	Internet of Things (IoT) applications for electronic label system (ELS)	Brinda el marco del sistema, el modelo de aplicación de IoT y los requisitos técnicos generales para ELS, principalmente a la industria minorista, proporcionando las referencias para el diseño y desarrollo de IoT para ELS en otras industrias (ISO/IEC, 2022c).

Nota. Algunas normas ISO para la reglamentación del IoT. Fuente: autores.

Normatividad técnica en LATAM

Para el caso particular de LATAM, cada país establece sus propias normas, leyes y regulaciones de acuerdo a su régimen y sistema político, sin embargo, todas ellas confluyen en un interés común: la protección de datos personales y la reglamentación del uso y la aplicación de las tecnologías. Dentro de las tecnologías que se encuentran reguladas se encuentran las aplicaciones de IoT, normatividades que indistintamente del país se han empezado a adoptar a partir del 2019, teniendo como referencia las normas ISO enunciadas anteriormente.

Tabla 13. Institutos u organizaciones regulatorias de normas técnicas en LATAM

País	Norma	Definición
Argentina	Instituto Nacional de Tecnología Industrial (INTI)	Adscrito al Ministerio de Economía, es el único organismo de certificación del ámbito público. Su objetivo es avalar los productos, procesos y profesionales que cumplan con las normas y especificaciones técnicas a través de certificaciones (Ministerio de Economía de Argentina, 2023).
	Instituto Argentino de Normalización y Certificación (IRAM)	Asociación sin ánimo de lucro, representante de ISO en Argentina. Se enfoca en el desarrollo de las normas técnicas sectorizadas (IRAM, n. d.).
Bolivia	Instituto Boliviano de Normalización y Calidad (IBNORCA)	Asociación privada sin ánimo de lucro y única representante de ISO en Bolivia. Adicionalmente, forma parte de la Asociación Mercosur de Normalización (AMN), Comisión Panamericana de Normas Técnicas (COPANT) y las Comisión Internacional de Electrotecnia (IEC) (IBNORCA, n. d.).
Brasil	Asociación Brasilera de Normas Técnicas (ABNT)	Representante de ISO en Brasil y miembro fundador de dicha asociación, así como de COPANT, AMN e IEC. Es la responsable de la elaboración de las normas brasileñas a través de sus diferentes comisiones CB, ONS y CEE (ABNT, n. d.).
Chile	Instituto Nacional de Normalización (INN)	Organismo técnico en materias de la infraestructura de la calidad con participación internacional en ISO (como miembro fundador) y en la Cooperación Interamericana de Acreditación (IAAC) (INN, n. d.).

País	Norma	Definición
Colombia	Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)	Organización privada sin ánimo de lucro encargado de la normalización colombiana en relación a procesos, productos y servicios, así como de su inspección, verificación y validación. Miembro de IQNET y único representante de ISO y COPANT en el país (ICONTEC, n. d.).
Costa Rica	Instituto de Normas Técnicas en Costa Rica (INTECO)	Asociación sin fines de lucro y ente nacional de normalización. Representante directo de ISO, IEC y COPANT (INTECO, n. d.).
Cuba	Oficina Nacional de Normalización (ONN)	Organización gubernamental del Ministerio de Ciencia, Tecnología y Medio Ambiente. Encargada de proponer, organizar y ejecutar la aplicación de las políticas estatales relacionadas con las normas de calidad. Basa su base normativa en varias normativas de ISO (ONN, 2019).
Ecuador	Servicio Ecuatoriano de Normalización (INEN)	Encargado de desarrollar, promover y difundir las normas técnicas ecuatorianas, adoptando también normas internacionales asociadas a ISO (INEN, n. d.).
El Salvador	Organismo Salvadoreño de Normalización (OSN)	Organización pública encargada de establecer y aplicar la normatividad técnica en los diferentes sectores productivos. Representante de ISO para El Salvador (OSN, n. d.).
Guatemala	Comisión Guatemalteca de Normas (CONGUANOR)	Adscrita al Ministerio de Economía de Guatemala, es la encargada de desarrollar las normas técnicas en el territorio y velar por su adopción y cumplimiento (Ministerio de Economía, n. d.).
Haití	No se encuentra información sobre regulación propia.	Según información del portal de información sobre normas OMC-ISO, Haití se encuentra en la lista de instituciones con actividades de normalización (ISO, 2016).

País	Norma	Definición
Honduras	Organismo Hondureño de Normalización (OHN)	Organización gubernamental encargada de la reglamentación técnica de Honduras siguiendo las directrices de ISO, IEC y ASTM (Desarrollo Económico Gobierno de la República de Honduras, n. d.).
México	Dirección General de Normas (DGN)	Adscrita a la Secretaría de Economía mexicana, se encarga de impulsar las normas, teniendo en cuenta la política económica y las reglamentaciones nacionales e internacionales. Ligada a las NMX y las NOM directamente (Secretaría de Economía, n. d.).
Nicaragua	Ministerio de Fomento de Industria y Comercio (MIFIC)	Ministerio público encargado del diseño, reglamentación y aplicación de las NTN y NTON, dentro de las cuales se abordan todos los aspectos legales y técnicos (MIFIC, n. d.).
Panamá	Dirección General de Normas y Tecnología Industrial (DGNTI)	Adscrito al Ministerio de Comercio e Industria, cuenta con el Departamento de Normalización Técnica, el cual es el encargado de la normalización y certificación de productos en la República de Panamá (Ministerio de Comercio e Industria, n. d.).
Paraguay	Instituto Nacional de Tecnología, Normalización y Metrología (INTN)	Entidad pública descentralizada adscrita al Ministerio de Industria y Comercio, encargado de la reglamentación que rige la calidad de los productos y servicios, así como la expedición de certificaciones. Cuenta con organismos técnicos especializados como ONC[1], ONM[2], ONN[3], ONI[4], OIAT[5] y DSE[6] (Ministerio de Industria y Comercio, n. d.).

[1] Organización Nacional de Certificación.

[2] Organismo de Metrología.

[3] Organismo Nacional de Normalización.

[4] Organismo Nacional de Inspección.

[5] Organismo de Investigación y Asistencia Tecnológica.

[6] Dirección de seguridad electrica

País	Norma	Definición
Perú	Comisión de Reglamentos Técnicos y Comerciales (CRT)	Instituto parte del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI). Es el encargado de aprobar y aplicar las Normas Técnicas Peruanas (NTP) al ser el organismo peruano de Normalización (INDECOPI, n. d.).
	INTERCERT	Empresa privada internacional con presencia a nivel mundial. Expide certificaciones ISO en los diversos sites más de gestión y sectores (INTERCERT, n. d.).
República Domini-cana	Instituto Dominicano para la Calidad (INDOCAL)	Entidad pública descentralizada adscrita al Ministerio de Industria, Comercio y Mipymes (MICM), encargada de la normalización industrial y científica. Se encarga adicionalmente de la reglamentación y adopción de las normas ISO en el territorio de la República Dominicana (INDOCAL, 2012)
Uruguay	Instituto Uruguayo de Normas Técnicas (UNIT)	Entidad representante exclusiva de ISO, IEC, COPANT y AMN en Uruguay. Sus funciones principales están ligadas al establecimiento de las normas UNIT, la adopción de normas internacionales, el estudio y difusión de normas técnicas, así como la realización de capacitaciones para la adopción de los marcos normativos de calidad en productos y servicios (UNIT, n. d.)
Venezuela	FONDONORMA (FN)	Organismo sin ánimo de lucro creado en 1973, es el encargada de realizar las actividades de normalización y certificación de los diversos sectores industriales y de servicios en Venezuela, adoptando las normas ISO a través de comités y comisiones técnicas (FONDONORMA, n. d.)

Nota. Institutos u organizaciones regulatorias de normas técnicas en LATAM. Fuente: autores.

Tendencias de implementación de IoT

La implementación del internet de las cosas puede llevarse a cabo a través de modelos según el rol y capacidades de la organización. Sin embargo, se presentan diversos modelos de implementación que varían en características, lo que conlleva ventajas y desafíos asociados. En relación a lo anterior, se establece la tabla 14, en la cual se presentan de forma general las principales concepciones, ventajas y desafíos de cada uno de los modelos más utilizados.

Tabla 14. Generalidades de las tendencias de implementación IoT

Tendencia	Descripción	Ventajas	Desafíos
Agricultura	La tendencia de aplicación de IoT en la agricultura es denominada agricultura de precisión. Dicha tecnología consiste en hacer uso de las Tecnologías de la Información (TI), sensores, imágenes satelitales, GPS y otros dispositivos electrónicos para aumentar la eficiencia y rendimiento de los cultivos, optimizando el uso de insumos y recursos en función de las necesidades específicas de cada uno (Durán, 2019)	Permite el uso focalizado de insumos según requerimientos, lo que aumenta la eficiencia. Optimiza procesos productivos mediante análisis de datos e información valiosa para la toma de decisiones. Reduce pérdidas y desperdicio mediante detección temprana de problemas en los cultivos. Facilita trazabilidad y cadenas de valor más responsables.	Exige cuantiosas inversiones iniciales en equipamiento y plataformas tecnológicas. Requiere de recursos humanos capacitados tanto en labores agronómicas como en tecnologías de la información. Puede encontrar resistencia en sectores más tradicionales reacios hacia la transformación digital.
Salud	Uso de dispositivos y sensores conectados a internet para la vigilancia y cuidado de pacientes de manera remota. Incluye un monitoreo constante de los signos vitales, sistemas de alertas controladas y asistencia remota (Alcatel, 2019)	Permite atención continua más allá de los centros médicos tradicionales. Alerta rápidamente sobre complicaciones médicas y emergencias. Reduce los costos del sistema de salud al evitar hospitalizaciones innecesarias. Insta a los pacientes a estar alerta de sus condiciones médicas.	Ciberseguridad de datos médicos sensibles. Estandarización de los protocolos y dispositivos. Integración de grandes volúmenes de información médica con otras plataformas digitales de salud. (Ferreira et al., 2021)

Tendencia	Descripción	Ventajas	Desafíos
Educación	Uso de dispositivos y objetos físicos interconectados de forma única con el fin de facilitar y mejorar los procesos de enseñanza y aprendizaje. En la actualidad, es comúnmente utilizado través de la adecuación de dispositivos de grabación y transmisión en tiempo real para la especificación de procesos puntuales en carreras técnicas (Rueda-Rueda et al., 2017).	Permite nuevas formas de interacción y experimentación. Motiva mayor interés y compromiso de los estudiantes. Fomenta la colaboración y el aprendizaje práctico. Habilita el análisis de desempeño en tiempo real. (Román et al., 2020)	Costos elevados para la mayoría de los centros educativos. Requiere actualización en las competencias y habilidades de los docentes para el correcto uso y apropiación de las tecnologías. Puede tener incidencia en la brecha educativa de las comunidades. Implica el reforzamiento de ciberseguridad y privacidad de la información de los centros educativos.
Transporte	El transporte de carga de mercancías y materias primas es parte central de la cadena de suministro en el intercambio comercial en América Latina. El control y seguimiento de esta actividad son vitales para un flujo económico eficiente y, lo que es más importante, sin pérdidas de dinero. La mayoría de los problemas que generan pérdidas financieras se dan en el transporte de carga por vía terrestre (Flores-Cortez & Gonzales Crespin, 2023).	Proporciona una visión en tiempo real de la ubicación. Optimiza las rutas de entrega, reduce costos de combustible y disminuye los tiempos de tránsito. Facilita el seguimiento preciso de inventarios. Permite predecir y programar el mantenimiento antes de que ocurran averías. Monitoreo y protección de las mercancías.	Las brechas de seguridad pueden poner en riesgo datos sensibles y la operación de la cadena de suministro. Diversos dispositivos y sistemas IoT utilizan estándares y protocolos diferentes, lo que puede dificultar la integración y la interoperabilidad entre ellos. Gestión adecuada y el cumplimiento de regulaciones de privacidad. La implementación de IoT puede requerir inversiones significativas en hardware, software y capacitación de personal.

Tendencia	Descripción	Ventajas	Desafíos
Seguridad	Uso de sensores y dispositivos interconectados para recolectar datos, monitorizar ambientes y activar alertas que permitan mejorar la seguridad física en hogares, ciudades y espacios públicos.		
Empresarial	Enfocado en la digitalización de procesos y la mejora de la productividad y el rendimiento. Con el IoT (Internet de las Cosas Industrial) se pueden conectar máquinas, dispositivos, informática en la nube, análisis y personas para mejorar procesos industriales (Ávila-Camacho & Moreno-Villalba, 2023).	Mejora la eficiencia y la productividad. Reducción de costos. Automatización de procesos. Análisis predictivo de la calidad y el mantenimiento. Monitoreo del estado de los activos y la optimización de los procesos.	Necesidad de una gran cantidad de potencia informática para cada dispositivo físico de IoT, especialmente si se utilizan máquinas complejas, y la seguridad de los datos.

Nota. Generalidades de las tendencias de implementación IoT. Fuente: autores.

Metodología

La metodología utilizada para el desarrollo del presente capítulo contó con un enfoque cualitativo, basada en una revisión bibliográfica, análisis de legislación y normatividad, así como visitas de campo a distintas entidades industriales y académicas en México.

Para la revisión bibliográfica se consultaron estudios recientes, artículos científicos e informes de IoT en América Latina. Esto permitió conocer investigaciones previas sobre la adopción y regulación de IoT en la región. Además, se analizó legislación relevante en México y Colombia para identificar el marco regulatorio actual de IoT en estos países.

Con el fin de complementar la información documental, se realizaron cuestionamientos a expertos en IoT en México, profundizando en la automatización de procesos industriales y su implementación en los mismos. Dichas preguntas aportaron percepciones y experiencias de primera mano sobres los procesos operativos y dejaron un panorama más claro del estado actual de estos procesos regulatorios y operacionales en México. La triangulación de las fuentes consultadas posibilitó realizar un análisis integral para comparar el estado actual del IoT en México y Colombia, considerando dimensiones regulatorias, aplicaciones sectoriales, proyectos, desafíos, crecimientos y adopción de estándares.

Como parte del trabajo de campo, se realizaron visitas a 2 empresas y 2 universidades mexicanas que han implementado soluciones de internet de las cosas en sus operaciones. Estas instituciones representan sectores industriales, académicos y de seguridad. El objetivo de las visitas fue conocer en sitio los procesos operativos relacionados con IoT que han adoptado estas compañías, observando la tecnología utilizada, la arquitectura implementada, los procedimientos asociados y los resultados obtenidos.

Resultados

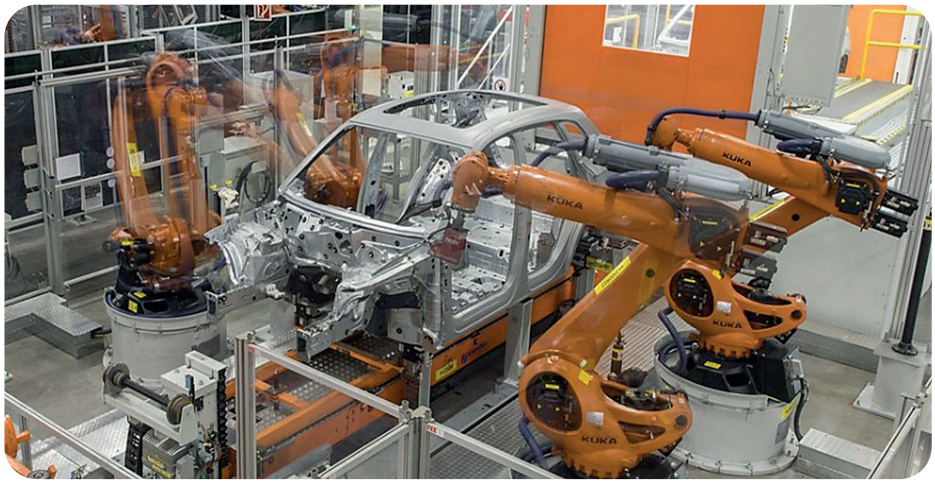
A partir de la revisión bibliográfica y la observación realizada en las visitas a las empresas mexicanas, así como los cuestionamientos realizados a expertos, se establecen los resultados presentados en la presente sección, dentro de la cual se presenta el análisis correspondiente a la visita a las fábricas de Audi en México, el comparativo de normas AID-ISO-IEC de Colombia y NMX para México; así mismo, se presenta un análisis de la evolución de ambos países en relación a la preparación para la adopción de nuevas tecnologías.

Audi México

En la reciente visita a la planta de producción de la línea Q5 de Audi, en San José de Chiapa, pudimos constatar que están a la vanguardia en cuanto a automatización de procesos avanzada, análisis de datos en tiempo real y conectividad de dispositivos, todo esto ligado a la industria 4.0 y entrando de a poco en la industria 5.0, que va enfocada a la sostenibilidad y prácticas responsables con el medio ambiente. La integración de robots industriales, como los de la marca KUKA, en la etapa de ensamblaje representa un avance crucial en la evolución de la manufactura inteligente en la industria 4.0. Estos robots no solo realizan tareas de ensamblaje de manera rápida y precisa, sino que también aportan al proceso de mejora continua.

Gracias a la automatización y el aprendizaje automático (*machine learning*), estos robots pueden adaptarse y optimizar sus operaciones con el tiempo. A medida que ejecutan tareas, recopilan datos en tiempo real, lo que incluye información sobre la calidad de los productos ensamblados y el rendimiento del sistema. Esta información se convierte en un activo valioso para el análisis de datos y la toma de decisiones futuras. La capacidad de analizar estos datos permite identificar patrones, tendencias y posibles áreas de mejora en el proceso de ensamblaje. Esto no solo conduce a una producción más eficiente y con menos errores, sino que también proporciona información crítica para la toma de decisiones estratégicas.

Figura 24. Proceso de ensamblaje mediante robots industriales



Nota. Proceso de ensamblaje mediante robots industriales. Fuente: Audi (2023).

Los componentes requeridos se ensamblan mediante una amplia variedad de técnicas, que van desde diversos tipos de soldadura hasta el uso de tecnología láser para completar la tarea. En este caso, se utiliza un gran número de robots de última generación; la industria 4.0 se hace un hueco en la planta mexicana (Audi, 2023).

De otra parte, aunque la automatización es bastante predominante en este proceso, aún se necesita de la mano de obra humana para ciertos procesos que todavía las máquinas no pueden realizar por más automatizado que sea el proceso (actualmente, el 80 % de la etapa de ensamblaje es realizada por robots).

Comparativo normativo

Como se estableció de forma general en el apartado de fundamentación teórica, específicamente en la tabla 12, aunque de forma general se cuenta con las directrices de instituciones como ISO, COPANT, IEC, AMN, entre otras, cada nación cuenta con sus propias normativas y reglamentaciones, así como instituciones público-privadas, para la normativización y reglamentación técnica en sus territorios. Para el caso particular de Colombia, se cuenta con el ICONTEC, mientras que en México se encuentra la Dirección General de Normas (DGN).

A continuación, se establece la tabla 15, en la cual se relacionan las normativas AID-ISO-IEC (Colombia) y NMX (México), en el caso particular del IoT.

