6.ª Edición

ESCOM
ESCUELA DE COMUNICACIONES MILITARES

REVISTA CIENTÍFICA

TECNOESCOM

ESCUELA DE COMUNICACIONES MILITARES

Agosto 2024
Anual - Volumen 6. No.1
Facatativá, Cundinamarca
CÓDIGO ISSN 2711-0761

REVISTA CIENTÍFICA

TECNOESCOM

ESCUELA DE COMUNICACIONES MILITARES

CIENCIA, DOMINIO
Y VIGILANCIA

Dirección: Carrera 5 Calle 15 - 00 Barrio Dos Caminos
Teléfono: 313 300 3799

EDITORIAL

La Escuela de Comunicaciones Militares del Ejército Nacional de Colombia, a través del Centro de Investigación, en esta nueva oportunidad, presenta a la comunidad académica el Sexto Volumen de la Revista de Divulgación Científica TECNOESCOM, conformada por la producción intelectual de estudiantes y docentes que, con un criterio sustentado en la práctica científica, así como en lo teórico-disciplinar y metodológico, exponen los productos de su desarrollo investigativo y tecnológico, los cuales aportan conocimiento y actualización en temas emergentes como lo son: ciberseguridad, Inteligencia Artificial, Industria 5.0 y los surgentes desafíos del IoT, entre otros contenidos de interés general.

Desde esta perspectiva, la ESCOM demuestra en la presente publicación, la importancia de la investigación como función sustantiva de la formación académica, para la construcción científica del conocimiento en el área de Ingeniería, Electrónica y Telecomunicaciones; es así que los temas que convocan este volumen, evidencian sin duda alguna, la madurez investigativa que ha alcanzado la institución, a nivel de pregrados, posgrados y semilleros de investigación, los cuales gracias al compromiso y determinación de sus destacados docentes, al igual que el acompañamiento y asesoría del personal que labora en el Centro de Investigación, han elevado la calidad de los productos de la ciencia cognitiva y la investigación empírica de la Escuela.

Invito a quienes tengan la oportunidad de leer este ejemplar, a auscultar cada concepto, propuesta y abordaje sistemático de su información, en aras de aportar a la solución de problemáticas similares a las aquí contenidas, en el entorno laboral o familiar que las requiera; igualmente, aquellos lectores que deseen aportar su experticia y conocimiento en el área mencionada, tienen las puertas de nuestra Álma Máter abiertas, con el propósito de ser publicados sus productos de investigación y, aportar de esta forma, a la construcción de ciencia en beneficio de la sociedad y del país.

Director de la Escuela de Comunicaciones
Teniente Coronel Edward Enrique Arévalo Ríos

"El genio se hace con un 1% de talento, y un 99% de trabajo"
(Albert Einstein)

CONTENIDO

ARTÍCULOS DE INVESTIGACIÓN

ARTÍCULOS DE REVISIÓN BIBLIOGRÁFICA

ARTÍCULOS DE LOS SEMILLEROS DE INVESTIGACIÓN

PRESENTACIÓN
REVISTA CIENTÍFICA TECNOESCOM

La revista Científica **TECNOESCOM**, es una publicación editada por la Escuela de Comunicaicones Militares del Ejército Nacional de Colombia, Centro de Investigación (CEINV), que presenta las investigaciones en diferentes áreas de impacto realizadas bajo la dirección académica de la institución, con el proposito de divulgar y contribuir a la extensión del pensamiento científico e investigativo.

PRESENTATION
SCIENTIFIC JOURNAL TECNOESCOM

The scientific journal **TECNOESCOM**, is a publication edited by the School of Military Communicationes of the National Army of Colombia, Research Center (CEINV, which presents research in different areas of impact conducted under the academic direction of the institution, in order to disseminate and contribute to the extension of research and scientific study.

1. Artículos
de Investigación

DESARROLLO DE UN SISTEMA DE MONITOREO ELECTRÓNICO DE SEÑALES FISIOLÓGICAS PARA CANINOS.

Sergio Steid Bohórquez Mahecha
Docente
steidbohorquez@gmail.com

Juan Camilo Cristiano Cortés
Auxiliar de ingeniería
juanca7744@gmail.com

RESUMEN- ***El presente artículo trata el diseño de un sistema de monitoreo no invasivo para la detección señales fisiológicas de caninos guías de las Fuerza Militares. El objetivo fue desarrollar un dispositivo electrónico integrado en un chaleco para obtener mediciones en tiempo real de temperatura, frecuencia cardíaca y respiratoria del canino. Se muestra la factibilidad técnica y utilidad potencial de este sistema para monitoreo no invasivo del estado de salud y bienestar del canino guía. Los aportes de la investigación, incluyen el diseño electrónico, el desarrollo de la aplicación móvil y la integración de tecnologías para medición y transmisión de señales fisiológicas.***

Palabras clave: Señales fisiológicas, sensor, sistema de monitoreo.

Abstract— The present article deals with the design of a non-invasive monitoring system for the detection of physiological signals of guide dogs for the Military Forces. The objective was to develop an electronic device integrated into a vest to obtain real-time measurements of the dog's temperature, heart rate, and respiratory rate. The technical feasibility and potential utility of this system for non-invasive monitoring of the health and well-being of the guide dog are demonstrated. The research contributions include the electronic design, the development of the mobile application, and the integration of technologies for measuring and transmitting physiological signals.

Keywords- monitoring system, Physiological signals, sensor.

I. INTRODUCCIÓN

Colombia se sitúa como el segundo país más afectado por la criminalidad a nivel mundial, únicamente superado por Congo [1], convirtiéndose así en una nación acosada por el crimen en todo el continente americano, junto con México, Honduras, Paraguay y Panamá, según el índice desarrollado por la Iniciativa Global Contra la Delincuencia Organizada Transnacional (GI-TOC por sus siglas en inglés), el cual evalúa los niveles de criminalidad y resiliencia en los 193 estados miembros de la ONU. Además, se destaca como uno de los países donde existen mayores centros de trata de personas y donde se exporta más cocaína al mundo, lo que está íntimamente ligado con las causas de la violencia y el conflicto interno en el país.

El conflicto interno del país ha situado a las Unidades Militares en la línea de frente de su misión constitucional, ya que son un objetivo prioritario para los terroristas y se ven continuamente afectadas por las actividades delictivas de organizaciones armadas fuera de la ley[2], mismas que emplean sustancias explosivas contra los miembros de la Fuerza Pública y sus unidades. Esto no solo pone en peligro la vida de personal militar y civil, sino que también causa daños a la infraestructura y debilita los procesos de seguridad institucional.

Por lo anteriormente expuesto, con el ánimo de mitigar la entrada de artefactos explosivos improvisados AEI o de sustancias ilegales y optimizar la seguridad a las Unidades Militares, se emplean técnicas de inspección vehicular y de personas mediante un binomio canino (militar - canino), quienes deben realizar el

proceso de revisión de paquetes, maletas y vehículos que ingresan, en arduas jornadas laborales, pero normalmente no se tiene en cuenta el estado físico y/o el estado de aptitud del canino en el momento de realizar su trabajo de búsqueda, dependiendo solo de la experiencia del Militar, quien puede decidir si el canino está fatigado o puede continuar su labor.

No obstante, por necesidad del servicio, los caninos se exponen a condiciones de fatiga y de golpes por oleadas de calor durante la jornada diaria, ya que prima la labor como es el caso de los caninos de la Policía Metropolitana de Barranquilla donde "Las jornadas de labores de estos caninos duran entre seis y ocho horas; sin embargo, el clima podría acortar el tiempo de trabajo. "Si hace mucho calor, el canino pierde rendimiento y debemos parar de trabajar" [3]. En las Fuerzas militares, son procesos normales de trabajo del canino, de 20 a 30 minutos en el área de operaciones o de 2 horas en ambientes urbanos en condiciones controladas.

En este orden de ideas, el único método para llevar a cabo la detección de explosivos u objetos no permitidos dentro de los Cantones o Bases de las Fuerzas Militares, es el empleo de caninos, quienes cumplen una función prioritaria en la Base, debido a que no se cuenta con otra alternativa para este trabajo. Por tal razón, se requiere un prototipo que mida las señales fisiológicas del canino en tiempo real para evitar enfermedades o problemas de salud, con circuitos electrónicos [4] y redes, permitiendo al guardia encargado monitorear todos los comportamientos de salud y el sobrefatigamiento del mismo.

Del anterior planteamiento del problema se considera como objetivo: "desarrollar un sistema de monitoreo electrónico para determinar las señales fisiológicas de temperatura, frecuencia cardiaca y respiratoria en caninos empleados durante la inspección de sustancias controladas, en las Fuerzas Militares".

El artículo propone el desarrollo de un sistema de monitoreo de frecuencia cardíaca, respiratoria y temperatura, en caninos de las Fuerzas Militares, de forma no invasiva (sin penetrar o realizar alguna incisión en la piel del animal), mediante el empleo de un chaleco con instrumentación electrónica, el cual será alimentado con baterías recargables de LIPO, con el fin de brindar una autonomía de más de 2 horas estimadas y obtener el monitoreo de las condiciones fisiológicas de las razas de caninos empleados específicamente en el Cantón Militar de Comunicaciones, para realizar labores de inspección de sustancias controladas (narcóticos, divisas, explosivos y búsqueda y rescate).

El presente artículo tiene como propósito beneficiar la labor de los caninos pertenecientes al Fuerzas Militares de Colombia, que detectan sustancias controladas. Entre ellos se encuentran las siguientes razas: pastor alemán, labrador retriever, doberman, rottweiller y el pastor belga mallinois, las cuales se destacan por ser fuertes, ágiles, vigilantes, obedientes, equilibradas, leales con su amo, con gran habilidad para la detección de narcóticos; igualmente, por su rapidez en competencias de exigencia física. Estos caninos poseen un pelaje moderado y un tamaño promedio, entre 60 y 62 cm, mismos que son seleccionados desde temprana edad, debido a que desde pequeños se pueden entrenar con más facilidad, haciendo posible que su desempeño sea mejor durante sus labores o entrenamientos [5][4].

Con base en lo anteriormente planteado, la utilidad práctica de la presente investigación consiste en que el prototipo será destinado a los caninos de las Fuerzas Militares, el cual se adaptará a una de las razas mencionadas anteriormente; igualmente, se podrá determinar su grado de temperatura, frecuencia cardíaca, así como respiratoria, y efectuar la toma decisiones en tiempo real, con respecto a la continuidad de las labores o descansos intermedios del canino, según éste lo requiera. Es decir, con el canino designado

para llevar a cabo las pruebas, se obtendrán los resultados del prototipo en funcionamiento.

De lo anteriormente mencionado se planteó la siguiente hipótesis "la implementación de un sistema de monitorización electrónico destinado a la captura en tiempo real de las señales fisiológicas, como la temperatura corporal, la frecuencia cardíaca y la frecuencia respiratoria, en los caninos que participan en la inspección de sustancias controladas en las Fuerzas Militares, facilitará la capacidad de supervisión más precisa de su estado físico. Esto, a su vez, contribuirá a la optimización de su bienestar y rendimiento, lo que resultará en una mejora sustancial de la eficacia en las tareas de detección de sustancias controladas".

II. ESTADO DEL ARTE

El ámbito de la investigación médica veterinaria, se enmarca en un contexto nacional e internacional el cual se encuentra en constante evolución. A nivel nacional, se ha evidenciado un interés creciente por abordar aspectos específicos de la salud de los caninos, mientras que, a nivel global, se han desarrollado tecnologías avanzadas para el monitoreo remoto de señales fisiológicas en animales.

A. Antecedentes nacionales

El proyecto presentado por el Centro de Investigación del Cantón Militar de comunicaciones "Dispositivo de electrónico no invasivo para medir de forma remota señales fisiológicas en caninos" [5], consistió en un prototipo de chaleco para un canino, en donde se midió la frecuencia cardíaca, frecuencia respiratoria y de temperatura. Se desarrolló con el fin de hacer un monitoreo de los caninos de la guardia del batallón, cuya labor es olfatear sustancias controladas, debido a que esta actividad causa fatiga y en algunos casos, no les es posible descansar debidamente, ocasionando enfermedades a mediano o largo plazo. Las variables fueron observadas a través de una interfaz gráfica en LabVIEW, lo que permitió visualizar un cambio brusco en las señales fisiológicas.

Con lo anteriormente planteado, en el Centro de Investigación se empleó tecnología que en su momento fue eficiente, pero ésta constantemente avanza y permite nuevas posibilidades como lo es crear un nuevo prototipo capaz de comunicar una aplicación móvil con los datos obtenidos del sensor para monitorear en tiempo real las señales fisiológicas del canino y visualizar de la manera más óptima posible, usando una IU.

En el proyecto de grado "Diseño de un prototipo que mida la frecuencia cardíaca en tiempo real de un equino entre los 2 y 6 años de edad durante su entrenamiento"[6], realizado en la Escuela de Comunicaciones Militares, consistió en medir la frecuencia cardíaca de un equino usando el sensor MAX30102 que esgrime comunicación I2C. En esta investigación, se hizo uso de módulos de comunicación NRF24L01 para enviar los datos entregados por el sensor, en el cual se utilizó la ESP32 como tarjeta de desarrollo, ya que trabaja a 32 bits de procesamiento.

En el anterior proyecto de grado se midió la frecuencia cardíaca de los equinos utilizando el sensor MAX30102, el cual se comunica mediante el protocolo I2C. Durante esta investigación, se emplearon módulos de comunicación NRF24L01 para transmitir los datos recopilados por el sensor. Para gestionar y procesar estos datos, se optó por utilizar la ESP32 debido a su capacidad de procesamiento. De esta manera, se estableció una conexión eficiente entre el sensor y la transmisión de datos, permitiendo monitorizar en tiempo real las señales fisiológicas de los equinos durante sus sesiones de entrenamiento.

En el proyecto titulado "Prototipo de sistema de monitoreo de variables fisiológicas en mascotas basado en internet de las cosas"[7], se midieron las variables fisiológicas de temperatura y el ritmo cardíaco. Para esto se planteó el uso

de sensores conectados a Internet, servicios en la nube para el almacenamiento y procesamiento de la información y una aplicación móvil para el despliegue de la información al usuario. El desarrollo del proyecto fue soportado metodológicamente en las etapas del ciclo de vida del software: análisis, diseño, desarrollo, implementación y pruebas. Como resultados principales, se destacó el collar inteligente, el cual permite medir variables fisiológicas, y la aplicación para visualizar la información. El sensor de temperatura escogido, es una opción viable para este prototipo.

En el proyecto de [7] se usaron variables para la medición de frecuencia cardíaca en caninos; se empleó una banda como soporte para integrar los sensores y colocarla al animal. Se utilizó un chaleco que permitió situar los sensores en puntos específicos para la toma de datos. Esta mejora posibilitó una mayor precisión en la obtención de las señales fisiológicas. Además, la incorporación de sensores de mayor exactitud contribuyó a que el prototipo fuera considerablemente más eficiente en la captura de los datos y en su posterior envío a una aplicación móvil.

En el proyecto "Desarrollo de un prototipo de monitoreo no invasivo de signos vitales y localización para caninos" [8], se desarrolló un arnés para un canino en donde se mide la frecuencia cardíaca, temperatura y frecuencia respiratoria. Los datos se transportaron por bluetooth y se visualizaron en una interfaz de usuario para smartphone. Igualmente, contó con un sistema GPS para la localización exacta y en tiempo real del canino.

B. Antecedentes internacionales

Los autores [9] de "Behavioral and Environmental Analytics from Potential Guide Dogs with IoT Sensor Data Informed by Expert Insight" presentaron un diseño deprototipo que mide señales vitales de caninos con implementación de DEEP LEARNING programada en Python, la cual funciona para medir y localizar los caninos guías, utilizando tecnologías como módulos wifi y GPS, al igual que sensores como humedad, temperatura y acelerómetro.

En consecuencia, se empleó un prototipo basado en DEEP LEARNING programado en Python y con diferentes módulos, para la implementación de los caninos del Cantón de las Comunicaciones en Facatativá. Se empleó una red bluetooth que permite el envío de datos a una aplicación móvil que se visualizó en una IU en tiempo real.

En el artículo "Non-contact vital signs monitoring of dog and cat using a uwb radar"[10], se presenta un modelo no invasivo para medir los signos vitales cuando las mascotas están en reposo; se aplicó un radar de banda ultra ancha para que se lograra la capacidad de detección y comodidad de comprobación. Fue desarrollado para los animales de la compañía de los autores, así que priorizaron la salud de sus mascotas cuyos resultados experimentales mostraron que el radar podía medir eficazmente la respiración de estas, en donde la tasa de presión fue superior al 95%.

Con el método de los radares se logró un porcentaje mayor al 95%, permitiendo tener una exactitud alta a diferencia de otros prototipos. Con base en la propuesta para el chaleco canino se implementó algunas de las configuraciones que se usaron en el prototipo para mejorar la precisión del chaleco, además se incluyen diferentes métodos de comunicación para la transmisión de los datos y con la implementación de una UI, se permite monitorear las señales fisiológicas de una manera sencilla.

El artículo"Wearable wireless biophotonic and biopotential sensors for canine health monitoring" [11], presentó un prototipo para monitorear continuamente las constantes vitales de los caninos con el objetivo de identificar las correlaciones fisiológicas con el estrés y la excitación fuera de los entornos de los laboratorios. El prototipo incluyó fotopletismograma y un electrocardiograma

para monitorear de forma remota y continua los signos del canino; se propusieron electrodos puntiagudos para que el pelaje del mismo no afectara con las lecturas de datos; así, los sensores se interconectaron con un sistema en chip y se empleó comunicación Bluetooth para transferir los datos a un smartphone u ordenador cercano para su almacenamiento y análisis.

La implementación de la comunicación Bluetooth en los sensores, posibilitó la transmisión constante de datos entre diversos dispositivos. En este contexto, el chaleco canino actuó como complemento en la transmisión de estos datos. A través de una programación adecuada y el desarrollo de una aplicación móvil, se logró un control más claro y preciso de las señales fisiológicas del animal.

Los autores [12] de la investigación "Internet of Things in Animal Healthcare (IoTAH): Review of Recent Advancements in Architecture, Sensing Technologies and Real-Time Monitoring" presentaron un prototipo para analizar los signos vitales y localización de los animales de granja con tecnología IoT, para detectar enfermedades a tiempo y así poder tratarlas. Estos fueron almacenados en la base diseñada en la nube privada, en donde las personas autorizadas pudiesen mirar los registros, cuyos resultados fueron prometedores y económicamente viables para garantizar la atención sanitaria al animal.

Mediante el uso de una base de datos, se logró mejorar la atención sanitaria, al permitir un almacenamiento ilimitado de información. Esto posibilitó el seguimiento de la condición en distintos periodos, aunque también aumentó los costos y el desarrollo debido a la creación de la misma. Por otro lado, el chaleco canino posibilitó la visualización en tiempo real de las señales fisiológicas de manera más clara a través de una interfaz de usuario (UI), todo ello con viabilidad en términos de costos de desarrollo.

Por otra parte, con el "Prototipo de monitor de signos vitales en pacientes veterinarios de especie canina utilizando IoT" [13], para el monitoreo de signos vitales de animales en cuidados intensivos, se aprovechó la tecnología de Internet de las Cosas para permitir su seguimiento remoto con solo acceso a Internet. Durante la fase de pruebas, se identificó que no se podía capturar la frecuencia cardíaca mediante sensores ópticos debido a las variaciones en la piel de los pacientes, comparadas con las de los humanos. No obstante, los resultados obtenidos del prototipo tras pruebas y comparaciones demostraron ser satisfactorios.

La incorporación del Internet de las Cosas (IoT) en la supervisión de los signos vitales permitió la introducción de nueva tecnología en el mercado. Sin embargo, al tratarse de un desarrollo en progreso, pueden existir distintas fallas que aún no han sido resueltas. Por otro lado, al utilizar un chaleco canino equipado con sensores de alta precisión y exactitud, se logró minimizar la cantidad de errores al ofrecer una solución confiable en el tiempo. Además, esta propuesta es rentable para diversas aplicaciones, como la medición de señales fisiológicas en los caninos.

En la tesis "Sistema electrónico de monitoreo de mascotas para la gestión de clínicas veterinarias utilizando VOIP e IOT" [14], de la Universidad Técnica de Ambato, se implementó un sistema electrónico de monitoreo en mascotas para la gestión de clínicas veterinarias utilizando VOIP e IOT y así llevar un adecuado manejo y control de los datos obtenidos a partir de un dispositivo medidor de signos vitales, a partir de una aplicación desarrollada en React Native. El sistema electrónico de monitoreo estuvo conformado por 3 niveles, como son: adquisición y transmisión de signos vitales, gestión de información y monitoreo y alojamiento en la nube.

En la mencionada tesis, se menciona el desarrollo de un chaleco electrónico que transmitía los datos de oximetría y frecuencia cardiaca del

canino captados por el sensor MAX30100 y los enviaba por comunicación bluetooth a un dispositivo smartphone que contaba con la aplicación desarrollada en React Native y desde ahí se enviaban los datos a la nube en donde la información podía ser visualizada por el veterinario.

III. PROCEDIMIENTO Ó METODOLOGÍA

En este apartado se detalla la metodología que se aplicó durante el desarrollo de la investigación. Los temas que se abordaron incluyeron: el paradigma, el tipo de investigación, el enfoque, el diseño de la investigación, el método aplicado, las técnicas de recolección de datos, los instrumentos de recolección, las técnicas de procesamiento de datos y el procedimiento de la investigación.

A. Paradigma

En el paradigma empírico – analítico, según [15]: "se concibe la realidad, hombre y sociedad como cosas que se pueden conocer objetivamente. Se estudia de manera fragmentada pues se observa y experimenta con un objeto a la vez. Dentro de la teoría de los intereses cognitivos de Habermas se corresponde con lo que éste denomina interés técnico. El conocimiento que se genera es instrumental por cuanto el fundamento del proceso es el control".

La presente investigación tiene un enfoque principalmente cuantitativo con algunos elementos cualitativos. Se trata de un estudio empírico - analítico para recolectar y analizar datos cuantitativos. Sin embargo, también incorpora técnicas cualitativas para complementar la comprensión del fenómeno estudiado.

B. Enfoque

El enfoque de investigación mixto según [16]:" implica una recolección, análisis e interpretación de datos cualitativos y cuantitativos que el investigador haya considerado necesarios para su estudio. Este método representa un proceso sistemático, empírico y crítico de la investigación, en donde la visión objetiva de la investigación cuantitativa y la visión subjetiva de la investigación cualitativa pueden fusionarse para dar respuesta a problemas humanos". (p. 19)

El enfoque es mixto, debido a que se necesita determinar las señales fisiológicas del canino y sus funciones en el Cantón Militar de Comunicaciones. Se asesorará con expertos (enfoque cualitativo) y es necesario tomar los datos arrojados por los sensores (enfoque cuantitativo).

C. Tipo

La investigación exploratoria [17]: "Es una búsqueda de información, con el propósito de formular problemas e hipótesis para una investigación más profunda de carácter explicativo. Estos estudios exploratorios tienen como objetivo "la formulación de un problema para posibilitar una investigación más precisa o el desarrollo de una hipótesis" (p. 134).

Esta investigación, se inició con un enfoque exploratorio para recabar información crucial sobre las señales fisiológicas de los caninos. Este primer paso fue esencial para adquirir un conocimiento preliminar y fundamental del tema en cuestión, formular preguntas específicas y elaborar la hipótesis que se indagará en etapas posteriores de la investigación.

Tipo de investigación tecnológica [18]:

Tiene como finalidad transformar la realidad existente a través de la obtención de un conocimiento práctico en vez de un conjunto de explicaciones teóricas como es el caso del método científico. Si bien es cierto que se apoya en la ciencia, su objeto de estudio o principios exigen que sus elementos metodológicos sean distintos (párr. 2).

El principal objetivo de esta investigación tecnológica es diseñar un prototipo que mida las señales fisiológicas de un canino de forma precisa y eficiente. Para lograr esto, es crucial integrar software y hardware especializados.

D. Método

El método inductivo-deductivo [19]: "Se complementan mutuamente: mediante la inducción se establecen generalizaciones a partir de lo común en varios casos, luego a partir de esa generalización se deducen varias conclusiones lógicas, que mediante la inducción se traducen en generalizaciones enriquecidas, por lo que forman una unidad dialéctica. De esta manera, el empleo del método inductivo-deductivo tiene muchas potencialidades como método de construcción de conocimientos en un primer nivel, relacionado con regularidades externas del objeto de investigación"(p. 12).

El uso del método inductivo-deductivo en esta investigación se basa en su capacidad para adaptarse a la naturaleza mixta del estudio y cumplir con los objetivos específicos establecidos. Este enfoque combina los métodos inductivos y deductivos en una orientación integral, lo que permite abordar los problemas de investigación desde una variedad de puntos de vista y obtener resultados más precisos y completos.

E. Técnicas de recolección de datos

La observación directa experimental [20]:

Debe ser seleccionada cuando queremos cambiar deliberadamente uno o más factores con el fin de identificar sus efectos sobre la(s) variable(s) respuesta. Para ello, es muy importante que tengamos un conocimiento previo sobre el efecto que estos cambios pueden originar en los resultados de la investigación, puesto que nos ayudará a realizar un adecuado planeamiento de la toma de datos (p. 12).

Para verificar la precisión y confiabilidad de los dispositivos al medir señales fisiológicas en caninos, se utilizó un método de observación directa experimental. Se diseñó un experimento en el que se calibraron los sensores y se compararon las mediciones obtenidas con valores reales conocidos.

F. Instrumentos de recolección de datos

La matriz de datos [21] "es una forma de sistematizar la información recogida de la realidad para investigar un problema y tratar de obtener conocimiento científico que intente explicar dicho problema a través del método de investigación científica" (p. 4).

En la investigación, la utilización de una matriz de datos es un método efectivo para organizar y analizar los datos recopilados de los sensores que miden las señales fisiológicas de los caninos. Este método de presentación y organización sistemática de datos, facilita la comparación y el análisis de múltiples variables.

G. Técnicas de procesamiento de datos

Una tabla [17] "Una tabla es la exposición de una serie de datos interrelacionados entre sí. Podríamos decir que es la imagen de los datos. Los datos colocados de arriba abajo constituyen las columnas, las series dispuestas en horizontal forman las filas" (p. 482).

La tabla es herramienta esencial para estructurar y presentar datos de manera precisa y sistemática. Su capacidad para organizar información en una matriz de datos bidimensional compuesta por filas y columnas, lo cual la hace útil.

H. Metodología

Metodología en Prototipo: según [22], "En la industria electrónica el término prototipo se refiere por lo general a un desarrollo tangible que servirá como modelo funcional

factible de réplica. No obstante, el término es amplio y contempla a cualquier forma gráfica o física, desde una simulación, pasando por software embebido, integración de módulos, piezas y componentes electrónicos y mecánicos; hasta un producto tangible funcional, escalable para fabricación" (párr. 1).

Fase 1: Tras un análisis detallado, se definieron los nuevos componentes electrónicos necesarios para medir de forma no invasiva las señales de temperatura, frecuencia cardíaca y frecuencia respiratoria en los caninos.

Fase 2: Se analizaron minuciosamente los requerimientos de los nuevos componentes y se exploraron múltiples opciones de diseño de circuitos. Las simulaciones fueron una herramienta clave para confirmar el correcto funcionamiento de los circuitos propuestos antes de su implementación física.

Fase 3: Las pruebas implicaron la activación simultánea de todas las funciones del prototipo durante una jornada completa de trabajo, que incluyó tareas de inspección y detección. Los resultados fueron satisfactorios, confirmando mediciones precisas y transmisiones confiables de los datos en tiempo real.

IV. ANÁLISIS RESULTADOS

A. Señales fisiológicas en caninos

Se determinó que la temperatura, frecuencia cardíaca y respiratoria son las mejores opciones de señales fisiológicas para medir de forma no invasiva. En la tabla 1 se observan las señales fisiológicas con los rangos.

TABLA I
Señales fisiológicas y rango en caninos

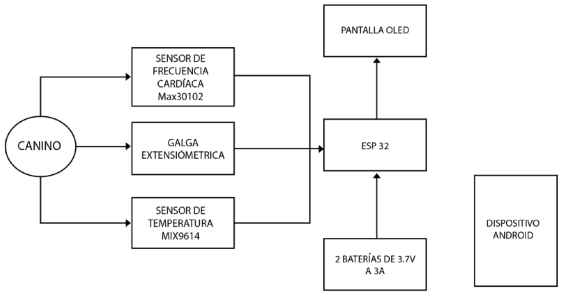
Señal Fisiológica:	Rango:
Temperatura	Adulto de 37.5 a 39 °C y joven de 38 a 39.5 °C
Frecuencia cardiaca	Adulto 60 a 100, Joven 80 a 120 pulsaciones por minuto
Frecuencia respiratoria	10a 30 respiraciones por minuto

B. Implementación

La frecuencia respiratoria, se midió realizando el conteo de las exhalaciones e inhalaciones del canino de manera indirecta, donde se utilizó un sensor de presión tipo resistivo, que se encuentra adherido a un cinturón que está ajustado alrededor del tórax.