Tabla 15. Comparativo de normatividad técnica Colombia vs. México

<table>
<tr><th>Colombia</th><th>México</th></tr>
<tr><td>AID-ISO-IEC 21823-1:2019</td><td>NMX-I-1362-NYCE-2021</td></tr>
<tr><td>Establece el marco de trabajo para la interoperabilidad de sistemas IoT. En esta norma se busca establecer un lenguaje común que permita el intercambio de información entre entidades bajo un mismo estándar de desarrollo (ISO/IEC, 2019a).</td><td rowspan="3">Reglamenta los procedimientos para encriptación para entornos IoT. Establece los métodos de codificación para la protección de los dispositivos IoT de comunicación, transmisión, almacenamiento y procesamiento de datos (Secretaría de Economía, 2021a).</td></tr>
<tr><td>AID-ISO-IEC 21823-2:2020</td></tr>
<tr><td>Brinda las condiciones y requisitos para la interoperabilidad en el transporte de información con el fin de permitir no solo el intercambio de información, sino una comunicación fluida entre interfaces dentro de sistemas IoT (ISO/IEC, 2020b).</td></tr>
</table>

AID-ISO-IEC 20924:2021	PROY-NMX-I-20000-7-NYCE-2021
Corresponde a la norma técnica sobre el vocabulario necesario para la implementación del IoT, presenta términos y definiciones, es decir, es una base terminológica (ISO/IEC, 2021).	Corresponde a una guía y actualización de las normas NMX-I-20000-1-NYCE-2019, NMX-CC-9001-IMNC-2015 y NMX-I-27001-NYCE-2015, relacionadas con los sistemas de gestión de la información en términos de calidad y seguridad de la información digital, brindando un lenguaje común de aplicación y desarrollo (Secretaría de Economía, 2021f).
AID-ISO-IEC 30141:2018	**NMX-I-20000-3-NYCE-2021**
La norma establece una arquitectura estándar para el internet de las cosas. Esta arquitectura de referencia caracteriza los componentes, relaciones y guías de diseño recomendadas para el desarrollo de sistemas de IoT interoperables. Incluye un modelo conceptual, un marco de trabajo de referencia y diferentes representaciones o vistas de la arquitectura integral de IoT (ISO, 2018).	Se enfoca en la reglamentación de la gestión de servicios; en ella se encuentra la orientación sobre los alcances de la norma NMX-I-20000-1-NYCE–2019, en la cual se establecen los requisitos de implementación y mantenimiento de los sistemas de gestión de servicios tecnológicos (Secretaría de Economía, 2021b).
AID-ISO-IEC-TR 30164:2020	**NMX-I-22301-NYCE-2021-1**
El documento caracteriza los conceptos, terminología, propiedades, casos de uso y tecnologías prevalentes en la computación de borde aplicada al internet de las cosas. Cubre áreas como gestión de datos, coordinación, procesamiento, funciones de red, computación heterogénea, seguridad y optimización de recursos de *hardware*/*software*. La norma busca identificar espacios donde se podrían desarrollar estándares para promover la interoperabilidad y el desarrollo ordenado de soluciones de computación de borde para IoT (ISO/IEC, 2020a).	Enfocada en la seguridad y resiliencia de los sistemas de gestión, específicamente en la implementación, mantenimiento y actualización de los sistemas de información enfocados en la continuidad de procesos y la respuesta a interrupciones y fallos (Secretaría de Economía, 2021c).
AID-ISO-IEC 30148:2019	No cuenta con norma homóloga.
Establece los estándares técnicos para las redes de medidores de gas mediante tecnología inalámbrica, especificando tanto la estructura de las redes como el protocolo de aplicación (ISO/IEC, 2019b).	

No cuenta con norma homóloga.	**NMX-I-22316-NYCE-2021** Reglamenta y brinda la información correspondiente al mejoramiento de la capacidad de recuperación de información de organizaciones de cualquier tamaño o tipo de organización (Secretaría de Economía, 2021d).
No cuenta con norma homóloga.	**NMX-I-4903-NYCE-2021** Establece los indicadores clave de desempeño (KPI) para ciudades inteligentes y sostenibles en relación a la evaluación de los ODS. Su objetivo principal corresponde a establecer las métricas de evaluación para considerar una ciudad o grupo como inteligente y sostenible (Secretaría de Economía, 2021e).

Nota. Comparativo de normatividad técnica Colombia vs. México.

Como se observa en la tabla anterior, Colombia no cuenta con una normatividad técnica propia relacionada con la adopción, apropiación y reglamentación de la aplicación del IoT. Sin embargo, adopta de manera rigurosa las normativas dadas por las normas internacionales ISO-IEC relacionadas con la temática, específicamente las establecidas en las normatividades listadas (información recolectada de la página oficial de ICONTEC) (ICONTEC, 2023).

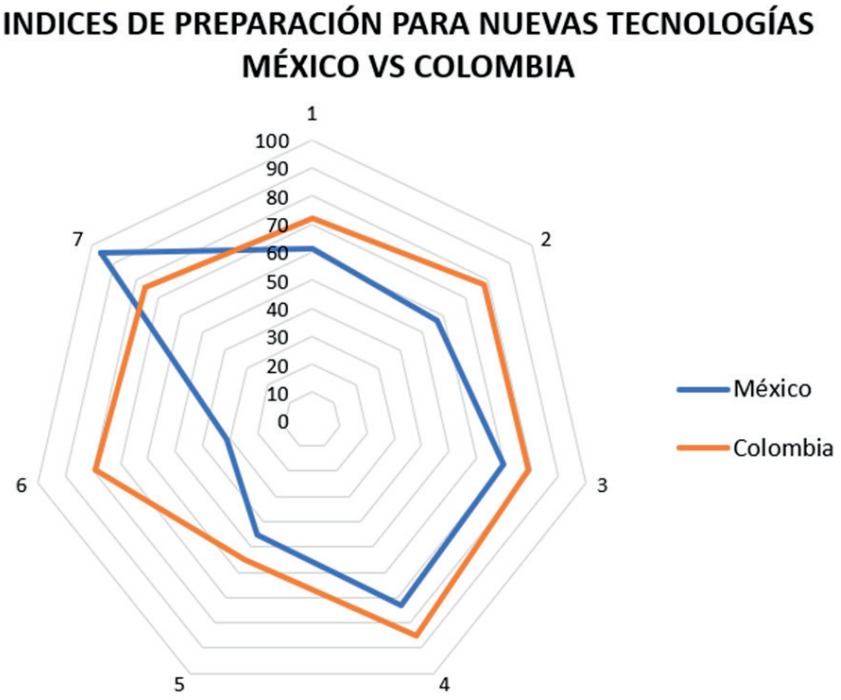
Posteriormente, se analiza la incidencia de esta decisión en los *rankings* internacionales de cada caso.

De otra parte, México cuenta con 6 normativas específicas que buscan regular aspectos fundamentales como ciberseguridad, privacidad, encriptación, comunicación y lineamientos en relación con los ODS, aspectos cruciales para la migración a la industria 4.0 y 5.0 en los distintos campos de implementación. Adicionalmente, México cuenta con la Asociación IoT México, enfocada en la capacitación de las normativas y procesos IoT, lo que le permite lograr un gran alcance en la difusión de información relacionada.

Preparación para la adopción tecnológica México vs. Colombia

En múltiples aspectos, México y Colombia cuentan con similitudes en torno a su nivel de desarrollo, sin embargo, en relación a la preparación de cada uno para la adopción de nuevas tecnologías, como es el caso del IoT, se encuentran diferencias sustanciales en factores dados por: 1) puntuación en LATAM 2022, 2) *ranking* en LATAM 2021, 3) rango TIC, 4) rango de habilidades, 5) rango I+D, 6) clasificación de la industria y 7) rango financiero (UNCTAD, 2023). Con el fin de establecer una mejor observación de dichas diferencias, se establece la figura 25.

Figura 25. Índices de preparación para nuevas tecnologías de México y Colombia



Nota. Índices de preparación para nuevas tecnologías de México y Colombia. Fuente: autores.

Como se puede observar, México presentó un ligero descenso en el *ranking* general en 2022 en comparación con el año 2021, pasando del puesto 57 al puesto 61. Aun así, se observa una tendencia positiva en la implementación de Tecnologías de la Información y las Comunicaciones (TIC), esto fundamentado en la tendencia al crecimiento del rango de habilidades. En adición, es importante tener en cuenta que el rango financiero de México para nuevas tecnologías se encuentra en 96, lo que sugiere un área de atención importante, teniendo como base para LATAM mínima de 19 obtenido por Chile y máxima de 157 para el caso de Haití.

Es imperativo establecer que el rango financiero corresponde a las diferencias dadas entre las empresas que más invierten en tecnología y aquellas que lo hacen en menor proporción, lo que está directamente ligado con la desigualdad en la tecnificación de procesos en la industria.

Para el caso particular de Colombia, se observa un crecimiento en el *ranking* general, al pasar del puesto 78 al 72, lo que destaca una mejora significativa relacionada con el rango TIC y el rango de habilidades e implementación. No obstante, el rango financiero se encuentra en 76, lo que sugiere una posición intermedia a nivel Latinoamérica, que requiere atención para lograr una disminución significativa en los índices de desigualdad tecnológica industrial.

Tanto México como Colombia muestran cambios en sus posiciones generales, México presentando un ligero descenso y Colombia mejorando en el *ranking*. Ambos países cuentan con áreas de mejora que confluyen en el rango financiero para el caso de México y una necesidad de mejora de Colombia en lo referente al rango de habilidades. Es fundamental considerar que la dinámica y los factores específicos presentados ofrecen una perspectiva general, pero no reflejan todos los aspectos de la realidad económica e industrial de los países analizados.

Conclusiones

La adopción del IoT ofrece una amplia gama de opciones en los distintos sectores donde se implemente, al permitir la recopilación y el análisis de datos en tiempo real, la automatización de procesos, la toma de decisiones más informada y la mejora de la eficiencia. La capacidad de conectar dispositivos y recopilar datos de manera inteligente abre nuevas oportunidades

para la mejora de productos y servicios, la optimización de operaciones y la resolución de problemas en diversas industrias.

La implementación de IoT en sectores clave de la economía como la agricultura de precisión, manufactura avanzada, logística y generación/distribución de energía está claramente en expansión tanto en México como en Colombia, impulsada por las mejoras en la eficiencia de las operaciones que permiten esta tecnología. Asimismo, se observa el surgimiento de ecosistemas dinámicos de *startups* dedicados al IoT en polos de innovación como Guadalajara y Ciudad de México en el caso mexicano y Bogotá y Medellín en el contexto colombiano. Esta base emprendedora robustecerá la capacidad para el desarrollo de soluciones IoT competitivas a nivel global.

Además, el Internet de las Cosas (IoT) desempeña un papel crucial en la creación de una mayor interconexión entre los sistemas y las personas, lo que fomenta la colaboración y la toma de decisiones más colaborativa. Esta conectividad permite la implementación de soluciones altamente personalizadas y adaptadas a las necesidades individuales, lo que a su vez impulsa la innovación en la forma en que vivimos, trabajamos y nos relacionamos con el entorno digital y físico. La recopilación y el intercambio de datos entre dispositivos y sistemas son fundamentales para crear soluciones más inteligentes y orientadas al futuro en una amplia variedad de sectores.

Dado lo anterior, el Internet de las Cosas (IoT) desempeña un papel fundamental en la transformación de la industria 4.0 al habilitar la recopilación y el intercambio de datos en tiempo real, la automatización avanzada y la toma de decisiones basada en datos. La convergencia de IoT e industria 4.0 está revolucionando la fabricación y la gestión de la cadena de suministro, mejorando la eficiencia, la calidad y la capacidad de adaptación en un entorno altamente competitivo. La integración efectiva de estas tecnologías será esencial para impulsar la innovación y la competitividad en la industria.

Un factor crucial en la implementación de la IoT es la seguridad, ya que es un componente crítico que permite garantizar la integridad, privacidad y protección de los datos y sistemas conectados. La implementación de medidas de seguridad robustas, como la autenticación, la encriptación y la gestión de parches, es esencial para mitigar las vulnerabilidades y riesgos asociados con el IoT. A medida que el IoT continúa su expansión en una variedad de sectores, la seguridad debe ser una prioridad para garantizar su adopción segura y sostenible.

De otra parte, a través del estudio presentado y la revisión minuciosa de las normatividades existentes en las dos naciones estudiadas (México y Colombia), se logra evidenciar un interés creciente de las mismas en el desarrollo de regulaciones en las diversas ramas e incidencias del IoT. Dichas normativas muestran un enfoque fuerte en el establecimiento de estándares comunes de comunicación e interconexión, así como la necesidad del reforzamiento en los parámetros de seguridad y privacidad de la información. Ambos países están respondiendo a la necesidad de regular y aprovechar el potencial del IoT en la industria, agricultura, logística, transporte, seguridad y salud.

Si bien Colombia no cuenta con una normatividad propia (NTC), los índices relacionados con la preparación para la adopción tecnológica del país indican un crecimiento fuerte. Lo anterior se debe en parte al establecimiento minucioso de las normas internacionales ISO de IoT sin modificaciones para todos los sectores a nivel nacional, lo que permite un lenguaje común no solo entre desarrollos nacionales, sino la comunicación directa con productos tecnológicos extranjeros.

Por su parte, México cuenta con las NMX para IoT que le permiten focalizar su interés de desarrollo y enfocar sus aplicaciones rumbo al cumplimiento de los ODS; aun así, se presenta un debilitamiento en el *ranking* internacional de preparación para tecnologías emergentes. Esto puede deberse en parte a su propia normatividad, la cual debe adaptarse constantemente a los estándares internacionales, lo que representa retrasos significativos en los tiempos de aplicación de las normas correspondientes.

Aun con el debilitamiento y caída de 4 puntos de México quedando en el puesto 61 en el estándar internacional de preparación para nuevas tecnologías, este país sigue estando por encima de Colombia, la cual, a pesar de avanzar 6 puestos, se encuentra en el puesto 72 a nivel mundial. El retroceso de México se debe principalmente al incremento en las brechas TIC, I+D, habilidades e inversiones industriales. Por el contrario, el fortalecimiento de Colombia se encuentra ligado a la reducción de las brechas tecnológicas en los diferentes sectores de interés, especialmente en la industria, la cual ha fortalecido su inversión.

Si bien el futuro luce promisorio, existen aún desafíos importantes compartidos entre los dos países estudiados para el despliegue masivo de IoT, especialmente en términos de privacidad y seguridad de los datos, la integración con legados tecnológicos y sistemas internos y la provisión

de conectividad confiable en zonas rurales. Superar estas barreras requerirá de políticas públicas activas, alianzas público-privadas, inversiones focalizadas y modelos de negocio sostenibles ligados a la industria 4.0 y la 5.0 emergente.

Referencias

ABNT (n. d.). Asociación Brasileña de Normas Técnicas (ABNT). Obtenido el 10 de noviembre de 2023 de https://abnt.org.br/institucional/sobre-abnt-2/

Alcatel (2019). *Internet de las Cosas en sanidad*. https://www.al-enterprise.com/-/media/assets/internet/documents/iot-for-healthcare-solution-brie f-es.pdf

Audi (2023). *Audi México*. https://www.audi.com.mx/mx/web/es/audi-en-mexico/planta-de-audi-en-mexico/la-nave-de-construccion-de-carrocerias-en-mexico.html

Ávila-Camacho, F. J. & Moreno-Villalba, L. M. (2023). "Internet de las Cosas (IoT). Retos para las empresas en la era de la industria 4.0". *Pädi Boletín Científico de Ciencias Básicas e Ingenierías del ICBI*, 10(20), 10-16. https://doi.org/10.29057/icbi.v10i20.9516

Bonilla, I., Tavizon, S., Morales, M., Guajardo, L. & Laines, C. (2016). "IOT, el internet de las cosas y la innovación de sus aplicaciones". *Universidad Autónoma de Nuevo León*, 2(1), 2313-2340. http://www.web.facpya.uanl.mx/Vinculategica/Revistas/R2/2313-2340-Iot,elinternet delascosasylainnovaciondesusaplicaciones.pdf

Bonneau, V., Copigneaux, B., Probst, L. & Pedersen, B. (2017). "Industry 4.0 in Agriculture: Focus on IoT aspects". *Digital Transformation Monitor*, July, 6. https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Agriculture 4.0 IoT v1.pdf

Campos, C. M., Maldonado, M. R. & Guerra, R. V. (2020). "Adopción de tecnologías digitales 4.0 por parte de pequeñas y medianas empresas manufactureras en la región del Biobío". En N. Unidas (ed.), CEPAL (1.ª ed., vol. 1). CAPAL. https://repositorio.cepal.org/server/api/core/bitstreams/f22a3152-c3c0-4b47-8e41-99603aa777e9/content

Deloitte (2018). *IoT para el sector empresarial en América Latina*. Centro de Estudios de Telecomunicaciones de América Latina, 250.

Desarrollo Económico Gobierno de la República de Honduras (n. d.). Organismo Hondureño de Normalización (OHN). Obtenido el 15 de noviembre de 2023 de https://sde.gob.hn/ohn/

Durán, E. (2019). "Análisis de la implementación del internet de las cosas en la agroindustria colombiana para optimizar y aumentar los procesos de producción". En *Ingeniero de sistemas* (vol. 1, Issue 1). https://repository.ucc.edu.co/server/api/core/bitstreams/bd18f7ac-1c9a-499c-9901-72c7b534c150/content

ELAC, Agenda Digital para A. L. y el C. (2021). "Tecnologías digitales para el nuevo futuro". En Naciones Unidas (ed.), *Educitec - Revista de Estudos e Pesquisas sobre Ensino Tecnológico* (Vol. 8, Issue jan./dez.). https://repositorio.cepal.org/server/api/core/bitstreams/879779be-c0a0-4e11-8e08-cf80b41a4fd9/content

Ferreira, J., Fabiola, M. & Higuera, M. (2021). "Nuevos desafíos en el desarrollo de soluciones para e-health en Colombia, soportados en Internet de las Cosas (IoT)". *Revista EIA*, 18(36), 1-6. https://revistas.eia.edu.co/index.php/reveia/article/view/1508

Flores-Cortez, O. O. & Gonzales Crespin, B. (2023). "Aplicación de tecnologías IoT en el control y seguimiento de transporte de carga terrestre". *Revista Minerva*, 6(1), 43-56. https://doi.org/10.5377/revminerva.v6i1.16416

FondoNorma (n. d.). FondoNorma. 16 de noviembre de 2023.

Friha, O., Ferrag, M. A., Shu, L. & Nafa, M. (2020). *A Robust Security Framework based on Blockchain and SDN for Fog Computing enabled Agricultural Internet of Things*. 2020 International Conference on Internet of Things and Intelligent Applications, ITIA 2020, February. https://doi.org/10.1109/ITIA50152.2020.9312286

Gallardo, A., Herrera, J., Carrillo, S., Aréchiga, M. & Ramos, E. (2023). "Internet de las cosas: teoría y práctica". En U. de Colima (ed.), 1.ª ed. http://ww.ucol.mx/content/publicacionesenlinea/adjuntos/Internet-de-las-cosas-DIG_533.pdf

Gómez-Carmona, O., Buján-Carballal, D., Casado-Mansilla, D., López-de-Ipiña, D., Cano-Benito, J., Cimmino, A., Poveda-Villalón, M., García-Castro, R., Almela-Miralles, J., Apostolidis, D., Drosou, A., Tzovaras, D., Wagner, M., Guadalupe-Rodríguez, M., Salinas, D., Esteller, D., Riera-Rovira, M., González, A., Clavijo-Ágreda, J. … Bujalkova, N. (2023). "Mind the gap: The AURORAL ecosystem for the digital transformation of smart communities and rural areas". *Technology in Society*, 74 (December 2022). https://doi.org/10.1016/j.techsoc.2023.102304

GSMA (2023). "5G in Latin America Unleashing the potential". En A. Adamowicz (ed.), 1.ª ed. GSMA Intelligence. https://www.gsma.com/latinamerica/wp-content/uploads/2023/07/290623-5G-in-Latam-ENG-1.pdf

IBNORCA (n. d.). Instituto Boliviano de Normalización y Calidad (IBNORCA). Obtenido el 10 de noviembre de 2023 de https://www.ibnorca.org/es/quienes-somos

ICONTEC (n. d.). Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). Obtenido el 11 de noviembre de 2023 de https://www.icontec.org/quienes-somos/

ICONTEC (2023). *Resultados para: "IoT"*. https://tienda.icontec.org/catalogsearch/result/?q=IoT

INDECOPI (n. d.). Comisión de Reglamentos Técnicos y Comerciales (CRT). https://www.midagri.gob.pe/portal/193-exportaciones/importancia-de- la-calidad-en-las-agroexportaciones/695-normas-tecnicas-peruanas#:~:text=Las Normas Técnicas Peruanas son,que se complementan entre sí.

INDOCAL (2012). Instituto Dominicano para la Calidad (INDOCAL). https://indocal.gob.do/sobre-nosotros/quienes-somos/

INEN (n. d.). Servicio Ecuatoriano de Normalización (INEN). Obtenido el 13 de noviembre de 2023 de https://www.normalizacion.gob.ec/

INN (n. d.). Instituto Nacional de Normalización (INN). Obtenido el 11 de noviembre de 2023 de https://www.inn.cl/quienes-somos

INTECO (n. d.). Instituto de Normas Técnicas en Costa Rica (INTECO). Obtenido el 12 de noviembre de 2023 de https://inteco.org/

INTERCERT (n. d.). INTERCERT. Obtenido el 17 de noviembre de 2023 de https://intercert.com.pe/

International Data Corporation (IDC) (2023). "IDC Latin America presentó las principales tendencias de los segmentos de TI y Telecom y las oportunidades para el mercado regional". https://www.idc.com/getdoc.jsp?containerId=prLA50472023

IRAM (n. d.). IRAM. Instituto Argentino de Normalización y Certificación. Obtenido el 12 de noviembre de 2023 de https://www.iram.org.ar/institucional/quienes-somos/

ISO (2016). Portal de información sobre normas OMC-ISO. https://tbtcode.iso.org/es/list-of-standardizing-bodies.html

ISO (2018). ISO/IEC 30141 Internet de las Cosas (IoT) Arquitectura de Referencia (Vol. 1). Organización Internacional de Normalización. https://www.iso.org/standard/65695.html

ISO (2021). ISO/IEC 20924 Internet de las Cosas (IoT) Vocabulario (Vol. 2). https://www.iso.org/standard/82771.html

ISO/IEC (2019a). AID-ISO-IEC 21823-1:2019. Internet de las cosas (IoT). Interoperabilidad para los sistemas de IoT. Parte 1: Marco de trabajo. ICONTEC. https://tienda.icontec.org/gp-aid-iso-iec-internet-de-las-cosas-iot-interoperabilidad-para-los-sistemas-de-iot-parte-1-marco-de-trabajo-aid-iso-iec21823-1-2019.html

ISO/IEC (2019b). AID-ISO-IEC 30148:2019. Internet de las cosas (IoT). Aplicación de la red de sensores para contadores de gas inalámbricos. ICONTEC. https://tienda.icontec.org/gp-aid-iso-iec-internet-de-las-cosas-iot-aplicacion-de-la-red-de-sensores-para-contadores-de-gas-inalambricos-aid-iso-iec30148-2019.html

ISO/IEC (2020a). AID-ISO-IEC-TR 30164:2020. Internet de las cosas (IoT). Computación en el borde (*edge computing*). ICONTEC. https://tienda.icontec.org/gp-aid-iso-iec-tr-internet-de-las-cosas-iot-computacion-en-el-borde-edge-computing-aid-iso-iec-tr30164-2020.html

ISO/IEC (2020b). AID-ISO-IEC 21823-2:2020. Internet de las cosas (IoT). Interoperabilidad para los sistemas de IoT. Parte 2: Interoperabilidad en el transporte. https://tienda.icontec.org/gp-aid-iso-iec-internet-de-las-cosas-iot-interoperabilidad-para-los-sistemas-de-iot-parte-2-interoperabilidad-en-el-transporte-aid-iso-iec21823-2-2020.html

ISO/IEC (2021). ISO/IEC 30147:2021 Information technology Internet of things Methodology for trustworthiness of IoT system/service (No. 1; Vol. 1, p. 31). ISO. https://www.iso.org/standard/53267.html

ISO/IEC (2022a). ISO/IEC 30142-2:2022 Internet of Things (IoT) Underwater acoustic sensor network (UWASN) Network management system (Vol. 1, p. 29). International Organization for Standardization. https://www.iso.org/standard/85500.html

ISO/IEC (2022b). ISO/IEC 30162:2022 Internet of Things (IoT) Compatibility requirements and model for devices within industrial IoT systems (Vol. 1, p. 44). International Organization for Standardization. https://www.iso.org/standard/53282.html

ISO/IEC (2022c). ISO/IEC 30169:2022 Internet of Things (IoT) IoT applications for electronic label system (ELS) (Vol. 1, p. 23). International Organization for Standardization. https://www.iso.org/standard/53289.html

ISO/IEC (2022d). ISO/IEC 30171-1:2022 Internet of Things (IoT) Base-station based underwater wireless acoustic network (B-UWAN) Part 1: Overview and requirements (Vol. 1, p. 11). International Organization for Standardization. https://www.iso.org/standard/53291.html

ISO/IEC (2022e). ISO/IEC 21823-4:2022 Internet of things (IoT) Interoperability for IoT systems (Vol. 4). ISO. https://www.iso.org/standard/84773.html

ISO/IEC (2022f). ISO/IEC 23093-1:2022 Information technology Internet of media things (No. 2; Vol. 2, p. 23). https://www.iso.org/standard/81586.html

ISO/IEC (2022g). ISO/IEC 27400:2022 Cybersecurity IoT acurity and privacy Guidelines (No. 1; Vol. 1, p. 42). International Standard. https://www.iso.org/standard/44373.html

ISO/IEC (2022h). ISO/IEC AWI 30149 Internet of things (IoT) Trustworthiness framework (Vol. 2). https://www.iso.org/standard/53269.html

ISO / IEC. (2023a). ISO / IEC 30161 – 2: 2023 Internet of Things (IoT) – Data exchange platform for IoT services – Part 2: Transport interoperability between nodal points. (Vol. 1, p. 20). International Organization for Standardization. https://www.iso.org/standard/86671.html

ISO/IEC (2023b). ISO/IEC 30179:2023 Internet of Things (IoT) – Overview and general requirements of IoT systema for ecological environment monitoring (Vol. 1, p. 15). International Organization for Standardization. https://www.iso.org/standard/53299.html

ISO/IEC (22021). AID-ISO-IEC 20924:2021. Internet de las cosas (IoT). Vocabulario. ICONTEC. https://tienda.icontec.org/gp-aid-iso-iec-internet-de-las-cosas-iot-vocabulario-aid-iso-iec20924-2021.html

Jahnke, A. (2020). *Las 4 etapas de la arquitectura IoT*. DIGI Connect Whit Confidence. https://es.digi.com/blog/post/the-4-stages-of-iot-architecture

López, M. (2021). *DevOps aplicado a sistemas IoT: definición e implementación de procesos continuos de monitorización y retroalimentación*. https://oa.upm.es/68043/

Martín, L., Sánchez, L., Lanza, J. & Sotres, P. (2023). "Development and evaluation of Artificial Intelligence techniques for IoT data quality assessment and curation". *Internet of Things* (Netherlands), 22. https://doi.org/10.1016/j.iot.2023.100779

MIFIC (n. d.). Ministerio de Fomento de Industria y Comercio (MIFIC). Obtenido el 14 de noviembre de 2023 de https://www.mific.gob.ni/Inicio/Comercio/Comercio-Interior/SNC/snn/enn/CatNor

Ministerio de Comercio e Industria (n. d.). Dirección General de Normas y Tecnología Industrial (DGNTI). Obtenido el 12 de noviembre de 2023 de https://dgnti.mici.gob.pa/

Ministerio de Economía (n. d.). Comisión Guatemala de Normas (CONGUANOR). Obtenido el 9 de noviembre de 2023 de https://portal.mineco.gob.gt/comisión-guatemalteca-de-normas

Ministerio de Economía de Argentina (2023). INTI Organismo de Certificación. Instituto Nacional de Tecnología Industrial. https://www.inti.gob.ar/areas/servicios-regulados/certificaciones/organismo-de-certificacion

Ministerio de Industria y Comercio (n. d.). Instituto Nacional de Tecnología, Normalización y Metrología (INTN). Obtenido el 14 de noviembre de 2023 de https://www.intn.gov.py/index.php/institucion/acerca-del-intn

ONN (2019). Oficina Nacional de Normalización. 506, 1-10.

OSN. (n. d.). Organismo Salvadoreño de Normalización (OSN). Obtenido el 1 de noviembre de 2023 de https://www.osn.gob.sv/

Peladarinos, N., Piromalis, D., Cheimaras, V., Tserepas, E., Munteanu, R. A. & Papageorgas, P. (2023). "Enhancing Smart Agriculture by Implementing Digital Twins: A Comprehensive Review". *Sensors*, 23(16), 1-38. https://doi.org/10.3390/s23167128

Plana Casarrubios, M. (2023). *Aplicación de algoritmos de inteligencia artificial en sistemas de IoT orientado a la domótica*.

Pons, M., Valenzuela, E., Rodríguez, B., Nolazco-Flores, J. A. & Del-Valle-Soto, C. (2023). "Utilization of 5G Technologies in IoT Applications: Current Limitations by Interference and Network Optimization Difficulties - A Review". *Sensors*, 23(8). https://doi.org/10.3390/s23083876

Quiñonez Muñoz, O. (2019). "Internet de las Cosas (IoT)". En L. Ibukku (ed.), 1.ª ed. https://www.perlego.com/es/book/2913651/internet-de-las-cosas-iot-pdf

Román, A., Román, J., Sandoval, S. & Cabello, M. (2020). "El Internet de las Cosas y su impacto en la educación". En *El internet de las cosas y su impacto en la educación*. http://ww.ucol.mx/content/publicacionesenlinea/adjuntos/IoT-PDF_498.pdf

Rueda-Rueda, J. S., Manrique, J. A. & Cabrera Cruz, J. D. (2017). *Internet de las Cosas en las instituciones de educación superior*. Congreso Internacional en Innovación y Apropiación de las Tecnologías de la Información y las Comunicaciones – CIINATIC 2017, September, 1-5. http://edu.mah.se/en/Course/DA650A

Secretaría de Economía (n. d.). Dirección General de Normas (DGN). Obtenido el 15 de noviembre de 2023 de https://e.economia.gob.mx/direccion-general-de-normas/

Secretaría de Economía (2021a). NMX-I-1362-NYCE-2021, "Telecomunicaciones-Procedimiento simple de encriptación para entornos de Internet de las Cosas (IOT)". *Diario Oficial de La Federación*. https://www.dof.gob.mx/nota_detalle.php?codigo=5642167&fecha=08/02/2022#gsc.tab=0

Secretaría de Economía (2021b). NMX-I-20000-3-NYCE-2021, Tecnologías de la información-gestión del servicio-Parte 3: Guía sobre la definición y aplicabilidad del alcance de la NMX-I-20000-1-NYCE-2019 (CANCELA A LA NMX-I-20000/03-NYCE-2014. *Diario Oficial de La Federación*. https://www.dof.gob.mx/nota_detalle.php?codigo=5642169&fecha=08/02/2022#gsc.tab=0

Secretaría de Economía (2021c). NMX-I-22301-NYCE-2021, Tecnologías de la información-Seguridad y resiliencia-Sistemas de gestión de la continuidad del negocio-Requerimientos (Cancela a la NMX-I-22301-NYCE-2015). *Diario Oficial de La Federación*. https://www.dof.gob.mx/nota_detalle.php?codigo=5642171&fecha=08/02/2022#gsc.tab=0

Secretaría de Economía (2021d). NMX-I-22316-NYCE-2021, Tecnologías de la información-Seguridad y resiliencia-Resiliencia organizacional-Principios y atributos. *Diario Oficial de La Federación*. https://www.dof.gob.mx/nota_detalle.php?codigo=5642172&fecha=08/02/2022#gsc.tab=0

Secretaría de Economía (2021e). NMX-I-4903-NYCE-2021, Telecomunicaciones-Indicadores clave de desempeño relacionados con las ciudades inteligentes y sostenibles, para evaluar el logro de los objetivos de desarrollo sostenible. *Diario Oficial de La Federación*. https://dof.gob.mx/nota_detalle.php?codigo=5642168&fecha=08/02/2022&print=true

Secretaría de Economía (2021f). PROY-NMX-I-20000-7-NYCE-2021, Tecnologías de la información-Gestión del servicio-Parte 7: guía sobre la integración y correlación de la NMX-I-20000-1 NYCE-2019 CON LA NMX-CC-9001-IMNC-2015 y la NMX-I-27001-NYCE-2015. *Diario Oficial de La Federación*. https://dof.gob.mx/nota_detalle.php?codigo=5628903&fecha=06/09/2021#gsc.tab=0

Sethi, P. & Sarangi, S. R. (2017). "Internet of Things: Architectures, Protocols, and Applications". *Journal of Electrical and Computer Engineering*, 2017. https://doi.org/10.1155/2017/9324035

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*, 3 (March), 192-204. https://doi.org/10.1016/j.iotcps.2023.04.006

Tariq, U., Ahmed, I., Kashif, A. & Shaukat, K. (2023). "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review". *Journal of Applied Security Research*, 18(3), 289-305. https://doi.org/10.1080/19361610.2021.1962677

UNCTAD (2023). "Technology and Innovation Report 2023". En Naciones Unidas (ed.), United Nations Conference on Trade and Development. https://unctad.org/system/files/official-document/tir2023_en.pdf

UNIT (n. d.). Instituto Uruguayo de Normas Técnicas (UNIT). Obtenido el 17 de noviembre de 2023 de https://www.unit.org.uy/

Desafíos y oportunidades en la implementación de computación en la nube en las organizaciones: Una mirada de los escenarios en Colombia y México

Challenges and opportunities in the implementation of cloud computing in organizations: a look at the scenarios in Colombia and Mexico

Gómez Gómez, Edgard Mauricio
Candidato a ingeniero de sistemas

Luna Prieto, Jhon Devisson
Candidato a ingeniero de software

Ortiz Reyes, Sara Ximena
Candidato a ingeniero de software

Quintero Mancilla, Brandon Sneyder
Candidato a ingeniero de software

Cardenas Lancheros, Esteban Alejandro
Docente del programa de ingeniería de software

Resumen

En la actualidad, la pandemia de COVID-19 ha obligado a las organizaciones a adaptarse a nuevos modelos de trabajo, impulsando la migración de sus activos tecnológicos a la nube. Este cambio se ha vuelto esencial en la industria tecnológica, donde el trabajo remoto se ha convertido en una norma. Las organizaciones ya no dependen de espacios físicos para sus empleados, lo que ha llevado a la necesidad de permitir el acceso a los recursos desde cualquier ubicación. Como resultado, se ha producido una migración significativa hacia la nube y la implementación de conexiones VPN (Red Virtual Privada, en inglés: Virtual Private Network) para garantizar la seguridad de los datos corporativos. Este enfoque no se limita al acceso a datos internos, sino que también abarca la disponibilidad de proyectos de *software*, documentación y otros recursos cruciales para los clientes. La transición hacia la nube no solo garantiza la continuidad de las operaciones internas, sino que también mejora la accesibilidad y la colaboración, lo que se ha vuelto fundamental en un entorno empresarial cada vez más globalizado y digital. Las organizaciones que adoptan esta tendencia están posicionándose de manera estratégica para afrontar los desafíos y oportunidades del futuro.

Por esta razón, en este documento queremos explicar la importancia de la transición a la nube y sus implicaciones; para ello, haremos una comparación entré Colombia y México, la cual nos brinda un panorama más claro sobre la utilización de dichos recursos y nos brinda un óptica no solo desde el punto de vista colombiano, sino también del exterior. A lo largo de este capítulo, podremos ver algunas características importantes, como, por ejemplo, tecnologías implementadas, capacidad de servidores e infraestructura, ventajas y desventajas y, sobre todo, diferencias en la implementación de la nube en ambos países.

Palabras clave: *computación en la nube, servicios en la nube, ciberseguridad, transformación tecnológica, migración tecnológica.*

Abstract

Currently, the COVID-19 pandemic has forced organizations to adapt to new work models, driving the migration of their technology assets to the cloud. This

shift has become essential in the technology industry, where remote work has become the norm. Organizations no longer rely on physical spaces for their employees, which has led to the need to enable access to resources from any location. As a result, there has been a significant migration to the cloud and the implementation of VPN (Virtual Private Network) connections to ensure the security of corporate data, this approach is not limited to internal data access, but also encompasses the availability of software projects, documentation, and other crucial resources for customers. The transition to the cloud not only ensures continuity of internal operations, but also improves accessibility and collaboration, which has become critical in an increasingly globalized and digital business environment. Organizations that embrace this trend are strategically positioning themselves to meet the challenges and opportunities of the future.

For this reason, in this document we want to explain the importance of the transition to the cloud and its implications, for this we will make a comparison between Colombia and Mexico, which gives us a clearer picture on the use of these resources and gives us an optic not only from the Colombian point of view but from abroad, throughout this chapter we will see some important features, advantages and disadvantages and especially differences in the implementation of the cloud in both countries.

Keywords: *cloud computing, cloud services, cybersecurity, technology transformation, technology migration.*

Cursos articulados

El proyecto "Desafíos y oportunidades en la implementación de computación en la nube en las organizaciones: una mirada de los escenarios en Colombia y México" ha sido concluido exitosamente. Durante su desarrollo, se abordaron cursos fundamentales, tales como "Gestión de Proyectos" y "Tecnologías de la Información", para entender los aspectos técnicos y de gestión involucrados en la implementación de la computación en la nube. Además, "Seguridad de la Información" y "Estudio de Casos Empresariales" ayudaron a identificar desafíos y oportunidades específicos en los contextos colombiano y mexicano. Este proyecto proporcionó una visión detallada de los escenarios de la computación en la nube en ambas naciones, contribuyendo significativamente al conocimiento en este campo.

Introducción

En la actualidad, las organizaciones se han visto en la necesidad de trasladar sus activos tecnológicos a la nube debido a los cambios en la forma de trabajar que han surgido como resultado de la pandemia de COVID-19. Este fenómeno es relevante en tecnología, donde muchas empresas ya no requieren espacios físicos para sus empleados, ya que han adoptado el trabajo remoto como norma. Como resultado, se ha tenido que habilitar el acceso a los recursos de las organizaciones desde cualquier ubicación, lo que ha implicado la migración de estos recursos a la nube y la implementación de conexiones VPN para garantizar la seguridad y la integridad de la información de la empresa. Este enfoque no se limita únicamente al acceso a los datos internos de la organización, sino que también abarca la disponibilidad de proyectos de *software*, documentación y otros recursos vitales para los clientes de las organizaciones (Núñez *et al.*, s. f.).

Al implementar y adaptar computación en la nube en las compañías, hay riesgos y desafíos que deben abordarse con estrategias de implementación para que las compañías no sufran un cambio tan drástico; se deben considerar estrategias de capacitación y de adaptación para los empleados, ya que no a todos se les facilita el uso de la nube. También es necesario tener una plataforma que centralice el acceso a la información que sea fácil de usar y amigable con el usuario. Para este escenario, también se debe contar con un sistema de seguridad, ya que cada empleado debe ingresar desde diferentes partes del mundo, desde sus hogares o desde el espacio externo a la oficina principal, como los *coworking*, que se han popularizado en los últimos años (Pathak, 2021).

Considerando las anteriores apreciaciones, se deduce que algunos de los problemas más importantes de una compañía al implementar computación en la nube son los riesgos de seguridad, desafíos de capacitación a los empleados para usar la plataforma designada como punto de acceso a la información, implementación de sistemas de seguridad como VPN (Red Virtual Privada, en inglés: Virtual Private Network) para acceder a las mismas, desafíos de infraestructura y conectividad y financieros.

El proyecto se enfoca en los desafíos y riesgos vinculados a la adopción de tecnología de la nube en entornos empresariales, así como en estrategias eficaces para abordarlos. La adopción de soluciones en la nube es una tendencia en constante crecimiento en el ámbito corporativo debido a su

capacidad para transformar operaciones, pero también conlleva obstáculos críticos, destacándose la seguridad de datos, la capacitación de empleados, la accesibilidad y conectividad y los costos de infraestructura. Para abordar estos desafíos, se realizará una comparación de la nube en los contextos mexicanos y colombianos para sugerir las mejores maneras de adopción; además, se proponen estrategias integrales, que incluyen medidas de seguridad sólidas, programas de capacitación, la selección de interfaces de usuario amigables y la elección de una infraestructura escalable. Las estrategias buscan garantizar una migración exitosa a la nube y optimizar los beneficios que esta tecnología puede ofrecer (AWS, 2021).

Este estudio comparativo entre los contextos de Colombia y México en relación con la adopción de la computación en la nube tiene como objetivo la identificación de patrones, lecciones aprendidas y estrategias exitosas que puedan aportar beneficios significativos tanto a estas naciones como a las empresas que operan en sus respectivos territorios. Al analizar y contrastar dichos contextos, se busca proporcionar una guía práctica y orientación estratégica con el fin de mejorar la adopción de la computación en la nube. Por ejemplo, al examinar cómo las empresas colombianas han enfrentado desafíos específicos en materia de seguridad de datos y cómo las empresas mexicanas han abordado cuestiones relacionadas con la capacitación de empleados, se pueden extraer valiosas lecciones aplicables en contextos similares. Asimismo, al destacar ejemplos concretos de empresas en ambos países que han logrado una adopción exitosa de la nube, este trabajo aspira a inspirar y proporcionar modelos a seguir para otras organizaciones que buscan aprovechar al máximo los beneficios de esta tecnología (Medel, 2018).

Este enfoque comparativo, respaldado por ejemplos concretos, permitirá una comprensión más profunda de las dinámicas que influyen en la adopción de la computación en la nube en Colombia y México y contribuirá a la formulación de recomendaciones específicas para mejorar este proceso en ambas naciones.

Contexto del proyecto

Estado del arte

Se ha observado un aumento constante en la adopción de la nube en todo el mundo debido a su potencial para reducir costos, mejorar la escalabilidad y proporcionar flexibilidad en la gestión de recursos informáticos (Conzultek, 2020).