La frecuencia cardíaca se determinó utilizando un sensor de pulsímetro, el cual es un dispositivo que integra los emisores de luz; el sensor mide la cantidad de luz reflejada por la piel del canino. La temperatura superficial se midió a través de un sensor de temperatura infrarrojo. Los datos de los sensores fueron recibidos por una tarjeta de desarrollo ESP32. Los datos fueron observados mediante una pantalla OLED. En la figura 1 se visualiza el diagrama de bloque.

Figura 1. Diagrama de bloques



C. Pruebas

Para verificar la frecuencia cardíaca en un canino, se tomó el pulso utilizando los dedos corazón e índice, ejerciendo una suave presión sobre la muñeca. Una vez que se percibe el pulso, se inicia un cronómetro y se cuentan los pulsos durante quince segundos. Posteriormente, se multiplica esta cifra por cuatro para obtener la frecuencia cardíaca en pulsaciones por minuto, como se observa en la figura 2.

Figura 2. *Medición de pulso cardíaco en canino*

Otra ubicación para medir el pulso, es en el muslo inferior, específicamente para palpar el latido de la arteria femoral y se practica el mismo proceso como se mencionó anteriormente, como se observa en la figura 3.

Figura 3. Medición de pulso cardíaco arteria femoral

Para la medición de la frecuencia respiratoria, se inicia un cronómetro con una duración de 1 minuto. Durante este período, se palpa el tórax del canino y se cuenta el número de veces que se expande o contrae la respiración, como se observa en la figura 4.

Figura 4. Medición de frecuencia respiratoria

La medición de la temperatura se realizó mediante un termómetro digital o de mercurio, introducido vía rectal. Este procedimiento fue llevado a cabo por un veterinario con el objetivo de evitar incomodidades y/o estrés para este, dado que podría generar molestias o dolor.

D. Resultados

Los resultados obtenidos en las pruebas iniciales demuestran la efectividad del sistema. Los valores de las constantes vitales se mantuvieron dentro de rangos normales durante los ejercicios de detección. Esto permitió monitorear el estado físico y estrés del canino para prevenirsituaciones de riesgo. Se realizaron pruebas a 12 ejemplares: caninos del Ejército, Fuerza Aeroespacial y policía colombiana. En las Tablas 2, 3 y 4, se presentan los datos obtenidos del último.

ejemplar que fue sometido a las pruebas Estas pruebas se realizaron en colaboración con el encargado de los caninos y un médico veterinario, quienes contribuyeron a la medición precisa de la temperatura, frecuencia cardiaca y respiratoria durante todo el proceso.

TABLA II
Análisis sensor de temperatura ejemplar 12

Sensor de temperatura superficial(C°)	Temperatura superficial tomada por el veterinario(C°)	Diferencia de temperatura Superficial(C°)	Error porcentual %
38,2	38,2	0	0,00%
38,2	38,2	0	0,00%
38,2	38,2	0	0,00%
39,6	39,6	0	0,00%
39,6	39,6	0	0,00%
39,6	39,6	0	0,00%
39	39	0	0,00%
39	39	0	0,00%
39	39	0	0,00%
		Total, error porcentual	0,00%

TABLA III
Análisis sensor de frecuencia cardíaca ejemplar 12

Sensor de Frecuencia Cardíaca Latidos/ Minuto)	Frecuencia Cardíaca tomada por el veterinario (Latidos/Minuto)	Diferencia de Frecuencia Cardiaca (Latidos/Minuto)	Error porcentual %
85	85	0	0,00%
85	85	0	0,00%
85	85	0	0,00%
111	111	0	0,00%
111	111	0	0,00%
111	111	0	0,00%
90	90	0	0,00%
90	90	0	0,00%
90	90	0	0,00%
		Total, error porcentual	0,00%

TABLA IV
Análisis sensor de frecuencia respiratoria ejemplar 12

Sensor de Frecuencia Respiratoria (Respiraciones/ Minuto)	Frecuencia Respiratoria del canino (Respiraciones/ Minuto)	Diferencia de Frecuencia Respiratoria (Respiraciones/ Minuto)	Error porcentual %
12	12	0	0,00%
12	12	0	0,00%
12	12	0	0,00%
17	17	0	0,00%
17	17	0	0,00%
17	17	0	0,00%
12	12	0	0,00%
12	12	0	0,00%
12	12	0	0,00%
		Total, error porcentual	0,00%

V. CONCLUSIONES

La medición no invasiva de las variables fisiológicas temperatura, frecuencia cardíaca y frecuencia respiratoria en caninos, puede ayudar a monitorizar la fatiga y prevenir el sobre entrenamiento en perros deportivos y de trabajo. El análisis del proyecto ha permitido identificar un conjunto de variables fisiológicas relevantes que cumplen con el criterio de evaluación no invasiva planteado en el objetivo inicial.

Se realizaron pruebas en tiempo real del prototipo activando todas sus funciones simultáneamente, con el fin de evaluar su funcionamiento, conectividad y autonomía en condiciones reales de trabajo. Las pruebas continuaron hasta el agotamiento total de la batería, estimando así su capacidad operativa continua durante la jornada de trabajo canina. Adicionalmente, se hicieron pruebas autorizadas en la Guardia del Cantón, donde los caninos ejecutaron sus tareas de detección habituales con el prototipo. Esto verificó su efectividad en el contexto real de operación.

VI. REFERENCIAS

[1] COLPRENSA, "Colombia es el segundo país más afectado por el crimen en el mundo," Colombia, p. 1, Oct. 19, 2021

[2] J. A. González Prieto, "La necesidad de aplicar la administración de riesgos en las unidades militares del Ejército Nacional."

[3] El Heraldo, "Caninos antinarcóticos: el poderoso olfato contra el crimen," 2021. https://www.elheraldo.co/judicial/caninos-antinarcoticos-el-poderoso-olfato-contra-el-crimen-819526.

[4] Y. W. Ávila, W. A. C. Carrero, and M. A. W. Hurtado, "Dispositivo de electrónico no invasivo para medir de forma remota señales fisiológicas en caninos," Rev. Colomb. Tecnol. Av., vol. 3, no. Especial, pp. 49–56, 2020.

[5] Fuerza Aeroespacial Colombiana, "Perseo, un superhéroe de cuatro patas," 2020. https://www.fac.mil.co/es/noticias/perseo-un-superheroe-de-cuatro-patas.

[6] E. R. Garcia Azuero and A. T. Canastero Quijano, "Diseño de un prototipo que mida la frecuencia cardiaca en tiempo real de un equino entre los 2 y 6 años de edad durante su entrenamiento," Escuela de Comunicaciones Militares, 2021.

[7] C. A. Rosales Marraui, "Prototipo de sistema de monitoreo de variables fisiológicas en mascotas basado en internet de las cosas," 2020.

[8] V. M. Mina Lucumi and A. Restrepo Moreno, "Desarrollo de un Prototipo de Monitoreo No Invasivo de Signos Vitales y Localización para Caninos," Institución Universitaria Antonio José Camacho, 2019.

[9] Z. Cleghern et al., "Behavioral and Environmental Analytics from Potential Guide Dogs with IoT Sensor Data Informed by Expert Insight," ACM Int. Conf. Proceeding Ser., 2020, doi: 10.1145/3446002.3446121.

[10] P. Wang et al., "Non-contact vital signs monitoring of dog and cat using a UWB radar," Animals, vol. 10, no. 2, 2020, doi: 10.3390/ani10020205.

[11] R. Brugarolas et al., "Wearable wireless biophotonic and biopotential sensors for canine health monitoring," Proc. IEEE Sensors, vol. 2014-Decem, no. December, pp. 2203–2206, 2014, doi: 10.1109/ICSENS.2014.6985477.

[12] G. S. Karthick, M. Sridhar, and P. B. Pankajavalli, "Internet of Things in Animal Healthcare (IoTAH): Review of Recent Advancements in Architecture, Sensing Technologies and Real-Time Monitoring," SN Comput. Sci., vol. 1, no. 5, pp. 1–16, 2020, doi: 10.1007/s42979-020-00310-z.

[13] L. F. Tull Soriano, "Prototipo de monitor de signos vitales en pacientes veterinarios de especie canina utilizando IOT." Universidad Nacional Pedro Henriquez Ureña, 2021.

[14] Y. C. León Troya, "Sistema electrónico de monitoreo de mascotas para la gestión de clínicas veterinarias utilizando VOIP E IOT," Universidad Técnica de Ambato, 2022.

[15] E. Pasek de Pinto and Y. Matos de Rojas, "Cinco paradigmas para abordar lo real," Universidad Privada Dr. Rafael Belloso Chacín Venezuela, 2006.

[16] A. Otero-ortega, "Enfoques de investigación," no. August, 2018.

[17] H. Ñaupas Paitán, M. R. Valdivia Dueñas, J. J. Palacios Vilela, and H. E. Delgado Romero, Metodología de la investigación Cuantitativa - Cualitativa y Redacción de la Tesis, 5th ed. 2018.

[18] EUROINNOVA, "¿Qué es la investigación tecnológica?" https://www.euroinnova.co/blog/que-es-la-investigacion-tecnologica.

[19] A. Rodríguez Jiménez and A. O. Pérez Jacinto, "Métodos científicos de indagación y de construcción del conocimiento," Revista Escuela de Administración de Negocios, Bogóta, Colombia, pp. 1–26, 2017.

[20] D. Llopis Castelló, "Metodología de la investigación," [Online]. Available: https://poliformat.upv.es/access/content/user/24389381/Contenido abierto al público/Metodología de la investigación/3.2 Metodología experimental.pdf.

[21] Dennis Chávez de Paz, "Conceptos y técnicas de recolección de datos en la investigación jurídico social," vol. 148, pp. 148–162, 2008, [Online]. Available: https://perso.unifr.ch/derechopenal/assets/files/articulos/a_20080521_56.pdf.

[22] D. Mayorquin Bejanaro, "Tipos y Fases de Prototipado Electrónico," Linkedin, 2023. https://es.linkedin.com/pulse/tipos-y-fases-de-prototipado-electrónico-mayorquin-bejarano.

DISEÑO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN FUNDAMENTADAS EN LA NORMA ISO 27001 PARA LOS ACTIVOS DE LA INFORMACIÓN EN EL ÁREA ADMINISTRATIVA DE LA EMPRESA GLOBAL DINAMIC VENTURES.

Ing. Gonzalo Rubiano Blanco
Analista de soporte técnico
grgonzaloru@gmail.com

Esp. Cindy Lorena Hernández Ruiz
Docente ESCOM
lorenhruiz@hotmail.com

Resumen: ***Este proyecto de investigación expone el diseño de políticas de seguridad de la información fundamentadas en la norma ISO 27001 para los activos de la información en el área administrativa de la empresa GLOBAL DINAMIC VENTURES, la cual busca proteger el activo más importante de su organización por medio de la creación de estrategias, métodos y procedimientos, preservando así la integridad, disponibilidad y confidencialidad de los datos a partir de estándares internacionales para la adopción y ejecución de buenas prácticas de prevención y gestión de la información.***

Palabras clave: Seguridad de la información, ISO 27001, activo de información, políticas, ciberseguridad.

Abstract— This research project exposes the design of information security policies based on the ISO 27001 standard for information assets in the administrative area of the company, which GLOBAL DINAMIC VENTURES and seeks to protect the most important asset of the company through the creation of policies, thus preserving the integrity, availability and confidentiality of data.

Keywords- Information security, ISO 27001, information asset, policies, cybersecurity.

I. INTRODUCCIÓN

En la era moderna, el uso de la tecnología ha experimentado una rápida transformación y adaptación en relación con la forma en que las personas trabajan, comunican, aprenden, interactúan, entre otros. Así lo afirma [1]. En 2022, los ciberdelitos aumentaron a 14.000 casos en comparación con el año 2021. Solo la vigencia 2020, durante la pandemia de COVID-19, se superó este incremento con más de 22.000 casos adicionales con respecto al 2019, representando un aumento del 109% (p.9), lo que sugiere una necesidad de tomar medidas preventivas y correctivas en materia de seguridad de la información para las personas y las empresas.

El presente artículo expone el análisis documental destinado al "Diseño de políticas de seguridad de la información fundamentadas en la norma ISO 27001 para los activos de la información en el área administrativa de la empresa "Global Dinamic Ventures" (Nombre institucional modificado con el fin de proteger y resguardar la privacidad de la organización y su información). El proceso en mención, parte de una norma internacional la cual brinda los cimientos para generar una base sólida en la búsqueda de la protección de la integridad, confidencialidad y disponibilidad de la información de la compañía.

La empresa "Global Dinamic Ventures" en adelante GDV, ha sufrido varios ataques a su infraestructura tecnológica, entre ellos, 2 ataques de Phishing (ver figura 1 y 2) y un ataque directo a la oficina encargada de la nómina, el cual logró comprometer seriamente los intereses y rentabilidad de la organización, dicho ataque fue efectuado externamente, eliminando el registro de toda la nómina debido a un

acceso no autorizado a la plataforma contable.

Figura 1. Ataque phishing perpetrado a GDV.

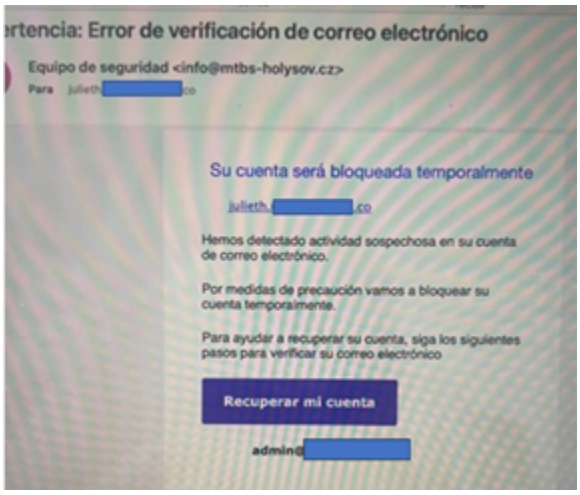
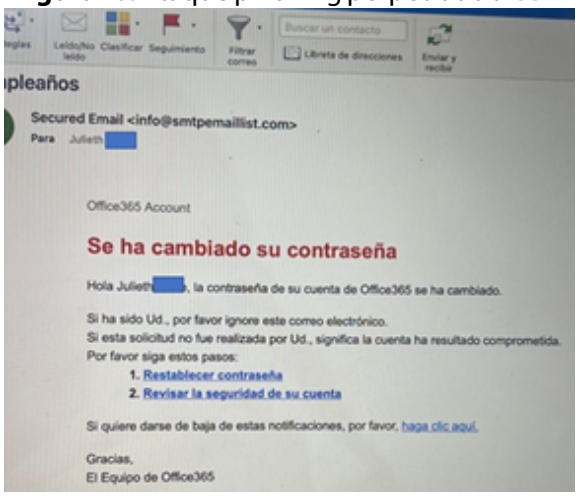


Figura 2. . Ataque phishing perpetrado a GDV



Las vulnerabilidades de seguridad de la información en la actualidad que afectan a la empresa GDV radican en la ausencia de políticas dirigidas a la protección de los activos de información. Como resultado, los equipos de cómputo carecen de directrices para salvaguardar los datos que almacenan, y el personal no ha recibido formación adecuada en lo que respecta a la gestión y protección de la información.

En este estudio, que consiste en la implementación y control de los activos anteriormente descritos, contribuirá a proponer una solución en materia de seguridad de la información a cualquier empresa que quiera proteger sus activos de información. Adoptar y aplicar los estándares propuestos en la norma ISO 27001 en su versión 2022 y comparar su estado inicial con el posterior a esta aplicación, permite la prevención, gestión y mitigación de vulnerabilidades ante las necesidades internas organizacionales. Esto reducirá riesgos, asegurará operaciones continuas y fortalecerá la reputación ante clientes y proveedores en busca de la mejora continua.

II. ESTADO DEL ARTE

Para la presente investigación, se tomaron como referencias tesis nacionales e internacionales sobre la implementación de la norma ISO 27001, acerca de las vulnerabilidades a las que están expuestas las organizaciones en su información y la solución que aportaron los investigadores a las organizaciones para tener diferentes perspectivas en el proceso de mitigación de riesgos en la seguridad de la misma.

A. Antecedentes Nacionales

Según [2] en la tesis de especialización titulada "Diseño y consolidación de un centro de respuesta ante incidentes de seguridad informática en la empresa Cibersecurity de Colombia Ltda." de la Universidad Abierta y a Distancia (UNAD), expone:

> El objetivo es lograr asegurar la información y esto consiste en hacer que los peligros sean conocidos, responsabilizados, dirigidos y minimizados por las organizaciones. Entregando informes detallados de tal forma que sea estructurado, eficiente y ajustable a los cambios. (p. 17-18)

La investigación realizada por el autor destaca por el enfoque y la solución que abordó, al consolidar un centro de respuesta a incidentes de seguridad para la empresa mencionada. Utilizó la norma ISO 27001 como marco, adaptándola a las necesidades de la organización e implementando medidas de seguridad eficaces.

Las organizaciones están inherentemente expuestas a riesgos de ciberseguridad. En efecto, un buen manejo y prevención de estos riesgos son fundamentales para el crecimiento y desarrollo estratégico de la empresa. Así se observa en la tesis de especialización de [3], correspondiente a la Universidad Nacional Abierta y a Distancia (UNAD), en donde se afirma:

> Cualquier organización que maneje tecnologías y sistemas de información, está expuesta a riesgos y ataques cibernéticos que puedan poner en jaque su buen funcionamiento, para proteger los datos se deben poner en práctica reglas, normas, leyes, protocolos, políticas y demás que contribuyan a gestionar la ciberseguridad con el fin de proteger los sistemas e infraestructuras informacionales. (p. 16)

En resumen, todas las empresas, sin importar su modelo de negocio, deben reconocer y abordar los riesgos inherentes a la conectividad en una sociedad globalizada. Esto significa analizar estos riesgos y aplicar medidas preventivas y correctivas para proteger su activo más valioso: la información.

De esta forma, se observa el importante papel que tiene la seguridad de la información en una organización. De acuerdo con [4], la ciberseguridad se ha convertido en una preocupación creciente para las empresas de todos los tamaños y sectores, debido a que la información que generan y almacenan puede ser objeto de ataques por parte de los cibercriminales.

B. Antecedentes Internacionales

El ciclo PHVA es un proceso continuo de mejora de adaptación del SGSI; se utiliza para garantizar que se mantenga la confidencialidad, integridad y disponibilidad de la información en una organización como lo expone [5] en su Proyecto de maestría denominado: : "Propuesta de mejora para la integración de las normas de calidad, seguridad de la información y centros de contacto con el cliente región España y Latam en una multinacional de telecomunicaciones" de la fundación Universidad de América.

•*Planificar:* Se espera que las organizaciones logren consolidar planes, objetivos y proyectos que se sitúen en orientación a la obtención de resultados.

• *Hacer:* Determinar una serie de actividades que logren cumplir a corto, mediano y largo plazo, con los planes y proyectos construidos en la etapa de la planificación.

• *Verificar:* Esta es una etapa fundamental en los procesos desarrollados en la empresa. Allí suelen presentarse las actividades correspondientes a la vigilancia y seguimiento.

• *Actuar:* Una vez verificadas, conscientemente, las dinámicas adelantadas por la organización, es necesario desarrollar e implementar acciones que puedan fortalecer el desempeño de los procesos. (Pág.40,41).

Lo anteriormente mencionado se puede aplicar a cualquier proceso de una organización como los sistemas de gestión de calidad, gestión ambiental o de seguridad de la información. Aunque el sector privado está interesado en el manejo y la confidencialidad de la información que usa, todavía no hay una gran demanda de organizaciones que buscan certificarse en la norma ISO 27001.

En el trabajo de grado de [6] titulado "Implementación ISO 27001 para el control de Delitos Informáticos en la división de Prensa DIRCII PNP, Lima,2022" de la universidad Cesar Vallejo, explica el alto impacto que trae

la implementación de la norma ISO 27001 incidiendo en el control de delitos informativos, en un 81.2%. Según el autor, en general, los resultados sugieren que la implementación de la norma ISO/IEC 27001:2013 puede ser efectiva para prevenir delitos informáticos.

Por este motivo, se considera que seguir las directrices internacionales, además de obtener reconocimiento internacional, proporcionará una mejor guía para mitigar los riesgos asociados a la seguridad de la información, y así garantizar la integridad, disponibilidad y confidencialidad de los datos.

En este sentido [7] en su tesis de maestría titulada "Norma ISO 27001 para el Control de la Seguridad de Información en una Consultoría Privada, Lima 2023" de la universidad Cesar Vallejo, afirma que la institución donde se dirigió el trabajo de grado pudo mejorar la accesibilidad de su información mediante la implementación de controles de seguridad, como encriptación de datos, contraseñas seguras y usuarios con privilegios para obtener información; además, le ha permitido a la gerencia tomar decisiones más rápidamente en caso de emergencias.

III. PROCEDIMIENTO Ó METODOLOGÍA

A. Paradigma de investigación.

El paradigma de investigación proporciona una orientación del proceso investigativo para comprender un fenómeno o problema en particular. [8] lo expresa como:

> Un paradigma de investigación es una concepción del objeto de estudio de una ciencia, de los problemas para estudiar, de la naturaleza de sus métodos y de la forma de explicar, interpretar o comprender los resultados de la investigación realizada. (p.8)

De igual manera existen variedad de paradigmas de acuerdo con el enfoque de investigación, cada uno con una perspectiva diferente que se han ido mejorando y adaptando a través del tiempo. Se pueden observar los siguientes tipos de paradigmas como lo son: empírico analítico, hermenéutico y holístico.

Así, la presente investigación se enmarca en el uso del enfoque empírico analítico debido a que "se basa en la elaboración de hipótesis y posterior confirmación mediante recopilación de datos y aplicación de razonamiento deductivo" [9, s.p.], dado que en esta investigación se plantea una relación causal sobre un fenómeno, entendido como la pertinencia de las políticas de seguridad de la información para salvaguardar los activos de información y su situación actual en la organización.

B. Tipo de investigación

El tipo de investigación que atañe al presente estudio es el descriptivo, el cual busca referir las características de un conjunto de elementos y su funcionamiento dentro de su sistema convencional, el cual consiste en "describir algunas características fundamentales de conjuntos homogéneos de fenómenos, utiliza criterios sistemáticos que permiten establecer la estructura o el comportamiento de los fenómenos en estudio, proporcionando información sistemática y comparable con la de otras fuentes" [10] (p.116). Ya que se busca diagnosticar, describir y determinar de manera imparcial del objeto de estudio.

Con base en lo expuesto anteriormente, es fundamental asegurarse de que la información recopilada sea precisa, veraz y sistemática. Esto requiere utilizar sistemas de recolección de datos adecuados, organizar y analizar dichos datos dentro de un marco teórico apropiado que respalde la investigación.

C. Enfoque de la investigación

Es la forma en que se decide resolver una pregunta de investigación o un problema

de particular según [11] lo define como:

> La naturaleza del estudio, la cual se clasifica como cuantitativa, cualitativa o mixta; y abarca el proceso investigativo en todas sus etapas: desde la definición del tema y el planteamiento del problema de investigación, hasta el desarrollo de la perspectiva teórica, la definición de la estrategia metodológica, y la recolección, análisis e interpretación de los datos. (párr. 1)

En este contexto de investigación se tomará en cuenta el enfoque cuantitativo, el cual [12] representa un conjunto de procesos secuenciales para comprobar ciertas suposiciones, parte de una idea que se delimita y una vez acotada se generan objetivos y preguntas de investigación. Se escogió este enfoque, ya que se recopilarán datos y se hará un análisis de estos para determinar el estado actual de la empresa en cuanto a seguridad de la información.

D. Diseño de la investigación

El diseño de la investigación influye en la calidad y validez de los resultados [13]:

> Como es un modelo estrictamente científico, que forma parte del proyecto de investigación que es un macro-modelo de carácter técnico-científico, administrativo y económico que permite evaluar si el propósito de investigar problemas e hipótesis científicas son pertinentes, justificables, viables y factibles. (p. 348)

El diseño de investigación aplicado es el cuasi -experimental, debido a que "cuando se conoce la existencia de variables extrañas, se sabe cuáles son, pero no es posible controlar su influencia en la variable dependiente" [14] (p.97). Por tanto, se conocen las variables como el factor humano el cual no puede ser controlado independientemente de las intervenciones que se realicen.

E. Método aplicado a la investigación

El método aplicado a la presente investigación, es el analítico deductivo ya que "tiene como objetivo central lograr la descripción o caracterización del evento de estudio dentro de un contexto particular" [15, p.223]. Al aplicar este enfoque se logra una comprensión profunda y detallada del tema de investigación planteado, buscando describir con precisión las propiedades y relaciones involucradas obteniendo información comprensiva y detallada y tener una visión clara del panorama tratado.

F. Universo

De acuerdo a la afirmación de [16], el universo es el conjunto de elementos bien sea (personas, sistemas, sucesos, base de datos, objetos entre otros) globales que pueden ser finitos e infinitos, y que son relevantes para el objeto de estudio. En este sentido, la empresa Global Dinamic Ventures será el universo, que delimitará el alcance de la investigación a llevar a cabo.

G. Población

De igual manera, la población son los "elementos accesibles o unidad de análisis que pertenece al ámbito especial donde se desarrolla el estudio" [17, p.3]. Esto significa que es el grupo total de elementos que poseen las cualidades o atributos de interés. De esta manera, el estudio abordará la participación de 190 personas en nómina, incluyendo personal administrativo y operativo.

H. Muestra

Es un subconjunto representativo de la población que se estudia: "es una porción de la población que se toma para realizar el estudio la cual se considera representativa (de la población)" [18]. Se utiliza para tener conclusiones o inferencias sobre la población en general.

El presente estudio adopta el tipo de muestreo de criterio por conveniencia no probabilístico, ya que "permite

seleccionar aquellos casos de una población limitando la muestra a solo estos casos" [19]. Debido a su fácil disponibilidad y conveniencia para esta investigación, se requiere información de personas en la organización que solo poseen el conocimiento, como: el jefe del área de tecnologías de la información, quien tiene los conocimientos técnicos de los sistemas de información actuales; adicionalmente, la alta gerencia quien dará una priorización estratégica dando liderazgo y compromiso.

I. Técnicas de recolección de datos

Son métodos estructurados para obtener información precisa de diversas fuentes; como lo explica [20]:

Las técnicas de recolección de datos organizan la investigación para obtener el nuevo conocimiento, desarrollando las siguientes actividades:

- Ordenar las etapas de la investigación.
- Elaborar los instrumentos de medición.
- Efectuar un control de los datos.
- Guiar la obtención de conocimientos (p.107).

Para la presente investigación, se aplicará la técnica de recolección de datos mediante el diseño, aplicación y control de una lista de chequeo, elemento que permite recopilar datos de manera organizada y estandarizada facilitando el análisis e interpretación de los resultados.

J. Instrumentos de recolección

De acuerdo con la técnica anteriormente planteada, siendo esta la lista de chequeo, se contempla como instrumento la hoja de control, que fue modificada con base en el trabajo de [21], quien da las pautas concretas para tener un punto de partida sólido para la identificación del estado actual de la compañía; así, ésta se modificará para las necesidades dela organización basada en su última actualización: la norma internacional versión 2022, que contiene 93 ítems evaluables.

IV. ANÁLISIS RESULTADOS

A continuación, se relacionan los objetivos con los que se estructuró el proyecto de investigación, junto con la respectiva solución a cada uno de ellos:

A. Objetivo 1

Determinar el estado actual de la seguridad de la información en los activos del área administrativa que atañen a la empresa Global Dinamic Ventures. Para el cumplimiento de este objetivo, se realizó un check list que fue modificado con base en el trabajo de [22] para identificar el estado inicial de la empresa en materia de seguridad de la información. Todos estos procedimientos fueron ejecutados conforme a la normativa ISO 27001:2022, garantizando así una actualización de enfoque y eficacia, cuyo detallado se presenta a continuación en la figura 3.

Figura 3. Lista de chequeo realizada a la organización GDV.

1. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN PRIMER CHEQUEO				
		SI	NO	OBSERVACIONES
1. Controles Organzacionales				
1,1	¿La organización define, publica y comunica políticas de seguridad de la información a sus empleados y partes externas pertinentes?		X	No se cuenta con política general
1,2	¿Se asignan roles y responsabilidades para el control de la implementación de la seguridad de la información?		X	
1,3	¿La organización establece una separación de deberes para reducir las posibilidades de modificación no autorizada o no intencional?		X	
1,4	¿La organización establece medidas correctivas sobre el uso indebido de los activos de la organización?		X	
1,5	¿La entidad cuenta con un listado de contacto con las autoridades pertinentes a temas relacionados con seguridad informática?. (Especialistas, ColCERT, Centro Cibernético Policial, Comando Conjunto cibernético o empresas privadas competentes en el área)		X	

1,7	¿Existe identificación y recopilación de información sobre incidentes y eventos que atentan contra la Confidencialidad, integridad y disponibilidad de la información que maneja la organización?		X	
1,8	¿Los proyectos y documentos gestionados en la organización, cuentan con procesos de gestión de Seguridad de la Información? (Copias de respaldo, criptografía, limitación de acceso, etc)		X	
1,9	¿La organización cuenta con un inventario actualizado de activos de la compañía, en el que se especifique el propietario o responsable de cada activo?			
1.10	¿La organización cuenta con un conjunto de reglas y procedimientos documentados para el uso aceptable y el manejo de la información y otros activos asociados?		X	
1,11	¿La organización cuenta con un procedimiento documentado para la devolución de activos por parte del personal y otras partes interesadas al cambiar o terminar su empleo, contrato o acuerdo?		X	
1,12	¿Se clasifica la información de acuerdo a requisitos legales, valor de criticidad y susceptibilidad de divulgación, generando un nivel apropiado de protección?		X	
1,13	¿Se etiqueta la información según esquemas de clasificación dado por la organización?		X	
1,14	¿Existen políticas, procedimientos y acuerdos establecidos para la transferencia segura de información en red, incluyendo el uso de claves y cifrado, tanto dentro de la organización como en colaboración con terceros o proveedores?		X	
1,15	¿La organización cuenta con políticas y procedimientos específicos para controlar tanto el acceso físico como lógico a la información y otros activos asociados, de acuerdo con las necesidades del negocio?		X	
1,16	¿Se realiza un proceso formal de registro, asignación y cancelación de usuarios y sus derechos de acceso, para evitar el ingreso no autorizado a sistemas y servicios?		X	
1,17	¿El acceso a la información y a las funciones de los sistemas de las aplicaciones, es restringida de acuerdo con la política de control de acceso?		X	
1,18	¿Se gestionan de manera apropiada los derechos de acceso a la información y otros activos asociados de acuerdo con la política y las reglas de control de acceso específicas de la organización, incluyendo su revisión, modificación y eliminación cuando sea necesario?		X	
1,19	¿La organización gestiona los riesgos de seguridad de la información asociados con el uso de los productos o servicios de los proveedores en la organización?		X	
1,2	¿Se establece y acuerda los requisitos de seguridad de la información pertinentes con cada proveedor en función del tipo de relación?		X	
1,21	¿La organización gestiona los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC en su organización?		X	
1,22	¿La organización tiene un proceso establecido para monitorear, revisar, evaluar y gestionar de manera periódica los cambios en las prácticas de seguridad de la información por parte de los proveedores y en la prestación de servicios relacionados?		X	
1,23	¿La organización establece procesos para la adquisición, uso, gestión y salida de los servicios en la nube según los requisitos de seguridad de la información de la empresa?		X	
1,24	¿La organización ha definido, establecido y comunicado claramente los procesos, roles y responsabilidades relacionados con la gestión de incidentes de seguridad de la información como parte de su planificación y preparación para abordar situaciones de seguridad?		X	
1,25	¿Hay evaluación y clasificación de los eventos e incidentes de seguridad de la información, según su criticidad e impacto dentro de La organización?		X	
1,26	¿Se establecen, documentan, implementan y mantienen procesos, procedimientos y controles para garantizar la continuidad de negocio ante incidentes de seguridad de la información?		X	
1,27	¿Se utiliza el conocimiento adquirido de los incidentes de seguridad de la información como insumo para fortalecer y mejorar continuamente los controles de seguridad de la información en la organización?		X	

1,28	¿Se recolecta y socializa la evidencia de los incidentes de seguridad de la información presentados dentro de la organización?		X	
1,29	¿Se determinan los requisitos para la seguridad de la información y la continuidad de la gestión de la misma, en situaciones adversas; por ejemplo, durante una crisis o desastre?(Seguros, almacenamiento externo en bancos de información)		X	
1,3	¿La organización planifica, implementa y mantiene la preparación de las TIC para cumplir con los objetivos de continuidad del negocio y los requisitos las TIC?		X	
1,31	¿La organización ha identificado, documentado y mantiene actualizados todos los requisitos legales, estatutarios, reglamentarios y contractuales que son relevantes para la seguridad de la información?		X	
1,32	¿Se implementan procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales, relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados?		X	
1,33	La organización implementa medidas de seguridad para proteger los registros contra pérdida, destrucción, falsificación y acceso no autorizado?		X	
1,34	¿La organización establece y documenta procesos para la identificación y cumplimiento de los requisitos relacionados con la preservación de la privacidad y la protección de la Información de Identificación Personal (PII)?		X	
1,35	¿La organización revisa periódicamente su enfoque de seguridad de la información, incluyendo personas, procesos y tecnologías, en intervalos planificados o cuando ocurren cambios significativos?		X	
1,36	¿Se realizan auditorías internas periódicamente, para garantizar la integridad, disponibilidad y confidencialidad de los equipos e información propia de los procesos realizados en la organización?		X	
1,37	¿Se publica y comunica a los empleados y a las partes externas pertinentes, las políticas de seguridad de la información?		X	
2. CONTROLES DE PERSONAS				
2,1	¿La organización verifica antecedentes de todos los candidatos a un empleo de acuerdo con las leyes, reglamentaciones y ética pertinentes?			
2,2	¿Los acuerdos contractuales con empleados y contratistas, establecen sus responsabilidades en cuanto a la seguridad de la información?			
2,3	¿Se brinda a colaboradores, educación y formación, para una toma de conciencia apropiada acerca del SGSI?, así como actualizaciones regulares sobre las políticas y procedimientos de la organización segmentada por cargos?		X	
2,4	¿Existe un proceso formal para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información?		X	
2,5	¿La organización establece políticas de terminación o cambio de responsabilidades a colaboradores, contratistas y/o proveedores?		X	
2,6	¿Se identifican, revisan y documentan los requisitos para los acuerdos de confidencialidad o no divulgación de acuerdo con las necesidades de la organización para la protección de la información?.(Proveedores, colaboradores,)"		X	
2,7	¿Implementan políticas y medidas de seguridad para proteger la información, procesamiento y/o almacenamiento de procesos para el desarrollo de teletrabajo?"		N/A	
2,8	¿Se exige al personal el reporte de eventos e incidentes referentes a la seguridad de la información en tiempo real?		X	
3. CONTROLES FÍSICOS				
3,1	¿Existe perímetro de seguridad física en las instalaciones de la organización? (CCTV, cercado eléctrico, vigilancia privada)			
3,2	¿Hay protección y restricción en el acceso físico a las instalaciones de la organización?. (RFID, Biométricos…)		X	
3,3	¿Se aplican sistemas de autenticación de acceso físico a las oficinas y recintos de la organización? (Áreas administrativas, cuarto de equipos)		X	
3,4	¿La organización realiza un monitoreo constante de sus instalaciones para prevenir y detectar accesos físicos no autorizados?		X	
3,5	¿La organización cuenta con protección contra amenazas externas y ambientales? (desastres naturales, ataques maliciosos o accidentes)			

3,6	¿Se diseñan y aplican procedimientos para trabajo en áreas seguras?			
3,7	¿Existen políticas de escritorio y pantalla limpia?		X	
3,8	¿La organización asegura que todo su equipo se encuentre ubicado de manera segura y protegida?		X	
3,9	¿Se generan medidas de seguridad y actas de responsabilidad para los equipos y activos que funcionan fuera de las instalaciones?"		X	
3,1	¿La organización gestiona los medios de almacenamiento de acuerdo con su ciclo de vida y cumple con los requisitos de clasificación y manipulación establecidos?		X	
3,11	¿El cableado de energía y datos está protegido ante interceptación, interferencia o daño?		X	
3,12	¿Los dispositivos electrónicos (Computadores, servidores, impresoras, dispositivos de red) están protegidos ante fallas del servicio de suministro eléctrico?"		X	
3,13	¿Se efectúa mantenimiento preventivo o correctivo a los equipos informáticos?			
3,14	¿Existen políticas que determinen la disposición de equipos para su reutilización?		X	
4. CONTROLES TECNOLÓGICOS				
4,1	¿La organización ha establecido procedimientos específicos para garantizar la protección de la información almacenada, procesada o accesible a través de los dispositivos finales del usuario?		X	
4,2	¿La compañía maneja perfiles de gestión de derechos de acceso privilegiado?		X	
4,3	¿Se realiza un proceso formal de registro, asignación y cancelación de usuarios y sus derechos de acceso, para evitar el ingreso no autorizado a sistemas y servicios?"		X	
4,4	¿La organización gestiona de manera adecuada el acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software utilizadas en sus proyectos?		N/A	La organización no cuenta con desarrollo de software propio
4,5	¿El acceso a la información y a las funciones de los sistemas de las aplicaciones, es restringida de acuerdo con la política de control de acceso?		X	
4,6	¿La organización realiza un control y ajuste de los recursos de acuerdo con los requisitos de capacidad actuales y futuros?		X	
4,7	¿La organización implementa y respalda la protección contra el malware a través de la conciencia adecuada de los usuarios, promoviendo prácticas de seguridad informática y proporcionando capacitación sobre la prevención de amenazas de software malicioso?		X	
4,8	¿La organización evalúa la exposición de la organización ante posibles vulnerabilidades del sistema de información, para evaluar y tomar medidas apropiadas para tratar los riesgos asociados?		X	
4,9	¿La organización establece, documenta, implementa, monitorea y revisa regularmente las configuraciones, incluidas las de seguridad, de hardware, software, servicios y redes, como parte de sus prácticas de gestión de seguridad de la información?		X	
4,1	¿Existe procedimientos para eliminar de forma segura la información almacenada cuando ya no es necesaria?		X	
4,11	¿Se aplica el enmascaramiento de datos de acuerdo con sus políticas internas, requisitos comerciales y la legislación vigente en materia de privacidad de datos?		X	
4,12	¿Existen medidas de prevención de fuga de datos en sus sistemas, redes y dispositivos que procesan, almacenan o transmiten información sensible?		X	
4,13	¿Se crean copias de respaldo de la información? (Back up) ?		X	
4,14	¿Hay controles de redundancia que cumplan con los requisitos orientados a la disponibilidad de los sistemas y tratamiento de datos?		X	
4,15	¿Existe un método de registro de actividad de los usuarios (Log)?		X	
4,16	¿Existe identificación de incidentes y eventos que atentan contra la Confidencialidad, integridad y disponibilidad de la información que maneja la organización?		X	
4,17	¿Se realiza la sincronización de relojes con una única fuente de referencia de tiempo?		X	
4,18	¿¿La compañía maneja perfiles de gestión de derechos de acceso privilegiado?		X	
4,19	¿Se controla la instalación de software en sistemas operativos?		X	
4,2	¿La empresa cuenta con controles para la protección de información en las redes, sistemas y aplicaciones e instalaciones de procesamiento de información?		X	

4,21	¿Se identifican los mecanismos de seguridad, niveles de servicio y requisitos de gestión de los servicios de red, ya sean internos o tercerizados?		X	
4,22	¿Segmentan redes de acceso a internet para personal administrativo?		X	
4,23	¿La organización gestiona el acceso a sitios web externos contra contenido malicioso?		X	
4,24	¿Se desarrollan e implementan políticas sobre el uso de controles criptográficos para la protección de la información?		X	
4,25	¿La organización ha establecido y aplicado reglas y prácticas para garantizar el desarrollo seguro de software y sistemas de información?		N/A	n/a
4,26	¿La organización identifica, especifica y aprueba los requisitos de seguridad de la información al desarrollar o adquirir aplicaciones?		X	
4,27	¿La organización implementa principios de ingeniería de sistemas seguros en todas las etapas de desarrollo de sistemas de información para garantizar la seguridad desde el inicio del proceso de desarrollo?		N/A	La organización no cuenta con desarrollo de software propio
4,28	¿La organización aplica principios de codificación segura en el desarrollo de software?		N/A	La organización no cuenta con desarrollo de software propio
4,29	¿La organización ha definido e implementado procesos de pruebas de seguridad en todas las etapas del ciclo de vida del desarrollo de software?		N/A	La organización no cuenta con desarrollo de software propio
4,3	¿La organización dirige, monitorea y revisa de manera efectiva las actividades relacionadas con el desarrollo de sistemas subcontratados?		X	
4,31	¿La organización mantiene entornos de desarrollo, prueba y producción separados y protegidos para prevenir la contaminación y asegurar la integridad de los sistemas y datos?		N/A	La organización no cuenta con desarrollo de software propio
4,32	¿Existe control de cambios a procesos de negocio que se realizan en la organización?		X	
4,33	¿La organización selecciona, protege y gestiona adecuadamente la información utilizada en pruebas evitando pérdida de información sensible durante estas?		X	
4,34	¿La organización planifica y acuerda de manera efectiva las pruebas de auditoría y otras actividades de aseguramiento que involucran la evaluación de sistemas operativos con la gerencia correspondiente y los evaluadores para garantizar una evaluación integral y precisa de los sistemas operativos?		X	

De la figura 3 se pueden observar alguno ítems marcados como N/A, que para el caso de la organización, esta no cuenta con desarrollo de software. Esta lista de verificación, fundamentada en la norma ISO 27001:2022, fue adaptada para posibilitar un análisis rápido y directo mediante preguntas cerradas.

B. Objetivo 2

Definir políticas de seguridad de la información en el área administrativa, de acuerdo con los estándares de la norma ISO 27001, en la organización.

Después de identificar el estado inicial, el enfoque se orienta hacia la definición de políticas, las cuales se dividen en cuatro categorías: organizacionales, de personas, de seguridad física y de recursos tecnológicos. Asimismo, cada una de estas categorías detalla la lista de verificación anterior con sus respectivos lineamientos, los cuales se adaptan de manera óptima al estándar internacional.

a. Políticas Organizacionales

La empresa establece una estructura organizativa sólida para garantizar la gestión efectiva de la seguridad de la información en toda la empresa a nivel interno, incluyendo roles y responsabilidades, comunicación, concienciación, auditoría y evaluación, mantenimiento, adecuación y eficacia.

Lineamientos generales

• Los dispositivos móviles ingresados a la empresa son una herramienta de trabajo y deben ser utilizados exclusivamente para las comunicaciones de los(as) funcionarios(as) y/o contratistas, para el desarrollo de las funciones laborales o de las obligaciones contractuales correspondientes.

• El acceso a la información de la empresa a través de dispositivos

móviles de propiedad de los empleados dispositivos BYOD, contratistas y/o terceros, se autorizan previa solicitud de los líderes de los procesos a través del área de IT y posterior visto bueno del líder de seguridad de la información.

• Se debe hacer uso de las herramientas y medios suministrados por la organización, para almacenar, transmitir, procesar y en general, para tratar la información a que tenga acceso mediante el uso de dispositivos móviles personales.

• En el momento de cesar la vinculación laboral o relación contractual que dio lugar a la autorización para el uso de dispositivos móviles privados para acceder a la información de la empresa, se deben eliminar los accesos a aplicaciones de la entidad en los que se almacene o transmita la información institucional, como por ejemplo, correo electrónico institucional, OneDrive de Office 365, Microsoft Teams, SharePoint, etc.

• En caso de cambio, pérdida o hurto de un dispositivo móvil personal con acceso a la información, el empleado contratista o tercero a quien se le haya autorizado el uso del dispositivo, es responsable de informar con carácter urgente a su jefe inmediato y a la alta dirección, a través de los canales de comunicación autorizados.

• Los empleados o contratistas que tengan asignados dispositivos móviles de la compañía, no deben conectarse en estos dispositivos a través de redes inalámbricas públicas.

• La empresa establece los responsables para el tratamiento de los incidentes de seguridad de la información en concordancia con las competencias, responsabilidades y los activos de información a su cargo.

• Los incidentes de seguridad deben ser registrados en una base de conocimientos y lecciones aprendidas. Esto permite que la información sea consultada en el futuro y utilizada para tomar decisiones acertadas en caso de incidentes similares.

• Todos los usuarios son responsables de las actuaciones realizadas con sus credenciales, mismas que fueron otorgadas por la organización para el uso de sistemas de información y recursos tecnológicos.

• Las cuentas de red se bloquean después de (5) intentos fallidos por contraseña o usuario incorrecto con desbloqueo automático de (15) minutos; además, el sistema solicitará cambio de clave después de cumplido un tiempo de (60) días calendario.

• Los cambios en los privilegios de acceso a los recursos tecnológicos, como servicios de red, sistemas de información y bases de datos, debido a nuevas contrataciones o cambios en el personal, ya sean temporales o permanentes, se llevan a cabo siguiendo el procedimiento establecido en la Gestión de Usuarios. Estos cambios se realizarán de acuerdo con las notificaciones proporcionadas por el área de recursos humanos, los jefes de departamentos y/o los supervisores.

• Se establecen con los proveedores TIC Acuerdos de Niveles de Servicio (ANS), para cada servicio con sus respectivas penalizaciones en caso de incumplimiento y se realizará un seguimiento periódico de la calidad de los productos.

b. Políticas de personas

Para garantizar la seguridad de la información, la empresa establece normas de conducta y procedimientos que rigen el comportamiento del personal en relación con la gestión de la información. Esto incluye la concientización sobre amenazas de seguridad, la responsabilidad de proteger la información y la identificación y reporte de amenazas o vulnerabilidadesque pongan en riesgo la integridad, disponibilidad e integridad de la información.

Lineamientos generales

• El área de recursos humanos, realiza las actividades necesarias para la selección de personal, asegurando la verificación de los requisitos mínimos para proveer los cargos y el cumplimiento de la normatividad vigente.

• Para el ingreso de nuevo personal de planta y la suscripción de contratos o convenios relacionados con servicios de tecnología y/o acceso a información, se debe garantizar que la persona acepte y firme una cláusula en la cual se informe sobre las políticas de seguridad de la información y acuerde mantener la confidencialidad de la información, con la suscripción de un acuerdo o compromiso de confidencialidad; este acuerdo se hará extensivo a todos los colaboradores de los contratistas o terceros para el caso de contratos o convenios.

• El área de recursos humanos es la responsable de Informar al área de TI, toda novedad de personal mediante el procedimiento establecido sobre terminación de contrato, nuevo ingreso, vacaciones u otro estado que deba revocar o activar permisos al personal.

• Los empleados deben conocer y aplicar los procedimientos de seguridad de la información vigentes sin pena de incurrir en faltas disciplinarias y/o contractuales; de igual manera, deben reportar oportunamente las debilidades e incidentes de seguridad de la información que detecten o que sean de su conocimiento y resguardar el acceso a los recursos informáticos asignados.

• Los responsables de los procesos y jefes de dependencias deben informar al área de TI, acerca de los permisos a las carpetas o recursos compartidos de los empleados y/o contratistas para los cuales están autorizados; así mismo, deben conocer y asegurar el cumplimiento de las políticas de seguridad de la información por parte de su equipo de trabajo.

• Se establece un procedimiento para notificar en caso de brecha de seguridad, incidente o sospecha de violación de seguridad deben ser reportado al Equipo de Seguridad de la Información de manera inmediata. Se determinará el impacto de la violación en los activos y se tomarán acciones disciplinarias de acuerdo con las políticas internas y la gravedad del incidente.

c. Políticas seguridad física

La empresa establece reglas para proteger las instalaciones y activos de información contra amenazas físicas. Esto incluye garantizar el acceso controlado a áreas sensibles para la organización, la protección de equipos y sistemas críticos y la implementación de medidas deseguridad física adecuadas para prevenir daños, robos y garantizar la integridad, disponibilidad y confidencialidad de la información.

Lineamientos generales

• En las dependencias donde se gestione, almacene y procese información de la empresa, se implementan controles de acceso seguro, con el fin de prevenir accesos no autorizados, adulteración, pérdida, consulta, daños e interferencia en el funcionamiento de los aplicativos e información.

• Las puertas de acceso a las oficinas e instalaciones de la organización, consideradas como áreas seguras y/o de acceso restringido, deben permanecer cerradas y aseguradas con el fin de prevenir el acceso de personal no autorizado.

• Las áreas de acceso restringido son protegidas con cerraduras, tarjetas de acceso u otros mecanismos de seguridad adecuados, como protección biométrica o doble autenticación de acuerdo con el rol del usuario.

• Se debe evitar el consumo de alimentos o bebidas en las áreas de trabajo que alberguen

información institucional en papel, equipos de cómputo, dispositivos electrónicos o cualquier medio de almacenamiento que pueda ser susceptible de dañarse debido a derrames de líquidos o residuos de alimentos.

• Todos los empleados y/o contratistas deben bloquear su sesión de trabajo en el sistema operativo del equipo de cómputo al momento de ausentarse de su puesto de trabajo, sin importar que esté configurado para bloquear la sesión de forma automática después de un tiempo determinado.

• La organización establece políticas claras para definir el proceso de disposición de equipos con el objetivo de promover su reutilización. Estas políticas garantizan la adecuada evaluación, limpieza y certificación de los equipos antes de ser puestos nuevamente en servicio, optimizando recursos y reduciendo residuos electrónicos.

• El área de TI debe elaborar el cronograma de mantenimiento preventivo, el cual será notificado a las dependencias con la debida anticipación, para asegurar la prestación del servicio a los usuarios. Adicionalmente, debe informarse el nombre e identificación del personal autorizado previamente a ser realizadas las actividades de mantenimiento, con el fin de evitar el riesgo de pérdida de equipos.

• El suministro eléctrico se mantiene a 110 voltios y con conexión a tierra, salvo indicación contraria del fabricante. Deben existir sistemas de respaldo, como UPS y plantas eléctricas, para garantizar un apagado controlado y operación continua de actividades críticas de la organización.

• Se debe mantener un entorno limpio y seguro en los escritorios físicos y áreas de trabajo, evitando la presencia de materiales o elementos que contengan información clasificada como confidencial, a menos que estén siendo utilizados por personal autorizado. En tal caso, dicho personal debe asegurarse de que la información confidencial esté debidamente resguardada en todo momento.

d. Políticas de recursos tecnológicos

La organización se compromete a salvaguardar activos de información críticos a través de la implementación de medidas tecnológicas avanzadas. Esto incluye el monitoreo continuo de amenazas, controles y gestión de copias de seguridad (backup), registros de logs, la autenticación multifactor, protección ante malware y código malicioso y el cifrado de datos para asegurar la confidencialidad, integridad y disponibilidad de la información.

Lineamientos generales

• Todos los equipos de cómputo deben tener instalado el software de antivirus debidamente actualizado y licenciado.

• Para proteger la información de la organización al distribuir archivos a otros usuarios internos o externos de la entidad, se debe contar con solución de antivirus que realice el análisis de los archivos y medios de almacenamiento en tiempo real.

• Está prohibido el uso y/o instalación de software no autorizado por la alta dirección y el área de TI. En caso de necesitar la instalación de algún software en los equipos de cómputo, se debe solicitar la autorización y apoyo en la instalación al área de TI.

• Se cuenta con personal facultado sea interno o externo para revisar periódicamente la información y el software instalado en los equipos de cómputo de la organización; aquel, realizará la eliminación de los archivos y/o la desinstalación inmediata del software no autorizado, que puedan generar riesgos para la seguridad de la información o incumplan con las políticas de seguridad de la entidad o la normatividad vigente relacionada con derechos de autor y propiedad intelectual.

• En caso de tener sospechas de instalación de código malicioso, éste debe notificarse por parte del funcionario al área TIC para su respectiva validación y tratamiento del mismo.

• El área de TI debe contar con un listado de aplicaciones críticas y componentes tecnológicos que deben ser respaldados, o un plan de backups, el cual debe ser revisado y actualizado de manera trimestral y/o cuando se presenten adiciones o modificaciones a la plataforma o infraestructura tecnológica.

• La frecuencia y alcance de los backups de la información, al igual que los periodos de retención, se deben establecer teniendo en cuenta la criticidad de la información respaldada, las necesidades de las diferentes dependencias o procesos de la entidad y/o por la legislación vigente aplicable.

• Se deben efectuar backups de la información antes y después de cualquier cambio en la configuración de algún componente de la plataforma tecnológica, que soporte las operaciones críticas de la entidad.

• Se deben almacenar los logs de ejecución y generación exitosa o fallida de los backups, por un periodo no menor a 1 año.

• Se realizan copias de seguridad adicionales para los componentes catalogados como críticos y procurar que estas sean almacenadas en ubicaciones diferentes.

• Se deben concretar los permisos de las acciones que se pueden realizar sobre la información (creación, lectura, borrado, modificación, copia, ejecución, etc.). Como norma general, siempre se otorgará el mínimo privilegio en el establecimiento de los permisos.

• Los relojes de los sistemas de procesamiento de información de la empresa se deben sincronizar con una única fuente de referencia de tiempo.

• En lo posible, los registros de eventos deben registrar como mínimo la siguiente información:

- Identificación de usuarios
- Actividades realizadas en el sistema
- Fechas y horas de acceso y salida de los sistemas
- Registros de acceso exitosos y denegados
- Cambios en las configuraciones de los sistemas
- Cambios en los privilegios de los sistemas
- Archivos a los que se tuvo acceso
- Direcciones y protocolos de red

• La alta dirección y el área de TI aseguran que, en los procesos de adquisición de nuevos sistemas de información o de mejora a las aplicaciones de software existentes, se incluyan los requisitos suficientes para garantizar la seguridad de la información, protegiendo la integridad, disponibilidad e integridad de la información.

• La organización implementa Autenticación de Múltiples Factores (MFA) para la protección de acceso no autorizado a la información en sistemas críticos; se deben usar mínimo dos factores de autenticación independientes como (algoritmo de contraseñas seguro, biometría, token de seguridad, autenticación basada en ubicación).

C. Objetivo 3

Diseñar controles de seguridad de la información para el área administrativa que permitan aumentar los niveles de seguridad de la empresa Global Dinamic Ventures.

Para la realización de este objetivo, se realizaron varios controles con el fin de aumentar los niveles en los ítems que se evaluaron en el primer objetivo y se listan a continuación:

a. Matriz de cumplimientos legales:

Permite establecer en la organización, la gestión eficaz de las responsabilidades legales, la mitigación de riesgos y el mantenimiento de un entorno operativo legalmente conforme.

b. Matriz de roles y responsabilidades:

Herramienta que sirve para clarificar y documentar las funciones y responsabilidades que debe seguir la empresa, dando claridad para la rendición de cuentas y eficiencia en la protección de los activos de la información.

c. Matriz de riesgos:

Permite evaluar y visualizar los riesgos existentes en la organización, asociados con la gestión de la seguridad de la información adicional; igualmente, otorga visión y priorización de los riesgos existentes.

d. Formato de registro de incidentes:

Tiene como objetivo, tener un control sobre los incidentes relacionados con seguridad de la información, con el fin de cumplir con los requerimientos de la norma ISO 27001; allí se podrán reportar incidentes que fueron controlados y los que siguen activos, para así determinar medidas preventivas y correctivas.

e. Imagen con líneas de atención ante incidentes de seguridad:

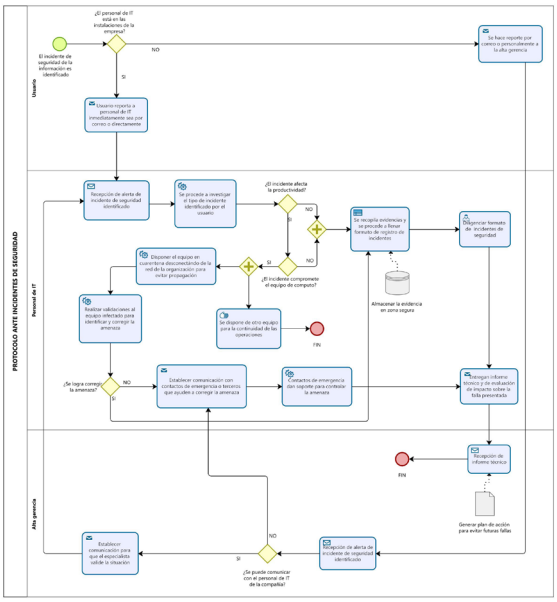
Se da cumplimiento a uno de los ítems calificables en la norma ISO 27001 que busca establecer comunicación con contactos de emergencia de entidades dedicadas a identificar amenazas, salvaguardar y proteger la seguridad de la información, como se muestra en la figura 4.

Figura 4. Líneas de atención ante incidentes de seguridad informática en Colombia

f. Creación de protocolo de emergencia ante ataques a la seguridad de la información

El siguiente protocolo se tiene como finalidad, dar una orientación a la empresa cuando ocurra un incidente de seguridad de la información. A continuación, se ha utilizado el software Bizzagi Modeler para crear de manera ordenada y estructurada un diagrama de flujo. Este diagrama brinda a la organización una guía sobre cómo actuar ante un incidente de seguridad, como se ilustra en la figura 5.

Figura5. Protocolo ante incidentes de inseguridad.



g.Aseguramiento de PC con programa CISCAT y el editor de políticas:

Acto seguido, se presenta el aseguramiento del equipo mediante el software CISCAT, mismo que presenta una guía de buenas prácticas para asegurar de una manera lógica al equipo contra el mal uso o ataques externos; este permite mediante la modificación del editor de registro, proteger aspectos técnicos que pueden llegar a ser un vector de ataque. Todo esto, para sistemas operativos Windows 10Pro con los que cuenta la organización; desde allí se habilitaron los logs para el registro de eventos, la periodicidad de cambio de contraseñas, habilitación de firewall, entre otras características que ayudan a la protección del equipo, entre otras más.