En el periodo comprendido entre 2021 y 2022, el mercado de la nube en México experimentó un crecimiento del 35 %, una cifra récord que se prevé que se mantenga en los próximos años, según el informe de IDC (en inglés, International Data Corporation) en 2022. Además, se estima que para 2030, de un total de 226,300 millones de pesos en este mercado, un 33 % se atribuirá a la nube pública, un 23 % a la nube privada y el resto a la nube híbrida, según un estudio de Huawei en el mismo año.

El estudio sobre la *Digitalización de pymes durante la contingencia* realizado por la empresa CONTPAQi reveló que el 35 % de las pequeñas y medianas empresas ya han adoptado *software* en la nube. Datos proporcionados por el IDC en 2022 indican que el 70 % de las empresas mexicanas se consideran maduras digitalmente, con una adopción del 60 % de soluciones basadas en la nube, mientras que el 10 % de estas empresas se clasifican como nativas digitales. Entre las empresas mexicanas que aprovechan los servicios en la nube se encuentran Grupo Bimbo, Quálitas, Levi's, Aeroméxico, Rotoplas, Fujifilm México, Actinver y Farmacias del Ahorro. Además, instituciones educativas como la UNAM y la Escuela Bancaria y Comercial han logrado un ahorro del 30 % mediante la adopción de servicios como SaaS (*Software as a Service*), migrando 95 de sus herramientas y aplicaciones internas a la nube de AWS (Atomic32, 2023).

El estudio de mercado de computación en la nube en Colombia realizado por IDC pronosticó que el mercado de la computación en la nube en Colombia alcanzaría los $2.000 millones de dólares para el año 2023 (IDC, 2022).

Según el estudio titulado *El impacto en la economía* llevado a cabo por la Universidad de los Andes revela que la computación en la nube posee el potencial de generar un impacto positivo en la economía colombiana.

Según el estudio, se estima que esta tecnología podría dar lugar a la creación de hasta 100.000 nuevos empleos y un incremento de $5.000 millones de dólares en el Producto Interno Bruto (PIB) de Colombia (UniAndes, 2023).

De acuerdo con la publicación titulada *La computación en la nube en Colombia: el futuro de la educación*, elaborada por la Universidad Nacional de Colombia, se identifica un potencial transformador de la computación en la nube en el ámbito educativo de Colombia. Las conclusiones de la publicación sugieren que las instituciones educativas colombianas deberían considerar la adopción de esta tecnología con el propósito de elevar la calidad de la educación en el país (Colombia, 2023).

En Colombia, la empresa Bancolombia, una de las instituciones financieras más grandes de Colombia, ha aprovechado la computación en la nube para mejorar sus operaciones y servicios. Han utilizado soluciones en la nube para optimizar su infraestructura tecnológica, reducir costos y ofrecer servicios bancarios en línea más eficientes y seguros (América, 2021). Así como también Rappi, el exitoso *startup* colombiano, ha utilizado la nube para escalar rápidamente su plataforma de entrega a domicilio. Gracias a la escalabilidad y flexibilidad que ofrece la nube, Rappi ha podido expandir sus operaciones no solo en Colombia, sino también en otros países de América Latina (AWS A, 2023).

En México, la empresa Cemex, compañía líder en la industria de materiales de construcción, ha implementado soluciones en la nube para optimizar sus procesos de negocio y mejorar la eficiencia en la gestión de la cadena de suministro; esto les ha permitido tomar decisiones más informadas y mejorar la colaboración en toda la empresa (ITSitio, 2019). Como también lo hizo Kueski, empresa *fintech* mexicana que ha utilizado la computación en la nube para ofrecer préstamos en línea de manera rápida y eficiente. Gracias a la escalabilidad de la nube, Kueski ha podido adaptarse a la creciente demanda de sus servicios y expandir su presencia en el mercado (PRYER, 2022; Infochannel, 2018). Estos son solo algunos ejemplos de cómo las empresas en Colombia y México han aprovechado la computación en la nube para mejorar sus operaciones, reducir costos y ofrecer servicios más eficientes y flexibles. Estos casos de éxito demuestran el potencial de la nube para impulsar la innovación y el crecimiento empresarial en ambas naciones.

Discusión

Los resultados de la visita a las empresas KIO Data Center y Audi en México, demuestran aspectos importantes en torno a la adopción de la nube y el desarrollo tecnológico. En Audi, se aloja información sobre sus procesos de ensamblaje en servidores en la nube ubicados en Alemania, lo que refleja una estrategia de gestión global. Este enfoque global se complementa con una tecnología de automatización de procesos que utiliza el *machine learning*, lo que agiliza la producción y el ensamblaje de carrocerías de manera significativa.

En cuanto a la infraestructura como servicio, se observa que estas organizaciones cuentan con una infraestructura robusta y madura que les permite ofrecer servicios de alojamiento, ciberseguridad, servidores, soporte y monitoreo de calidad.

Las visitas a estas empresas en México han permitido apreciar las diferencias notables en la ubicación estratégica, tecnología implementada, enfoque en la nube y desarrollo tecnológico en comparación con Colombia. Estas diferencias reflejan las particularidades de cada entorno y sus estrategias de innovación y desarrollo.

Según los aspectos mencionados, se puede concluir que la adopción de la nube en México está altamente estandarizada. Un ejemplo ilustrativo es el caso de los empleados de Audi, quienes muestran un alto grado de familiaridad con esta tecnología. Explican que todos los datos y análisis relevantes se almacenan en servidores ubicados en Alemania y que la operación de la ensambladora depende en gran medida de estos servidores destinados para el almacenamiento de información crítica. Además, destacan que cuentan con planes de contingencia sólidos para hacer frente a posibles ataques cibernéticos, junto con programas de capacitación y concienciación dirigidos a los empleados.

Adicionalmente, en Audi explican que las máquinas utilizadas en el ensamblaje de automóviles se programan mediante el uso de *machine learning* con el objetivo de agilizar y optimizar el proceso de producción. Es importante resaltar que esta disciplina de *machine learning* permite la identificación de patrones en datos masivos y la realización de predicciones que, a su vez, habilitan a las máquinas para llevar a cabo tareas específicas de manera autónoma. No obstante, es relevante subrayar que, a pesar de la autonomía

de estas máquinas en su funcionamiento, siempre están bajo la supervisión y control de personal humano.

KIO Data Center es una empresa mexicana líder en el sector de centros de datos y servicios de tecnología de la información, con presencia en México, Panamá, Guatemala, Colombia, República Dominicana y España. Ofrece soluciones de infraestructura como servicio (IaaS) y servicios relacionados para empresas de diversos sectores. KIO se enfoca en la seguridad de la información y la disponibilidad de los servicios, monitorear servicios en la nube pública, privada e híbrida, lo que es fundamental para sus clientes. Algunos de sus clientes en el sector de la nube son Google Cloud, AWS, Azure y Huawei.

El proceso de contratación de servicios de nube en la empresa KIO se basa en la comprensión del negocio de los posibles clientes. A partir de este entendimiento, se realiza la presentación de una propuesta de arquitectura de nube completa, que incluye costos y otros elementos esenciales. Esto tiene como objetivo brindar a los clientes una comprensión clara de los servicios que están contratando y facilitar un acompañamiento más efectivo durante el proceso de adopción de la nube. Esta aproximación beneficia a los negocios de los clientes al garantizar una implementación exitosa y alinear sus necesidades con las soluciones de nube de KIO.

No obstante, se destaca que las empresas de gran envergadura, con considerables volúmenes de información y un alto número de usuarios, demandan un acompañamiento más personalizado. Este acompañamiento se despliega en fases que abarcan la planificación, la operación, el soporte y la garantía de disponibilidad de la información.

Se hace énfasis en la seguridad cibernética para protección de la información y la pérdida de información como los más grandes desafíos de la migración a la nube, KIO ofrece el servicio de CyberSoc, el cual consiste en tener profesionales especializados, certificaciones e inteligencia artificial para identificar y detectar vulnerabilidades, con el fin de responder oportunamente ante cualquier amenaza.

Este estudio se propone diseñar un marco de comparación entre Colombia y México que represente los pasos y las estrategias involucradas en la migración de operaciones críticas a la nube y, a su vez, muestre las ventajas y desafíos potenciales de la adopción de la nube, considerando factores como costos operativos, infraestructura, conectividad, eficiencia, mayor escalabilidad e innovación.

Así mismo, proponer un plan de acción basado en los hallazgos y experiencias, que incluya medidas concretas para la implementación de mejoras en la adopción de la computación en la nube en las organizaciones.

Metodología

Se propone la siguiente metodología con el fin de dar cumplimiento a los objetivos específicos; se encuentra dividida en tres fases:

- **Fase 1:**

  Recolección y análisis de bibliografía y datos relacionados con entornos organizacionales en el escenario de Colombia y México, para obtener información valiosa, que den lugar a evidenciar tendencias y conocimientos que formarán la base de la comparación.

  ✓ **Método de investigación:**

  El método de investigación utilizado para la fase es el método de recolección de bibliografías, que nos ayuda a identificar un grupo de información, para poder llegar a un resultado de datos.

  ✓ **Actividades:**

  Recopilar bibliografía y datos sobre la implementación de la computación en la nube en los países Colombia y México, donde podamos obtener evidencias y cifras reales de las implementaciones realizadas.

  Analizar la información y extraer la que realmente genera valor dentro del ejercicio de establecer una comparativa entre los escenarios de Colombia y México en materia de implementación de computación en la nube.

  ✓ **Producto:**

  El producto propuesto consiste en una solución de recopilación de datos basada en bibliografías. Esta herramienta tiene como objetivo ayudarnos a analizar la información recolectada y poder realizar un análisis en método gráfico.

- **Fase 2:**
  Diseño de un marco de comparación entre Colombia y México que represente los pasos y las estrategias involucradas en la migración de operaciones críticas a la nube y, a su vez, muestre las ventajas y desafíos potenciales de la adopción de la nube.

  ✓ **Método de investigación:**

  El método es el de la investigación documental y de estudio comparativo; en este método se analizaron y compararon prácticas de adopción de la computación en la nube en Colombia y México, basado en documentos, registros históricos, libros, artículos y otras fuentes escritas.

  ✓ **Actividades:**

  Evaluar la preparación para la implementación en la nube: evaluar la infraestructura, costos, eficiencia y escalabilidad actuales en Colombia y México para identificar la idoneidad de la migración a la nube en
  ambas regiones.

  Analizar los beneficios y desafíos de la implementación en la nube: comparar las ventajas potenciales, como ahorros y eficiencia, con los desafíos, como la conectividad y la resistencia al cambio, de la migración a la nube en Colombia y México, resumiendo las diferencias clave.

  ✓ **Producto:**

  El producto de esta segunda fase es la presentación de un cuadro comparativo en el cual se muestran los diferentes aspectos: desafíos, beneficios, alcances, los cuales nos mostrarán el punto de vista de cada país según la migración a la nube.

- **Fase 3:**

  Propuesta de un plan de acción basado en los hallazgos y experiencias, que incluya medidas concretas para la implementación de mejoras en la adopción de la computación en la nube en las organizaciones.

- ✓ **Método de investigación:**

  Método analítico en el cual se realizó una descomposición del cuadro comparativo para posteriormente realizar el plan de acción enfocado.

- ✓ **Actividades:**

  Recopilar hallazgos y experiencias relacionados con la adopción de computación en la nube en organizaciones en los contextos colombianos y mexicanos.

  Elaborar el plan de acción basado en los hallazgos y experiencias recopilados; el plan contendrá medidas concretas para mejorar la adopción de computación en la nube.

- ✓ **Producto:**

  El producto propuesto es un plan de acción estratégico diseñado para impulsar la adopción exitosa de la computación en la nube en el contexto de la industria 4.0 en México y Colombia. Este plan de acción se basa en un análisis detallado de los desafíos de ambas naciones en la adopción de la nube y se centra en la creación de una estrategia para maximizar las ventajas de la tecnología.

Resultados del desarrollo de las fases metodológicas

Fase 1. Recolección de bibliografía y análisis de datos

Colombia

Bancolombia implementó soluciones en la nube de AWS para modernizar sus sistemas bancarios centrales. Esto les permitió lanzar nuevos productos digitales un 50 % más rápido (AWS Bancolombia, 2021).

Grupo Nutresa, durante la última década, ha liderado una iniciativa de modernización tecnológica en la cual ha implementado con éxito un sistema privado de computación en la nube en colaboración con IBM. Este avance tecnológico ha permitido la unificación de toda la información de

sus negocios, que incluyen cárnicos, café, pastas, chocolates, helados y galletas, y abarca operaciones en múltiples países, como Perú, Venezuela, Costa Rica, Estados Unidos, México y República Dominicana. Grupo Nutresa se destacó como pionero en la ado

pción de tecnología en la nube en Colombia, siendo uno de los primeros en utilizar servicios de infraestructura compartida, lo que eventualmente se conoció como *cloud computing*. Este cambio tecnológico ha tenido un impacto significativo en la eficiencia operativa, ya que redujo el tiempo necesario para realizar copias de seguridad de 8 horas a aproximadamente 40 minutos (IALIMENTOS, 2020).

Colombina, desde 2007, ha logrado mejorar su eficiencia al implementar sistemas unificados de información a través de una plataforma tecnológica adquirida. Esto ha permitido a la empresa gestionar de manera más efectiva la distribución y las ventas en su extensa red de tenderos, que es una de las más grandes en Colombia. Colombina decidió tercerizar su tecnología de la información y eligió a IBM como socio debido a su experiencia local y capacidades globales. Jesús Antonio Brand, *Chief Information Officer* (CIO) de Colombina, destaca que IBM ha contribuido constantemente a la innovación y al servicio de la empresa. El proyecto de Colombina implica la tercerización de su plataforma de información, que abarca procesos como producción, facturación y distribución, respaldados por el Centro de Innovación de IBM. Esta asociación garantiza la continuidad y eficiencia en la gestión de la empresa (IALIMENTOS, 2020).

Postobón, una compañía colombiana que cuenta con un amplio catálogo de bebidas azucaradas con sede en Medellín, es una de las empresas más grandes de Colombia y una de las principales en América del Sur. Desde 2019, Postobón ha elegido Ofi para administrar sus servicios en la nube que se ejecutan en Amazon Web Services (AWS). Esto les proporcionó mayor agilidad y una reducción del tiempo de comercialización de nuevos productos (Bearsthemes, 2019)

Grupo Éxito ha estado utilizando las capacidades de la plataforma de mercado de VTEX para permitir que más de 1.000 minoristas se conecten y vendan sus productos, amplíen su alcance y faciliten el acceso de los clientes a una amplia variedad de productos en un solo lugar. Junto con otras funcionalidades como VTEX Intelligent Search (un sistema de búsqueda de ajuste fino), Éxito ha recibido comentarios positivos al realizar la migración

de Oracle ATG a VTEX. También han experimentado mejoras continuas, que culminaron con la serie Día sin IVA (Gheorghiade, 2020).

La aerolínea Avianca utiliza AWS para ejecutar sus sitios web y aplicaciones móviles. Han logrado una disponibilidad del 99,99 % para sus aplicaciones críticas de cliente (AWS Avianca, 2021).

Grupo Argos adoptó servicios en la nube para reducir costos de IT en un 30 %. También mejoraron la flexibilidad y agilidad en el desarrollo de nuevas aplicaciones (Grupo Argos, 2021).

Tecnoquímicas, la compañía farmacéutica, adoptó AWS para modernizar sus sistemas y agilizar el cumplimiento regulatorio. Lograron migrar 35 aplicaciones críticas a la nube en menos de 3 meses (Garces, 2020).

Bodytech, la cadena de gimnasios, implementó soluciones de *big data* en AWS para entender mejor el comportamiento de los clientes. Esto les permitió diseñar mejores estrategias de mercadeo y ventas (e-core, 2023).

Rappi, la empresa emergente de *delivery*, opera completamente sobre la infraestructura en la nube de AWS. Esto les permite escalar rápidamente para satisfacer la demanda en 6 países de Latinoamérica (AWS Rappi, 2023). Coca-Cola, la compañía de bebidas, migró su centro de datos principal a AWS. Coca-Cola Andina crea lagos de datos en AWS y aumenta la productividad de análisis en un 80 % para mejorar la toma decisiones basadas en datos (CPG, 2021).

México

Mex Rent a Car, la empresa mexicana de alquiler de autos, ha obtenido ahorros mensuales de más de $7.500 dólares estadounidenses y ha podido extender sus capacidades a ofrecer servicios de facturación automática, un mejor servicio al cliente, campañas de *marketing* optimizadas, *forecasting* (pronósticos) y análisis de datos. Tales han sido los beneficios que la empresa ahora está compartiendo su experiencia con otros y podría convertirse en el futuro cercano en un socio de AWS, ayudando a otras empresas a migrar a la nube (AWS Mex Rent a Car, 2021).

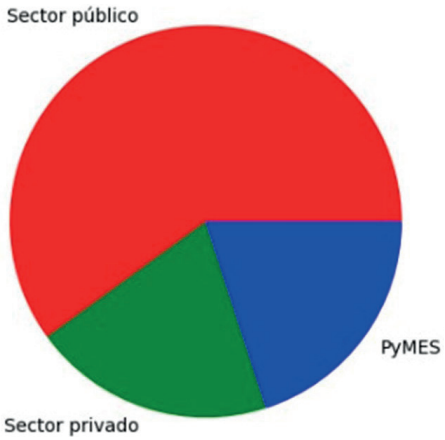
Konfío, la empresa mexicana, fue creada con el reto de ayudar a las pequeñas y medianas empresas mexicanas a crecer. Su misión es la de permitir que las pymes se enfoquen en hacer crecer su negocio y no necesariamente en cómo conseguir capital o fondearse para su expansión. Para esto, Konfío tenía el desafío de ofrecer servicios de manera más atractiva que aquellos que le acercaban a las pymes los bancos tradicionales. Desde que empezó sus operaciones, Konfío decidió apoyarse en la tecnología AWS. Tecnologías como AWS Lambda, por ejemplo, le permiten a Konfío tomar decisiones muy rápidamente para acelerar los procesos y responder a las solicitudes de los clientes de forma casi inmediatas (AWS Konfío, 2020).

Telmex y Amazon Web Services firmaron un acuerdo de colaboración estratégica que permitirá a las organizaciones de los sectores público y privado acelerar su migración a la nube, además de impulsar su adopción entre pequeñas y medianas empresas (pymes) en México. Analistas de IDC estiman que el mercado de nube en México crezca alrededor del 28,9 % anual entre 2021 y 2026 (Datacenter Dynamics, 2023).

INE es el Instituto Nacional Electoral de México. La Unidad Técnica de Servicios de Informática del INE administra la mayor parte de los sistemas de TI del INE y respalda, entre sus diversas responsabilidades, todos los procesos electorales en México. INE buscó soluciones en la nube con el objetivo de obtener más seguridad y solidez para divulgar los resultados de las últimas elecciones presidenciales en 2018. Desde la conexión con miles de dispositivos móviles, desde la potencia informática de Amazon Elastic Compute Cloud y el almacenamiento de datos con Amazon Simple Storage Service, seguridad con AWS WAF y AWS Shield, INE utilizó todo el poder de las tecnologías de AWS para gestionar una elección nacional sin problemas, garantizando la seguridad y la agilidad de los datos. INE aún tuvo el apoyo del socio Advanced Consulting Partner de AWS, iNBest (AWS INE, 2019).

Análisis de datos expresados en gráficos

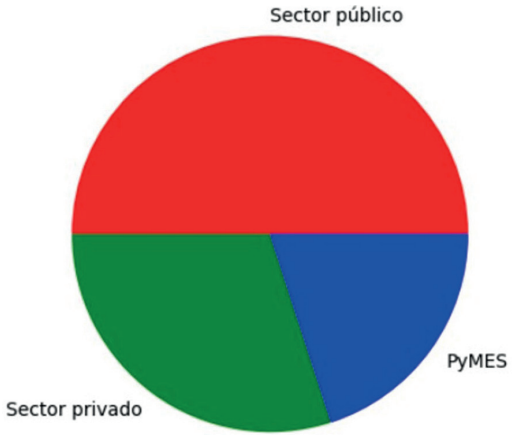
Figura 26. Porcentaje de empresas que han adoptado la nube por sector en 2023 en Colombia



Nota. Porcentaje de empresas que han adoptado la nube por sector en 2023 en Colombia. Fuente: autores.