Todos estos controles los determina el informe generado por el programa CISCAT, que busca mejorar la seguridad de los equipos y que puede ser empleado por cualquier organización que quiera implementar políticas y procedimientos para proteger contra ataques de seguridad.

h. Creación de matriz DOFA

A continuación, se presenta la matriz DOFA que busca evaluar fortalezas, amenazas, oportunidades y debilidades de la empresa en seguridad de la información, adicionalmente, en el cruce de variables se obtienen las estrategias que fueron parte fundamental para la construcción de las políticas, y las recomendaciones entregadas a la organización. Ver Tabla I:

Análisis D.O.F.A. JIT LOGISTICS S.A.S		Fortalezas		Debilidades
	F1	Disposición de recursos para inversión en seguridad de la información	D1	Infraestructura de seguridad desactualizada
	F2	Actualización continua de sistemas de software usados por la organización	D2	Falta de inversión en seguridad de la información
	F3	Principales servicios tecnológicos alojados en la nube	D3	No hay personal idóneo en relación a seguridad de la información
	F4	Uso de software libre (gratuito) que se adapta a las necesidades de la empresa anivel de seguridad de la información (firewall, antivirus de prueba gratuito, gestores para encriptar información)	D4	Falta de conciencia sobre la seguridad de la información entre los empleados
	F5	Copias de seguridad de la información	D5	Procesos de seguridad ineficientes

Oportunidades		Estrategias F-O	Estrategias D-O
Feria de seguridad internacional de seguridad ESS+ (1 vez al año)	O1	(F1 - O1) Participación de la feria internacional para adquisición de nuevas tecnologías que se adapten a las necesidades y aprovechar el conocimiento sobre nuevas tecnologías y generar contactos clave.	(D1-O1) Aprovechamiento de la feria para aprovechar los últimos avances tecnológicos a nivel de seguridad de la información para crear un plan estratégico para actualización de infraestructura en seguridad
Kits y recursos de ciberseguridad ofrecidos por MasterCard para Pymes	O2	(F2 - O2) Incluir los recursos ofrecidos por MasterCard para proteger y robustecer los sistemas de seguridad de la información	(D2-O2) Implementación de herramientas gratuitas como la ofrecida por MasterCard para generar estrategias de prevencion ante amenazas de la seguridad de la información.
Marcos internacionales para la seguridad de la información como la norma ISO 27001	O3	(F3-O3) Oportunidad de implementación de la norma para fortalecer los servicios en la nube mediante un marco internacional	(D3-O3) Desarrollar capacidades con el personal interno disponible mediante capacitación gratuita online abasándose en la norma internacional ISO 27001
Desarrollo de programas de formación en seguridad de la información dados por la MINTIC (siempre disponibles)	O4	(F4-O4) Escoger críticamente el software libre usado basado en los conocimientos adquiridos en las capacitaciones ofrecidos para reducir los impactos que puede generar el software libre	(D4-O4) Incluir dentro del plan de capacitaciones al personal los ofrecidos por el MINTIC sobre seguridad de la información
Cursos gratuitos dirigidos a PYMES en seguridad de la información ofrecidos por la universidad Australia Deakin para prevención de desastres de seguridad.	O5	(F5-O5) Aprovechar la capacitación gratuita y fortalecer las prácticas de seguridad de la información de las PYMES para la correcta gestión de las copias de seguridad	(D5-O5) Mejorar la eficiencia en la seguridad de la información fortaleciendo la postura y reduciendo los riesgos asociados mediante la capacitación y certificación

Amenazas		Estrategias F-A	Estrategia D-A
Ataques de ingeniería social para sustraer información	F1	(F1-A1) Uso de los recursos para creación de métodos de doble autenticación y concientización del personal mediante capacitaciones realizada por personal capacitado	(D1-A1) Evaluación mediante auditoria e identificación de vulnerabilidades de ingeniería social para generar estrategias oportunas
Aumento de ciberataques anivel nacional y evolución de los mismos como (Phishing, Rasomware, DDoS)	F2	(F2-A2) Revisión periódica de últimos parches de seguridad en los sistemas informáticos actuales de la organización y generación de planes de contingencia ante futura materialización de incidentes de seguridad.	(D2-A2) Establecer un plan de inversión a largo plazo en seguridad de la información, definición de políticas y que ayuden a mitigar la materialización de los posibles ataques
Leyes que sancionan delitos informáticos con penas punitivas y económicas (ley 1273 de 2009)y (ley 1581 de 2012)para tratamiento de la información	F3	(F3-A3) Mejorar bajo los estándares nacionales la protección de datos (PII) y reducción de amenazas que puedan generar pérdidas económicas o daño a la reputación de la empresa	(D3-A3) Fortalecer la cultura de seguridad de la información con el personal generando conciencia sobre el cumplimiento legal y normativo en la organización
Suspensión de activiades administrativas, por fallas o falta de suministro de energía eléctrica	F4	(F4-A4) Adquisición de UPS para darle continuidad a los procesos críticos de la empresa	(D4-A4) Generar plan de continuidad del negocio para mantener operativas las actividades críticas y definición de procedimiento para que los usuarios puedan acceder y trabajar con información crítica
Externalización de servicios tecnológicos	F5	(F5-A5) Respaldar la información de servicios tercerizados por interrupciones de los servicios externos para seguir con la continuidad del negocio	(D5-A5)Identificar y abordar las debilidades actuales mediante políticas para poder anticiparse a las amenazas asociadas con la externalización de servicios y mejorar

Se entregó a la organización un manual de instalación del programa, así como recomendaciones (ver Anexo 8) que deben ser tenidas en cuenta, para completar el aseguramiento a todos los equipos. Además, es fundamental determinar la eficacia de los controles. Esto implica someterlos a un proceso de prueba antes de su implementación y obtener validación y aprobación por parte de la alta gerencia. Dichos controles son esenciales para asegurar el cumplimiento de la normativa ISO 27001.

i. Entrega de recomendaciones

Con el propósito de ayudar a la organización en la búsqueda de un entorno seguro en lo concerniente a la seguridad de los datos, se dejó una serie de recomendaciones para llevar a cabo - a largo plazo -, aquellas actividades y procesos que no se pueden cumplir por temas organizacionales de la compañía, donde se incluyen:

- La forma de implementar un directorio activo con recomendaciones técnicas y generales.
- Sugerencias para el uso incorrecto de los activos de información.
  Indicaciones para la continuidad del negocio.
- Capacitaciones en sitios web para que el personal dedicado pueda tener una información gratuita en materia de seguridad de la información.
- Acuerdos de confidencialidad.
- Actas de responsabilidad.
- Sugerencia para la implementación de un sistema de doble autenticación para sistemas sensibles.
- Uso de una UPS más robusta para suplir necesidades básicas.
- Métodos para tratar y gestionar las copias de respaldo.
- Auditorías internas o externas.
- Sugerencia de uso de un firewall y antivirus para los equipos.

C. Objetivo 4

Evaluar el estado posterior al diseño de políticas de seguridad de la información para garantizar el fortalecimiento y continuidad de las estrategias de aseguramiento en la organización.

Con el objetivo de evaluar y ajustar las políticas de seguridad de la información, para garantizar su eficacia continua y fortalecer la capacidad de la organización con el propósito de enfrentar los desafíos de seguridad en curso, se determinó hacer una nueva lista de chequeo para validar la mejora.

Es decir, este análisis permitirá determinar la eficacia de las políticas y controles efectuados en la organización, identificando mejoras y validando la adaptación al cambio de la compañía, como se observa en seguida, en la tabla 2:

La información contenida en la Tabla III, permite verificar que la inversión en seguridad, tanto en el personal como en la infraestructura, no solo permite aumentar los niveles de controles y políticas, sino que también proporciona mejoras sustanciales. Esto se traduce en la capacidad de crear controles y estrategias más eficaces y sólidos para proteger la organización, salvaguardando su activo más preciado: la información.

Las políticas y controles en la organización, identifican mejoras y validan la adaptación al cambio.

TABLA II

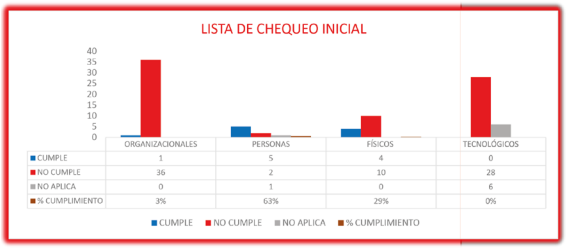
Cuadro comparativo primera lista de chequeo con segunda lista

LISTA DE CHEQUEO INICIAL

CONTROLES	# ítems	CUMPLE	NO CUMPLE	N/A	% CUMP
ORGANIZACIONALES	37	1	36	0	3%
PERSONAS	8	5	2	1	63%
FÍSICOS	14	4	10	0	29%
TECNOLÓGICOS	34	0	28	6	0%
TOTAL	93	10	76	7	11%

LISTA DE CHEQUEO FINAL

CONTROLES	# ítems	CUMPLE	NO CUMPLE	N/A	% CUMP
ORGANIZACIONALES	37	16	21	0	43%
PERSONAS	8	5	2	1	63%
FÍSICOS	14	8	6	0	57%
TECNOLÓGICOS	34	6	22	6	18%
TOTAL	93	35	51	7	38%



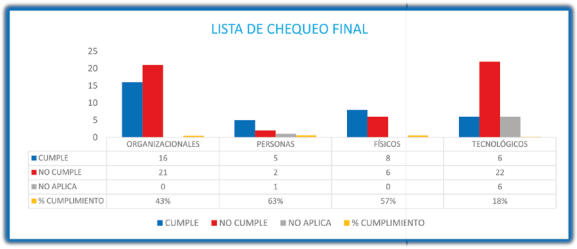


TABLA III

COSTO MENSUAL

SUELDO BASICO	4.100.000

SEGURIDAD SOCIAL		
CONCEPTO	**APORTE EMPLEADOR**	**VALOR APORTE**
SALUD	8,50%	348.500
PENSIÓN	12,00%	492.000
ARL	0,52%	21.402
CAJA DE COMPENSACIÓN	4,00%	164.000
	TOTAL SEGURIDAD SOCIAL	**1.025.902**

PRESTACIONES SOCIALES		
CONCEPTO	**% PRESTACIÓN**	**VALOR PRESTACIÓN**
PRIMA	8,33%	341.667
CESANTIAS	8,33%	341.667
INTERESES A LAS CESANTIAS	12,00%	41.000
VACACIONES	4,34%	177.940
	TOTAL PRESTACIONES SOCIALES	**902.273**

COSTO TOTAL MES	**6.028.175**
COSTO ANUAL	**72.338.104**

	COSTOS INICIALES	**COSTOS RECURRENTES**
Firewall Fortigate 60e	$ 3.570.000	-
Licencia (anual)	$ 1.599.000	1.599.000
Analista de seguridad (Mensual)	$ 6.028.175	6.028.175
Software como servicio (SaaS)	En cotización	
Antivirus o Endpoint (anual)	$ 1.728.243	$ 1.728.243,00
TOTAL	$ 12.925.418	$ 9.355.418

V. CONCLUSIONES

La información contenida en la Tabla III, permite verificar que la inversión en seguridad, tanto en el personal como en la infraestructura, no solo permite aumentar los niveles de controles y políticas, sino que también proporciona mejoras sustanciales. Esto se traduce en la capacidad de crear controles y estrategias más eficaces y sólidos para proteger la organización, salvaguardando su activo más preciado: la información.

El diseño de políticas de seguridad de la información basadas en la norma ISO 27001, constituye una estrategia eficiente para la protección de los datos de la empresa Global Dinamic Ventures. Así mismo, la creación de estas políticas promueve la preservación de la confidencialidad, integridad y disponibilidad de la información y dará un mejor espectro situacional endonde se encuentra la empresa, en cuanto a seguridad de la información, permitiendo la comprensión de su nivel de vulnerabilidad.

a ser víctima de ataques cibernéticos.

Una vez realizada la última lista de chequeo, se concluyó que el diseño de políticas y la aplicación de controles a la organización mejoró sustancialmente, según los lineamientos de la norma ISO 27001 para la protección de la integridad, confidencialidad y disponibilidad de la información que administra la empresa, dando una visión más clara en temas relacionados a ciberseguridad, siendo estauna estrategia efectiva que la prepara para un mundo digitalmente cambiante.

VI. REFERENCIAS

[1] TIC TAC CSIT, «CSIT,» Abril 2023. [En línea]. Available: https://www.ccit.org.co/estudios/estudio-anual-de-ciberseguridad-2022-2023/#:~:text=Precisamente%2C%20el%20estudio%20revela%20que,con%20mayor%20n%C3%BAmero%20de%20registros.. [Último acceso: 10 11 2023].

[2] A. R. Luis, «Diseño y consolidación de uncentro de respuesta ante incidentes de seguridad informática en la empresa cibersecurity de colombia ltda,» 2020. [En línea]. Available: https://repository.unad.edu.co/handle/10596/52511.

[3] A. A. Alejandra, Diseño de un modelo para la gestiónde incidentes en ciberseguridadbasado en la norma iso27002:2013 para la empresa proyectos de inversión vial andino S.A.S, Bogotá, 2022, p. 16.

[4] Q. M. Luis, Cifrado de la información y su incidencia actual en la seguridad de la información para pequeñas empresas pymes en colombia, Bogotá, 2020.

[5] E. G. Jesus Alexander, Implementación ISO 27001 para el Control de Delitos Informáticos en la División de Prensa DIRCII PNP,Lima,2022, Lima, 2022.

[6] B. A. Yasmani Fernando, Norma ISO 27001 para el Control de la Seguridad de Información en una Consultoría Privada, Lima 2023, Lima, 2023.

[7] Z. M. Monica Piedad, Propuesta de mejora para la integración de las normas de calidad, seguridad de la información y centros de contacto con el cliente, región españa & latam en una multinacional de telecomunicaciones, España, 2022, pp. 40,41.

[8] G. Fredy, «¿Qué es un paradigma? Análisis Teórico, Conceptual Y Psicolingüístico Del Término,» de ¿Qué Es Un Paradigma? Análisis Teórico, Conceptual Y Psicolingüístico Del Término, Caracas, 2005, p. 8.

[9] Consultores, Bastis, «Desarrollo de tesis, Investigación Cuantitativa,» 2021.

[10] G. P. Guevara alban, A. E. Verdesoto Arguello y N. E. Castro Molina, «Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción),» de Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción), Babahoyo, Saberes del conocimiento, 2020, p. 116.

[11] L. D. Mata Solis, «El enfoque de investigación: la naturaleza del estudio,» de El enfoque de investigación: la naturaleza del estudio, 2019.

[12] R.HernándezSampieri,«Metodologíadelainvestigación,» Ciudad de México, MC Graw Hi, 2018.

[13] H. Ñaupas Paitan, M. R. Valdivia Dueñas y J. J. Palacios Vilela, «Metodología de la investigación Cuantitativa -Cualitativa y Redacción de la Tesis,» Ediciones de la U, 2018.

[14] C. Espinoza Montes, «Metodología de la investigación tecnológica,» Huancayo, soluciones Gráficas S.A.C, 2014.

[15] J. Hurtado de Barrera, «Metodología de la Investigación holística,» Caracas, SYPAL, 2000, p. 223.

[16] Y. A. Buitrago, P. Hernández Rivero y C. Hernández Ruiz, Propuesta de diseño de la primera fase del sistema de gestión de seguridad de la información para la fundación educativa, Facatativá: Escom, 2020.

Revista TECNO**ESCOM**
ISSN 2711-0761. Vol. 6. No. 1

ESTÁNDAR PARA EL CICLO DE DESARROLLO SEGURO DE LAS APLICACIONES INFORMÁTICAS DEL EJÉRCITO NACIONAL

TE. Juan Botina Narváez
Oficial Ejército
juanbotinanarvaez@cedoc.edu.co

ST. Jean Murcia Torres
Oficial Ejército
jeanmurciatorres@cedoc.edu.co

SS. Fabio Ortiz Córdoba
Suboficial Ejército
fabioortizcordoba@cedoc.edu.co

RESUMEN- ***Las aplicaciones informáticas se han convertido en una herramienta fundamental para el funcionamiento de los procesos operacionales y administrativos de las Fuerzas Militares, incluyendo al Ejército Nacional. Sin embargo, el desarrollo de estas aplicaciones puede conllevar riesgos de ciberseguridad, que afecten la confidencialidad, integridad y disponibilidad de la información sensible.***

La investigación tiene como propósito fundamental, diseñar un estándar del ciclo de desarrollo de software que mejore las condiciones de ciberseguridad en las aplicaciones informáticas del Ejército Nacional. Para ello, se realizó un análisis de brechas en relación con el estado actual a nivel de seguridad de algunas aplicaciones tecnológicas de la institución. Posteriormente, se realizó un estudio de los estándares y mejores prácticas del ciclo de desarrollo del software que se encuentran disponibles a nivel mundial y que se acoplan a las necesidades de la Fuerza. Con base en este análisis, se crearon las políticas y lineamientos de ciberseguridad para el ciclo de desarrollo seguro de aplicaciones del Ejército. Finalmente, se definió el proceso de ciclo de desarrollo seguro para el Ejército Nacional.

Resultados esperados:

Análisis de la brecha que identifique los riesgos y vulnerabilidades del proceso de desarrollo de aplicaciones informáticas en el Ejército Nacional.

Análisis de los estándares para el desarrollo de software que cumpla con las condiciones de ciberseguridad del Ejército Nacional.

Desarrollo de políticas y lineamientos de ciberseguridad para el ciclo de desarrollo seguro de aplicaciones del Ejército Nacional, que incluya las recomendaciones dadas por los mencionados estándares.

Un proceso de ciclo de desarrollo seguro para el Ejército Nacional.

Palabras clave: Aplicaciones informáticas, ciberseguridad, desarrollo de software, estándar, Ejército Nacional.

Abstract— Computer applications have become a fundamental tool for the functioning of the operational and administrative processes of the Military Forces, including the National Army. However, the development of these applications may entail cybersecurity risks, which may affect the confidentiality, integrity and availability of sensitive information.

By designing a software development cycle standard that improves the cybersecurity conditions of the National Army's computer applications. To this end, a gap analysis was carried out in relation to the current state at the security level of some technological applications of the institution. Subsequently, an analysis was carried out of the standards and best practices of the software development cycle that are available worldwide and that adapt to the needs. Based on this analysis, cybersecurity policies and guidelines will be created for the institution's secure application development cycle. Finally, the secure development cycle process for the National Army was defined.

Expected results:

Analysis of the gap that identifies the risks and vulnerabilities of the computer application development process in the National Army. An analysis of the standards for the development of software that meets the cybersecurity conditions of the National Army. Development of cybersecurity policies and guidelines for the secure application development cycle of the National Army, which includes the recommendations given by the aforementioned standards.

A secure development cycle process for the National Army.

Keywords— Computer applications, cybersecurity, software development, standard, National Army

I. INTRODUCCIÓN

Con el fin de mejorar sus procesos operacionales y administrativos, el Ejército Nacional ha venido desarrollando aplicaciones a la medida; no obstante, los mencionados aplicativos no se han realizado acorde con los lineamientos de mejores prácticas en temas de seguridad.

Por lo tanto, el desarrollo del estándar representa una iniciativa esencial para fortalecer la ciberseguridad del Ejército Nacional. Este estándar, construido sobre los mejores estándares y prácticas internacionales, ha sido adaptado meticulosamente para satisfacer las necesidades específicas de la Fuerza. Contiene políticas y directrices que abarcan todas las fases del ciclo de desarrollo de software, desde la planificación hasta la operación y mantenimiento.

Con el fin de proteger la información sensible del Ejército Nacional, incluyendo datos personales así como información clasificada y sistemas críticos, se desarrolló el estándar para el ciclo de desarrollo seguro de las aplicaciones informáticas del Ejército Nacional, el cual contribuye en asegurar y garantizar la confidencialidad, integridad y disponibilidad de la información desde el desarrollo de las aplicaciones informáticas en el Batallón de Interoperabilidad de Comunicaciones y Computación - BAICC para el Ejército Nacional, a lo largo del año 2023.

II.ESTADO DEL ARTE

A. Antecedentes nacionales

Según la tesis de investigación de la Universidad Externado de Colombia, denominada "Propuesta de un Plan Estratégico de Seguridad y privacidad de la Información para el Departamento Administrativo de la función pública (DAFP) [1], las organizaciones deben contar con un sistema estructurado que gestione la seguridad de sus activos en las entidades públicas, favoreciendo con estas acciones la identificación de los riesgos que puedan causar perjuicio, así como el establecimiento de políticas de prevención para intervenir las problemáticas detectadas, evitando con ello que sucedan episodios como la fuga de información, entre otros(p.14).

Debido a lo mencionado anteriormente, es importante la implementación de un sistema estructurado de seguridad informática, teniendo en cuenta que muchas organizaciones manejan información confidencial de sus clientes, proveedores y empleados; así mismo, las amenazas cibernéticas son una realidad para cualquier empresa, generando consecuencias catastróficas.

En relación con la seguridad informática, la investigación llevada a cabo por la Universidad Francisco de Paula Santander [2], en Ocaña, sostiene que las organizaciones en Colombia, dada la sensibilidad de su información, se

enfrentan a una exposición a violaciones en sus sistemas. Han detectado que las vulnerabilidades y amenazas que presentan los sitios web en la intranet son un factor débil en términos de seguridad informática. Además, se evalúa la vulnerabilidad existente a través del recurso humano, lo que permite la detección de amenazas y la adopción de medidas para reducir la inseguridad.

Esto se refiere a que el personal en las empresas y organizaciones son parte vulnerable, debido a la falta de conciencia en seguridad informática, errores humanos involuntarios y malintencionados, que permiten abrir brechas en la seguridad, teniendo en cuenta la falta de políticas y procedimientos en seguridad informática para minimizar estos riesgos.

Según el trabajo investigativo de la Universidad Externado de Colombia, denominada "Modelo de Seguridad de la Información para la Empresa Comestibles RICOS S.A", la empresa presenta un estado de vulnerabilidad y riesgo a causade la ausencia de un modelo de seguridad de la información aplicado dentro de la empresa; así, esta se encuentra expuesta a ser víctima de un incidente de seguridad y a ser más sensible ante un posible ciberataque [3, p.11].

La Empresa a la cual se hace alusión, por falta de un modelo de seguridad informática, puede colocar en riesgo la seguridad de sus datos sensibles y confidenciales, generando la interrupción del negocio y dañar la buena reputación de la empresa. Por otra parte, en la Tesis, producto de investigación del Instituto Tecnológico Universitario, denominada "Modelo de ciberseguridad en las unidades de medición fasorial (PMU) del nuevo sistema inteligente de supervisión y control avanzado en tiempo real (ISAAC)" [4], se encontró que las organizaciones en Colombia encargadas de operar equipos industriales o prototipos diseñados para cumplir funciones de supervisión y control, no cuentan con un modelo de protección informática o ante ciberataques.

Teniendo en cuenta que mencionados equipos se instalan en las redes de operación de los distintos agentes del mercado, con una distribución geográfica dispersa en el territorio nacional colombiano. Entre sus funciones se encuentran entregar información a los distintos agentes y alimentar los datos del operador del sistema eléctrico, quienes son los únicos autorizados para tener acceso a su administración y configuración.

En la tesis de investigación de la Universidad Francisco de Paula Santander Ocaña [5], se afirma que, de acuerdo con un análisis de la capacidad de la ciberseguridad en la dimensión tecnológica en lo que concierne a respuesta a incidentes y protección de la infraestructura crítica en Colombia, bajo una perspectiva sistémica desde la organización, se pretendió tener una aproximación a la problemática derivada de la interconectividad a nivel mundial y particular en una empresa del sector colombiano en lo concerniente a la ciberseguridad, analizada desde la respuesta a incidentes y la protección de infraestructuras críticas.

Esta última afectada directamente por los incidentes de seguridad o eventos no prevenidos que pueden aumentar la probabilidad de afectación a la continuidad de los negocios que son soportados con tecnología (p.16).

Lo anterior hace referencia a que los incidentes de seguridad pueden ocurrir por falta de medidas de seguridad informática adecuadas y ataques informáticos. Por lo tanto, es importante adoptar medidas de seguridad adecuadas y desarrollar planes de contingencia para minimizar los riesgos y así mantener la integridad, confidencialidad y disponibilidad de los servicios informáticos.

B. Antecedentes internacionales

Según la publicación en la revista cubana de ciencias informáticas, en el artículo titulado "requisitos de seguridad para aplicaciones web", en el cual se indica que para los procesos de desarrollo de software se incrementa el riesgo de ostentar posibles vulnerabilidades, por lo que la informaciónque estas aplicaciones procesan deben ser un activo de información crucial para la organización; por lo tanto, se debe tener un análisis de los requisitos para salvaguardar el ciclo de desarrollo en los pilares de la seguridad [6] .

Las tendencias tecnológicas para el desarrollo de aplicaciones están en dirección al desarrollo web, especialmente para el uso de microservicios; en la presente tesis de maestría titulada: "Investigación Estudio de métricas y patrones de seguridad en microservicios" [7], muestra un punto de relevancia para realizar la construcción del protocolo de seguridad para el desarrollo de aplicaciones por los diferentes patrones y métricas analizados.

Por otra parte, según el artículo "Fases de un ataque a un sistema informático" [8], en el cual se mencionan las fases de un ataque a un sistema informático efectuadas con mayor frecuencia; en consecuencia, se arriesga la seguridad de la información recolectada por los diferentes sistemas de información, afectando la confidencialidad, integridad y disponibilidad de la información de las empresas privadas, públicas y estatales.

Igualmente, en el artículo titulado: "Amenazas de seguridad a considerar en el desarrollo de software" de la Universidad Autónoma del Estado de Hidalgo, México[9, p.2], se muestra la importancia a considerar para el desarrollo de software, como lo son las amenazas que existen en cuanto a la privacidad y seguridad de la información, las cuales pueden significar grandes pérdidas económicas y acceso a información confidencial por parte de usuarios sin autorización o la caída de los sistemas.

En relación con una investigación de Lima Perú, titulada: "Análisis de la protección de la información digital de las Fuerzas Armadas en el marco de la Política de Seguridad y Defensa Nacional en la región Lima, 2018" [10], ésta tenía como objetivo principal, analizar la protección de la información digital de los centros de informática del Cuartel General del Ejército del Perú, de la Marina de guerra y de la Fuerza Aérea, en el marco de la ciberseguridad de la Política de Seguridad y Defensa Nacional, en la cual se realizó el análisis de diferentes aristas para investigación, como lo son: políticas de seguridad, infraestructura informática, recursos económicos, amenazas, problemas y las diferentes entidades informáticas.

Por lo tanto, es importante adoptar estas mismas aristas de la investigación para desarrollar planes con el fin de minimizar los riesgos y así mantener la integridad, confidencialidad y disponibilidad de los servicios informáticos.

C. Estándares a nivel mundial

En el ámbito internacional existen estándares, los cuales proponen mejores prácticas, las cuales se han desarrollado con el fin de garantizar que el software se desarrolle de manera segura, minimizando los riesgos de vulnerabilidades y posibles ataques, entre los cuales se destacan los siguientes:

OWASP (Open Web Application Security Project): De acuerdo con Fernández, el "OWASP promueve el desarrollo de software seguro, centrándose principalmente en el "back-end"[11, p. 03].

NIST SP 800-53: El Instituto Nacional de Normas y Tecnología de Estados Unidos (NIST) establece la guía para el cumplimiento de las obligaciones que define la ley federal de protección de la información de Estados Unidos [12, p.1].

BSIMM (Building Security In Maturity Model): A pesar de que no es un estándar en sí mismo, sino un modelo que describe las prácticas de seguridad para el desarrollo de software de empresas, proporciona una evaluación de madurez y ofrece información sobre las mejores prácticas utilizadas en la industria. Como lo expresa Synopsys, es "Una herramienta de evaluación comparativa objetiva y basada en datos, que lo ayuda a crear un mejor programa de seguridad de software" [13, p.1].

El CERT Oracle Secure Coding Standard. Estos estándares se enfocan en crear lineamientos para el desarrollo de software, como lo explican Largo, Mohinmdra, Seacord: son "Pautas específicas para escribir código seguro para Java proporciona reglas diseñadas para eliminar las prácticas de codificación inseguras …"[14, p. 1].

CWE (Common Weakness Enumeration): A pesar de que no es un estándar de desarrollo en sí, se puede catalogar como una lista de debilidades de seguridad comunes en el software. Como lo expresa CWE:

> Es una lista desarrollada por la comunidad de tipos de debilidades de software y hardware. Sirve como un lenguaje común, una vara de medir para las herramientas de seguridad y como una línea de base para los esfuerzos de identiPcación, mitigación, prevención de debilidades. [15, p. 1].

III. PROCEDIMIENTO Ó METODOLOGÍA

La formulación del marco metodológico en una investigación, consiste en descubrir los supuestos del estudio para reconstruir datos, a partir de conceptos teóricos habitualmente operacionalizados. Significa detallar cada aspecto seleccionado para desarrollar dentro del proyecto de investigación que debe ser justificado por el investigador [16, p. 1]. A continuación, se propone la metodología que se llevará a cabo para la presente investigación, en la cual se tratará el proceso de verificación y validación para analizar el problema planteado.

A. Paradigma de Investigación

La investigación se basará en el paradigma positivista, seleccionado, debido a que es el enfoque que mejor se ajusta a las características y requisitos de la investigación.

De acuerdo con [17], el paradigma positivista representa ciertas características que se hace necesario precisar: su interés es explicar, controlar y predecir, la naturaleza de la realidad; la describe como dada, singular, tangible, fragmentable y convergente (p. 31).