Sector público : 60 %
Sector privado : 20 %
Pymes : 20 %

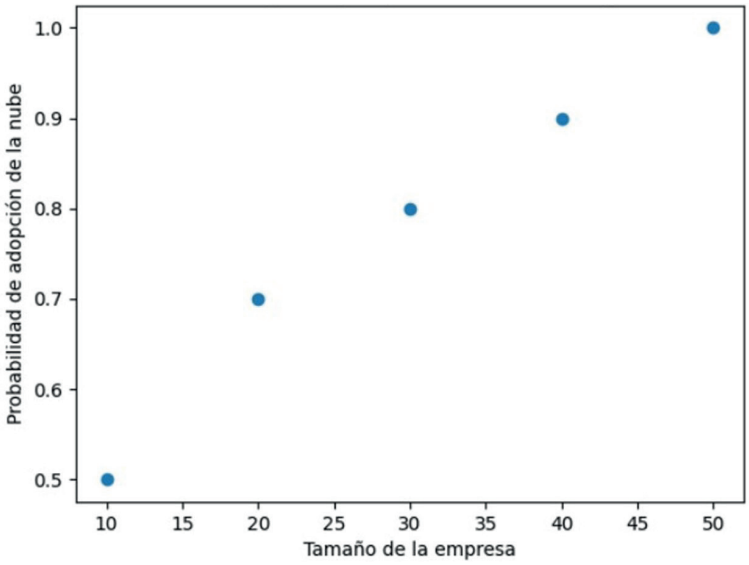
Figura 27. Porcentaje de empresas que han adoptado la nube por sector en 2023 en México



Nota. Porcentaje de empresas que han adoptado la nube por sector en 2023 en México. Fuente: autores.

Sector público : 50 %
Sector privado : 30 %
Pyme : 20 %

Figura 28. Relación entre el tamaño de la empresa y la probabilidad de adopción de la nube en Colombia



Nota. Relación entre el tamaño de la empresa y la probabilidad de adopción de la nube en Colombia. Fuente: autores.

Fase 2. Marco de comparación entre Colombia y México

Tabla 16. Marco de comparación

País Comparación	Colombia	México
BENEFICIOS	• **Reducción de costos:** al utilizar servicios en la nube, las organizaciones pueden evitar la inversión inicial en infraestructura y hardware, así como los costos de mantenimiento y actualización.	**Reducción de costos:** la computación en la nube permite a las empresas y organizaciones reducir los costos de infraestructura, ya que no necesitan invertir en servidores y equipos costosos. Además, los servicios en la nube suelen tener un modelo de pago por uso, lo que permite a las empresas pagar solo por los recursos que utilizan.

País Comparación	Colombia	México
BENEFICIOS	• **Acceso remoto:** los servicios en la nube permiten acceder a la información y aplicaciones desde cualquier lugar y en cualquier momento, siempre y cuando se tenga una conexión a internet. • **Mayor flexibilidad:** las organizaciones pueden adaptarse rápidamente a los cambios del mercado y a las necesidades del negocio, ya que la nube ofrece una amplia gama de servicios y opciones. • **Mayor colaboración:** la nube facilita la colaboración entre equipos de trabajo, permitiendo compartir y editar documentos de forma simultánea.	**Escalabilidad y flexibilidad:** la nube ofrece la capacidad de escalar rápidamente los recursos informáticos según las necesidades de la empresa. Esto permite a las organizaciones adaptarse fácilmente a cambios en la demanda y evitar la infrautilización o sobrecarga de recursos. **Acceso remoto:** la computación en la nube permite a los usuarios acceder a sus datos y aplicaciones desde cualquier lugar y en cualquier momento, siempre que tengan una conexión a internet. Esto facilita el trabajo remoto y la colaboración entre equipos distribuidos geográficamente. **Actualizaciones automáticas:** los proveedores de servicios en la nube se encargan de mantener y actualizar la infraestructura y el software, lo que libera a las empresas de la carga de realizar estas tareas. Esto garantiza que las aplicaciones estén siempre actualizadas y seguras. **Mayor capacidad de almacenamiento:** la nube ofrece una capacidad de almacenamiento prácticamente ilimitada, lo que permite a las organizaciones almacenar grandes cantidades de datos sin preocuparse por el espacio físico. **Mayor seguridad:** los proveedores de servicios en la nube suelen contar con medidas de seguridad avanzadas para proteger los datos de sus clientes. Esto incluye copias de seguridad automáticas, cifrado de datos y sistemas de detección de intrusiones.

País Comparación	Colombia	México
DESAFÍOS	• **Seguridad:** la seguridad de los datos es uno de los principales desafíos en la nube, ya que implica confiar en terceros proveedores de servicios para proteger la información. • **Privacidad:** existe la preocupación de que los datos almacenados en la nube puedan ser accedidos por terceros sin autorización. • **Dependencia de la conexión a internet:** para acceder a los servicios en la nube es necesario contar con una conexión a internet estable y confiable. • **Cumplimiento normativo:** almacenar datos en la nube puede implicar cumplir con regulaciones y normativas específicas en cuanto a la privacidad y seguridad de la información.	**Seguridad y privacidad:** aunque los proveedores de servicios en la nube implementan medidas de seguridad, existe la preocupación de que los datos almacenados en la nube puedan ser vulnerables a ataques cibernéticos o accesos no autorizados. Además, algunos países tienen regulaciones estrictas sobre la privacidad de los datos, lo que puede dificultar la adopción de la nube. **Dependencia de la conexión a internet:** la computación en la nube requiere una conexión a internet confiable y rápida. Si la conexión se interrumpe o es lenta, puede afectar la disponibilidad y el rendimiento de los servicios en la nube. **Interoperabilidad y portabilidad:** mover datos y aplicaciones entre diferentes proveedores de servicios en la nube puede ser complicado debido a la falta de estándares y la dependencia de las tecnologías propietarias. Esto puede dificultar la migración de una nube a otra o la integración de servicios de diferentes proveedores. **Riesgo de dependencia del proveedor:** al utilizar servicios en la nube, las organizaciones pueden volverse dependientes de un proveedor específico. Si el proveedor experimenta problemas o decide cambiar sus políticas o precios, puede afectar la continuidad del negocio. **Cumplimiento normativo**: algunas industrias y países tienen regulaciones específicas sobre la ubicación y el acceso a los datos. Esto puede dificultar la adopción de la nube si los proveedores no cumplen con los requisitos regulatorios.

País Comparación	Colombia	México
ALCANCES	• Almacenamiento de datos: permite almacenar grandes volúmenes de datos de manera segura y accesible desde cualquier lugar. • Procesamiento de datos: la nube ofrece capacidad de procesamiento para realizar análisis de datos complejos y ejecutar aplicaciones de alto rendimiento. • Colaboración: facilita la colaboración entre equipos de trabajo, permitiendo compartir y editar documentos de forma simultánea. • Desarrollo de aplicaciones: los desarrolladores pueden utilizar la nube para crear, probar y desplegar aplicaciones de manera más rápida y eficiente. • Internet de las cosas (IoT): la nube es fundamental para el almacenamiento y procesamiento de datos generados por dispositivos conectados a internet, como sensores y dispositivos inteligentes.	**Empresas:** la computación en la nube ofrece a las empresas la capacidad de acceder a recursos informáticos de alta calidad sin la necesidad de invertir en infraestructura costosa. Esto les permite ser más ágiles y competitivas en el mercado. **Gobierno:** los gobiernos pueden aprovechar la computación en la nube para mejorar la eficiencia en la prestación de servicios públicos, promover la colaboración entre agencias y mejorar la transparencia y la participación ciudadana. **Usuarios individuales:** los usuarios individuales pueden beneficiarse de la computación en la nube al acceder a aplicaciones y servicios desde cualquier dispositivo con conexión a internet. Esto les permite tener acceso a sus datos y aplicaciones personales en cualquier momento y lugar. **Investigación y desarrollo:** la computación en la nube ofrece a los investigadores y científicos la capacidad de acceder a recursos informáticos de alto rendimiento para realizar análisis complejos y procesamiento de datos a gran escala. **Educación:** la computación en la nube puede mejorar la educación al permitir a los estudiantes y profesores acceder a recursos educativos en línea, colaborar en proyectos y acceder a herramientas de aprendizaje en línea.

Nota. Marco de comparación Colombia-México. Fuente: autores.

Fase 3. Plan de acción

Evaluación y planificación

Se evaluará el estado actual de adopción de la computación en la nube y se elaborará un plan estratégico para mejorarlo.

- **Evaluación conjunta:** realizar una evaluación conjunta de la infraestructura actual de adopción de la nube en Colombia y México, identificando desafíos y oportunidades comunes.

- **Análisis del estado actual:** evaluar la infraestructura de TI existente, la adopción de la computación en la nube y los desafíos actuales.

- **Desarrollo de estrategia regional:** desarrollar una estrategia regional de adopción de la nube que aborde los desafíos de seguridad, privacidad y cumplimiento normativo. Esta estrategia debe incluir un análisis de costo-beneficio y un enfoque en los beneficios compartidos.

Implementación y optimización

Se implementarán soluciones en la nube y se optimizará de manera continua el entorno en la nube.

- **Implementación de infraestructura y capacitación del personal:** iniciar la implementación de la infraestructura en la nube en ambas naciones, compartiendo recursos y buenas prácticas, además de proporcionar capacitación conjunta al personal sobre la adopción de *cloud computing* y las mejores prácticas.

- **Monitoreo y mejora continua regional:** implementar un sistema de monitoreo conjunto para evaluar el rendimiento de los servicios en la nube en ambos países y realizar revisiones regionales periódicas y optimizaciones basadas en los datos de rendimiento y seguridad compartidos.

Evaluación y seguimiento

Se evaluarán los resultados de la implementación y se realizarán ajustes según sea necesario.

- **Evaluación postimplementación regional:** evaluar el impacto de la adopción de la nube en la eficiencia, la escalabilidad y la competitividad de las organizaciones en Colombia y México.

- **Planificación de mejoras regionales:** desarrollar un plan de acción regional conjunto que incluya mejoras adicionales en la adopción de la nube y la colaboración entre los dos países.

Conclusiones y recomendaciones

Se recomienda que las organizaciones, independientemente sean de Colombia o México, busquen mejorar la adopción de la computación en la nube, implementando el plan de acción que aborde los desafíos de seguridad, privacidad y cumplimiento normativo propuesto de manera sistemática.

Colombia tiene un margen de participación en el mercado de la nube del 8 % a comparación de México, que tiene un margen del 23 %; la buena noticia es que, según Forbes Latinoamérica, tendrá un margen de crecimiento para el 2025 del 40 %; se estima que un 85 % de las organizaciones habrán adoptado *cloud-first* (implementarán soluciones en la nube para los futuros desarrollos).

Las organizaciones deberán implementar planes de capacitación, herramientas y estrategias de ciberseguridad para lograr la implementación exitosa de la nube, considerando que los objetivos de la ciberseguridad son la prevención, detección y recuperación y que el principal foco de ataques cibernéticos son los usuarios, según los diferentes ataques, como hombre en medio o *phishing*.

Referencias

CPG (2021). Coca-Cola Andina. https://aws.amazon.com/

America, P. T. (2021). "Bancolombia elige a AWS para migrar sus aplicaciones a la nube". https://prensariotila.com/

Atomic32 (2023). *¿Qué es "cloud computing"?* LinkedIn.

AWS (2021). *Información general sobre el marco para la adopción de la nube de AWS*. Documento técnico de AWS.
AWS, A. (2023). "Rappi optimiza un 90 % su costo-beneficio en la nube de AWS gracias a FinOps". https://aws.amazon.com/
AWS Avianca (2021). Avianca, AWS. https://aws.amazon.com/
AWS Bancolombia (2021). "Bancolombia: primera empresa latinoamericana en migrar Murex a la nube de Amazon Web Services (AWS)". AWS.
AWS INE (2019). "INE utilizó las tecnologías de AWS para gestionar una elección nacional en la nube". https://aws.amazon.com/
AWS Konfío (2020). "Konfío utiliza AWS para ayudar a las pymes mexicanas a crecer". https://aws.amazon.com/
AWS Mex Rent a Car (2021). "Mex Rent a Car, acelerando el motor con AWS Cloud". https://aws.amazon.com
AWS Rappi (2023). "Caso práctico de Rappi". https://aws.amazon.com/
Bearsthemes (2019). *Postobon en la nube*. https://www.ofinow.com/
Bernal, C. (2016). *Metodología de la investigación*. Colombia: Pearson.
Caballero López, J. E. (septiembre de 2009). http://scielo.isciii.es/pdf/mesetra/v55n216/revision.pdf
Colombia, U. N. (2023). *Transformación digital en instituciones de educación superior. Modelo de implementación*. Universidad Nacional de Colombia, Facultad de Ingeniería y Arquitectura, Departamento de Ingeniería Industrial Manizales, Caldas, Colombia.
Conzultek (2020). *Computación en la nube*. https://blog.conzultek.com /.
Datacenter Dynamics (2023). "Telmex y AWS firman un acuerdo de colaboración para acelerar la adopción de la nube de las empresas en México". https://www.datacenterdynamics.com .
e-core (2023). "Bodytech migra a AWS y mejora la seguridad de la infraestructura". https://www.ecore.com/
Garces, M. I. (2020). *Soluciones business intelligence*. https://repository.icesi.edu.co/
Gheorghiade, S. (2020). "Mil pedidos por minuto: planificación y arquitectura de Peak Retail de VTEX y Grupo Éxito". https://aws.amazon.com/
Grupo Argos (2021). "Grupo Argos y adopción en la computación en la nube". https://www.grupoargos.com/
IALIMENTOS (2020). "Nutresa y Colombina optimizan sus sistemas tecnológicos". https://www.revistaialimentos.com/
IDC (2022). "Compradores de infraestructura digital empresarial: transformación de las relaciones estratégicas con los proveedores en 2022". http://www.idccolombia.com.co/
Infochannel, S. (2018). "AWS reconoce a empresas por modelos de nube". https://infochannel.info/

ITSitio (2019). *CEMEX GO, el caso de éxito de IBM en transformación digital*. https://www.itsitio.com/

John, A. (2016). *Normas básicas de higiene del entorno en la atención sanitaria*. India: Organización Mundial de la Salud. http://apps.who.int/iris/bitstream/handle/10665/246209/9789243547237spa.pdf;jsessionid=98A5D7C69806F077F4D7F5B862DCA0BB?sequence=1

Medel, A. C. (2018). *¿Vale la pena el cloud computing en Latinoamérica? Una exploración del mercado actual y sus proyecciones*. LinkedIn.

Pryer, J. (2022). "Kueski elige a Provenir para impulsar sus ambiciosos planes de crecimiento y expansión". https://www.provenir.com/

UniAndes (2023). *El impacto en la economía*. https://waf.virtual.uniandes.edu.co/

Ciberseguridad en América Latina: un análisis comparativo entre Colombia y México

Cybersecurity in Latin America: a comparative analysis between Colombia and Mexico

Cruz Mesa, Wilson Alexander
Candidato a ingeniero de software

Escudero Ávila, Michael Armando
Candidato a ingeniero de software

Quiñones Ciprián, Harold David
Candidato a ingeniero de software

Velasco Romero, Andrés Felipe
Candidato a ingeniero de software

Solorzano Suárez, José De Los Santos
Docente del programa de ingeniería de sistemas

Resumen

En un mundo cada vez más interconectado y digital, la ciberseguridad se ha convertido en una preocupación crítica que impacta a gobiernos, empresas y ciudadanos. Esta investigación se centra en un análisis comparativo de la ciberseguridad en dos países latinoamericanos que son Colombia y México. El problema central de estos dos países es la creciente amenaza cibernética que enfrentan, con un aumento constante de ciberataques que amenazan la seguridad de datos, la infraestructura crítica y la privacidad ciudadana. Nuestro objetivo principal es examinar y contrastar las estrategias de ciberseguridad en Colombia y México; se espera que los beneficiarios sean los gobiernos, empresas y organizaciones en estos países, además de la comunidad en general, para que cuenten con entornos digitales más seguros. Esta investigación adopta un enfoque interdisciplinario y comparativo, considerando aspectos técnicos, legales y políticos de la ciberseguridad en ambos países; se utilizará la recopilación y análisis de datos cualitativos y cuantitativos, junto con información que nos brindaron algunos encargados de ciberseguridad en las entidades corporativas, como en KIO, donde se observó que los servicios no solo son eficientes, sino respaldados por un enfoque sólido en ciberseguridad para reforzar la confianza en sus servicios.

La singularidad de esta investigación radica en su enfoque comparativo específico en dos naciones latinoamericanas, lo que permitirá una comprensión profunda de los desafíos únicos que enfrenta la región en ciberseguridad, esperando que las recomendaciones resultantes sean altamente relevantes y adaptables a la realidad de ambos países.

Palabras clave: *ciberseguridad, protección de datos, estrategias de ciberseguridad, confianza en servicios, América Latina.*

Abstract

In an increasingly interconnected and digital world, cybersecurity has become a critical concern that impacts governments, companies and citizens. This research focuses on a comparative analysis of cybersecurity in two Latin American countries: Colombia and Mexico, the The central problem of these

two countries is the growing cyber threat they face, with a constant increase in cyber attacks that threaten data security, critical infrastructure and citizen privacy, our main objective is to examine and contrast the cybersecurity strategies in Colombia and Mexico , the beneficiaries are expected to be governments, companies and organizations in these countries, as well as the community in general so that they have safer digital environments. This research adopts an interdisciplinary and comparative approach, considering technical, legal and political aspects of cybersecurity in both countries, the collection and analysis of qualitative and quantitative data will be used, along with information provided to us by some cybersecurity managers in corporate entities, as in KIO where it was observed that the services are not only efficient but supported by a solid focus on cybersecurity, to reinforce confidence in their services.

The uniqueness of this research lies in its specific comparative focus on two Latin American nations, which will allow a deep understanding of the unique challenges faced by the region in cybersecurity, hoping that the resulting recommendations will be highly relevant and adaptable to the reality of both countries.

Keywords: *cybersecurity, data protection, cybersecurity strategies, trust in services, Latin América*

Cursos articulados

Durante su ejecución de este proyecto, se aplicaron los conocimientos adquiridos en cursos esenciales como "Seguridad de la Información" y "Análisis de Riesgos", los cuales proporcionaron una base sólida para el análisis comparativo de la ciberseguridad en Colombia y México. Además, se utilizaron los *insights* obtenidos de "Política de Seguridad" y "Derecho Informático" para comprender los aspectos legales y políticos relacionados con la ciberseguridad en ambos países. Estos cursos jugaron un papel fundamental en la realización de un análisis profundo y significativo de la ciberseguridad en América Latina, permitiendo abordar de manera efectiva los desafíos y oportunidades en este campo.

Introducción

En la actual era digital, la ciberseguridad es un aspecto clave y de vital importancia en los diferentes sectores de la sociedad, teniendo en cuenta que la tecnología ha transformado el mundo en todos los ámbitos, y con ello ha aumentado la necesidad de salvaguardar la información crítica empresarial, la infraestructura esencial y la privacidad personal. Este documento ofrece un análisis comparativo de la ciberseguridad en América Latina, centrándose especialmente en países como México y Colombia. Para contextualizar e ilustrar la relevancia de este estudio comparativo, es importante conocer lo concerniente a ciberseguridad y su relevancia a nivel global.

En la actualidad, en el contexto de la revolución digital, la ciberseguridad se ha convertido en una preocupación de interés general, impulsada por la rápida evolución tecnológica que ha transformado radicalmente todos los aspectos de la sociedad. Esta transformación ha generado una necesidad urgente de comprender la situación actual de la ciberseguridad en la región de América Latina y el resto del mundo.

Para apreciar la magnitud de este estudio, es fundamental definir con precisión el concepto de ciberseguridad. De acuerdo con Varona (2021) en su tesis *Modelo dinámico de ciberseguridad en estándares ISO para instituciones en Colombia*, la ciberseguridad se define para incluir una amplia gama de prácticas, técnicas y medidas destinadas a proteger los sistemas, redes y datos digitales del acceso no autorizado y la actividad maliciosa. Sin embargo, es importante enfatizar que la ciberseguridad es más que tecnología. Su enfoque integral también incluye dimensiones jurídicas, éticas y humanas.

La importancia de la ciberseguridad ha trascendido la categoría de un término de moda para consolidarse como una prioridad ineludible en nuestro entorno interconectado. Como se indica en el ensayo de Bekerman (2021) *Algunas medidas de ciberseguridad en Argentina, Colombia, Egipto, Francia, Grecia, Japón, Singapur y Turquía*, la prevención de los ciberataques es un motivo de gran preocupación a nivel internacional. Las Naciones Unidas expresaron su preocupación de que la interferencia con la seguridad en línea pudiera violar los derechos fundamentales consagrados en la Carta. La era digital expone a los países, incluida América Latina, a riesgos cibernéticos que trascienden barreras y dominios. Antes de dar inicio al

análisis comparativo, es imperativo examinar el corpus existente de investigación, incluyendo tesis y ensayos que han explorado la ciberseguridad en México y Colombia.

Entre estos trabajos, resalta la tesis *Modelo dinámico de ciberseguridad basado en estándares ISO para instituciones de educación superior en Colombia* (Varona, 2021), el cual proporciona valiosos conocimientos sobre la implementación de los estándares ISO en el contexto colombiano. Asimismo, Cano (2022), en su análisis denominado *Perspectiva nacional de ciberseguridad para Colombia al 2030*, profundiza en los esfuerzos dirigidos a enfrentar los desafíos en ciberseguridad, especialmente en los ámbitos político, social, económico y cultural. Por otro lado, el estudio *Teletrabajo en Colombia: análisis del estado de la ciberseguridad en las pequeñas y medianas empresas*, evidencia la crítica importancia de la ciberseguridad en el contexto del teletrabajo, especialmente para las pequeñas y medianas empresas (Palacios *et al.*, 2021).

Este documento se estructura en tres secciones. La primera sección se denomina "Contexto" y tiene como objetivo brindar una visión general de los temas tratados en el documento. Se enfoca en proporcionar al lector información específica sobre cuestiones relacionadas con la ciberseguridad en los contextos de Colombia y México. La segunda sección, titulada "Marco metodológico", se dedica a la metodología identificada a través de visitas e investigaciones realizadas en diversas empresas y entidades en ambos países. Estas visitas y estudios nos permitieron conocer legislaciones y normativas que desempeñan un papel fundamental en la implementación de medidas de ciberseguridad. Finalmente, en la tercera sección, llevamos a cabo un análisis comparativo entre Colombia y México. Se examinan las diferencias en tecnologías, enfoques metodológicos y normativas relacionadas con la protección de la privacidad tanto a nivel personal como empresarial en ambos países

Metodología

La metodología que se implementará para llevar a cabo este análisis comparativo será la mixta, que es un enfoque de investigación que combina elementos tanto cuantitativos como cualitativos en un solo estudio o investigación.

A continuación, se presentan los instrumentos y fases de la investigación:

- **Fase 1. Construcción de herramientas, levantamiento de la información.**

  En el marco de estudio de ciberseguridad de Colombia y México, se realizó un minucioso levantamiento de información de ambos países. Este proceso inició con la identificación de fuentes confiables, tales como tesis y ensayos de entidades académicas, gubernamentales y corporativas de ambos países. Gracias a esta información, se conoció sobre herramientas especializadas para analizar amenazas cibernéticas, así como técnicas de análisis forense digital para revisar incidentes previos. También se realizaron entrevistas a personal encargado de la ciberseguridad en entidades corporativas, donde brindaron información que enriquecieron la compresión de desafíos y buenas prácticas. Toda esta información fue la base para un documento de ciberseguridad que fusionó estrategias y recomendaciones para fortalecer la seguridad digital en ambos países.

- **Fase 2. Inmersión internacional empresarial.**

  Se visitaron dos empresas y dos universidades en el país de México para observar el comportamiento de la gestión de la industria 4.0. Se inicia el recorrido con Audi, donde se observa que más de 100 máquinas tienen implementadas tecnologías 4.0 con sus respectivas medidas de seguridad de *software* para que no sean vulnerables a ataques cibernéticos; se destacaron nuevas tecnologías, como son los *cobots*, y que buscan su enfoque en la "economía circular"; además, se presentó su *Smart Factory*, donde lo usan para manufacturación de vehículos y llevan sus registros diarios.

  La siguiente empresa fue KIO Networks, establecida en 2002 y con sede en México, que ofrece una amplia gama de servicios de tecnología de la información fundamentales para sus clientes. Su objetivo principal es garantizar una operación efectiva de los sistemas de TI de sus clientes mediante la planificación, ejecución y gestión de infraestructuras tecnológicas.

- **Fase 3. Análisis de la información.**

  Durante las visitas a las empresas y universidades en México y Colombia, se hizo evidente la diversidad en cuanto a tecnologías de automatización y *software* utilizadas para la gestión de la ciberseguridad. Esto refleja la importancia de la adaptabilidad y la constante evolución en el campo de la ciberseguridad, ya que diferentes organizaciones eligen soluciones que mejor se ajusten a sus necesidades y recursos disponibles. También se destacó la presencia de equipos forenses de ciberseguridad, un enfoque vital para identificar y mitigar amenazas en tiempo real, lo que subraya la importancia de la detección y respuesta temprana en un mundo cibernético cada vez más hostil.

  Además, se observó un énfasis significativo en la regulación y el control del flujo de información personal en México. Esto es una señal positiva de la conciencia y la protección de la privacidad de los datos en el país. Las universidades en México se están preparando para enfrentar diversos desafíos futuros al enfocarse en tecnologías emergentes. Esto demuestra un compromiso hacia la innovación y el desarrollo de capacidades avanzadas de ciberseguridad en un entorno que evoluciona rápidamente. En resumen, las visitas resaltaron la importancia de la adaptación, la regulación y la preparación para enfrentar los desafíos cambiantes en el ámbito de la ciberseguridad en México y Colombia.

Resultados

La ciberseguridad es un tema de creciente importancia en la era digital. Los ataques cibernéticos pueden tener un impacto significativo en las organizaciones, los gobiernos y los individuos. Como podemos ver en el ensayo de Luis Joyanes Aguilar (2015) llamado *Estado del arte de la ciberseguridad*, esto no solo afecta a los países más desarrollados y tecnológicos del mundo, sino que también demuestra que cualquier sistema de información es vulnerable a ataques, sin importar qué tan insignificante parezca, y que tener protegidos estos recursos es un deber de todas las entidades.

Para que la ciberseguridad se establezca de manera efectiva, es importante que los países adopten reglas y estándares que permitan a las empresas y entidades cumplir con lo necesario para proteger su información de

manera adecuada. Hace algunos años, ya se mencionaba en el informe de Rodrigo Cortés Borrero (2015) llamado *Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia* que Colombia apostaba por la ciberseguridad, mostrando que el principal enfoque en la ciberseguridad se da en las entidades gubernamentales, siguiendo los siguientes estándares y normas:

- Documento CONPES 3701 de 2011.
- Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009.
- Circular 052 de 2007 (Superintendencia Financiera de Colombia).
- Norma Técnica NTC-ISO/IEC Colombiana 27001.

Aparte de estos estándares, se crean las siguientes normas para darle el manejo y el uso adecuado a la información de los usuarios de manera general en todas las entidades del país que guarden información de los usuarios:

- Ley 527 de 1999 – Comercio electrónico.
- Ley 599 de 2000 – Código Penal colombiano.
- Ley 603 de 2000 – Control de legalidad de *software*.
- Ley 962 de 2005 – Ley antitrámites.
- Ley 1150 de 2007 – Modificación al Estatuto de Contratación Pública.
- Ley 1266 de 2008 – *Habeas data*.
- Ley 1273 de 2009 – Delitos informáticos.
- Ley 1341 de 2009 – Sociedad de la información y las TIC.
- Ley 1581 de 2012 – Protección de datos personales.

Si bien ahora no estamos dentro de los diez primeros a nivel mundial, logramos consolidarnos en el puesto 81 a nivel global y el puesto 9 en el continente americano en el Índice Mundial de Ciberseguridad llevado a cabo por la ITU (Unión Internacional de Telecomunicaciones) en 2020, donde se evidencia que Colombia apuesta por medidas técnicas y un gran desarrollo en ciberseguridad, pero no se tienen presentes las medidas legales y la normatividad de esta.

Figura 29. Desarrollo de Colombia

Colombia (República de)

Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas técnicas
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
63,72	9,14	17,58	6,67	14,42	15,93

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Nota. Tomado de Unión Internacional de Telecomunicaciones (2020). Índice Mundial de Ciberseguridad 2020. ITU Publicaciones.

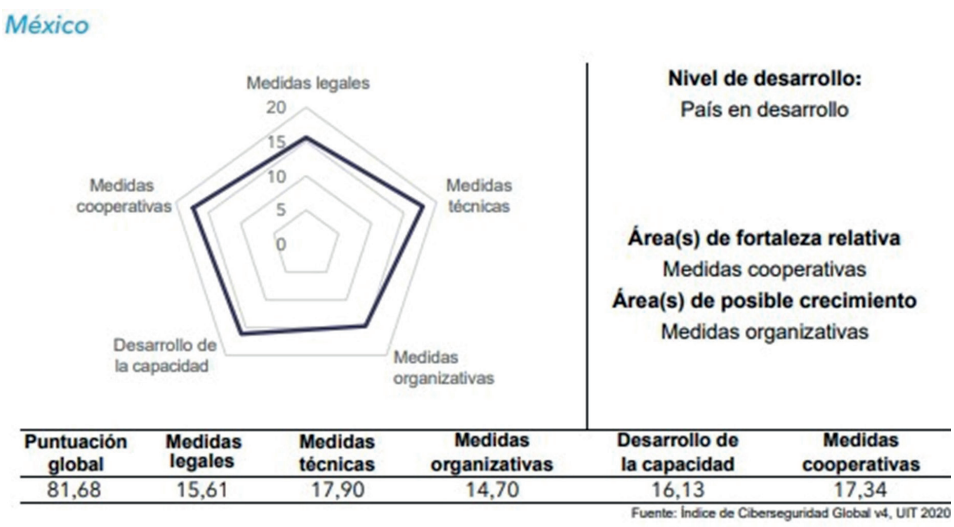
En México, se puede notar un panorama más general en medidas de normas y reglas aplicadas a la mayoría de las empresas que necesiten el manejo de la ciberseguridad, si bien no están explícitamente descritas las empresas que deben seguir estas normas y estándares en la normativa mexicana. Aun así, se recomienda el uso de los siguientes estándares y medidas como medidas básicas para cualquier tipo de empresa, ya sea pequeña, media o grande, según el estudio de caso *Políticas internas de ciberseguridad en las pequeñas y medianas empresas mexicanas* (García, 2023), donde evidencian las siguientes normativas que se usan en México, las cuales son:

- ISO 27002
- ISO 27001
- NIST

México ocupa el puesto número 52 a nivel global y el puesto número 4 en el continente americano en el Índice Mundial de Ciberseguridad llevado a cabo por la ITU (Unión Internacional de Telecomunicaciones) en 2020, invirtiendo mucho más que Colombia en medidas legales y normativas. Esto puede deberse a que en México las industrias que necesitan e invierten

en su ciberseguridad son mucho mayores y en una escala un poco mayor, dando la necesidad de una normativa más eficiente y eficaz.

Figura 30. Desarrollo de México



Nota. Tomado de Unión Internacional de Telecomunicaciones (2020). Índice Mundial de Ciberseguridad 2020. ITU Publicaciones.

Tabla 17. Cuadro comparativo entre México y Colombia

Aspecto	Colombia	México
Posición en Índice de Ciberseguridad 2020 (según la ITU)	Puesto 81 a nivel global y puesto 9 en América	Puesto 52 a nivel global y puesto 4 en América
Enfoque en ciberseguridad	Enfoque técnico con énfasis en estándares ISO	Enfoque más amplio con regulaciones y normativas específicas
Normativas destacadas	-Norma Técnica NTC ISO/IEC colombiana 27001	-ISO 27002 -ISO 27001 -NIST
Fortalecimiento normativo y legal	Necesita fortalecer su marco normativo y legal	Tiene regulaciones específicas y obligatorias para ciberseguridad

Aspecto	Colombia	México
Colaboración público-privada	Se enfoca en colaboración y buenas prácticas	La colaboración es esencial para promover mejores prácticas
Capacitación y certificación	Promoción de capacitación y estándares internacionales	Enfoque en promover la capacitación y certificación en ciberseguridad

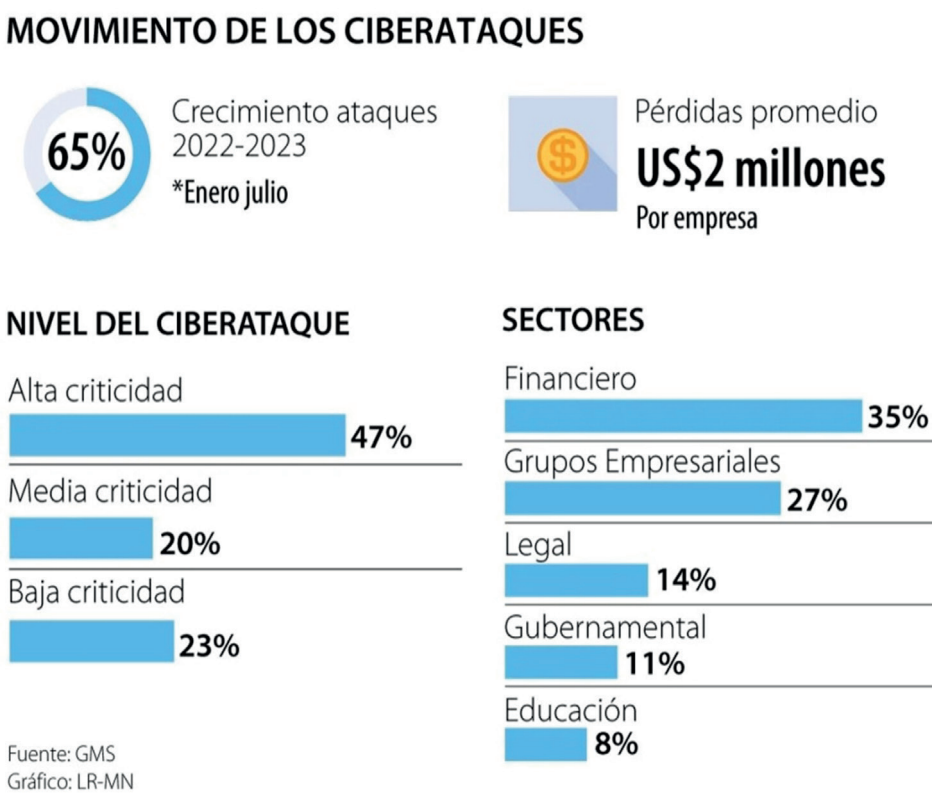
Nota. Cuadro comparativo entre México y Colombia. Fuente: autores.

Discusión

Figura 31. Ciberataques en México

Nota. Tomado de eSemanal. (2023). "México fue el objetivo de más de 14 mil millones de intentos de ciberataques en el primer semestre de 2023".

Figura 32. Crecimiento de ciberataques en Colombia



Nota. Tomado de La República. (2023). "Ciberataques subieron un 65 %, siendo los bancos e industriales sus blancos más comunes".

En las gráficas anteriores, se logra evidenciar que los ciberataques son un problema grave y creciente que afecta tanto a las empresas como a los ciudadanos de América latina, específicamente en México y Colombia. Estos ciberataques generan pérdidas millonarias y ponen en riesgo la seguridad, la privacidad y el desarrollo de las organizaciones y las personas.

Según los resultados obtenidos a lo largo de la investigación, se han identificado algunas diferencias y similitudes en los enfoques de México y Colombia en situaciones actuales en este ámbito. Se reflejaron algunas recomendaciones para ambos países, que vienen siendo:

Colombia:

1. **Fortalecimiento normativo y legal:** Colombia debería continuar con la labor de fortalecer el marco normativo y legal en el ámbito de la ciberseguridad para asegurar un enfoque más amplio y completo. Esto implicaría actualizar y ampliar las leyes y regulaciones relacionadas con la ciberseguridad, garantizando la protección de datos personales y la responsabilidad en caso de ataques cibernéticos.

2. **Colaboración público-privada:** fomentar la colaboración entre las entidades gubernamentales, el sector privado y la sociedad civil es esencial. Se deben establecer operaciones estratégicas para fomentar las mejores prácticas y conocimientos sobre protección cibernética con el fin de coordinar la respuesta ante incidentes de vulnerabilidad cibernética.

México:

1. **Ampliación de normativas específicas:** México debe trabajar en el desarrollo de normativas específicas y obligatorias para cualquier tipo de empresa, con el propósito de establecer requisitos de ciberseguridad y buenas prácticas que se deben seguir. Esto garantiza un nivel mínimo de protección en todo el ámbito empresarial.

2. **Capacitación y certificación:** promover la capacitación y certificación en ciberseguridad para profesionales y organizaciones es fundamental. Hay que buscar incentivar el acople de estándares internacionales como la ISO 27001 y la NIST, lo que puede elevar los niveles de preparación y respuesta contra ataques cibernéticos.

Conclusiones

Ambos países, Colombia y México, se enfrentan a un crecimiento constante de la amenaza cibernética, lo cual pone en peligro la seguridad de los datos, la infraestructura crítica y la privacidad de los ciudadanos en América Latina.

Colombia se destaca por su enfoque técnico en ciberseguridad, haciendo hincapié en la implementación de estándares ISO y tecnologías específicas en este campo. Por otro lado, México adopta un enfoque más amplio

que incluye regulaciones y normativas específicas aplicables a empresas de cualquier tamaño.

La necesidad de fortalecer el marco normativo y legal en el ámbito de la ciberseguridad es fundamental en ambos países. Esto implica la actualización y ampliación de las leyes y regulaciones relacionadas con la ciberseguridad para garantizar una mayor protección de los datos personales y la responsabilidad en caso de ataques cibernéticos.

La colaboración entre las entidades gubernamentales, el sector privado y la sociedad civil es esencial en ambas naciones. Deben establecerse operaciones estratégicas que promuevan las mejores prácticas y el intercambio de conocimientos sobre la protección cibernética con el fin de coordinar una respuesta efectiva ante incidentes de vulnerabilidad cibernética.

Recomendaciones:

Para Colombia:

Es necesario actualizar y ampliar las regulaciones relacionadas con la ciberseguridad para garantizar una mayor protección de los datos y establecer una mayor responsabilidad en caso de ataques cibernéticos.

Se debe fomentar la colaboración entre las entidades gubernamentales y el sector privado para compartir mejores prácticas y conocimientos en ciberseguridad.

Para México:

México debería desarrollar regulaciones específicas y obligatorias en ciberseguridad que sean aplicables a empresas de todos los tamaños. Esto establecerá requisitos mínimos de protección en todo el ámbito empresarial.

Se debe promover la capacitación y certificación en ciberseguridad tanto para profesionales como para organizaciones. La adopción de estándares internacionales como ISO 27001 y NIST puede elevar los niveles de preparación y respuesta contra los ataques cibernéticos.

Referencias

Aguilar, L. J. (2010). *Estado del arte de la ciberseguridad*.

B., J. M. (11 de julio de 2023). "Ciberataques subieron un 65 %, siendo los bancos e industriales sus blancos más comunes". Obtenido de *La República*: https://www.larepublica.co/empresas/repor te-ciberseguridad-2023-a-empresas-ysectores-3701737

Borrero, R. C. (2015). *Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia*. Universidad de los Andes.

Bueno Munar, L. D. (2022). *Ciberseguridad en Colombia, avances y retos*.

Castaño, S. M. (2021). *Ciberseguridad de las empresas financieras*.

Departamento Nacional de Planeación (2011). *Lineamientos de política para ciberseguridad y ciberdefensa*. CONPES.

Díaz, M. R. (2020). *Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia*. Bogotá.

Santiago Chinchilla, E. J. (2017). *Riesgos de ciberseguridad en las empresas*.

eSemanal (15 de agosto de 2023). eSemanal. Obtenido de "México fue el objetivo de más de 14 mil millones de intentos de ciberataques en el primer semestre de 2023": https://esemanal.mx/2023/08/mexico-fue-el-objetivo-de-mas-de-14-mil-millones-deintentos-de-ciberataques-en-el-primer-semestre-de-2023/

García, A. A. (2018). *Ciberseguridad nacional en México y sus desafíos*.

Granados Correa, S. M. (2020). *Definición de una arquitectura de ciberseguridad para los sistemas de control industrial críticos de empresas de distribución de energía en Colombia*.

Llanos Palacios, R. D. (2021). *Teletrabajo en Colombia: análisis del estado de la ciberseguridad en pequeñas y medianas empresas*.

Ospina, M. & Sanabria, P. (2020). *Desafíos nacionales frente a la ciberseguridad en el escenario global*. Bogotá.

Molina Puentes, E. I. (2019). *Ciberseguridad y ciberdefensa: una mirada reflexiva a las fuerzas militares de Colombia*.