El paradigma positivista y su correspondiente enfoque cuantitativo, facilitarán la evaluación del estado actual de las aplicaciones informáticas desarrolladas y en proceso de desarrollo por parte del personal de la Compañía de Desarrollo de Software del Batallón de Interoperabilidad de Comunicaciones y Computación del Ejército Nacional. Esta evaluación se centrará en la seguridad de la información sensible y estratégica de la institución.

B. Tipo de Investigación.

De acuerdo con el alcance de esta investigación, se adoptará el tipo de investigación descriptiva. En ella, se destaca el empleo de la técnica de encuestas aplicadas a expertos en desarrollo de aplicaciones seguras, así como al personal del Ejército Nacional involucrado en el proceso de desarrollo de software.

C. Enfoque de Investigación.

El desarrollo del presente proyecto se llevará a cabo mediante la aplicación de una metodología centrada en el enfoque cuantitativo, el cual ha sido elegido por su pertinencia con respecto a las características y objetivos específicos de la investigación. La meta

principal de este estudio consiste en establecer un estándar de desarrollo seguro de software para las aplicaciones del Ejército Nacional. En este contexto, el enfoque cuantitativo se presenta como la elección más apropiada para abordar eficazmente las tareas planteadas.

D. Diseño de la Investigación

El diseño de investigación pre-experimental, de acuerdo con Ramos, [18], la variable dependiente debe ser medida con algún instrumento en dos momentos: pre y post-test [p.4].

En el próximo paso de la investigación, se procederá con la configuración y aplicación de un diseño pre-experimental, con el fin de obtener respuestas fundamentales para abordar los desafíos en el ámbito de la ciberseguridad. Así mismo, de acuerdo con la problemática planteada, se ejecutará a explorar y evaluar las estrategias, técnicas y mejores prácticas para fortalecer las aplicaciones del Ejército Nacional.

E. Universo

Según Condori - Ojeda [19], el universo o también llamado población objeto, son "Elementos (personas, objetos, programas, sistemas, sucesos, base de dato…) globales, finitos e infinitos" (p. 3).

Por tanto, para el presente proyecto de grado se planteó como universo, la Brigada de Interoperabilidad de Comunicaciones, Computación y Ciberdefensa, el cual cuenta con una 140 efectivos; la referida Brigada, tiene las capacidades de comunicaciones, comando, control, computación, ciberdefensa y guerra electrónica.

F. Población

De acuerdo con [19], trata los "elementos accesibles o unidad de análisis que pertenecen al ámbito especial donde se desarrolla el estudio" (p. 3).

Dentro del trabajo realizado para la presente investigación, la población se define como el Batallón de Interoperabilidad de Comunicaciones y Computación, el cual cuenta con 67 efectivos; el citado Batallón, es el responsable de la gestión y administración, soporte de la infraestructura tecnológica del Ejército Nacional, así como el desarrollo de software a la medida.

G. Muestra

Acorde con lo descrito por [19], la muestra es "Parte representativa de la población, con las mismas características generales de la población" (p. 3):

Se planteó como muestra, la Compañía B, la cual cuenta con 20 efectivos. Es de resaltar, que la mencionada compañía es la responsable del desarrollo de aplicaciones orientadas a apoyar los procesos operacionales y administrativos del Ejército Nacional.

H. Técnicas

Encuesta y análisis documental.

I. Instrumentos para recolección de datos

Encuesta: Cuestionario en línea, Formularios de Google

J. Procedimiento

Figura 1. Fases del procedimiento metodológico

Fase 0: *Análisis de Brecha*

Esta fase es la etapa inicial en la que se llevó a cabo el análisis de los informes de brecha de seguridad sobre el estado actual de las aplicaciones informáticas del Ejército Nacional, y un diagnóstico por medio de una encuesta al personal encargado del desarrollo de software, con el fin de identificar las brechas existentes que podrían afectar la seguridad y la eficacia del desarrollo de las aplicaciones. Este análisis es la base fundamental para alcanzar el objetivo general del proyecto.

Fase 1: *Análisis de Estándares y Mejores Prácticas*

En esta fase se analizaron los estándares y mejores prácticas del ciclo de desarrollo seguro de software NIST Special Publication 800-218 - OWASP versión 4.0, de marzo de 2019. La finalidad es comprender a fondo los enfoques reconocidos y recomendados para garantizar la seguridad en el desarrollo de aplicaciones del Ejército Nacional.

Fase 2: *Creación de Políticas de Ciberseguridad*

En esta fase, se desarrollaron las políticas de ciberseguridad que guiarán el ciclo de desarrollo seguro de aplicaciones del Ejército Nacional. Estas políticas establecerán las directrices, procedimientos y prácticas que deben seguirse en cada etapa del ciclo para garantizar la seguridad de las aplicaciones. Se considerarán las mejores prácticas y estándares previamente analizados, así como las necesidades y requisitos específicos del Ejército Nacional. Las políticas abordarán aspectos como el manejo de datos sensibles, el control de acceso, la autenticación, la integridad de los datos y la mitigación de riesgos en el proceso de desarrollo.

Fase 3: *Definición del Proceso del Ciclo de Desarrollo Seguro*

En esta fase, se definió en detalle el proceso del ciclo de desarrollo seguro específico para el Ejército Nacional. De esta forma, se establecerán las etapas lógicas del ciclo, las actividades a realizar en cada una, los roles y responsabilidades de los servidores del Ejército Nacional involucrados y los entregables esperados en cada fase. El proceso se diseñará teniendo en cuenta las políticas de ciberseguridad establecidas, alineado con las mejores prácticas y estándares internacionales analizados en la Fase 1. Se buscará que el proceso sea coherente, escalable y adaptable a las necesidades cambiantes del Ejército Nacional.

Fase 4: *Selección de Herramientas Estándar para el Desarrollo Seguro.*

En esta fase, se llevará a cabo la selección de las herramientas que formarán parte del estándar para el desarrollo seguro de las aplicaciones del Ejército Nacional. Se evaluarán diferentes soluciones tecnológicas disponibles en el mercado que sean compatibles con el ciclo de desarrollo seguro, definido en la Fase 3.

Se considerarán herramientas para satisfacer los requisitos de seguridad, la interoperabilidad de las comunicaciones y su idoneidad para el entorno del Ejército Nacional.

IV. ANÁLISIS RESULTADOS

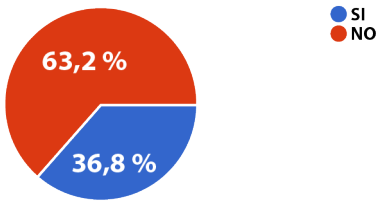
Se realizó una encuesta de carácter politómico, dirigido al personal del Batallón de Interoperabilidad de Comunicaciones y Computación, específicamente a quienes se encuentran encargados del proceso de desarrollo de software; se socializó el conocimiento relacionado con políticas, estándares gubernamentales o internacionales, para el desarrollo seguro de aplicaciones de manera general. Por lo anteriormente mencionado, se realizó un análisis individual a cada pregunta que se aplicó.

A continuación, se presenta cada pregunta de la encuesta aplicada y su respectivo análisis:

1. Pregunta: ¿Está usted actualizado en

el conocimiento sobre la existencia de estándares gubernamentales que regulen y promuevan el desarrollo de software seguro? Los resultados se observan en la Figura 2:

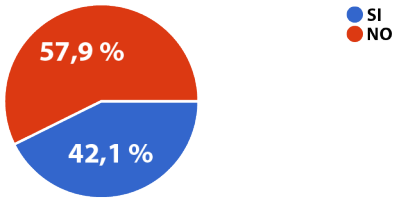
Figura 2. Estadística pregunta N°1 encuesta



Por lo anterior se puede analizar que el 63.2% de los encuestados manifestaron que no tienen conocimiento sobre la existencia de los estándares gubernamentales que promueven el desarrollo seguro del software, a su vez se percibió que el 36.8% de los encuestados sí están familiarizados con dichos estándares.

2. Pregunta: ¿Está usted actualizado en el conocimiento sobre la existencia de estándares en el Ejército Nacional, que regulen el desarrollo de software seguro? Ante la cual se obtuvieron las siguientes respuestas, presentadas en la Fig. 3:

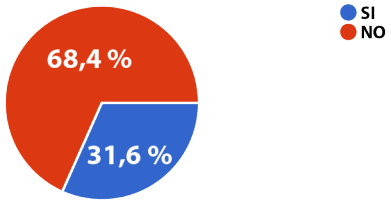
Figura 3. Estadística pregunta N° 2 encuesta



Por lo que se puede analizar que el 57.9% de los encuestados manifiestan que no tienen conocimiento sobre la existencia de los estándares en el Ejército Nacional que promuevan el desarrollo seguro del software; a su vez, se constata que el 42.1% de los encuestados sí están familiarizados con dichos estándares.

3. Pregunta: ¿Tiene conocimiento acerca de estándares de desarrollo de seguro de software, como OWASP o NIST? En la Fig. 4 se observan los resultados a la pregunta N°3:

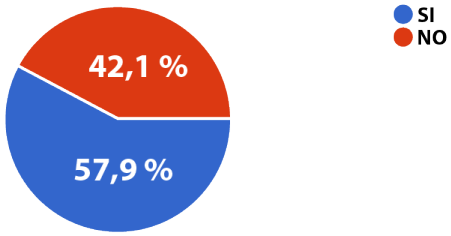
Figura 4. Estadística pregunta N° 3 encuesta



De acuerdo con lo anterior, se analiza que, el 68.4% de los encuestados manifiestan que no tienen conocimiento sobre la existencia de los estándares OWASP y la NIST, los cuales están encargados de generar buenas prácticas para el desarrollo seguro del software; a su vez, el 31.6% de los encuestados afirman que sí están familiarizados con dichos estándares.

4. Pregunta: ¿Se encuentra capacitado con respecto a las funciones, responsabilidades e importancia del desarrollo seguro para el Ejército Nacional? la respuesta se presenta en la Fig.5:

Figura 5. Estadística pregunta N° 4 encuesta

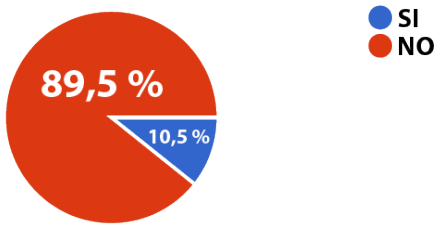


Por lo tanto ,se infiere que el 57.9% de los encuestados manifiestan que sí están capacitados en las funciones y responsabilidades para el desarrollo seguro del software; a su vez se observa que el 42.1% de los encuestados, no han sido capacitados en la responsabilidad que deben tener para

el proceso de desarrollo de aplicaciones.

5. Pregunta: ¿En la Compañía de Desarrollo de Software, existe un documento que establece las políticas para la protección de las infraestructuras sobre desarrollo de software y sus componentes? El resultado arrojó los porcentajes mostrados en la Fig.6:

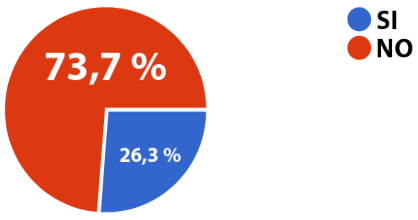
Figura 6. Estadística pregunta N° 5 encuesta



De acuerdo con los resultados, se puede analizar que el 89.5% de los encuestados manifiestan que no cuentan con un documento en el cual se establezcan políticas para el desarrollo seguro del software.

6. Pregunta: ¿La Compañía de desarrollo de software dispone de un documento que abarque la protección de los procesos a lo largo de todo el Ciclo de Vida del Desarrollo de Software (SDLC), incluyendo la seguridad de los componentes de software de código abierto que se está desarrollando? Los resultados se exponen en la Fig.7:

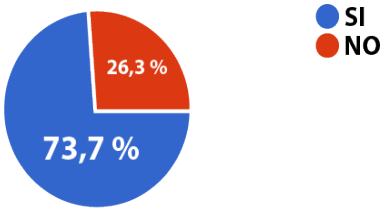
Figura 7. Estadística pregunta N° 6 encuesta



A partir de la anterior Fig. se puede analizar que el 73.7% de los encuestados manifiestan que dentro de la compañía de desarrollo de software, no cuentan con un documento que abarque la protección de los procesos a lo largo de todo el SDLC.

7. Pregunta: ¿En la Compañía de Desarrollo de Software, están claramente definidos los roles y responsabilidades en relación con el Ciclo de Vida del Desarrollo de Software (SDLC)?" Los resultados se observan en la Figura 8:

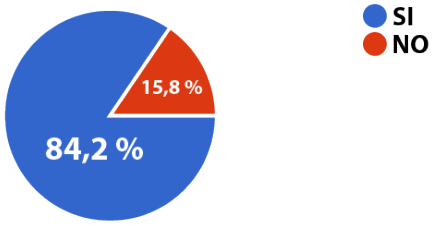
Figura 8. Estadística pregunta N° 7 encuesta



Como se observa, el 73.7% de los encuestados manifiestan que sí tienen definido los roles y responsabilidades para SDLC del software; a su vez, el 26.3% de los encuestados no tiene definido sus roles o responsabilidades dentro de la compañía para el proceso del desarrollo de software.

8. Pregunta: ¿Se lleva a cabo una revisión periódica de todas las funciones y responsabilidades de los miembros en la Compañía de desarrollo de software? La respuesta se encuentra en la Figura 9:

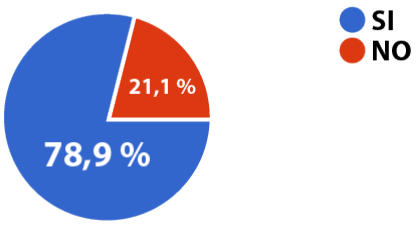
Figura 9. Estadística pregunta N° 8 encuesta



En la Fig. 9, se puede analizar que el 84.2% de los encuestados manifestaron que sí realizan una revisión periódica de sus funciones y responsabilidades para todos los integrantes de la compañía de desarrollo de software.

9. Pregunta: ¿La Compañía de Desarrollo de Software dispone de un repositorio de código que almacena todas las formas de este, incluyendo el código fuente, ejecutable, con acceso restringido solo para el personal autorizado? en la Fig.10, se expone la respuesta a la pregunta 9:

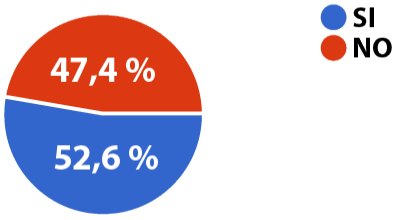
Figura 10. Estadística pregunta N° 9 encuesta



Según las apreciaciones, el 78.9% de los encuestados manifiestan que sí realizan el uso de un repositorio para almacenar sus códigos fuentes como generación de buenas prácticas para el proceso de desarrollo de software y que solo pueden ingresar algunas personas. Esto sugiere que la mayoría de los encuestados reconocen la importancia de utilizar un repositorio para gestionar y almacenar sus códigos fuente, lo que puede contribuir a una mejor organización, colaboración y seguimiento de cambios en el proceso de desarrollo de software. Además, el hecho de restringir el acceso a algunas personas indica una preocupación por la seguridad y la gestión adecuada de los recursos en el repositorio.

10. Pregunta: ¿La Compañía de desarrollo de software lleva a cabo análisis de riesgos o identificación de vulnerabilidades de seguridad durante el proceso para desarrollo de aplicaciones?" A continuación, en la Fig. 11, se exponen las respuestas arrojadas por el personal encuestado:

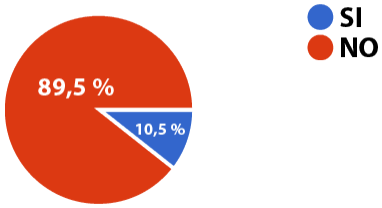
Figura 11. Estadística pregunta N° 10 encuesta



Se puede observar que el 52.6% de los encuestados indican que realizan un análisis de riesgos o identifican vulnerabilidades durante el proceso de SDLC. Sin embargo, el 47.7% no lleva a cabo estos análisis, lo que podría resultar en malas prácticas o brechas durante el desarrollo de aplicaciones.

11. Pregunta: ¿La Compañía de desarrollo de software tiene un "programa de divulgación de vulnerabilidades" que permite a los investigadores de seguridad conocer el programa y reportar posibles vulnerabilidades de manera efectiva? En la Fig. 12, se observan los resultados:

Figura 12. Estadística pregunta N° 11 encuesta



El 89.5% de los encuestados respondieron negativamente a la pregunta sobre la existencia de un programa de divulgación de vulnerabilidades. Esto indica que los investigadores de seguridad no cuentan con un mecanismo claro para conocer el programa y reportar posibles vulnerabilidades.

Políticas y lineamientos de ciberseguridad para el ciclo de desarrollo seguro de aplicaciones del Ejército Nacional

Se diseñaron siete políticas para establecer pautas de desarrollo seguro, adaptadas de los análisis de los estándares NIST Special Publication 800-218 y de la versión 4.0 de OWASP. Estas políticas definen un conjunto de directrices que abarcan herramientas, responsabilidades y métodos necesarios para garantizar un desarrollo seguro.

Estas políticas serán esenciales para el BAICC "Batallón de Interoperabilidad de Comunicaciones y Computación" que realiza procesos de desarrollo de software para proteger la confidencialidad, integridad y disponibilidad de la información que se almacena, procesa y trasmite los aplicativos.

TABLA I. Resumen de políticas para el desarrollo seguro.

ID	POLÍTICA	OBJETIVO
PDS-P1	Sistema de control de versiones	Permite garantizar la integridad y trazabilidad del código fuente.
PDS-P2	Definición de roles y responsabilidades	Asigna las responsabilidades claras y específicas para el SDLC
PDS-P3	Factor de autenticación	Proteger la confidencialidad de los datos.
PDS-P4	Verificación de Código Malicioso	Detectar y corregir vulnerabilidades del código fuente.
PDS-P5	Protección de datos	Permite la garantía de integridad de los datos.
PDS-P6	Codificación de código	Permite la prevención de ataques.
PDS-P7	Gestión de Sesiones	Garantiza la correspondiente identidad de los usuarios.

La implementación de las políticas descritas en la Tabla 1, contribuye a mitigar el riesgo de ciberataques a las plataformas desarrolladas, garantizando así la seguridad de la información de los usuarios de estos sistemas informáticos.

Cada política se basa en estándares específicos diseñados para alcanzar este objetivo.

TABLA II. Estándares de la política PDS-P1.

ESTÁNDAR	OBJETIVO
PDS-P1-E1	Establecer la implementación de alguna herramienta de control de versiones.
PDS-P1-E2	Establecer la estructura mínima de las ramas requeridas por cada proyecto.
PDS-P1-E3	Establece como se debe realizar la documentación para las actualizaciones de código fuente.
PDS-P1-E4	Establece la correcta gestión de permisos en la herramienta de control de versiones.

El conjunto de estándares que se relacionan en la tabla 2, permite contar con mejores prácticas para el control y versionamiento del código fuente de cada aplicación desarrollada.

TABLA III. Estándares de la política PDS-P2.

ESTÁNDAR	OBJETIVO
PDS-P2-E1	Asegurar que cada proyecto de desarrollo de software cuente con un gerente de proyecto.
PDS-P2-E2	Asegurar que cada proyecto de desarrollo de software cuente con un analista.
PDS-P2-E3	Asegurar que cada proyecto de desarrollo de software cuente con desarrolladores.
PDS-P2-E4	Asegurar que cada proyecto de desarrollo de software cuente con un evaluador del software.
PDS-P2-E5	Asegurar que cada proyecto de desarrollo de software tenga un propietario o responsable por la parte funcional.

Los estándares presentados en la Tabla 3 facilitan la asignación y garantía de responsabilidades específicas para cada función en los proyectos de desarrollo de software. Esto asegura la integridad de los requisitos de seguridad en todas las etapas del ciclo de vida del desarrollo de software.

TABLA IV. Estándares de la política PDS-P3.

ESTÁNDAR	OBJETIVO
PDS-P3-E1	Garantizar que todo desarrollo cuente con un módulo de seguridad
PDS-P3-E2	Debe asegurar que las contraseñas tengan características mínimas.
PDS-P3-E3	Garantizar que las contraseñas de acceso se encuentren cifradas
PDS-P3-E4	Garantizar que las aplicaciones tengan la opción de uso de doble autenticación.

Los estándares presentados en la Tabla 4, tienen como objetivo mejorar el uso de contraseñas seguras en los aplicativos de software, lo que contribuye a prevenir el acceso no autorizado.

TABLA V. Estándares de la política PDS-P4.

ESTÁNDAR	OBJETIVO
PDS-P4-E1	Garantiza la identificación y mitigación de vulnerabilidades del código fuente.
PDS-P4-E2	Garantiza la identificación y mitigación de vulnerabilidades de las aplicaciones desplegadas.
PDS-P4-E3	Garantiza la protección de los datos sensibles.
PDS-P4-E4	Garantiza que se debe realizar un análisis SCA
PDS-P4-E5	Garantiza utilizar otras herramientas de análisis para mejorar la seguridad de las aplicaciones.

Los estándares presentados en la Tabla 5, facilitan la identificación de vulnerabilidades, lo que contribuirá a reducir el riesgo de sufrir ataques cibernéticos en las aplicaciones desarrolladas.el riesgo de sufrir ataques cibernéticos en las aplicaciones desarrolladas.

TABLA VI. Estándares de la política PDS-P5.

ESTÁNDAR	OBJETIVO
PDS-P5-E1	Garantiza la integridad de los datos
PDS-P5-E2	Garantiza la reducción de la exposición de datos.
PDS-P5-E3	Garantiza la seguridad de las comunicaciones de las aplicaciones.

El conjunto de estándares relacionados en la tabla 6, asegura la integridad de la información que se procesa, almacena y envía en las aplicaciones.

TABLA VII. Estándares de la política PDS-P6.

ESTÁNDAR	OBJETIVO
PDS-P6-E1	Garantizar la protección de los datos que entran como los que salen
PDS-P6-E2	Garantiza la prevención de extracción de información.

Estos estándares, descritos en la Tabla 7, se enfocan en garantizar que las aplicaciones realicen la codificación de salida, lo que dificulta la extracción de datos confidenciales de la información.

TABLA VIII. Estándares de la política PDS-P7.

ESTÁNDAR	OBJETIVO
PDS-P7-E1	Garantiza que el proceso de autenticación de los usuarios sea seguro.
PDS-P7-E2	Garantizar que todos los token queden asegurados de manera adecuada.
PDS-P7-E3	Asegurar que las sesiones inactivas se cierren de manera exitosa para asegurar la disponibilidad de la aplicación.
PDS-P7-E4	Realizar la implementación de re-autenticación del usuario.

El conjunto de estándares que se relacionan en la Tabla 8, se enfocan en salvaguardar los sistemas informáticos contra amenazas de seguridad vinculadas a la falsa autenticación y la autorización de usuarios no autorizados.

• *Proceso de ciclo de desarrollo*

El proceso define de manera detallada las etapas lógicas de construcción, los roles involucrados y el análisis de herramientas para el ciclo de desarrollo seguro de aplicaciones, tomando como referencia las mejores prácticas de OWASP y NIST.

En consecuencia, se han definido cinco perfiles, cada uno con tareas específicas durante el proceso de desarrollo seguro. Estos perfiles son los siguientes:

Gerente de proyecto: Es el responsable de realizar el proceso de supervisar, examinar y proyectar el SDLC, para que el producto se desarrolle con los requisitos de seguridad.

Analista: Es el encargado de recopilar, documentar y analizar los requisitos de seguridad del SDLC.

Desarrolladores: Son los indicados de desarrollar el software, siguiendo las medidas de seguridad definidas.

Evaluador del software: Es el responsable de realizar los diferentes análisis dinámicos o estáticos, para identificar errores o vulnerabilidades en el código del software.

Propietario de productos: Es el funcionario que realiza las pruebas en conjunto con el personal de desarrolladores y operaciones, para garantizar que el software sea seguro y funcional.

Así mismo, se propusieron diferentes tipos de herramientas, como:

Las herramientas de tipo IAST, permiten realizar el proceso de identificación de las vulnerabilidades de las aplicaciones informáticas en tiempo real, con el fin de prevenir y mitigar ataques y fortalecer la seguridad de las aplicaciones.

Las herramientas de tipo SAST, facilitan la realización de pruebas de seguridad. Estas herramientas se centran también en la revisión del código fuente, pero dicha revisión se efectúa a nivel estático para identificar vulnerabilidades y riesgos de seguridad.

Las herramientas de tipo DAST, realizan pruebas de seguridad que simulan ataques a una aplicación en tiempo real, para identificar posibles vulnerabilidades.

Las herramientas de tipo SCA, cuentan con un proceso de enfoque orientado a la identificación, evaluación y rastreo de los componentes que son implementados en el software, realizando una comprensión detallada de la estructura de la aplicación.

El proceso CI, Automatiza la integración del código fuente en un repositorio central, garantizando la compatibilidad del código, la detección y corrección rápida de errores, y el establecimiento de una base sólida para la colaboración entre equipos de desarrollo.

El proceso CD, Automatiza el proceso de entrega de nuevas versiones del software a los entornos de producción de manera eficaz, lo que ayuda a reducir riesgos y mejorar la eficiencia en la entrega a los usuarios finales.

La herramienta de control de versiones GitLab, ofrece un conjunto de beneficios para realizar la trazabilidad e integridad de todo el código fuente, para los proyectos de SDLC y permite al desarrollador tener una o varias copias del código.

Con los roles y herramientas analizadas anteriormente, se permite tener un aspecto clave para el proceso de desarrollo seguro de software, permitiendo la detección de vulnerabilidades desde la primera versión y una revisión continua, así como la gestión de proyectos y la colaboración efectiva entre equipos de desarrollo. A continuación, se procede a realizar la inclusión del proceso lógico desarrollado, como se puede ver en la Figura 13.

Figura 13. Código QR del BPM para el desarrollo seguro.

V. CONCLUSIONES

El análisis de brecha enfocado al personal encargado de desarrollo de software del Ejército Nacional con respecto al estado actual de las aplicaciones informáticas del Ejército Nacional, permitió obtener una visión de las áreas a mejorar y de las posibles fallas en los procesos asociados en el desarrollo de aplicaciones. Este análisis ha arrojado una serie de vulnerabilidades sobre aspectos críticos que requieren atención y acción, permitiendo así una base sólida para la toma de decisiones y la implementación de mejoras significativas. Los hallazgos resultantes de este análisis, son de carácter confidencial para la institución.

Los estándares internacionales NIST Special Publication 800-218 y OWASP versión 4.0 de marzo de 2019, generan un profundo conocimiento acerca de las mejores prácticas del ciclo de desarrollo seguro, siendo un componente esencial para fortalecer la seguridad y la eficiencia en el proceso de desarrollo de software dentro de la institución.

La elaboración de políticas y estándares establecen un marco sólido y coherente para garantizar la seguridad en el ciclo de desarrollo de las aplicaciones. El estándar planteado no solo cumple con los estándares internacionales de seguridad cibernética, sino que también, se han adaptado a las necesidades específicas y a la naturaleza confidencial de las operaciones del Ejército Nacional.

Recomendaciones

El estándar para el ciclo de desarrollo seguro de aplicaciones en el Ejército, aporta a la reducción de los riesgos de seguridad ante los cuales se enfrentan las aplicaciones y por tanto, la información operacional y administrativa de la Fuerza.

Es crucial que el estándar para el ciclo de desarrollo seguro de aplicaciones sea implementado correctamente, monitoreado de forma continua y actualizado según sea necesario para mantenerlo alineado con los cambios tecnológicos constantes o los riesgos emergentes.

Con el fin de permitir una adecuada implementación del estándar, se debe realizar su inclusión, con base en las Directivas permanentes 200 y 201 del Ejército Nacional.

Es necesario realizar análisis continuos en diversas aplicaciones para identificar y corregir posibles vulnerabilidades. Estos análisis deben llevarse a cabo siguiendo las pautas establecidas en el estándar para el ciclo de desarrollo seguro de aplicaciones en el Ejército.

Es fundamental reconocer la importancia de contar con marcos de referencia como OWASP y NIST en materia de seguridad del software. Estos marcos ofrecen directrices y recomendaciones que contribuyen al desarrollo de software más seguro.

VI. REFERENCIAS

[1] Olmos Sosa, Oiris; Ivonne, Quesada Perez, «Universidad Externado de Colombia,» 2019. [En línea]. Available: https://bdigital.uexternado.edu.co/server/api/core/bitstreams/f69bc021-8fa3-4859-9dab-008e0b2d1074/content. [Último acceso: 08 05 2023].

[2] Aguilar Quintero, Norly Alejandra, «Universidad Francisco de Paula Santander ocaña,» 2019. [En línea]. Available: http://repositorio.ufpso.edu.co/bitstream/123456789/419/1/32686.pdf. [Último acceso: 08 05 2023].

[3] Cortez Bolivar, William;Silva Triviño, Oscar, «Universidad Externado de Colombia,» 2022. [En línea]. Available: https://bdigital.uexternado.edu.co/server/api/core/bitstreams/77fec933-c8d2-48e8-bcbf-12e8134d7485/content. [Último acceso: 08 05 2023].

[4] Villa trujillo, Ruben Dario, «Instituto Tecnológico Metropolitano,» 2019. [En línea]. Available:https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/4463/Rep_Itm_mae_Villa.pdf?sequence=1. [Último acceso: 08 05 2023].