Moreno Pérez, L. M. (2019). *Los nuevos retos en materia de ciberseguridad para Colombia*.

Mosquera, A. V. (2019). *Ciberseguridad en Colombia*.

Restrepo, H. A. (2023). *Comercio electrónico: importancia de la ciberseguridad en las transacciones electrónicas realizadas en las plataformas de compra online y en redes sociales en Colombia*. Bogotá.

Santafe Cruz, L. Y. (2023). *Evaluación del sistema de control interno de la ciberseguridad en Colombia en los últimos años*.

Taborda, M. A. (2021). *Dynamic Cybersecurity Model based on ISO standards for Higher Education Institutions in Colombia*.

Unión Internacional de Telecomunicaciones. (2020). *Índice Mundial de Ciberseguridad 2020*. ITU Publicaciones.

Metologías ágiles: implementación en organizaciones de industrias 4.0

Agile methodologies: implementation in industry 4.0 Organizations

Chaparro Calderón, Jhojan David
Candidato a ingeniero de telecomunicaciones

Contreras Gómez, Andrés Felipe
Candidato a ingeniero de sistemas

Leguizamo Rojas, Faiver
Candidato a ingeniero de sistemas

Suescun Padilla, Ángela María
Candidato a ingeniero de sistemas

Barbosa Castro, Neider Duan
Docente del programa de ingeniería de sistemas

Resumen

La aplicación de metodologías ágiles en un entorno de industria 4.0 y en la infraestructura de Tecnologías de la Información (TI) es el desafío que radica en la necesidad de adaptar estas metodologías, que desde un inicio son diseñadas para la gestión de proyectos en el ámbito de la tecnología de la información, a la industria manufacturera en pleno proceso de transformación digital.

Palabras clave: *industrias, automatización, ágil, interconexión, Scrum, adaptabilidad, IOT, fabricación.*

Abstract

In this chapter, we delve into the application of agile methodologies in an Industry 4.0 environment and within the Information Technology (IT) infrastructure. The challenge we encounter lies in the need to tailor these methodologies, originally designed for project management in the realm of information technology, to the manufacturing industry currently undergoing digital transformation.

Keywords: *industries, automation, agile, interconnection, scrum, adaptability, IOT, manufacturing.*

Cursos articulados

Como parte del desarrollo de métodos ágiles para la industria 4.0, aplicamos los conocimientos adquiridos en cursos específicos a lo largo del programa. Estas materias, como Sistemas Digitales, Sistemas Expertos y Seguridad de la Información e Internet de las Cosas, son fundamentales para nuestro enfoque. Adicional, enumeramos algunos cursos relacionados que nos permiten llevar a cabo el desarrollo de este capítulo:

1. Metodología para el Manejo de la Información: en la Industria 4.0, la gestión ágil de datos e información es esencial para adaptarse rápidamente a las cambiantes demandas de datos. Las metodologías ágiles se aplican en el desarrollo de sistemas de gestión de la información flexibles.

2. Arquitectura Empresarial: es clave en la industria 4.0, proporcionando el marco para diseñar sistemas tecnológicos y procesos empresariales. La integración de metodologías ágiles en la estructura empresarial permite una adaptación ágil a los cambios tecnológicos y los paradigmas empresariales.

3. Gestión de Servicios de Tecnologías de la Información: en la industria 4.0, la gestión de servicios de tecnologías de la información se centra en la provisión de servicios digitales, como la monitorización en tiempo real, el mantenimiento predictivo y la ciberseguridad. Estos servicios son esenciales para el funcionamiento eficaz en un entorno digital en constante cambio.

Introducción

El uso de metodologías ágiles en la era de la industria 4.0 va más allá de ser una tendencia; representa un avance crucial que redefine la gestión de proyectos y transforma la infraestructura de Tecnologías de la Información (TI).

En un entorno caracterizado por una constante evolución tecnológica y una alta demanda de soluciones, es menester contar con herramientas que permitan avanzar al ritmo de la industria. Aquí es donde las metodologías ágiles comienzan a desempeñar un papel fundamental, convirtiéndose en uno de los pilares esenciales en la construcción del progreso y el fortalecimiento de las empresas que se dirigen hacia la industria 4.0 y la 5.0.

Actualmente, los proyectos tradicionales son insuficientes. Por esta razón, la investigación y el desarrollo en este campo se vuelven esenciales para afrontar los desafíos presentes y futuros que enfrentan tanto las empresas como los profesionales de Tecnologías de la Información (TI).

La adopción de enfoques ágiles se convierte en una prioridad para mantenerse competitivo y ágil en un mundo empresarial que demanda innovación constante. Estas metodologías permiten a las organizaciones ser más flexibles y receptivas a las demandas cambiantes del mercado, acelerando el ciclo de desarrollo y proporcionando un marco para la mejora continua.

Metodología

La metodología utilizada en la elaboración de esta investigación se basa en un método de investigación basado en una revisión sistemática de literatura, basándose en el enfoque propuesto por Barbara Kitchenham y colaboradores. Aunque esta propuesta fue originalmente diseñada para áreas como ciencias humanas y medicina, han surgido varias adaptaciones que han permitido llegar a un enfoque claro a la ingeniera buscando una estrategia, la que se desglosa en tres etapas principales: 1) planificación, 2) ejecución y 3) redacción del informe.

Para llevar a cabo la elaboración de este capítulo, se empleó un método de investigación basado en una revisión bibliográfica y un estudio comparativo entre la aplicación de metodologías ágiles en la industria 4.0 en Colombia y México.

La investigación se fundamenta en una metodología que incorpora una revisión sistemática de literatura, apoyándose en el enfoque propuesto por Barbara Kitchenham y colaboradores (Khan *et al.*, 2012; Kitchenham & Charters, 2007; Ramachandran, 2012). Aunque este enfoque fue diseñado originalmente para áreas como las ciencias humanas y la Medicina, adaptaciones subsiguientes permiten su aplicación en el ámbito de la ingeniería (Carrizo *et al.*, 2018). Dicha estrategia se desglosa en tres etapas esenciales: la planificación, la ejecución y la redacción del informe.

Para la elaboración del presente capítulo, se adoptó una revisión bibliográfica detallada y un estudio comparativo, centrando la atención en la aplicación de metodologías ágiles en la industria 4.0, específicamente en Colombia y México. Se llevó a cabo una búsqueda minuciosa en bases de datos académicas, revistas científicas y publicaciones especializadas en ingeniería de sistemas y metodologías ágiles. De los documentos identificados, se seleccionaron aquellos que proporcionaban una perspectiva actualizada de las metodologías ágiles en el contexto de la industria 4.0 colombiana.

Posteriormente, se extrajo información relevante sobre las metodologías más adoptadas, sus características y su relevancia en la industria.

En paralelo, se realizó una exploración en México con el propósito de comprender cómo se implementan y aplican estas metodologías en su industria 4.0. Se seleccionaron empresas líderes en el sector que adoptan metodologías ágiles. Durante estas exploraciones, se llevaron a cabo entrevistas con especialistas y se observaron prácticas ágiles, con el fin de entender su aplicabilidad en el contexto mexicano.

Con toda la información recopilada, se procedió a un análisis comparativo, centrando el interés en identificar similitudes y diferencias, así como ventajas y desafíos en la aplicación de metodologías ágiles en la industria 4.0, contrastando las experiencias de Colombia y México.

Resultados

En comparación con métodos tradicionales para gestión de proyectos versus metodologías agiles, tienen un impacto positivo en diferentes escenarios que van desde la administración de proyectos hasta la entrega del producto.

Los siguientes aspectos son los que se pueden considerar parte del resultado:

- Aceleración de proyectos.
- Adaptación y flexibilidad.
- Calidad en producto.
- Sinergia en equipos colaborativos.
- Crecimiento e innovación.
- Administración de recursos.
- Importancia al cliente: generación de entrega de valor.

La industria 4.0 es un concepto que se caracteriza por ser un innovador modelo industrial para la organización y la autogestión de sistemas de producción completamente automatizados. Este enfoque involucra un proceso de aprendizaje autónomo e interactivo, con las nuevas tecnologías digitales e internet como elementos centrales, según lo indican Rodríguez Salamanca y Vargas Rozo (2020).

Continuando con este enfoque, las empresas son cada día más conscientes de que el mercado está tomando un enfoque diferente en los últimos años. La transformación digital de las organizaciones se ha convertido en algo necesario e imprescindible. El mundo está cambiando a un ritmo acelerado, pues hablamos de la transformación digital 4.0, también conocida como la Cuarta Revolución Industrial. Los cambios son cada vez más radicales, menos previsibles e inciden directamente en el día a día de las organizaciones y profesionales. La experiencia demuestra que planificar proyectos empresariales con plazos de seis meses o más está quedando obsoleto. En el contexto de la transformación digital 4.0, donde los cambios son cada vez más radicales y menos previsibles, resulta evidente que los proyectos de larga duración ya no son efectivos. Es en este escenario donde el *agile management*, según Patricia (2020), adquiere un papel protagónico.

Nuevamente, Rodríguez Salamanca y Vargas Rozo (2020) consideran el caso de una empresa pyme en Bogotá que demanda modelos de pensamiento más acordes con la realidad y las tendencias; por lo tanto, la ideología ágil se basa en la mentalidad del estratega, convirtiéndose en una competencia o habilidad que permite innovar, maximizar el desarrollo de proyectos y diseñar estrategias que generen valor para los clientes y la organización. Resulta esencial considerar ciertos criterios para alinear la mentalidad con los principios de negocios ágiles y la industria 4.0.

De acuerdo con Boehm (1979) en su libro *Software Engineering as It Is*, la inclinación del sector se dirige hacia el desarrollo en un menor tiempo y a una vida más corta de los productos finales. En este contexto, la entrega de valor del producto en plazos muy cortos para llegar al mercado marca la diferencia.

Aplicación de metodología ágil en la fabricación industrial como parte de la industria 4.0

En la actualidad, numerosas empresas y sectores industriales se encuentran en un proceso de transformación digital. En la industria manufacturera, este proceso es complejo y afecta a casi todos los niveles de producción. En algunos casos, es un paso necesario para reducir los costos de producción; para otros, es una oportunidad para reconsiderar los procesos de negocio y construir una producción digital completa con la implementación de los conceptos de industria 4.0.

La transición hacia la industria 4.0 se basa en la recopilación, almacenamiento, procesamiento y análisis de datos, para identificar oportunidades de impacto en la producción. Un elemento crucial es el planteamiento de la organización de las actividades empresariales, que debe integrar enfoques de gestión adaptables y la capacidad de acceder a información sobre el progreso de la producción. Esto impulsará la mejora de los procedimientos comerciales actuales.

Esta transición se basa principalmente en los principios de recopilación, almacenamiento y procesamiento de datos, seguido del análisis y la posibilidad de impacto en la producción. Un elemento crucial radica en el planteamiento de la organización de las actividades empresariales; la integración de enfoques de gestión adaptables y la capacidad de acceder a información sobre el progreso de la producción impulsarán la mejora de los procedimientos comerciales actuales.

Las prácticas ágiles han surgido en la industria de TI como respuesta a los constantes cambios en productos y requisitos, así como a la excesiva planificación. Sin embargo, la aplicación de metodologías ágiles ya no se limita únicamente al campo de la tecnología de la información; en la actualidad, se utilizan estos métodos de planificación en otros sectores industriales.

Para que se consideren metodologías de desarrollo ágiles, deben respaldar los valores y principios establecidos en el Manifiesto Ágil. La principal ventaja del enfoque ágil radica en la velocidad de cambio y adaptación que tiene el proceso. Esta capacidad de adaptación no siempre tiene que estar relacionada con la productividad; puede estar dirigida a la optimización de procesos internos. En consecuencia, permite mejorar la eficiencia mediante cambios organizativos y, al mismo tiempo, evaluar la eficacia de la implementación de la automatización o la adopción de nuevas tecnologías, como pueden ser IA, realidad virtual (VR), seguridad informática, entre otras.

¿Cuáles son las ventajas de las metodologías ágiles?

En primer lugar, es crucial comprender que las metodologías ágiles se originan con el propósito de priorizar la interacción en los procesos y facilitar la colaboración con el cliente, especialmente cuando surgen necesidades de modificación durante la fase de desarrollo del proyecto.

1. **Entregas rápidas y continuas.**

   Uno de los aspectos más destacados de las metodologías ágiles radica en su capacidad para realizar entregas rápidas y continuas de *software* plenamente funcional.

2. **Conceptualizan el proyecto en componentes cohesivos.**

   La capacidad de dividir el proyecto en componentes que pueden adaptarse de manera flexible, complementarse entre sí y resolverse en cortos plazos simplifica la realización de modificaciones, ya que solo afectan a la parte correspondiente y se ejecutan en poco tiempo.

3. **Fomentan la colaboración en el trabajo.**

   Además de los beneficios en cuanto a los procesos, también promueven la colaboración multidisciplinaria, la autonomía y la transparencia. Al trabajar con fluidez y flexibilidad hacia un objetivo común, los equipos logran resultados más efectivos.

4. **Predicen resultados y minimizan riesgos.**

   Mediante revisiones continuas y la adaptación a los cambios, se obtiene una visión predictiva del resultado, lo que, por exclusión, minimiza los riesgos de cometer errores irreparables.

5. **El cliente se integra como un miembro más del equipo.**

   Gracias a la interacción continua con los clientes y al trabajo multidisciplinario, se logran resultados verdaderamente satisfactorios, lo que convierte al cliente en un miembro más del equipo. Esto da lugar a proyectos eficaces y, en consecuencia, proporciona una experiencia gratificante para los clientes

Ruta para la implementación de metodologías ágiles en industrias que evolucionarán a 4.0

De acuerdo con la velocidad de evolución de las industrias, muchas organizaciones tienden a unirse al proceso de avance a industrias 4.0. Para llegar a esto, de manera inicial es recomendable adoptar un modelo de metodología ágil, lo cual simplificará significativamente los proyectos que contemplen para su avance a este tipo de industrias.

Figura 33. Metodologías tradicionales vs. metodologías ágiles

Nota. Tomado de Excelence Management.

Definición de objetivos

Es importante que las compañías u organizaciones tengan claridad en el objetivo que se quiere al implementar metodologías ágiles. De esta manera, el alcance, implementación y desarrollo de la metodología serán más eficientes. Cuando hablamos de la claridad en los objetivos, nos referimos a cómo las empresas se apoyan en metodologías eficientes y, como resultado, logran una adecuada integración para llevar a cabo una implementación exitosa. Por esta razón, destacamos los beneficios que una organización puede obtener al llevar a cabo este proceso de manera regular:

- Capacidad de respuesta a cambios dinámicos.
- Entrega continua y ágil de soluciones tecnológicas.
- Trabajo conjunto entre el cliente y el equipo en todo el ciclo de vida.
- Simplicidad y eliminación de trabajo innecesario.
- Atención continua a la excelencia técnica y al buen diseño.

Tal como lo resalta el informe de Bioul, Escobar, Álvarez, Nardin y Aparicio (2010), el uso de metodologías ágiles ha experimentado un crecimiento notable en el mercado, lo cual ha generado un aumento en los debates y discusiones en torno a su aplicación. Se plantean cuestiones cruciales, tales como: ¿cuál es el nivel de adopción de las metodologías ágiles?, ¿cuáles de ellas son las más prevalentes en la práctica?, ¿es posible implementarlas

de manera integral? Estos interrogantes arrojan un enfoque significativo sobre la percepción de si las metodologías ágiles pueden llegar a constituir la base de los procesos de desarrollo en el futuro.

Evaluación de metodología tradicional

Es necesario evaluar el proceso de administración de proyectos que actualmente se tenga, es indispensable para dar el paso a metodologías ágiles. Esto permitirá conocer el estado actual de los proyectos que se tengan en curso para fortalecerlos o, si lo que se busca es implementar en nuevos proyectos, para realizar comparaciones sobre efectividad.

a. Verificación

Realizar un estudio previo a los proyectos a los que se les puede aplicar el uso de las metodologías ágiles. Los expertos en implementación de este tipo de herramientas recomiendan ejecutarlo inicialmente en proyectos que no generen alto impacto y paulatinamente agregar los demás conforme al avance.

b. Recolección y presentación de datos

Investigar sobre metodologías y conceptos que se hayan usado con anterioridad, verificar resultados y así determinar qué solución será la más idónea para la compañía u organización.

c. Elección de metodología ágil

De acuerdo con los previos análisis, se puede conocer el estado de los proyectos, personal y empresa, para poder elegir de manera más efectiva el modelo que más sea acorde con lo que se requiere. Para una elección más objetiva, es necesario conocer los conceptos básicos de cada metodología ágil actualmente vigente:

- **Scrum**

  Es un marco de trabajo de procesos que ha sido usado para gestionar el desarrollo de productos complejos desde principios de los años 90. Según Schwaber y Sutherland (2013), Scrum no es un proceso o una técnica para construir productos; en lugar de eso, es un marco de trabajo dentro del cual se pueden emplear varias

técnicas y procesos. Scrum muestra la eficacia relativa de las prácticas de gestión de producto y las prácticas de desarrollo, de modo que podamos mejorar.

El marco de trabajo Scrum consiste en los equipos Scrum, roles, eventos, artefactos y reglas asociadas. Cada componente dentro del marco de trabajo sirve a un propósito específico y es esencial para el éxito de Scrum y para su uso. Las reglas de Scrum relacionan los eventos, roles y artefactos, gobernando las relaciones e interacciones entre ellos. Las reglas de Scrum se describen en el presente documento.

- **Kanban**

En pocas palabras, se trata de una herramienta para gestionar el trabajo. Es un método que se utiliza para administrar una variedad de servicios profesionales, que a menudo se denominan trabajo de conocimiento. La aplicación del método Kanban implica adoptar un enfoque holístico para pensar en tus servicios con el objetivo de mejorarlos desde la perspectiva de tus clientes. Con el método Kanban, puedes visualizar el trabajo de conocimiento que, de otra manera, permanecería invisible y cómo avanza a través de un flujo de trabajo. Esto te ayuda a operar tu negocio de manera efectiva, lo que incluye comprender y gestionar los riesgos al entregar tus servicios a los clientes.

"Kanban es ampliamente conocido por su uso en equipos para aliviar la sobrecarga y recuperar el control sobre el trabajo realizado. Aunque esto generalmente proporciona beneficios rápidos, la aplicación del método Kanban a una mayor escala, como en una línea de servicio que abarca el trabajo de varios equipos o diferentes partes de organizaciones, ofrece oportunidades aún más significativas" (Kanban University, 2021).

- **XP**

Extreme Programing es un enfoque de la ingeniería de *software* formulado por Kent Beck; se considera el más destacado de los procesos ágiles de desarrollo de *software*. Al igual que estos, la programación extrema se diferencia de los métodos tradicionales

principalmente en que presenta más énfasis en la adaptabilidad que en la previsibilidad (Universidad Unión Bolivariana, 2019).

Elección de software

SCRUM

- **Jira Software (Atlassian):** Jira es una solución versátil con funcionalidades diseñadas para Scrum, como la capacidad de crear tableros Kanban, planificar *sprints*, realizar un seguimiento de historias de usuario y estimaciones ágiles. También ofrece informes personalizables para el monitoreo del progreso del proyecto.

- **Scrumwise:** se enfoca exclusivamente en Scrum, proporcionando características específicas como la gestión de la pila de productos, el seguimiento de la velocidad del equipo y la facilitación de las reuniones de *sprint*.

KANBAN

- **Kanban Tool:** esta herramienta está diseñada especialmente para la metodología Kanban, ofreciendo tableros Kanban visuales, límites para el trabajo en progreso, análisis de flujo y herramientas para optimizar el proceso.

LEANKIT

- ✓ **LeanKit:** corresponde a otra alternativa popular para la gestión de proyectos Kanban. Proporciona una vista visual del flujo de trabajo y facilita la optimización de procesos.

EXTREME PROGRAMMING (XP)

- **VersionOne:** este recurso tecnológico versátil admite la metodología XP. Ofrece características como la planificación de entregas, seguimiento de la velocidad y gestión de tareas, elementos fundamentales para las prácticas de XP, como la programación en pareja y la programación extrema.

- **Targetprocess:** este recurso ágil se adapta a diversas metodologías, incluyendo XP. Ofrece características para planificación, seguimiento y colaboración del equipo.

Capacitación y contratación

El implementador deberá analizar el estado actual de los colaboradores y administradores de los proyectos, con el objetivo de conocer el nivel académico a nivel de uso de herramientas de metodologías ágiles. Al realizar este proceso, se puede determinar si se requiere contratación de personal con estas habilidades o, en su defecto, llevar capacitación y certificaciones a los colaboradores.