[5] Barbosa Fernández, Miguel Ángel, «Universidad Francisco de Paula Santander Ocaña,» 2020. [En línea]. Available: http://repositorio.ufpso.edu.co/xmlui/bitstream/handle/123456789/2259/34237.pdf?sequence=1. [Último acceso: 08 05 2023].

[6] Yisel Niño, Nemery Silega, «Revista Cubana de Ciencias Informáticas,» 10 09 2018. [En]. Available: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992018000500015&lang=es. [Último acceso: 07 05 2023].

[7] Penagos Sanchez, Juana Victoria, «rinacional.tecnm.mx,» 04 01 2023. [En línea]. Available: https://rinacional.tecnm.mx/handle/TecNM/4960. [Último acceso: 08 05 2023].

[8] j. c. Condori, «https://www.umsa.bo/,» 2020. [En línea]. Available: https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/107/93. [Último acceso: 08 05 2023].

[9] Gabriel Sanchez Bautista,Lizbeth Ramirez chavez, «repository.uaeh.edu.mx,» 05 01 2022. [En línea]. Available: https://repository.uaeh.edu.mx/revistas/index.php/xikua/article/view/8118. [Último acceso: 07 05 2023].

[10] Villarrubia Marcelo, Gabriel Ángel, «Google Academico,» 2021. [En línea]. Available: http://200.60.64.68/bitstream/handle/20.500.13097/254/TESIS%20CRL%20VILLARRUBIA.pdf?sequence=1&isAllowed=y#page=65&zoom=100,108,825. [Último acceso: 07 05 2023].

[11] I. Camilo Fernandez, "The OWASP Foundation OWASP Introducción a OWASP", 2004. [En línea]. Disponible en: http://www.owasp.org.

[12] C. 94043 Google LLC 1600 Amphitheatre Parkway Mountain View, "NIST 800-53", https://cloud.google.com/security/compliance/nist800-53?hl=es, el 26 de mayo de 2022.

[13] Synopsys Home Page, "Building Security In Maturity Model (BSIMM)", https://www.synopsys.com/software-integrity/software-security-services/bsimm-maturity-model.html, 2023.

[14] D. M. R. C. S. Fred largo, "The cert oracle secure coding standard for java", https://dl.acm.org/doi/book/10.5555/2049728, el 18 de septiembre de 2011.

[15] CWE, "2023 CWE Top 25 Most Dangerous Software Weaknesses", https://cwe.mitre.org/, el 1 de agosto de 2023.

[16] Á. E. Azuero Azuero, "Significatividad del marco metodológico en el desarrollo de proyectos de investigación", Revista Arbitrada Interdisciplinaria Koinonía, vol. 4, núm. , p.110, jul. 2019, doi: 10.35381/r.k.v4i8.274.

[17] "El Positivismo y la Investigación Científica he positivism and the scientiic research".

[18] C. Ramos-Galarza, "Editorial: Diseños de investigación experimental", CienciAmérica, vol. 10, núm. 1, pp. 1–7, feb. 2021, doi: 10.33210/ca.v10i1.356.ciAmérica, vol. 10, núm. 1, pp. 1–7, feb. 2021, doi: 10.33210/ca.v10i1.356.

[19] Condori-Ojeda, «Universo, población y muestral», 2015. [En línea]. Available: url: https://www.aacademica.org/cporfirio/18.pdf-

2. Artículos
de Revisión Bibliográfica

Revista TECNO**ESCOM**
ISSN 2711-0761. Vol. 6. No. 1

EXPLORANDO EL UNIVERSO DEL IOT: HISTORIA, FUNDAMENTOS Y DESAFÍOS ACTUALES

SM(R) Oscar Javier Jerez González
Docente Educación Militar
oscarjerezgonzalez@cedoc.edu.co

RESUMEN- ***La presente revisión sistemática tiene como propósito hacer una exploración de los aspectos relevantes de IoT como el origen, evolución y los desafíos que actualmente enfrenta esta tecnología. Mediante la metodología aplicada, se revisaron 43 artículos que fueron clasificados por temáticas, idioma (inglés y español) y país de origen. Se tomaron como ejes temáticos de desarrollo, los fundamentos de IoT, arquitectura y protocolos de comunicación y de aplicación, las utilidades de IoT en distintos ámbitos y algunas generalidades de seguridad. Se considera como resultado importante que IoT es una tecnología que ha modificado la forma de vida humana y la manera como se llevan a cabo diversas actividades. Es una tecnología adaptativa a las diferentes tecnologías emergentes, y cada día la seguridad en IoT está cobrando más importancia por parte de los fabricantes de dispositivos y por parte de los actores principales, aunque sigue siendo un desafío.***

Palabras clave: : IoT, arquitectura, protocolos, aplicaciones, seguridad.

Abstract— The purpose of the present systematic review is to explore the relevant aspects of IoT, including its origin, evolution, and the challenges this technology currently faces. Throughout the applied methodology, 43 articles were reviewed and classified by topics, language (English and Spanish), and country of origin. Architecture and communication protocols, IoT usefulness in different fields, and some security generalities were taken as theme axes. It is considered an important result that IoT is a technology that has modified our lifestyle and the way we develop different activities. It is an adaptive technology to the different emergent technologies, and every day, security in IoT is becoming more important on the part of device manufacturers as well as main actors, although it remains a challenge.

Keywords- IoT, Architecture, protocols, applications, security.

I. INTRODUCCIÓN

En el año 1999 por primera vez Kevin Ashton usó el término Internet of Things (IoT), en el caso específico en el que se agregó tecnología por radio frecuencia (RFDI) a la cadena de suministro de Procter y Gamble [1, p.11], para referirse a la interconectividad que tienen los dispositivos a través de internet. Sin embargo, la idea que amalgama el IoT propiamente dicho, ya se había concebido mucho antes, aún desde el origen mismo de las comunicaciones inalámbricas, como lo manifiesta Nikola Tesla en 1926:

> Cuando la tecnología inalámbrica se aplique perfectamente, toda la Tierra se convertirá en un cerebro gigante, que de hecho lo es, ya que todas las cosas son partículas de un todo real y rítmico... y los instrumentos a través de los cuales podremos hacer esto serán asombrosamente simples en comparación con nuestros teléfonos actuales. Un hombre podrá llevar uno en el bolsillo de su chaleco [2, p.288].

Evans [3] describe que el IoT se materializó entre 2008 y 2009, cuando el número de dispositivos conectados a internet, superó al número de personas existentes en el planeta:

En el siglo XXI, de la mano con la Inteligenci Artificial, el IoT está alcanzando su mayor auge. Por ello, surge la necesidad imperante desde el punto de vista de los actuales desafíos de la información y la comunicación, con la integración de servicios y dispositivos, de comprender los rudimentos de esta tecnología y, cómo es posible a futuro contribuir en la solución de una gran problemática que aqueja el presente, y es la vulnerabilidad de la información de los usuarios que en su interacción diaria con los distintos dispositivos, están sujetos a ciberataques de distintos niveles, situación que puede estar afectando "el despliegue masivo de los productos y servicios de internet de las cosas"[4].

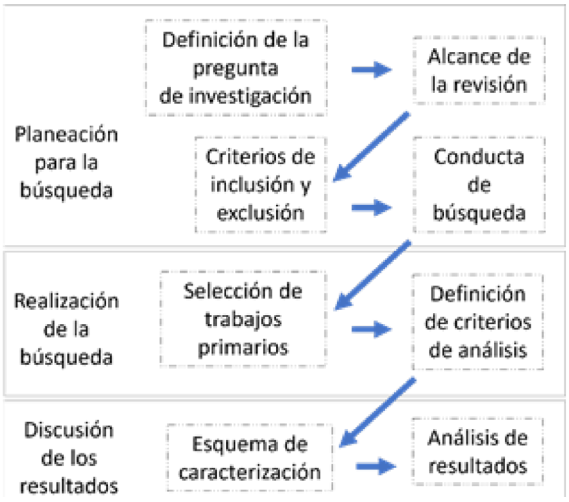
El presente artículo tiene como propósito, hacer una revisión sistemática de bibliografía de tipo cualitativa, para analizar el origen y evolución, así como una identificación de la arquitectura, algunas de las tecnologías desarrolladas e implementadas, generalidades y retos de la seguridad física y de lainformación y algunos casos de éxito que se han planteado en el Internet of Things IoT, o en español, Internet de las cosas IdC.

Se estima necesario consolidar los fundamentos generales que sustentan a la tecnología IoT, no solo desde la configuración física en cuanto a las redes de sensores inalámbricos que recopilan datos sino, contemplando además las distintas tecnologías que validan su comunicación, y cómo al estar soportada sobre IPv6 para garantizar la interoperabilidad entre los distintos dispositivos, se causan vulnerabilidades y amenazas a los usuarios dado que el internet de las cosas es de acceso público. Sin embargo, surgen propuestas que presentan contramedidas a estos aspectos y que son de interés en la presente revisión.

II. METODOLOGÍA

El presente artículo es el resultado de una revisiónsistemática de tipo cualitativa, que contempló 43fuentes bibliográficas en total, basada en el método de Bárbara Kitchenham, quien propone tres fases: "1) planificación de la búsqueda, 2) realización de la búsqueda y, 3) presentación del informe de revisión", descritos en la Figura 1 [5].

Figura 1. Procesos del Mapeo Sistemático [6].



Fuente: elaboración propia, basada en la fuente de referencia.

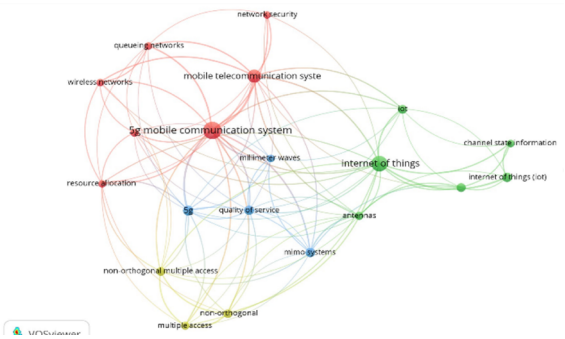
Para atender a las dos primeras fases de la revisión: planificación y realización de la búsqueda, fueron tenidos en cuenta los aspectos que se relacionan a continuación.

A. Estrategias de búsqueda

Se definió la ecuación de búsqueda para identificar los artículos de interés, bajo las estructuras: "IoT" AND ("Technology & Architecture" OR "Massive Device Connectivity IoT"); "History AND Evolution of IoT" OR "IoT Technology & Architecture" y, sus posibles variantes. Las 43 fuentes seleccionadas para la presente revisión tienden a resolver las preguntas: ¿Cuál es el significado del Internet de las Cosas? ¿Cuáles son los elementos que componen el Internet de las Cosas? ¿Hay una arquitectura definida para el Internet de las Cosas? ¿Cómo garantizar la protección de datos personales en un entorno IoT? ¿Qué desafíos

representan la masificación de los productos y servicios IoT?, obteniendo la correlación mostrada en la Figura 2.

Figura 2. Mapa de Coorrelación de Etiquetas de las 43 fuentes bibliográficas, usando VOSviewer.



Fuente: elaboración propia, usando VOSviewer

Para atender a las dos primeras fases de la revisión: planificación y realización de la búsqueda, fueron tenidos en cuenta los aspectos que se relacionan a continuación.

B.Bases de datos y fuentes de la revisión

Las bases tomadas como referencia, se relacionan en la Tabla 1, y se puede observar en la Figura 3, la densidad de artículos extraídos de cada fuente.

TABLA I. Relación de las bases de datos o fuente de la información consultadas

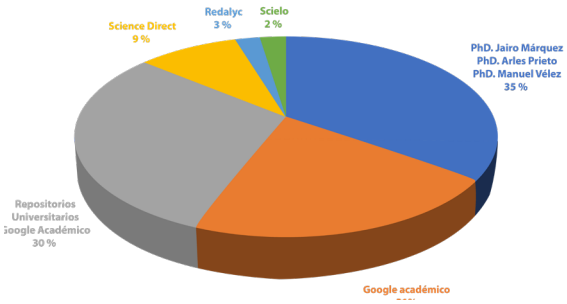
BASE DE DATOS	DESCRIPTORES	N° DE ARTÍCULOS
Google Académico	IoT Fundamentos - Arquitectura - Protocolos de comunicación	9
Repositorios Universitarios - Google Académico	IoT Fundamentos - Arquitectura - Protocolos de comunicación	13
Fuente externa - Ingenieros expertos	Tecnologías y Ciberseguridad IoT	15
Science direct	IoT - Arquitectura - Protocolos de comunicación	4
Redalyc	IoT Fundamentos - Arquitectura -	1
Scielo	IoT Fundamentos - Arquitectura – Implementación de IoT	1

Fuente: elaboración propia.

Cabe destacar que la presente revisión contempla las recomendaciones de fuentes bibliográficas que hacen parte del repositorio personal de tres ingenieros expertos en el tema de interés, o en su defecto, fueron facilitadores de sus propias publicaciones, así:

Experto 1: PhD. Jairo Eduardo Márquez Díaz
Experto 2: PhD. Arles Prieto Moreno
Experto 3: PhD. Manuel Andrés Vélez Guerrero

Figura 3. Porcentaje de artículos consultados en las bases de datos.



Fuente: elaboración propia.

Como se observa en la Figura 3, el 51% de

los recursos bibliográficos fueron extraídos de Google Académico, el 14% de bases de datos (consultores bibliográficos) y el 35% de la información suministrada por los expertos, considerados aquí como fuentes externas.

C. Criterios de inclusión

Se establecieron como criterios de inclusión, los siguientes:

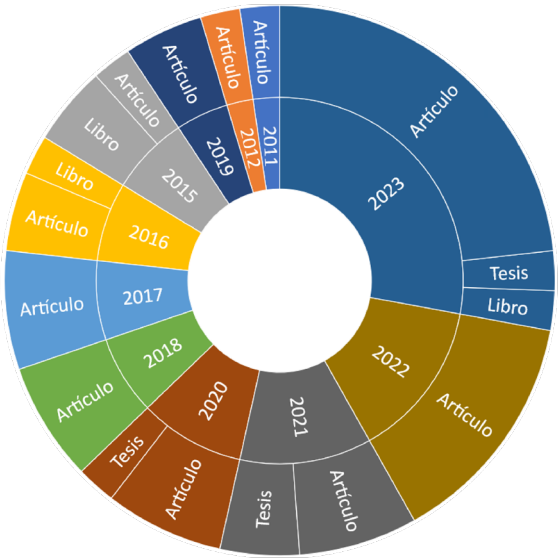
a. Se examinaron publicaciones dirigidas específicamente al desarrollo e implementación del Internet de las Cosas, y últimas tecnologías relacionadas con el empleo de sensores, actuadores, comunicación bidireccional y algunos temas secundarios que fueron derivando de estos y, la aplicación de tecnologías e industria digital.

Se hallaron artículos, libros y tesis de repositorios de Universidades, cuya literatura aborda los orígenes y fundamentos básicos del Internet de las Cosas IdC o IoT, conectividad masiva, tecnologías y arquitectura IdC o IoT, protocolos de comunicación y seguridad en IdC o IoT, y aplicaciones actuales de IdC o IoT. Como ya se comentó, se consultó con tres ingenieros expertos en el tema, quienes de su repositorio personal facilitaron algunos recursos bibliográficos que cumplían con los criterios aquí descritos. El 91% son artículos, el 9% son libros y el 11% son tesis.

b. Se contempló la información publicada en inglés y español desde los inicios de IdC o IoT año 2011, hasta el año 2023. El 58% son publicaciones en español y el 42% son publicaciones en inglés.

c. No se limitó el país de origen, teniendo en cuenta que frente a algunas temáticas, no se encuentra literatura abundante.

Figura 4. Caracterización del tipo de publicaciones por año.

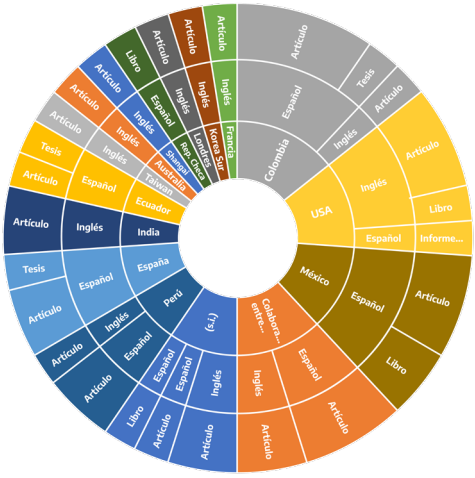


Fuente: elaboración propia.

En la Figura 4, se caracterizan los artículos seleccionados para revisión, de acuerdo con el año y el tipo de publicación. El 18.6% de las publicaciones revisadas, son de los años 2011 a 2016, al igual que el porcentaje de publicaciones hechas durante los siguientes tres años, entre 2017 y 2019; por otra parte, el 9.3% son publicaciones del año 2020; el 11.6%, corresponde al año 2021, el 14% es del año 2022 y el 27.9% es de la anualidad 2023.

Es de resaltar, que no solo para el grupo de artículos seleccionados se tiene esta tendencia en la producción bibliográfica por año, sino que es un comportamiento generalizado. En los últimos cuatro años, el número de publicaciones que contemplan el tema, ha tenido un crecimiento vertiginoso, como se evidenncia en el diagrama solar de la Figura 4. En este sentido, el IoT es un tema que cada vez está llamando más la atención de los académicos.

Figura 5. Relación de publicaciones revisadas con respecto al país de origen.



Fuente: elaboración propia.

En la Figura 5, se observan las publicaciones revisadas en relación con el país de origen, el idioma y el tipo de publicación. El 37.2% es de Latinoamérica, donde las publicaciones de Colombia representan el 16.3%; el 14% son de Europa, en la misma proporción, y el 14%, son el resultado de colaboraciones entre instituciones de diferentes países. Así mismo, el 11.63% es de Estados Unidos; y en Asia, el 9.3% son publicaciones que no refieren un país de origen (s.i.). Po último, el 2.33% son publicaciones de Australia. Es de resaltar, que el número de publicaciones cuyo país de origen es Colombia, sobresalen por su calidad. Ocurre de igual forma, en la publicación de Saavedra [7] *et.al.*

B. Criterios de exclusión

Para los propósitos de la presente revisión, se contempló un número límite de 50 artículos. Se consideraron artículos que fuesen publicados en revistas indexadas para garantizar la calidad, así como tesis de los últimos 3 años, pertenecientes a repositorios universitarios. Así mismo, los libros relacionados en esta revisión, fueron sugeridos por los expertos consultados, atendiendo los siguientes criterios de exclusión:

a) Temáticas

Se excluyeron artículos que profundizaran el tema de sistemas de monitoreo en IoT, que, aunque es un tema de gran relevancia, es de tal grado de amplitud que amerita ser trabajado de manera independiente. Se excluyeron además los temas de consumo de energía en la implementación tecnológica de IoT, donde se aborda el IoT verde, ciudades y hogares inteligentes.

b) Principales limitaciones

Algunos artículos de interés demandan un alto costo para su acceso.

III.RESULTADOS

A. Fundamentos de IoT

a) Breve contextualización del Internet de las Cosas (IoT).

Como aspecto inicial, es importante reconocer a qué se le da el nombre de Internet de las Cosas, descrito habitualmente por su sigla IoT o IdC, teniendo en cuenta que ha ido evolucionando conforme su progresiva implementación.

Cabe retomar aquí la idea de Kevin Ashton en 1999, quien por primera vez enunció el IoT [8], cuando vislumbró que a partir de la tecnología RFID (Radio Frequency IDentification) los dispositivos de una cadena de suministros -mediante sensores -, podían emitir información que fuera empleada para el conteo y rastreo de productos. Así, Ashton usó el término "Internet de las cosas" para referir un sistema en el cual objetos del entorno físico, podían establecer conexión a la Internet mediante el uso de sensores y protocolos de comunicación.

Weber en 2010 [10], propone una de las primeras definiciones, así: IoT (Internet of things/ Internet de las cosas) es una arquitectura

emergente basada en la Internet global que facilita el intercambio de bienes y servicios entre redes de la cadena de suministro, que tiene un impacto importante en la seguridad y privacidad de los actores involucrados (p.23); es de resaltar la visión que tiene el autor sobre lo que en años recientes hemos visto materializado en cuanto a IoT, específicamente a nivel industrial.

Luego, como lo describe Evans [3], surge en 2011 el concepto que plantea el IBSG de Cisco, dentro de los primeros intentos por definir el IoT, como "el punto en el tiempo en el que se conectaron a Internet más 'cosas u objetos' que personas". Surge así la idea de que los objetos que rodean al ser humano, "tienen la capacidad" de capturar datos que pueden ser interconectados de manera masiva para transmitir esos mismos datos, adicionalmente a todo lo que en adelante puede derivar de esa interconexión.

En 2012, Cama, De la-Hoz y Cama [8],[9], proponen que desde el punto de vista de algunos investigadores, el IoT es un modelo que abarca a las tecnologías de comunicación inalámbrica, como las redes de sensores inalámbricos, redes móviles y actuadores, con cada uno de los elementos denominados 'objeto o cosa' y con una dirección única, refiriéndose a la posibilidad de asociar la MAC a cada dispositivo en la web; definición que sugiere una visión más amplia y aporta a los dos conceptos referidos anteriormente.

En la actualidad, ya se concibe que el Internet de las cosas (IoT) es una tecnología revolucionaria que impulsa los avances en las telecomunicaciones y mejora la calidad de vida de las personas en todo el mundo [10]. En este orden de ideas, se puede observar que en el principio, el IoT fue considerado como un sistema de interconexión de dispositivos, pasando luego a considerarse como una arquitectura emergente, luego como un modelo tecnológico y finalmente, como una tecnología que tiene la capacidad no solo de modificar el modo de vida, sino también la economía en todo el planeta [7,8,11], y muy seguramente, con la capacidad de influir en las políticas gubernamentales.

El alcance que tiene el IoT para propiciar estas transformaciones, estaría fundamentado en tres pilares: la densidad de los datos recopilados mediante las redes de sensores, la analítica de esos datos y, la automatización de los procesos [12].

b) Importancia creciente en la interconexión de dispositivos

Resulta interesante observar a lo largo del tiempo, cómo han surgido visionarios en el campo de los paradigmas tecnológicos, cuyas innovaciones han tenido un gran impacto al modificar la capacidad de adaptación humana y, en consecuencia, el mejoramiento de su calidad de vida.

Desde hace casi un siglo, Tesla logró imaginar cómo cambiaría el mundo a partir de sus descubrimientos [2, p.288]. Hoy, no solo se ve materializado su ideal, sino también, se ha incentivado el perfeccionamiento de la interconexión de las redes de sensores mediante RFID, creando dispositivos electrónicos cada vez más versátiles, autónomos y con la capacidad de adaptarse a las necesidades del usuario [9], [13], generando y procesando cantidades de información de magnitudes que sobrepasan la capacidad de estimación.

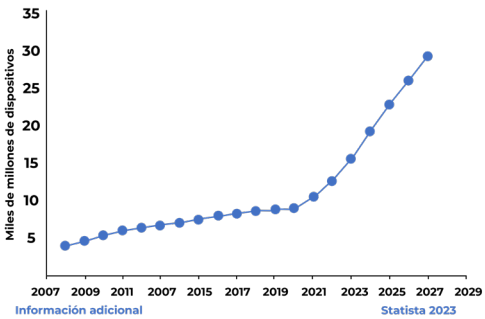
Así mismo, es importante destacar la gran importancia de la interconexión de dispositivos, ya que los datos capturados por los sensores se convierten en información que aporta sabiduría atemporal para el ser humano. Esta información trasciende en la evolución de la humanidad y debería llevar siempre beneficios para una sociedad en constante crecimiento, consciente de la necesidad de crear ambientes sustentables y sostenibles para garantizar la permanencia de la vida de todos los seres [3, p.7].

Actualmente, la información es

considerada un activo más de las empresas y las instituciones; la posibilidad que ofrece IoT, y más aún de la mano con la Inteligencia Artificial [14, p.16], abre un mundo de posibilidades, que deberían propender por una efectiva calidad de vida de los seres vivos y la gobernabilidad. En este caso, se hace referencia a que, En este caso, se hace referencia a que, con todo el conocimiento que se extrae de la abrumadora cantidad de datos disponible, se espera que la humanidad alcance una mayor equidad y sea capaz de tomar decisiones que beneficien a todos, reduciendo al mínimo las guerras. También se espera que ésta sea más consciente de la importancia de preservar los recursos naturales y garantizar la supervivencia de las especies en el planeta, en lugar de utilizar la información para adaptarse a entornos fuera de la Tierra, como algunas entidades proponen, se sugiere utilizarla para beneficio de la vida en el propio mundo.

Así mismo, es de considerar que la sabiduría que se tiene cada más sobre el entorno, le da a los seres humanos una especie de"poder" sobre otros coetáneos y sobre los recursos. Es así como actualmente, la IoT reviste cada más importancia; como se observa en la Figura 6, se hace una estimación del número de dispositivos conectados a nivel mundial. Cabe decir que estos datos están en constante cambio debido al rápido crecimiento de esta tecnología:

Figura 6. Dispositivos conectados (Internet de las cosas) a nivel mundial de 2015 a 2027 (en miles de millones de unidades)



Fuente: Statista.com
* Excluyendo M2M (máquina a máquina).
** Previsión desde 2017 a 2027

Se espera que el número de dispositivos conectados a la IoT siga creciendo exponencialmente en los próximos años. Las proyecciones indican cifras que van desde decenas de miles de millones hasta más de cien mil millones de dispositivos en el futuro cercano [3, p. 3; 15]. Así mismo, se estima que el mercado mundial de IoT crezca de manera exponencial, estimado para 2026, en un poco más de una decena de millones de dólares [17].

c)Impacto del IoT en la sociedad y la industria

Los dispositivos IoT se utilizan en una amplia variedad de sectores, que incluyen la salud, la industria, hogares inteligentes, ciudades inteligentes, agricultura, automoción y más. Por ello, se espera un alto impacto en la sociedad y en la industria, misma que ya se está vivenciando.

En lo que respecta a su impacto social, los dispositivos IoT en el hogar proporcionan mayor comodidad y eficiencia en la vida diaria, cambiando la forma en que se interactúa con otras personas y con el entorno, en las últimas dos décadas [17]. Los dispositivos de salud conectados y wearables (dispositivos que hacen parte de los accesorios portables o "vestibles"), permiten un monitoreo constante de la salud, lo que facilita la prevención y gestión de enfermedades. Dispositivos médicos conectados y sistemas de gestión de la salud basados en IoT, mejoran la atención médica [14,18,30].

Por otra parte, las aplicaciones de IoT en el ámbito urbano, contribuyen a la gestión eficiente del tráfico, la iluminación pública, la recolección de residuos y otros servicios, mejorando la calidad de vida en entornos citadinos. Los sistemas de seguridad basados en IoT, como cámaras de vigilancia y sistemas de alarma, ofrecen una mayor seguridad y protección tanto en hogares como en espacios públicos.

Así, el impacto que tiene IoT a nivel social e industrial, se ve reflejado en la manera como se realiza una diversidad de actividades [19].

En cuanto su impacto en la industria, la IoT ha impulsado la transformación digital en ésta, a partir de la interconexión de máquinas y sistemas, mejorando la eficiencia, reduciendo costos y permitiendo la producción personalizada. La monitorización en tiempo real a través de dispositivos IoT, mejora la visibilidad y gestión de la cadena de suministro, reduciendo los tiempos de entrega y los costos asociados. De esta forma, ha revolucionado la agricultura al proporcionar soluciones para el monitoreo de cultivos, el riego automatizado y la gestión eficiente de recursos [11,14].

Actualmente, suele subdividirse la tecnología IoT de acuerdo con su campo de aplicación. Se habla, por ejemplo, de IoE para referirse al internet del todo [14, p. 12], el cual ha sido ampliamente difundido, estudiado y aplicado en el Internet Industrial de las cosas (IIoT); también se encuentran: el IoT basado en Agricultura (Ag-IoT); Ganadería Conectada; IoT Salud (en el que es habitual hablar de los wearables); IoT en educación, Smart home y Smart cities [7, 14, 19, 20], cuyas generalidades se abordarán más adelante. Se suman además, otros ejes de estudio emergentes que contemplan múltiples posibilidades, como el Internet Social de las Cosas SIoT, o el Internet de las Nano – Cosas, IoNT.

B. Arquitectura del IoT

a) Arquitectura propia de sistemas IoT

La arquitectura de Internet de las cosas, engloba la estructura y diseño de los sistemas IoT, desde la captura inicial de los datos hasta su procesamiento y presentación en aplicaciones y servicios. Es de resaltar que la arquitectura de IoT es la responsable de la seguridad de la información que se genera a través de los distintos niveles. Se garantiza la compatibilidad compatibilidad entre los dispositivos IoT, gracias a la versión actual de comunicación IP que es IPv6 [15,16, 21, 22].

Algunos autores coinciden en que la tecnología IoT acompañada de otras tecnologías emergentes, no está definida bajo una única arquitectura universal. Diversas fuentes describen una estructura mínima requerida de tres capas o niveles [15, 16, 23]. Otros, estiman necesario cinco o, hasta siete capas [22, p. 64, 24, 25, 26].

En el presente artículo, se consideran cinco capas o cinco niveles para definir la arquitectura de IoT y, garantizar de una manera efectiva la aplicación en los distintos ámbitos, de acuerdo con [24], Figura 7, en donde se contemplan dos aspectos importantes: la conectividad y la ciberseguridad.

Figura 7. Arquitectura de IoT

Fuente: [24]

La primera de ellas, es la habitualmente denominada *capa de percepción* (dispositivos) [15, 16, 22, 23], que básicamente está asociada al hardware: sensores y actuadores, encargados de capturar los datos del entorno.

La segunda, que puede denominarse como: "*capa de puertas de enlace*", es la encargada de la conexión desde el dispositivo o redes de dispositivos de la *capa de percepción* hacia la red pública [24]. Dicho en otros términos, justamente es la puerta que permite que los datos tengan la posibilidad de ir hacia la *capa de red*.

La tercera, designada como *capa de red*, es el canal de comunicación a través de los cuales empiezan a viajar los datos capturados en la *capa de percepción* (WiFi, Zigbee, Bluetooth, red de telefonía móvil, LoRaWan, NFC (Near Field Communication), RF puro) [23].

En cuarto lugar, la *capa de infraestructura* [22] es el lugar donde los datos, tras recorrer los canales de comunicación, llegan a los repositorios, bases de datos, almacenamiento y procesamiento en la nube [22, 24]. En este punto, los datos dejan de ser simples datos para transformarse en información.

Por último, se describe la *capa de aplicación* [15, 16, 22, 24] la cual permite la interacción con el ser humano y/las instituciones o empresas tomadoras de decisiones. Es aquella donde la información pasa al siguiente nivel, convirtiéndose en conocimiento al ser usado en las distintas soluciones. Evocando a Evans, se evidencia a través de estas distintas fases cómo los datos del entorno, luego son información, para convertirse en conocimiento y finalmente, en sabiduría humana [3].

No se puede dejar de lado la *gestión y seguridad* de la información, que desde la perspectiva actual, es una función y responsabilidad de cada uno de los elementos y procesos intervinientes en la arquitectura IoT [20, 21,24].

b) Protocolos de comunicación MQTT, CoAP

Es importante tener en cuenta que, en la *capa de red* se requiere un lenguaje de interpretación de los datos que han sido capturados en la primera capa por las redes de sensores y actuadores. Así mismo, se requieren protocolos en la *capa de aplicación.*

Es posible asociar desde la perspectiva de Evans [3] que, cada vez que los datos van sufriendo una transformación, se requiere un protocolo que los transforme y/o los interprete "información", se requieren los protocolos de comunicación; y, para pasar de "información" a "conocimiento", se requieren los protocolos de aplicación. Lo anterior, porque ese "conocimiento" debe ser convertido en "sabiduría", lo cual es un proceso propio de la mente humana.

Por ello, se requieren los protocolos de comunicación, que varían dependiendo de la aplicación [21]. Para el caso, se analizarán dos protocolos de comunicación usados para la supervisión de dispositivos asociados a servidores *back-end: MQTT* y *CoAP.*

MQTT (Transporte de Telemetría de Cola de Mensajes):

Es un protocolo de mensajería eficiente creado para facilitar la comunicación entre dispositivos en redes que tienen restricciones de ancho de banda o experimentan alta latencia. Desarrollado por IBM en la década de 1990, este protocolo se ha convertido en un estándar abierto muy utilizado en el ámbito del Internet de las cosas (IoT) [15, 16, 21, 26].

MQTT se fundamenta en el principio de publicación y suscripción, donde los dispositivos tienen la capacidad de enviar mensajes a categorías específicas denominadas "temas". Otros dispositivos pueden suscribirse a estos, para recibir los mensajes pertinentes, posibilitando así una comunicación eficaz y desvinculada entre los dispositivos [26].

MQTT permite la conservación de sesiones, lo que implica que los clientes pueden reanudar la comunicación desde el último estado conocido después de haberse desconectado y vuelto a conectar. La implementación segura de *MQTT* implica la integración de métodos de autenticación y cifrado. Esta precaución es fundamental, especialmente al utilizarlo en entornos delicados, como aplicaciones industriales o dispositivos médicos conectados. [8, 15, 16, 21, 26, 27, 28, 29].

CoAP (Protocolo Constrained Application):

Es un protocolo de aplicación diseñado para facilitar la comunicación eficiente entre dispositivos en redes de baja potencia, funcionando sobre el *Protocolo de Datagramas de Usuario (UDP).* Por esta razón, es ideal para entornos de red con recursos limitados, como dispositivos IoT (Internet de las cosas) y redes de sensores [1, 9, 28, 29, 30].

Su estructura eficiente minimiza la sobrecarga de datos y facilita la implementación en dispositivos con recursos limitados. sigue un modelo cliente-servidor, donde los dispositivos pueden realizar solicitudes a servidores CoAP para recuperar o modificar recursos. Igualmente, admite múltiples formatos de representación de datos, como XML, JSON y CBOR (Concise Binary Object Representation), lo que proporciona flexibilidad en la transmisión de información [1, 9,24, 27, 28, 29, 30].

c) Protocolos de aplicación MFI, Nest, OIC

Los protocolos de la capa de aplicación no están estandarizados [21], debido a que dependen del propósito del fabricante en relación con la oferta de sus productos y servicios, lo que puede representar un riesgo de seguridad.

MFI

Pertenece a Apple, empresa que asegura la compatibilidad entre dispositivos y accesorios electrónicos diseñados para funcionar con sus productos como el iPhone, iPad y iPod. Esta compatibilidad facilita el uso de las aplicaciones [21].

Nest

Google adquirió la compañía Nest, ampliando su oferta para incluir diversos productos destinados a smart home, como cámaras de seguridad, detectores de humo y monóxido de carbono, así como sistemas de seguridad para el hogar. Los productos de Nest generalmente se integran en entornos de hogares inteligentes y suelen ser controlados mediante aplicaciones móviles [21].

OIC (Open Interconnect Consortium)

Es un consorcio industrial [21] que ha desarrollado y promovido estándares para la conectividad y la interoperabilidad entre dispositivos en el Internet de las cosas (IoT), del cual hacen parte Samsung, Intel, Broadmcom, Atmel y Dell. El OIC se ha centrado en el desarrollo de un marco de estándares y protocolos para permitir la comunicación efectiva entre dispositivos en un entorno IoT diverso.

C. Seguridad en la comunicación IoT

a) Importancia de la seguridad en la comunicación IoT

Aunque se han logrado progresos en la seguridad del Internet de las cosas (IoT), existen diversos desafíos que representan amenazas para la integridad, confidencialidad y disponibilidad de los dispositivos y la información conectada [13,15,16,21,22,24, 30-35].

Dada la diversidad de dispositivos IoT y su conectividad, hay más puntos de entrada para posibles ataques cibernéticos. Los atacantes pueden aprovechar las vulnerabilidades en la seguridad de los dispositivos para acceder a datos sensibles o controlar dispositivos de forma no autorizada [13,15,16,21,22,24, 30-35].

Muchos dispositivos IoT recopilan y transmiten datos sensibles, como información personal, datos de salud o datos de ubicación. Si se vulnera la seguridad de estos dispositivos, se podrían exponer estos datos a amenazas, comprometiendo la privacidad y la seguridad de los usuarios [13,15,16,21,22,24, 30-35].

b) Medidas de seguridad comunes y mejores prácticas

En cuanto a medidas de seguridad, se han desarrollado y promovido estándares y directrices de seguridad específicos para IoT. Organizaciones y consorcios, como la *Internet Engineering Task Force (IETF)* y el *Industrial Internet Consortium (IIC)*, han trabajado en la creación de normas que aborden aspectos clave de la seguridad en IoT [13,15,16,21,22,24, 30-35].

Además, se ha dado mayor importancia a la autenticación fuerte y a la gestión de identidades en dispositivos IoT. La aplicación de protocolos de autenticación robustos ayuda a asegurar que solo los dispositivos autorizados puedan acceder a la red. La encriptación de datos en los dispositivos IoT se ha fortalecido, lo que garantiza que la información transmitida entre dispositivos y servidores esté protegida contra la interceptación no autorizada. [13,15,16,21,22,24,30-35]

Por otra parte, los fabricantes están mostrando mayor interés en las actualizaciones de seguridad para los dispositivos IoT. Es perentorio, enviar e implementar actualizaciones de firmware de forma segura para hacer frente a las vulnerabilidades que se descubren una vez que los dispositivos ya están en uso [43,44,45].

D. Algunas aplicaciones del IoT

Desde la optimización de procesos industriales hasta la mejora de la calidad de vida en la sociedad, el IoT continuará evolucionando a medida que la tecnología avance y se integre aún más en diversos aspectos de la vida humana. Algunas aplicaciones se relacionan a continuación.

a) Internet Industrial de las Cosas IIoT

Según Saavedra et al., el Internet Industrial de las Cosas (IIoT) hace referencia a la aplicación de tecnologías de la Internet de las Cosas en entornos industriales y empresariales. El IIoT se enfoca en la optimización y mejora de procesos en sectores industriales. Igualmente, según Rabanal et al. [11,14 p.13], éste se describe bajo algunas características:

La capacidad de recopilar datos en tiempo real, permite la monitorización y el mantenimiento predictivo de maquinaria y equipos industriales, lo que reduce el tiempo de inactividad y la mejora en la eficiencia operativa.

La IIoT contribuye a una cadena de suministro más eficiente mediante la monitorización en tiempo real de los procesos de producción (manufactura), inventario y distribución, compra y venta masiva de productos, lo que permite una toma de decisiones más rápida y precisa. También se utiliza para mejorar la seguridad en el entorno laboral, mediante la monitorización de condiciones peligrosas y la implementación de sistemas de alerta temprana [29].

La IIoT es un componente clave de la cuarta revolución industrial (Industria 4.0), lo que implica la integración de tecnologías avanzadas tanto en la fabricación, como en la automatización, la robótica y la digitalización de procesos. La IIoT ayuda a lasindustrias a gestionar de manera más eficiente el consumo de energía al proporcionar datos detallados sobre el uso de recursos [13, 14, 29, 30].

b) IoT basado en Agriculture (Ag-IoT)

Rudrakar y Rughani [38], en su artículo publicado en octubre de 2023, consideran que la Agricultura impulsada por la Internet de las Cosas (Ag-IoT), es una tecnología de comunicación en desarrollo que tiene gran auge entre empresarios agrícolas y cultivadores. Es utilizada para llevar a cabo diversas tareas rurales con el objetivo de incrementar la productividad, mejorar la supervisión y disminuir los costos laborales.

Ag-IoT, es considerada dentro de la gama

IoT, toda vez que está sustentada en los tres pilares descritos inicialmente: interconectividad, analítica de datos y automatización de procesos. De acuerdo con la revisión realizada por Rudrakar y Rughani [38], Ag-IoT ofrece soluciones particularmente, de la siguiente manera:

Las redes de sensores conectadas, se utilizan para monitorear factores como la humedad del suelo, la temperatura, la calidad del aire y la radiación solar. A su vez posibilitan la automatización agrícola facilitando la gestión más precisa del riego inteligente (optimizando el recurso agua) y la fertilización, entre otras tareas, como: la siembra, la cosecha y el control de plagas.

La recopilación masiva de datos generados por sensores IoT, permite análisis avanzados y modelos predictivos. Esto ayuda a los agricultores a tomar decisiones informadas sobre la planificación de cultivos, la gestión de riesgos y la optimización de rendimientos.

Por último, la combinación de la IoT con otras tecnologías emergentes, está transformando gradualmente la forma en que se desarrollan los procesos agrícolas. Se espera que sea una alternativa ante la demandante seguridad alimentaria a nivel global.

c) IoT Salud o Salud Conectada

Según AlShorman el Internet de las Cosas (IoT) en el ámbito de la salud, a menudo denominada "IoT Salud" o "Salud Conectada," ha tenido un impacto significativo en la atención médica y la gestión de la salud [39].

Wearables IoWT y dispositivos de seguimiento personal, como relojes inteligentes, monitores de actividad física y otros wearables que son versátiles y ergonómicos, pueden recopilar datos sobre la actividad física, la frecuencia cardíaca [40], el monitoreo de la diabetes [39], el sueño y otros parámetros de salud. Estos datos permiten un seguimiento personalizado, ya que son extraídos de manera continua y en tiempo real, siempre que el paciente porte el dispositivo.

Es de resaltar, que los IoWT, se dividen en tres tipos: los portátiles, los implantables y los moleculares [18], lo que facilita el monitoreo remoto de pacientes fuera del entorno hospitalario. Dispositivos conectados recopilan datos vitales y síntomas, proporcionando a los profesionales de la salud información en tiempo real para la toma de decisiones, modificando la forma de atención en el área de la salud, toda vez que ahora es el paciente el que inicia la recopilación de los datos y no el profesional de la salud, como es lo convencional [30].

La IoT facilita la telemedicina, permitiendo consultas médicas a distancia y la supervisión de pacientes a través de videoconferencias y dispositivos conectados [41].

d) IoT en educación

La Internet de las Cosas (IoT) también ha comenzado a desempeñar un papel importante en el ámbito de la educación, transformando la forma en que se enseña y se aprende [27, 35, 43].

La implementación de dispositivos IoT en las aulas, permite la creación de aulas inteligentes. Sensores y dispositivos conectados, pueden optimizar la gestión del espacio, controlar el entorno (iluminación, temperatura, etc.) y facilitar la interactividad entre profesores y estudiantes; de esta forma, pueden utilizarse para el seguimiento y evaluación del rendimiento de los discentes. Esto incluye la recopilación de datos sobre la participación, el progreso en las tareas y el rendimiento en las evaluaciones [27, 35].

En este sentido, dispositivos IoT pueden utilizarse para crear experiencias de aprendizaje más interactivas. Por ejemplo, pizarras interactivas conectadas a la red o dispositivos de respuesta en tiempo real, para la participación

de los estudiantes [27,35].

La recopilación y análisis de datos a través de dispositivos IoT, pueden utilizarse para personalizar los entornos de aprendizaje, adaptándolos a las necesidades individuales de cada estudiante [27, 35].

e) Ganadería Conectada

La implementación de la Internet de las Cosas (IoT) en la ganadería y la producción pecuaria, también conocida como "Ganadería Conectada" o "Agricultura Ganadera Inteligente", ha introducido innovaciones similares a las de la agricultura. Estas innovaciones mejoran la eficiencia, la gestión y la salud de los animales, optimizando la producción. A continuación, se describen algunas formas en las que la IoT se ha integrado en este sector. [42].

Los dispositivos IoT se aplican en la ganadería para monitorear la salud y ubicación del ganado y permiten un seguimiento individual. Sensores de temperatura, dispositivos de seguimiento y monitoreo, pueden proporcionar información sobre la ubicación, el comportamiento, la actividad y la salud mediante la detección temprana de enfermedades y el seguimiento de parámetros vitales de cada animal. Los sensores conectados controlan factores del entorno como la temperatura, la humedad y la calidad del aire en los establos o pastizales, asegurando condiciones óptimas para el ganado [42].

E. Desafíos y tendencias

Debido a la adopción e integración de tecnologías digitales avanzadas como el Internet de las cosas - IoT, estamos experimentando una transición de un mundo hiperconectado a uno digitalizado en los aspectos económicos y sociales [37]. En este entorno, coexisten y se fusionan la economía convencional, con las formas de organización y de gobernanza, y la economía digital, con nuevos modelos de negocios, producción y estructura empresarial.

Esto da lugar a un nuevo sistema digitalmente interconectado en cuanto a la oferta y demanda de productos y servicios, generando la necesidad de repensar y llevar a cabo ajustes en los aspectos organizativos, institucional y normativo, en las entidades públicas y privadas.

El vertiginoso crecimiento de las tecnologías emergentes, debe llevar a la consideración de un entorno global adaptativo y en constante cambio. Un desafío trascendente reside en entender y atender - además de las necesidades de los usuarios, en cuanto a productos y servicios -, los aspectos inherentes a la seguridad de los datos personales sensibles debido a que, a medida que la tecnología IoT se ha expandido, las amenazas y vulnerabilidades de la información, han aumentado.

IV.DISCUSIÓN

La arquitectura IoT admite cada vez más posibilidades de mejora, particularmente con respecto a la seguridad de los usuarios. La masiva y creciente industria del IoT, que para el año 2023 se estimaba en un crecimiento económico del 11% (alrededor de 4.500 millones de dólares), sugiere la necesidad urgente de incorporar atributos de ciberseguridad como un desafío prioritario, que debe ser asumido por parte de todos los actores involucrados: empresas fabricantes de dispositivos y aplicaciones, instaladores y operadores de tecnología IoT, entes gubernamentales, desarrollares, implementadores, y por supuesto, los usuarios finales, cobijados por el bienestar y la seguridad que debe ofrecer una tecnología diseñada principalmente para facilitar el desarrollo de tareas y brindar confort.

Čolaković y Hadžialić, señalan que las aplicaciones recientes del Internet de las cosas - IoT y las tecnologías emergentes, tienen el potencial de impulsar el futuro desarrollo del IoT, mediante una nueva arquitectura denominada

Cloud of Things o incluso el Internet de las Nano-Cosas - IoNT. Además, la integración de tecnologías web en el Web of Things – WoT, ofrece un catálogo más extenso de capacidades y funcionalidades innovadoras [46].

Actualmente, el IoT amalgama un universo de posibilidades que junto con tecnologías como 5G, inteligencia artificial, Machine Learning, Big Data, robótica, servicios en la nube e industria 5.0, pueden llevar a pensar no solo en un sistema global interconectado digitalizado, sino en nuevas formas de percibir e interactuar en la cotidianidad. Aspectos fundamentales que afectan a los seres humanos, como la salud, la seguridad alimentaria, el aprendizaje y la profesionalización, e incluso la equidad social, podrían experimentar cambios significativos de manera impredecible en un futuro cercano. En períodos cortos de tiempo, se ha observado cómo muchas de las formas tradicionales de realizar tareas y actividades, han sido totalmente transformadas por el avance vertiginoso de la tecnología inteligente.

Finalmente, la recolección y el monitoreo de datos a través de sensores y actuadores para IoT, así como el análisis de estos datos para convertirlos en información, son de interés prioritario para múltiples empresas y/o entidades interesadas en la identificación de gustos y necesidades de los usuarios, situación que en primera instancia incentiva la oferta de productos y servicios, con un valor agregado que consiste en brindar además, la posibilidad de que sean adaptativos conforme a los requerimientos individuales y, en segundo lugar, el proporcionar una data en tiempo real que puede ser usada para la prevención, el diagnóstico, y la toma de decisiones.

V.CONCLUSIONES

Al finalizar esta revisión, lo que se puede estimar como prioritario, es que más allá de la importancia que revisten las tecnologías emergentes, lo es la captura de datos. Desde el inicio de la humanidad, los datos han cumplido la misma función que cumplen ahora: la de permitir interpretar el entorno y adaptarlo según las necesidades, facilitando las tareas y brindando ambientes más cómodos. Aquí cobra gran relevancia la postura presentada por Evans [3], quien explica que los datos se convierten en información, la información se convierte en conocimiento y el conocimiento se convierte en sabiduría, misma que trasciende las generaciones.

De esta manera, el Internet de las cosas (IoT), en conjunto con otras tecnologías emergentes y en constante evolución, permite la recopilación y el análisis de una gran cantidad de datos de manera más sencilla y efectiva. Por ende, se espera que estas tecnologías trasciendan proporcionalmente al nivel de sabiduría humana, impulsando no solo las interacciones sociales, sino también la gobernanza y la economía global. Es necesario romper las barreras que establecen la soberanía de los países y priorizar la calidad de vida para todos los seres en nuestro planeta.

Indubitablemente, el Internet de las Cosas es el pilar fundamental de la actual revolución industrial, conocida como la Industria 5.0. Esta revolución se basa en la masificación de tecnologías que permiten que los productos y servicios sean considerados como inteligentes, con dos características clave que los hacen cada vez más adaptables: la capacidad de comprender su entorno y la capacidad de actuar con base en esta comprensión. Por consiguiente, la masificación de productos y servicios IoT, fortalece la economía global no sólo en el ámbito tecnológico, sino que también, permea todos los ejes, aspectos sociales, culturales, políticos, educativos, de salud, desarrollo de la ciencia y la investigación, modificando de esta manera, el modo de vida humano y la percepción de su entorno.

La cultura y educación al usuario final, juegan un papel fundamental en la implementación y masificación de IoT en cuanto

a ciberseguridad, dado que la falta de concienciación frente a la exposición de los datos, es actualmente la situación más propicia para la amenaza y vulneración de la información en la arquitectura de IoT. Habitualmente, el usuario no reconoce la importancia de la exposición de sus datos personales, debido a que no es consciente de que terceros puedan acceder a estos, a través de las diferentes conexiones de redes inalámbricas.

VI.REFERENCIAS

[1] J. Salazar, S. Silvestre. "Internet de las cosas." Techpedia. České vysoké učení technické v Praze Fakulta elektrotechnická. 2016. Disponible en: https://psm.fei.stuba.sk/pages/95/LM08_F_ES.pdf

[2] T. Nilufer, and S. Hailes. "Crime in the age of the Internet of Things." Routledge Handbook of Crime Science. Routledge, 2018. 288-308.

[3] E. Dave. "Internet de las cosas. "Cómo la próxima evolución de Internet lo cambia todo. Cisco Internet Bussiness Solutions Group-IBSG 11.1 (2011): 4-11. Disponible en: http://audentia-gestion.fr/cisco/IoT/internet-of-things-iot-ibsg.pdf

[4] J. A, Sánchez-Alcón, , L, López-Santidrian, and J. F. Martínez-Ortega. "Solución para garantizar la privacidad en el Internet de las Cosas." El profesional de la información 24.1 (2015): 62-70. Disponible en: https://oa.upm.es/41198/1/INVE_MEM_2015_227635.pdf

[5] Rudas, J. S., L. M. Gómez, and A. O. Toro. "Revisión sistemática de literatura. Caso de estudio: Modelamiento de un par deslizante con fines de predecir desgaste." Prospectiva 11.1 (2013): 50-58. Disponible en: https://dialnet.unirioja.es/descarga/articulo/4697704.pdf

[6] Carrizo y C. Moller, "Estructuras metodológicas de revisiones sistemáticas de literatura en Ingeniería de Software: un estudio de mapeo sistemático", Ingeniare. Rev. Chil. Ing., vol. 26, pp. 45–54, noviembre de 2018. Disponible: https://doi.org/10.4067/s0718-33052018000500045

[7] J. J. Saavedra-Neira, M. I. Hernández-Barba, y A. C. Mendoza-De Los Santos, "Aplicaciones y beneficios IOT como alternativa en el gobierno TI: Revisión sistemáticade literatura", Revista Científica de la UCSA, vol. 10, no 1, pp. 120–138, 2023, doi: 10.18004/ucsa/2409-8752/2023.010.01.120.

[8] Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. The internet society (ISOC), 80, 1-50 https://acortar.link/MvUieW

[9] Cama-Pinto, A, De-La-Hoz-Franco, E, Cama-Pinto, D Las redes de sensores inalámbricos y el Internet de las cosas. [Internet]. Corporación Universidad de la Costa; 2012 [citado: 2023, septiembre] https://repositorio.cuc.edu.co/bitstream/handle/11323/1546/7.%20Las%20redes%20de%20sensores%20inal%c3%a1mbricos.pdf?sequence=1&isAllowed=y

[10] R. H. Weber, "Internet of Things–New security and privacy challenges.", Comput. law & secur. rev., vol. 26(1), p. 23, 2010.

[11] E. H. Rabanal-Chávez, N. Campos-Vásquez, C. M. Pérez-Heredia, R. K. Manturano-Chipana, y M. A. D. Díaz, "Internet of Things (IoT)-Scope, Applicability and Communication Models Internet de las Cosas (IoT)-Ámbito de Aplicación y Modelos de Comunicación", Proceedings of the LACCEI international Multi-conference for Engineering, Education and Technology, vol. 2022-July, pp. 18–23, 2022, doi: 10.18687/LACCEI2022.1.1.652.

[12] Alsharif, MH; Jahid, A.; Kelechi, AH; Kannadasan, R. Green IoT: una revisión y direcciones futuras de investigación. Simetría 2023, 15, 757. p. 10. https://doi.org/10.3390/

[13] F. J. Ávila-Camacho y L. M. Moreno-Villalba, "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, vol. 10, no 20, pp. 10–16, 2023, doi: 10.29057/icbi.v10i20.9516

[14] A. Román Gallardo, J. R. Herrera Morales, S. Sandoval Carrillo, M. Andrade Aréchiga y E. M. Ramos Michel, Internet de las cosas Teoría y práctica, 235a ed. Colima - México, 2023.

[15] R. R. Cristian Jiménez, "Ciberseguridad del IoT- Un Análisis en Países de la Unión Europea", RISTI: Revista Ibérica de Sistemas e Tecnologías de Información, ISSN-e 1646-9895, No. Extra 39, 2021, págs. 461-476, pp. 161-

476, 2021, Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8597361

[16] J. Wang, M. K. Lim, C. Wang, y M. L. Tseng, "The evolution of the Internet of Things (IoT) over the past 20 years", Comput Ind Eng, vol. 155, no May, 2021, doi: 10.1016/j.cie.2021.107174

[17] N. N. Dao, "Internet of wearable things: Advancements and benefits from 6G technologies", Future Generation Computer Systems, vol. 138, no January, pp. 172–184, 2023, doi: 10.1016/j.future.2022.07.006. https://www.sciencedirect.com/science/article/abs/pii/S0167739X22002345

[18] A. M. G. Esperón, M. D. D. Dapena, F. M. Pérez, J. V. B. Martinez, y I. L. Fonseca, "Desafíos de las pruebas de aplicaciones IoT en ciudades inteligentes", Revista Cubana de Transformación Digital, vol. 4, no 2, pp. 220–221, 2023, Disponible en: https://rua.ua.es/dspace/bitstream/10045/135274/1/Guemes-Esperon_etal_2023_Rev-CubanaTransformacionDigital.pdf

[19] J. E. M. Díaz, "Cybersecurity and Internet of Things. Outlook for this decade", Computación y Sistemas, vol. 26, no 3, pp. 1191–1204, 2022, doi: 10.13053/CYS-26-3-3925

[20] Díaz Márquez, J. «Dossier sobre inteligencia artificial, Robótica e Internet de las Cosas», Revista de Bioética y Derecho - Perspectivas bioéticas, vol. 46, pp. 86-100, 2019, Disponible en: www.bioeticayderecho.ub.edu

[21] L. F. Gélvez-Rodríguez y L. M. Santos-Jaimes, «Internet de las Cosas: una revisión sobre los retos de seguridad y sus contramedidas», Revista Ingenio, vol 17, n.o 1, pp. 56-64, ene. 2020, doi: 10.22463/2011642x.2370.

[22] P. K. Sadhu, V. P. Yanambaka, y A. Abdelgawad, "Internet of Things: Security and Solutions Survey", Sensors, vol. 22, no 19, pp. 1–51, 2022, doi: 10.3390/s22197433

[23] M. González Díez y J. Panadero Martínez Miguel Martín Mateo, «Internet de las cosas. Privacidad y Seguridad», 2020. Disponible en: http://hdl.handle.net/10609/116427

[24] K. Chen et al., "Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice," J. Hardw. Syst. Secur., vol. 2, no. 2, pp. 97–110, 2018

[25] H. Ning, H. Liu, and L. T. Yang, "Cyberentity security in the internet of things," Computer (Long. Beach. Calif)., vol. 46, no. 4, pp. 46–53, 2013

[26] G. Fortino et al., "Interoperability, Safety and Security in IoT", 2017. Disponible en: http://www.springer.com/series/8197

[27] A. Giménez, R. Tutores, : Sara, B. Clavero, J. Vicente, y B. Dualde, «Aplicación de la tecnología de Internet de las Cosas en el ámbito educativo», Disponible en: https://riunet.upv.es/bitstream/handle/10251/170674/Gimenez%20-20Aplicacion%20de%20la%20tecnologia%20de%20Internet%20de%20las%20Cosas%20en%20el%20ambito%20educativo.pdf?sequence=1

[28] A. Liñan Colina, A. Vives, A. Bagula, M. Zennaro, y E. Pietrosemoli, INTERNET DE LAS COSAS. 2015. Disponible en: http://wireless.ictp.it/Papers/InternetdelasCosas.pdf

[29] N. Mitton, H. Chaouchi, T. Noel, T. Watteyne, A. Gabillon, y P. Capolsini, «Interoperability, Safety and Security in IoT», 2016. [En línea]. Disponible en: http://www.springer.com/series/8197

[30] G. Fortino et al., "Interoperability, Safety and Security in IoT", 2017. Disponible en: http://www.springer.com/series/8197

[31] Zabala Jaramillo, Luis Alberto. Gestión de la seguridad en el internet de las cosas. BS thesis. Universidad Piloto de Colombia, 2016. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2721/Trabajo%20de%20grado3304.pdf?sequence=1&isAllowed=y

[32] Martínez, Juan-Manuel, et al. "La seguridad en Internet de las Cosas: Analizando el tráfico de información en aplicaciones para iOS." ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica 6.1 2017, 77-96. https://www.redalyc.org/journal/5122/512253717005/512253717005.pdf

[33] L. F. Gélvez-Rodríguez y L. M. Santos-Jaimes, «Internet de las Cosas: una revisión sobre los retos de seguridad y sus contramedidas», Rev. Ingenio, vol. 17, n.º 1, pp. 56–64, ene. 2020. https://revistas.ufps.edu.co/index.php/ingenio/article/view/2370/2893

[34] Juan Fernando Saa Ayala, "Análisis De Un Sistema De Seguridad Basado En El Internet De Las Cosas", Tesis de Grado, vol. 1, p. 41, 2023, Disponible en: http://dspace.utb.edu.ec/handle/49000/14249

[35] L. F. G.-G. Alexandra Babilonia Ospina, M. C. B.-G. Alejandro Valencia-Arias, y R. B. G. Ledy Gómez-Bayona, Juan Camilo Patiño-Vanegas, "Tendencias investigativas en ciberseguridad del Internet de las Cosas (IoT)", RISTI: Revista Ibérica de Sistemas e Tecnologias de Informação, ISSN-e 1646-9895, No. Extra 39, 2021, págs. 461-476, no October, pp. 73–86, 2023, Disponible en: https://www.researchgate.net/publication/374809458_Tendencias_investigativas_en_ciberseguridad_del_Internet_de_las_Cosas_IoT

[36] A. Ordoñez, "Estado del arte de los métodos de seguridad de datos aplicados en Internet de las cosas", Tesis, pp. 1–100, 2022, Disponible en: http://dspace.ups.edu.ec/bitstream/123456789/5081/1/UPS-CYT00109.pdf

[37] Agenda Digital para America Latina y el Caribe. ELAC, "Tecnologías digitales para el nuevo futuro", Educitec - Revista de Estudios y Pesquisas sobre Ensino Tecnológico, vol. 8, no jan./dez., p. e198522, 2022, Disponible en: https://hdl.handle.net/11362/46816

[38] S. Rudrakar y P. Rughani, "IoT based agriculture (Ag-IoT): A detailed study on architecture, security and forensics", Information Processing in Agriculture, no August, 2023, doi: 10.1016/j.inpa.2023.09.002.