Implementación

En este punto ya se han tomado las elecciones más importantes para implementar la metodología ágil seleccionada. No obstante, el proceso no ha finalizado y entra en la etapa más crucial. Implementar puede ser de las tareas más complejas, sin embargo, con la planeación y estructuración correctas no se deberían generar impactos a la producción.

Durante la implementación, algunos especialistas coinciden en ejecutar las siguientes tareas:

- Planificar y hacer seguimiento.
- Eliminar actividades que no aporten valor.
- Monitorear el progreso y medir la calidad.
- Promover el trabajo en equipo.

Evaluación

Se convierte en la etapa final de la implementación, ya que en esta parte se conoce el resultado de los proyectos tras implementar metodologías ágiles. Con estos datos, se pueden tomar decisiones sobre futuras migraciones y mejoras dentro del proceso.

Comparación

Tras finalizar la implementación y permitir la vida del ciclo del proyecto, se pueden comparar los resultados frente a proyectos que hayan manejado metodologías tradicionales. De esta manera, se podrá medir el éxito y

mostrar los buenos resultados al hacer uso de metodologías ágiles dentro de una compañía.

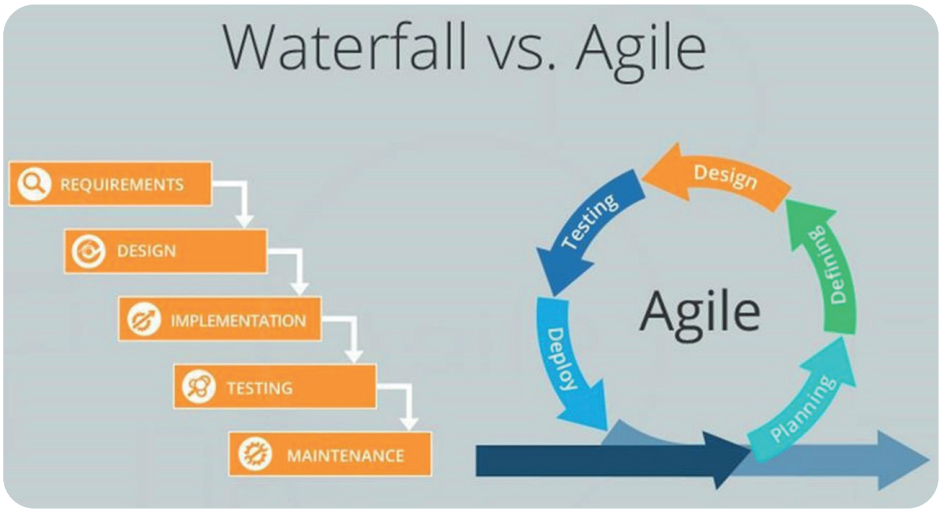
Metodologías ágiles: un análisis de los desafíos organizacionales para su implementación

Las organizaciones de desarrollo de *software* valoran la gestión de proyectos como competencia estratégica clave, que requiere procesos estandarizados, pero también adaptabilidad en un entorno empresarial cambiante para mantener la competitividad, reducir costos, tiempos y mejorar la calidad. Del mismo modo, como lo mencionan Flores Cerna, Sanhueza Salazar, Valdés González y Reyes Bozo (2022), la adopción de metodologías ágiles, presentadas en el Manifiesto Ágil de 2001, se ha convertido en una práctica común. Estas metodologías enfatizan la colaboración, la adaptabilidad, la entrega incremental y la satisfacción del cliente, alejándose de los enfoques tradicionales que requieren definir todas las necesidades del cliente de antemano.

Dada la creciente adopción de metodologías ágiles en pequeñas y medianas empresas tecnológicas que siguen enfoques tradicionales, estas enfrentan desafíos en su implementación debido a la falta de comprensión de los principios ágiles, lo que a menudo conduce a tasas de fracaso en la adopción. El objetivo es identificar y abordar las brechas específicas en estas empresas al adoptar prácticas ágiles, lo que es fundamental para garantizar una implementación exitosa. Por lo tanto, en la figura 34, podemos observar que la metodología ágil es flexible y adaptable, permitiendo cambios, mientras que la cascada es rígida y lineal.

La agilidad en el proceso de creación de productos es un factor esencial que ha sido objeto de estudio a lo largo de varios años. Este concepto ha evolucionado con el tiempo debido a diversas fuerzas que influyen en la forma en que se desarrollan los productos. Estas fuerzas incluyen la competencia internacional, la fragmentación de los mercados debido a la demanda diversificada, la creciente sofisticación y exigencia de los clientes, el entorno económico en constante cambio y la transformación digital. Este último aspecto implica avances tecnológicos que impulsan una respuesta ágil, mejoras en la calidad y una mayor responsabilidad social por parte de las empresas en el mercado. En resumen, la agilidad se convierte en una ventaja al permitir a las organizaciones adaptarse rápidamente a los cambios y aprovecharlos (Quitian Monroy, 2022).

Figura 34. Metodología en cascada vs. ágil



Nota. Metodología en cascada vs. ágil. Basado en https://universidadeuropea.com/blog/agile-vs-waterfall/

Impacto del uso de mitologías ágiles dentro de la industria 4.0

En Colombia, la adopción de metodologías ágiles ha ido en constante crecimiento. Las empresas han reconocido la necesidad de ser más flexibles y adaptables para enfrentar los desafíos cambiantes del mercado. En muchas organizaciones, se han implementado métodos ágiles como Scrum y Kanban, lo que ha permitido una mayor colaboración y una entrega incremental de productos y servicios. La comunidad de profesionales ágiles en Colombia ha crecido significativamente, con la realización de conferencias y eventos que promueven el intercambio de conocimientos y buenas prácticas en el ámbito de las metodologías ágiles.

En contraste, México ha experimentado un rápido aumento en la adopción de metodologías ágiles en empresas de diversos sectores. Esto se debe en parte a la influencia de empresas tecnológicas de renombre que han establecido operaciones en el país. En este país, se ha visto un aumento en la capacitación y certificación de profesionales en metodologías ágiles, lo que ha impulsado la implementación de estos enfoques en la gestión de proyectos. Además, las empresas mexicanas han demostrado una fuerte orientación hacia la mejora continua, lo que ha llevado a la incorporación de elementos de metodologías ágiles en sus procesos.

Tabla 18. Uso de metodologías ágiles en industrias 4.0

AÑO	SCRUM	KANBAN	EXTREME PROGRAMMING (XP)	LEAN STARTUP	OTROS
2010	10 %	5 %	2 %	1 %	82 %
2020	50 %	20 %	10 %	5 %	15 %
2023	70 %	25 %	10 %	5 %	0 %

Nota. Porcentaje de uso de las diferentes metodologías respecto al tiempo, del año 2010 al 2023, de acuerdo con estimaciones sobre las tendencias más recientes.

Como se puede observar en la tabla, el uso de las metodologías ágiles ha ido en aumento de manera significativa. En el 2023, Scrum es el modelo más utilizado, seguido respectivamente por Kanban (Next U, 2023).

Lo anterior se debe a diferentes factores, como, por ejemplo, la entrega de proyectos con mayor velocidad, capacidad de adaptación al cambio y mejoras constantes sobre el producto final.

Teniendo en cuenta las tendencias sobre el desarrollo de *software* y la gestión de proyectos, las metodologías ágiles permiten un trabajo dinámico entre los equipos, lo que permite colaboración y mejores resultados. En este orden de ideas, los principios que las metodologías ágiles tienen son:

- Centrado en clientes.
- Colaboración.
- Adaptación.

Discusión

En el marco de la inmersión internacional en la Ciudad de México el mes de septiembre de 2023, se resaltan las visitas empresariales a Audi y al centro de datos KIO con presencia en 5 países. Un factor común en estas visitas es, sin duda, el avance tecnológico aplicado en cada uno de los procesos de fabricación y de tratamiento de los datos respectivamente. Estas empresas aplican en gran medida la automatización posicionándose como modelo de implementación de las industrias 4.0.

En Colombia, si bien muchas empresas han comenzado a adoptar tecnologías avanzadas, el nivel de adopción de la industria 4.0 puede variar considerablemente y no todas las empresas han alcanzado el mismo grado de automatización. Sin embargo, Colombia se destaca por su enfoque en metodologías ágiles para asegurar el éxito de sus proyectos tecnológicos.

En conclusión, mientras que empresas en México se destacan por los avances tecnológicos y la automatización, es importante reconocer que Colombia, como país, cada día se esfuerza más por la adopción de la industria 4.0 y el uso de las metodologías ágiles y está a la vanguardia de grandes empresas en América Latina como Audi y el centro de datos KIO. Colombia ha demostrado su capacidad para adaptarse a las demandas tecnológicas cambiantes y asegurar el éxito de sus proyectos a través de la implementación de metodologías ágiles, lo que la posiciona como un referente en la región. La combinación de avances tecnológicos y enfoque en la eficiencia operativa está llevando a Colombia a un futuro prometedor en términos de innovación y desarrollo empresarial.

Conclusiones y recomendaciones

Las metodologías ágiles promueven la colaboración y la comunicación asertiva entre equipos multidisciplinarios, lo que es esencial en la industria 4.0, donde la integración de tecnologías y la interconexión de sistemas son fundamentales. A pesar de los beneficios, la adopción de metodologías ágiles en México y Colombia puede enfrentar resistencia cultural en algunas organizaciones, puesto que requiere un cambio de mentalidad y una mayor autonomía de los equipos.

Colombia requiere de nuevos enfoques de reforma estructural que vayan más allá de las reformas de mercado. Una política industrial 4.0 debe ser guiada por misión, es decir, que no solo corrija faltas del mercado, sino que maximice el impacto de transformación económica mediante la creación de nuevas actividades tecnológicas.

La adopción de tecnologías de la industria 4.0 conlleva desafíos significativos, pero aporta grandes beneficios, como el empoderamiento de los líderes organizacionales, la utilización efectiva de la información para impulsar la productividad, la optimización de procesos y la permanencia en el mercado, la reducción de errores en la producción, la capacidad de

prever problemas antes de que ocurran, la toma de decisiones respaldada por evidencia y, por supuesto, un incremento en la satisfacción del cliente a través de productos y servicios personalizados. Para lograr esto, se recomienda que las organizaciones promuevan una cultura ágil que se inicie con una transformación cultural; esto implica fomentar la colaboración, descentralizar la toma de decisiones y cultivar una mentalidad de aprendizaje constante.

Referencias

Ayala, L. F. (2019). *Diseño de un modelo de perfilamiento para el rol crítico en metodologías ágiles (Scrum), para la gestión de proyectos tecnológicos en la empresa financiera Lujumasti*. Obtenido de tesis de especialización, Universidad EAN: http://hdl.handle.net/10882/9579.

Bernal, C. (2016). *Metodología de la investigación*. Colombia: Pearson.

Bioul, G., Escobar, F., Álvarez, M., Nardin, A. & Aparicio, E. R. (2010). *Metodologías ágiles, análisis de su implementación y nuevas propuestas*. Argentina: Universidad CAECE.

Boehm (1979). *Software Engineering: Barry W. Boehm's Lifetime Contributions to Software Development, Management, and Research*. Fourth Edition.

Caballero López & J. E. (septiembre de 2009). http://scielo.isciii.es. Obtenido de http://scielo.isciii.es/pdf/mesetra/v55n216/revision.pdf

Calderón, A. & Dámaris, S. (2007). *Metodologías ágiles*. Obtenido de https://d1wqtxts1xzle7.cloudfront.net/53222887/Metodologias_Agileslibre.pdf?1495404476=&response-contentdisposition=inline%3B+filename%3DUniversidad_Nacional_de_Trujillo.pdf&Expires=1698024672&Signature=a6sTZm0HRocXBhoN~Mvmi0x-2Gj7nvl-yf6tpy0gyPXhpA2tC6w

Cámara Valencia (2023). *20 herramientas Agile para la gestión de tu proyecto*. Obtenido de https://ticnegocios.camaravalencia.com/servicios/tendenci as/herramientas-agile-paragestion-proyectos/

Flores-Cerna, F., Salazar, S., González, V. & Reyes Bozo, L. (2022). "Metodologías ágiles: un análisis de los desafíos organizacionales para su implementación". Obtenido de *Revista Científica*: https://doi.org/10.14483/23448350.18332

Jacquez-Hernández, M. V. & Torres, V. G. (2018). *Modelos de evaluación de la madurez y preparación hacia la industria 4.0: una revisión de literatura*. Obtenido de https://www.redalyc.org/journal/2150/215057003004/215057003004.pdf

John, A. (2016). *Normas básicas de higiene del entorno en la atención sanitaria*. India: Organización Mundial de la Salud. Obtenido de http://apps.who.int/iris/bitstream/handle/10665/246209/9789243547237spa.pdf;jsessionid=98A5D7C69806F077F4D7F5B862DCA0BB?sequence=1

Kanban University (2021). *The Official Guide to the Kanban Method*.

Obtenido de https://resources.kanban.university/wp-content/uploads/2021/0 6/The-OfficialKanban-Guide_A4.pdf

KIO Networks (s. f.). *¿Qué es el almacenamiento de datos?* Obtenido de https://www.kionetworks.com/blog/data-center/que-es-el-almacenamiento-de-datos

Kitchenham, B. & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering*. Obtenido de https://www.cs.auckland.ac.nz/~norsaremah/2007%20Guidelines%20for%20performing%2 0SLR%20in%20SE%20v2.3.pdf

Mejía-Neira, Á. J.-O. (2019). "Influencia de la ingeniería de software en los procesos de automatización industrial". *Información Tecnológica*, 30(5), 221-230. Obtenido de https://dx.doi.org/10.4067/S0718-07642019000500221

Next U (19 de julio de 2023). Linkedin. Obtenido de https://es.linkedin.com/pulse/metodolog%C3%ADas-%C3%A1giles-4-ejemplos-de-las-m%C3%A1s-utilizadas

Oñate, A. F. (s. f.). *Metodologías ágiles Scrum, XP, SLeSS, Scrumban, HME, Mobile-D y MASAN empleadas en la industria de dispositivos móviles: un contraste en favor de la industria del desarrollo móvil*. Obtenido de https://repositorio.upeu.edu.pe/bitstream/handle/20.500.12840/3906/Abel_Trabajo_Bachille rato_2020.pdf?sequence=1&isAllowed=y

Patricia (s. f.). *Agile Management, una de las claves de la transformación digital 4.0*. Obtenido de Euncet Business School: https://blog.euncet.com/agilemanagement-transformacion-digital/

Quitian Monroy, J. S. (2022). *Caracterización y comparación de metodologías ágiles y tradicionales de desarrollo de producto*. Obtenido de Ciencia e Ingeniería Neogranadina: https://doi.org/10.18359/rcin.5168

Ramachandran, M. (2012). *Guidelines Based Software Engineering for Developing Software Components*. Obtenido de https://www.scirp.org/journal/paperinformation.aspx?paperid=16668

Ramírez, C. E. & Gómez-Gil, P. (2012). *Análisis empírico sobre la adopción de las metodologías ágiles en los equipos de desarrollo de software en empresas mexicanas*. Obtenido de https://ccc.inaoep.mx/~pgomez/publications/congress/ERCANI12.pdf

Rodríguez Salamanca, C. H. (2020). *Diseño de un plan estratégico para la aplicación de metodologías ágiles e industria 4.0 en las empresas pymes*

de Bogotá: caso empresa Bienaventuranza IPS. Obtenido de http://repository.udistrital.edu.co/handle/11349/27978

Schwaber, K. & Sutherland, J. (julio de 2013). *La guía definitiva de Scrum: las reglas del juego*. Obtenido de https://scrumguides.org/docs/scrumguide/v1/Scrum-Guide-ES.pdf

Turner, C. & Oyekan, J. (2023). *Manufacturing in the Age of Human-Centric and Sustainable Industry 5.0: Application to Holonic, Flexible, Reconfigurable and Smart Manufacturing Systems*.

Turner, C. & Oyekan, J. (2023). "Manufacturing in the Age of Human-Centric and Sustainable Industry 5.0: Application to Holonic, Flexible, Reconfigurable and Smart Manufacturing Systems". *Sustainability 2023*, 15, 10169. Obtenido de https://doi.org/10.3390/su151310169.

Universidad Unión Bolivariana (2019). *Programación extrema (XP)*. Obtenido de https://ingenieriadesoftware.mex.tl/images/18149/PROGRAMACI%C3%93N%20EXTRE MA.pdf

Conclusiones

En este libro, reflejo del compromiso y la pasión investigativa de los estudiantes de la Facultad de Ingeniería y Tecnología de la Fundación Universitaria Compensar, se despliega un detallado análisis comparativo que abarca esferas clave de la ciberseguridad, las tecnologías de la información y los avances de la industria 4.0, enfocándose especialmente en las dinámicas y particularidades que caracterizan a Colombia y México. Este viaje de descubrimiento y colaboración en México ha permitido a los estudiantes no solo aplicar sus conocimientos académicos, sino también expandirlos, enfrentándose a realidades y desafíos contemporáneos en un contexto global.

El cuerpo del libro, articulado a través de sus capítulos, refleja una intersección única entre la teoría académica y la aplicación práctica, evidenciando la profunda influencia de una educación multidisciplinar. Aunque los cursos tomados por los estudiantes no estaban específicamente diseñados para abordar la era digital e industrial 4.0, la diversidad de materias, como introducción a las telecomunicaciones, manejo de la información, redes de datos, *switching and routing*, instalación de antenas y telefonía, sistemas digitales y administración de redes, ha provisto una base robusta para un entendimiento integral. Este trasfondo académico ha sido fundamental en permitirles analizar con profundidad temas como la ciberseguridad, la computación en la nube y las tecnologías IoT, mostrando cómo una educación variada y completa puede preparar a los futuros profesionales para enfrentar y entender las complejidades de un mundo tecnológicamente avanzado y en constante cambio.

La estructura de cada capítulo del libro, meticulosamente diseñada, facilita una comprensión clara y ordenada de los temas tratados. Cada capítulo se divide en tres secciones esenciales:

- **Contexto:** esta sección es crucial para establecer una base sólida de conocimiento, situando al lector en el panorama actual de las tecnologías y la ciberseguridad en Colombia y México. Al proporcionar una visión general detallada, esta parte del capítulo prepara el terreno para un análisis más profundo, ofreciendo los antecedentes necesarios para una comprensión integral de los temas discutidos.

- **Marco metodológico:** aquí, los autores detallan la metodología empleada en su investigación, una parte vital del estudio que añade rigor y profundidad. Las visitas e investigaciones en empresas y entidades de ambos países enriquecen el análisis con experiencias prácticas y observaciones directas, permitiendo una evaluación más precisa y cercana a la realidad de las metodologías ágiles en la industria 4.0 y de los proveedores de *cloud computing*.

- **Análisis comparativo:** la sección final de cada capítulo es donde se concreta el análisis comparativo entre Colombia y México. Esta parte es fundamental para identificar y destacar tanto las similitudes como las diferencias en tecnologías, enfoques metodológicos y normativas relacionadas con la ciberseguridad y la protección de la privacidad. Este análisis comparativo no solo subraya las tendencias y riesgos en la región, sino que también resalta la importancia de las legislaciones y políticas en la implementación de estrategias efectivas de ciberseguridad.

Los hallazgos presentados en el libro son un reflejo de esta estructura rigurosa y detallada. Se han identificado tendencias y estrategias clave en áreas como la implementación de la computación en la nube, la selección de tecnologías IoT y las prácticas de *ethical hacking*, aplicadas en sectores industriales y educativos. La comprensión de los procesos operativos IoT y las metodologías ágiles en la industria 4.0 aportan una visión relevante sobre cómo las variaciones regionales y las diferencias en los enfoques metodológicos influyen en la adopción y gestión tecnológica en ambos países.

En conclusión, este libro no solo evidencia la relevancia de una formación académica amplia y diversificada en la comprensión de temas complejos como la ciberseguridad y las tecnologías emergentes, sino que también resalta la importancia de una estructura metodológica sólida y bien definida para la realización de investigaciones comparativas efectivas. Los hallazgos aquí descritos ofrecen una perspectiva valiosa sobre la evolución de la tecnología, la ciberseguridad y la industria 4.0 en el contexto latinoamericano, poniendo especial énfasis en los casos de Colombia y México, y destacando la contribución significativa de los estudiantes en el avance de estos campos críticos en un mundo interconectado y tecnológicamente avanzado.