[39] AlShorman, O., Alshorman, B., & Alkahtani, F. "A review of wearable sensors based monitoring with daily physical activity to manage type 2 diabetes." International Journal of Electrical and Computer Engineering (IJECE), 2021, 11(1), 646. https://doi.org/10.11591/ijece.v11i1.pp646-653

[40] Singh, N. P., Kanakamalla, A., Shahzad, S. A., Divya Sai, G., & Suman, S. Remote Monitoring System of Heart Conditions for Elderly Persons with ECG Machine Using IOT Platform. Journal of Information Systems and Telecommunication (JIST), 2022, 10(37), 11-19. https://doi.org/10.52547/jist.15692.10.37.11

[41] M. F. M. Sam, A. F. M. F. Ismail, K. A. Bakar, A. Ahamat, y M. I. Qureshi, "The Effectiveness of IoT Based Wearable Devices and Potential Cybersecurity Risks: A Systematic Literature Review from the Last Decade", International journal of online and biomedical engineering, vol. 18, no 9, pp. 56–73, 2022, doi: 10.3991/ijoe.v18i09.32255

[42] M. Aranda, et al. IoT aplicado a la ganadería extensiva. Consejo Federal de Decanos de Ingeniería, 2021. https://confedi.org.ar/wp-content/uploads/2021/05/Articulo10-RADI17.pdf

[43] J. A. Saltos Morán, L. J. Moran Burgos, J. G. Proaño Ganchozo, y J. C. Gamarra Arévalo, "El internet de las cosas. Desafíos para la participación y el aprendizaje infantil", Recimundo, vol. 7, no 1, pp. 336–347, 2023, doi: 10.26820/recimundo/7. (1).enero.2023.336-347.

[44] K. Chen et al., "Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice," J. Hardw. Syst. Secur., vol. 2, no. 2, pp. 97–110, 2018

[45] H. Ning, H. Liu, and L. T. Yang, "Cyberentity security in the internet of things," Computer (Long. Beach. Calif)., vol. 46, no. 4, pp. 46–53, 2013

[46] ČOLAKOVIĆ, Alem; HADŽIALIĆ, Mesud. Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. Computer networks, 2018, vol. 144, p. 17-39. https://www.sciencedirect.com/science/article/abs/pii/S1389128618305243

SEGURIDAD DE LA INFORMACIÓN EN LA GENERACIÓN DE CONTENIDO PARA REDES SOCIALES: DESAFÍOS Y SOLUCIONES EN EL CONTEXTO DEL USO DE INTELIGENCIA ARTIFICIAL

Jorge Armando Rivas Rojas
E-mail: joariro@gmail.com

RESUMEN- ***Con el invento del computador, el ser humano aportó una herramienta que le permitiera realizar múltiples labores. A lo largo de los años el procesamiento de la información ha sobrepasado los límites concibiendo hoy en día la denominada inteligencia artificial (IA). Esta investigación de tipo documental realizada bajo el enfoque cualitativo y el paradigma hermenéutico, tiene como objetivo principal describir los impactos y efectos del uso de la Inteligencia artificial para la generación de contenido en las redes sociales; para ello, se abordarán tanto riesgos como vulnerabilidades, al igual que las normativas, regulaciones y su impacto desde el ámbito de "seguridad de la información". En los resultados obtenidos se encontró que los principales riesgos y vulnerabilidades se relacionan con la privacidad, el aumento de la posibilidad de engaño, la vigilancia y la manipulación de los datos por parte de terceros para obtener provecho; en las normativas se evidenció que la legislación actual carece de estatutos en cuanto a las responsabilidades de quienes producen y son beneficiarios de la IA, requiriendo la implementación de nuevas regulaciones en el marco de las capacidades del aprendizaje y la autonomía; con respecto a la evaluación del impacto, se determinó que la IA tiene un potencial inminente a nivel empresarial; es una tecnología progresiva que genera la necesidad de establecer medidas de control que limiten su capacidad de superar a las personas. La investigación concluye afirmando que la IA tiene grandes beneficios, pero que a su vez representa muchos riesgos, los cuales exigen el establecimiento de medidas que controlen en forma inmediata su acelerada evolución, más aún teniendo en cuenta que es un pilar para la economía y el desarrollo humano.***

Palabras clave: *Datos, Generación de contenido, Información, Inteligencia Artificial, Redes Sociales.*

Abstract— With the invention of the computer, humans contributed with a tool that allowed them to perform multiple tasks. Over the years, information processing has surpassed its limits, giving rise to what is now known as artificial intelligence (AI). This documentary research, carried out under a qualitative approach and the hermeneutic paradigm, aims to describe the impacts and effects of using artificial intelligence for generating content on social media. To achieve this, both risks and vulnerabilities will be addressed, as well as regulations and their impact within the field of "information security". The results obtained revealed that the main risks and vulnerabilities are related to privacy, increased potential for deception, surveillance, and manipulation of data by third parties for their own benefit. Regarding regulations, it was evident that current legislation lacks statutes regarding the responsibilities of those who produceand benefit from AI, requiring the implementation of new regulations within the framework of learning abilities and autonomy. In terms of impact assessment, it was determined that AI has imminent potential at the business level, being a progressive technology that necessitates the establishment of control measures to limit its capacity to surpass human capabilities. The research concludes by affirming that AI has great benefits but also represents significant risks, which demand the immediate establishment

of measures to control its rapid evolution, particularly considering its importance as a pillar for the economy and human development.

Keywords- *Data, Content Generation, Information, Artificial Intelligence, Social Networks.*

I. INTRODUCCIÓN

La denominada quinta revolución industrial ha traído consigo innumerables avances tecnológicos que han llegado hasta la puesta en marcha de robots e inteligencia artificial para la elaboración de tareas que son repetitivas. Esto tiene como objetivo permitir que las personas se enfoquen en la innovación y la resolución de problemas impredecibles [1]; con todo esto, es importante realizar un análisis de vulnerabilidades y riesgos en la seguridad y ciberseguridad con el fin de salvaguardar la información, la confidencialidad y la privacidad de los datos que están expuestos en el ambiente virtual y se ven influenciados por la inteligencia artificial (IA).

El uso de IA en la creación de contenido para las redes sociales está en auge. Las empresas y las personas intentan mantener una presencia activa en estas plataformas; sin embargo, esta práctica plantea intranquilidad sobre la seguridad de los datos e información de los usuarios, la calidad y la autenticidad del contenido generado. Además de esto, también existe la preocupación de que este tipo de automatización aumente la generación de contenido falso y poco confiable. Existen muchos factores sociales que pueden intervenir en la forma en que las personas actúan; algunos de ellos son: la edad, el género, el estrato social y la ubicación geográfica, entre otras.

Las redes sociales han cambiado drásticamente la comunicación, siendo actualmente utilizadas por miles de personas en todo el mundo, lo que ha conllevado a un aumento en la demanda de contenido, cuyas herramientas de generación en su mayoría se han vuelto automatizadas, a partir de la inteligencia artificial, lo que ha planteado preocupaciones sobre la calidad y la autenticidad del contenido generado.

El objetivo general de esta investigación, consiste en describir los impactos y efectos del uso de la inteligencia artificial en la generación de contenido para redes sociales. Los objetivos específicos son: identificar las principales vulnerabilidades y riesgos de seguridad asociados al uso de IA en la generación de contenido para redes sociales; evaluar las normativas y regulaciones existentes en cuanto al uso de IA en el contexto de las redes sociales y determinar el impacto que tienen en la seguridad de la información, todo, considerando las limitaciones técnicas y económicas de las empresas y organizaciones involucradas.

II.METODOLOGÍA

Esta investigación se realizó teniendo en cuenta el enfoque cualitativo que permite analizar y describir la información encontrada para dar respuesta a problemáticas planteadas [2]; esto se efectuó a través de una investigación documental en la que se efectuó la revisión de distintas fuentes académicas en las que se consultaron artículos, investigaciones y trabajos acerca de la seguridad informática y el uso de IA en la generación de contenidos para las redes sociales. La investigación documental con enfoque cualitativo enmarca el problema de investigación, determinando la importancia e influencia de cada una de las variables [3].

La investigación se fundamentó en el paradigma hermenéutico que posibilita la interpretación y comparación cualitativa de la literatura consultada, pudiendo comprender los distintos puntos de vista por medio del contraste de la información [4]. El método utilizado fue el inductivo que permite analizar la información particular para llegar a una conclusión general que responde a los objetivos de la investigación [5].

La búsqueda de información se realizó aplicando los descriptores "Inteligencia artificial", "Redes sociales, contenidos IA", "Riesgos y vulnerabilidades de la IA", y "Regulación de la IA". Se consultaron bases de datos como Scielo, Redalyc y Google académico. En total fueron consultados alrededor de 80 artículos y trabajos de investigación de los cuales se seleccionaron 51. La tabla 1, clasifica los descriptores, bases de datos y el número de artículos encontrados por cada uno:

TABLA I
Bases de datos y descriptores aplicados en las búsquedas

BASE DE DATOS	DESCRIPTORES	ARTÍCULOS
Google Académico	Inteligencia artificial	8
	Redes sociales, contenidos IA	3
	Riesgos y vulnerabilidades IA	8
	Regulación IA	11
		5
Scielo	Inteligencia artificial	8
Redalyc	Inteligencia artificial	7
	Redes sociales, contenidos IA	1

Fuente: Propia

- Criterios de inclusión: a. publicaciones que relacionarán los temas: inteligencia artificial y redes sociales; regulación, riesgos y vulnerabilidades de la inteligencia artificial; b. estudios nacionales e internacionales;c. Investigaciones en español e inglés.

- Criterios de exclusión: a. Artículos que no tuvieran relación con los objetivos planteados; b. publicaciones con fecha anterior al año 2018.

-Principales limitaciones: Las principales limitaciones estuvieron relacionadas con la escasa información acerca de cómo opera la inteligencia artificial en las redes sociales.

III. ESTADO DEL ARTE

La innovación tecnológica se ha sumado a la vida cotidiana jugando un rol trascendental, haciendo que mecanismos de difusión como la televisión y los espacios virtuales como las redes sociales, se convirtieran en una fuente indefinida de información a la que se puede acceder en cualquier momento y espacio; ahora bien, en esto se debe hacer alusión a aquellos espacios que son públicos, privados e íntimos, que como se sabe, constituyen un elemento de alta vulnerabilidad ante las tecnologías recientes [6]. La inteligencia artificial, en este sentido, tiene herramientas y algoritmos que permiten el bloqueo instantáneo de cierta información, como borrar comentarios e incluso cerrar cuentas [6].

Es importante destacar que la generación de contenido para redes sociales utilizando inteligencia artificial se ha convertido en una técnica ampliamente utilizada en los últimos años. Esto se debe a que permite crear contenido que se adapta a las expectativas de los usuarios y mejora la eficiencia en la producción de información. Sin embargo, su implementación plantea desafíos que deben ser abordados desde diversas perspectivas, especialmente en cuanto a la protección de la privacidad y seguridad de los usuarios. La IA [7] puede ser utilizada para recopilar y procesar información personal a través de la generación de contenido automatizado, algo que puede resultar en la exposición de información confidencial y mayor riesgo a los ataques de ingeniería social y la creación de contenido malicioso.

Para abordar este problema [8], se han propuesto soluciones como la encriptación de datos y la implementación de técnicas de privacidad diferencial. Además, se ha investigado la necesidad de implementar normas y políticas claras para el uso de la IA en la generación de contenido para redes sociales. Según estudios, se requiere una regulación adecuada para asegurar los derechos de los individuos y garantizar la transparencia de las empresas que utilizan la

IA en la generación de contenido para redes sociales.

Algunos desafíos de la inteligencia artificial que se pueden mencionar, están relacionados con la calidad y autenticidad, pues la IA debe ser capaz de crear contenido original y atractivo que se ajuste a las expectativas de los usuarios; en este sentido, se ha investigado la capacidad de la IA para crear contenido emocionalmente atractivo mediante el uso de procedimientos que procesan el lenguaje y analizan sentimientos [9].

La IA puede ser utilizada para crear contenido falso o manipulado que afecta la veracidad y la confiabilidad de la información [10]; también puede ser interpretado de diferentes maneras llegando a afectar la percepción y la forma en la que se comportan los individuos en las redes sociales [11].

En cuanto al aspecto económico, el uso de la IA para la generación de contenido puede tener un impacto significativo en el segmento de la industria digital y los medios de comunicación [12], debido a que sirve para automatizar los procesos productivos y mejorar la eficiencia de la publicidad en línea, lo que se traduce en una reducción de los costos y una mayor rentabilidad para las empresas.

Por otra parte, el uso de la IA también puede tener un impacto negativo en los puestos de trabajo de las empresas relacionadas con los medios de comunicación y la publicidad. La implementación de la IA destinada a la producción de contenido, puede resultar en la automatización de procesos y la necesidad de formar a los trabajadores en el manejo de la tecnología. Por lo tanto, se requiere un enfoque equilibrado para abordar los desafíos que plantea el uso de la IA en la generación de contenido para las redes sociales, abordando las problemáticas relacionadas con la privacidad y la seguridad de los cibernautas, con el propósito de garantizar no solo la calidad, sino también, la autenticidad del contenido con base en el establecimiento de políticas y regulaciones claras que aborden los impactos económicos y sociales de su empleo [13].

A. Inteligencia artificial

La inteligencia artificial se define como la destreza de los computadores en la realización de actividades que pueden hacer las personas; es la capacidad que tienen las máquinas para aprender y trabajar con los datos utilizando algoritmos y con ello, tomar decisiones de la misma forma como lo haría una persona [14]. La diferencia con los individuos radica, en que las máquinas no descansan analizando y procesando grandes volúmenes de información a la vez. En este orden de ideas, la IA se categoriza según Kerns [15] en débil y fuerte; las categorizadas débiles, son sistemas estrechos diseñados para realizar tareas específicas como Siri, robots industriales y asistentes personales; y las categorizadas fuertes, cuentan con capacidades similares a las del cerebro, diseñadas mediante programación; es una IA que emplea el conocimiento para encontrar soluciones de forma autónoma.

Según Hintze [16], profesor de la Universidad de Michigan, la Inteligencia Artificial puede ser clasificada en cuatro tipos: aquellos que manejan una tarea específica pero no tienen memoria; los de memoria limitada, que se basan en experiencias pasadas para advertir sobre decisiones futuras. Las denominadas "Teoría de la mente", que tienen inteligencia social para entender las emociones prediciendo el comportamiento humano. Por último, las que tienen conciencia de sí mismas y su estado actual; estas no existen todavía, siendo precisamente las que representan una amenaza a futuro.

La inteligencia artificial [17] puede ser un programa informático que actúa como asistente de voz, motor de búsqueda o incluso un sistema de reconocimiento facial. Puede estar anexa en aparatos de hardware como automóviles, drones o robots avanzados.

En consecuencia, la inteligencia artificial se puede aplicar entre otras, a las siguientes situaciones: reconocimiento o clasificación de imágenes, aumento en la eficiencia de estrategias de marketing y comerciales; procesamiento de todo tipo de datos, mantenimiento predictivo, distribución de contenidos (marketing, difusión de información); y protección contra amenazas de seguridad; además, puede dar sugerencias o predicciones relacionadas con asuntos importantes en áreas como la educación, la salud, el trabajo, las relaciones interpersonales, entre otras [18].

En este orden de ideas, la IA mediante algoritmos progresivos, estructura los datos y encuentra regularidades que le permiten fortalecer habilidades y enseñarse a sí misma, llegando incluso al punto de tener la capacidad de hacer recomendaciones [19]. En la actualidad, es utilizada en muchos campos mejorando la velocidad, eficacia y precisión de los humanos.

Para el año 2020, al menos 4,2 billones de aparatos tenían dispositivos de voz con Inteligencia Artificial. Se estima que para el año 2025 haya más de 190,61 billones [20]; por consiguiente, su uso se proyecta en un aumento en el PIB de 15.7 trillones para el 2030. Sin embargo, pese a estos avances se considera que, gracias a ello, al menos el 38% de los trabajos puedan estar en riesgo para esa época [21]. La sociedad cada día es más dependiente de la IA, lo que incrementa los riesgos debido a que está en proceso de escalonamiento. La realidad es que a largo plazo las tareas van a requerir menos personal debido a la automatización de los trabajos [22].

B. Redes sociales en el entorno de la I.A.

Las redes sociales son espacios virtuales usados socialmente para publicar, compartir y consultar información de cualquier tipo con personas conocidas o no, teniendo como ventaja la facilidad para interactuar con otros en cualquier momento y lugar [23]. Algunas de las redes sociales más reconocidas, son: Facebook, WhatsApp, Instagram, Tiktok y X que, aunque suponen rapidez en las relaciones y en la información, también son consideradas como "alto riesgo" en materia de seguridad.

La IA entra en el entorno de las redes sociales, debido a su capacidad para proporcionar en el menor tiempo cantidades descomunales de datos que los mismos usuarios generan y que son descifrados con el fin de agilizar procesos y hacer el trabajo más eficiente y efectivo. Hoy en día, las redes sociales son parte integral de las relaciones personales y comerciales; tienen influencia en todo tipo de personas, por lo que son empleadas para mejorar la imagen personal y de las marcas; con la inteligencia artificial, se identifican los temas en tendencia dentro de las redes sociales a través del monitoreo de los comentarios y visitas de los usuarios [24].

A nivel empresarial, las redes sociales permiten crear estrategias que impactan el entorno digital que, al ser combinadas con la IA, ofrecen canales de comunicación efectivos, con beneficios que llevan a las organizaciones a conseguir los objetivos que se proponen. La combinación permite automatizar tareas como las de servicio al cliente y la captación de nuevos prospectos [25], lo cual significa que se alcanzan efectivamente los objetivos de dichas estrategias.

C. Riesgos y vulnerabilidades de seguridad asociados al uso de IA

La inteligencia artificial plantea muchos interrogantes y conflictos que generan preocupaciones; uno de ellos, son las aplicaciones que se pueden dar en la animación de fotos y videos los cuales se podrían usar de forma tergiversada con fines publicitarios o de difamación; ejemplo de ello es el fenómeno popular denominado "deek fake" una aplicación que permite imitar la apariencia o el sonido de una persona llegando a ser tan convincente que puede engañar a los individuos y a los algoritmos de seguridad [26].

La IA tiene muchas ventajas, pero plantea retos en el momento de hablar de discriminación, garantías, transparencia e inteligibilidad de los procesos decisorios, lo que puede traducirse en la concentración del poder y la riqueza en minorías, además de existir la posibilidad de que llegue a superar la capacidad humana a largo plazo, riesgo que puede llevar a la pérdida del control de las personas pudiendo incluso atacar sin advertencia o provocación [27].

La ONU, resalta las aristas positivas de la inteligencia artificial y reconoce las negativas. Dentro de las positivas resalta la experiencia en donde cada persona encuentra la información que solicita de manera inmediata; sin embargo, esto al mismo tiempo implica una dificultad en el acceso a otros puntos de vista, es decir, interfiere con la posibilidad de visualizar ideas u opiniones que se tengan de otras posiciones [28]. En el mismo sentido [29], explica como en Facebook a través de los datos de navegación y las vistas de los usuarios, la inteligencia artificial perfila las historias y temas ocultando los que no concuerdan con un perfil específico, limitando las posibilidades y la autodeterminación del usuario. En este sentido, la IA podría llegar a afectar la libertad de expresión pues le es imposible evaluar el contexto, los aspectos culturales y los usos del idioma.

Cristina Pombo [30], coordinadora de fAir LAC, una alianza regional para uso responsable de la tecnología, identifica riesgos como la filtración de datos personales que puedan comprometer la información; el acceso, vigilancia y manipulación de la información que alimenta la inteligencia artificial por organizaciones privadas; los filtros de burbuja que se presentan cuando se hace circular un hecho o idea varias veces por las redes sociales fomentando sesgos preconcebidos y el acceso ilimitado a la información, sin tener un plan de acción para utilizarla.

La IA por medio de un sistema Machine Learning puede crear rostros ficticios altamente realistas que son empleados en delitos y estafas. estos rostros basados en algoritmos del Deep Learning permiten ser incorporados a imágenes, audios y videos [31]; esto representa un riesgo debido a la creación de identidades falsas que por su credibilidad aumentan las posibilidades de timo. En este sentido, la inteligencia artificial promueve engaños facilitando la entrega de datos confidenciales, claves, números de cuentas y otros productos que sirven para incrementar los delitos en línea [31].

Yendo más lejos, la inteligencia artificial supone un peligro en cuestiones relacionadas con las armas autónomas, en especial armamentos nucleares que no necesitan supervisión, tales como los drones inteligentes de ataque donde las órdenes sin especificaciones pueden afectar la convergencia de los objetivos esperados por el personal y por la máquina [32]. Un caso de este tipo, fue presentado por la revista Semana, en Estados Unidos [33] para el mes de junio de 2023; en él se muestra cómo en un ejercicio de simulación realizado por la Fuerza Aérea en la que se probaba la capacidad de respuesta de un dron para detectar, identificar y destruir blancos que representaran una amenaza, el dispositivo en una primera prueba, eliminó al operador (simulado) por considerarlo como un obstáculo para el logro de su objetivo; para una segunda prueba, se corrigieron las especificaciones al dron aludiendo no lastimar a su operador, entonces el dron siguió las indicaciones; sin embargo, continuó considerando a su operador como una barrera por lo que destruyó la antena de comunicación que él utilizaba para darle órdenes.

En este contexto, según la cita de Paula Adamo Idoeta [35] de la BBC News, el Profesor Stuart Russell de la Universidad de California compara la inteligencia artificial (IA) con un genio liberado de la botella. Esto se debe a que la IA sirve de base para construir máquinas con modelos estándar, programadas para alcanzar o maximizar objetivos mediante la mejor solución posible. En este caso, las máquinas pueden comportarse como psicópatas al perseguir sus objetivos de manera obsesiva, sin considerar

otros factores e incluso ignorando instrucciones de detenerse.

En las redes sociales la tarea de la IA, consiste en mejorar la experiencia del usuario proporcionándole contenidos que se adapten a sus preferencias, con el fin de que permanezcan más tiempo en ellas. Esto crea adicción, depresión, disfunción social y polarización, generando desinformación, algo que causa daño a la sociedad. Russel, afirma que los algoritmos no son sometidos a escrutinio para ser verificados, causando que sigan trabajando hasta lograr sus objetivos, sin tener en cuenta los daños colaterales[35]. Entonces, la IA está inmersa en las redes sociales manipulando a las personas haciéndolas más vulnerables hasta el punto de transformarlas, provocando divisiones sociales y afectación a la democracia.

D. Regulación de la I.A.

Para el año 2016, la Unión Europea como estrategia para la política exterior y de seguridad, evidenció la necesidad de crear normas mundiales en los ámbitos de inteligencia artificial, robótica, aparatos pilotados a distancia y biotecnología [35]. El marco legislativo de las innovaciones digitales debería, en este sentido aclarar la propiedad y el uso de los datos que se generan en contextos industriales y los sistemas que actuarían con autonomía y que representarían un desafío a las normas de responsabilidad y seguridad [36]. Con esto, la Comisión brindó unas recomendaciones generales en la creación de códigos y estatutos para la puesta en marcha de la inteligencia artificial y la responsabilidad de acuerdo con su uso [35].

En 2018, el Comité Económico y Social Europeo aprobó el "Dictamen del Comité Económico y Social Europeo sobre Confianza, privacidad y seguridad de consumidores y empresas en el internet de las cosas" [37], destacando la oportunidad que representa para empresas y personas, la capacidad de las máquinas para tomar decisiones automáticas sin intervención humana. Sin embargo, también reconocieron la necesidad de establecer una normativa que garantice la privacidad, seguridad e intimidad, debido a los vacíos legales en las normas europeas e internacionales.

Para el 2019, se suscribió en la Comisión del Parlamento Europeo, una comunicación como fase piloto para la implementación práctica del desarrollo y uso de la IA, basándose en normativas ya existentes como el Reglamento General de Protección de Datos, ciberseguridad y de la privacidad y las comunicaciones.

En 2020, el Consejo Europeo aprobó el Reglamento General de Protección de Datos (GDPR), que establece las reglas para el procesamiento y protección de datos personales de los usuarios en la Unión Europea. Esta normativa plantea importantes sanciones y multas a las organizaciones que no cumplan con las normas de privacidad y seguridad [38]. En 2021, la Comisión Federal de Comercio de los Estados Unidos (FTC), emitió una orden a Facebook donde debía cambiar sus políticas de privacidad. Esta orden requería que Facebook brindara a los usuarios más control sobre sus datos y al mismo tiempo, revelara cómo usa los mismos.

En Colombia, el marco normativo viene limitado al proceso de fabricación y comercialización visto desde las características de seguridad y el factor de calidad; en cuestiones relacionadas con labores similares a las de una persona ejecutadas por las IA, no se establece un marco legislativo aplicable. La normativa hasta el momento no ha establecido las responsabilidades en la gestión del riesgo a cada uno de los actores que otorgan las instrucciones y autonomía a la IA [39]; tampoco se ha hecho alusión a los términos de aprendizaje, autonomía, conciencia, razonamiento, capacidad de comprensión, emociones e inteligencia, los cuales son términos que tendrán otro significado en los espacios digitales. Así mismo,

no existe regulación en la implementación de procedimientos para las empresas que atiendan aspectos éticos, legales, de control y operativos que contemplen la posibilidad de que se presenten víctimas, daños materiales o alteraciones de la producción o de la información [39].

E. Operatividad de la IA en las redes sociales

X, llamado anteriormente Twitter: Las directrices y políticas generales de esta red social están estrechamente relacionadas con asuntos de interés público. La plataforma proactivamente identifica las publicaciones que podrían ser de utilidad informando a los usuarios; entre ellas se incluyen aquellas emitidas por funcionarios gubernamentales. En consecuencia, la red social otorga prioridad a la difusión de estos contenidos basándose en criterios específicos, como el cumplimiento de ciertas reglas; por ejemplo, que la cuenta del autor esté verificada, que tenga más de 100,000 seguidores y que pertenezca a un miembro del gobierno o a un candidato con cargo político [28].

Pese a esto, puede darse el caso de que un funcionario efectúe una publicación que vulnere las reglas, evento en el cual la plataforma emite un aviso en donde se puede elegir entre dos opciones: conservar la publicación o de lo contrario, ser eliminada. De esta forma se presenta un mensaje que contextualiza a los demás usuarios refiriendo el incumplimiento de la regla. Entonces, la IA disminuye la probabilidad de interactuar con la publicación por medio de los "me gusta" o las "publicaciones" [28]. Este ejemplo se muestra en la figura 1.

La normativa aún no ha establecido responsabilidades en la gestión del riesgo a cada actor que otorga autonomía a la IA

Figura 1. Medidas usando inteligencia artificial de Twitter

Fuente: Inteligencia Artificial, algoritmos y libertad de expresión. [28]

Facebook: Utiliza estrategias que consisten en quitar cuentas o contenidos que violen las normas de comunidad o políticas de publicidad con el fin de hacer una reducción en la distribución de noticias y contenido falso; las estrategias también informan a las personas acerca del contexto de las publicaciones que visualizan [28].

Igualmente, Facebook [40] aplica la IA en la revisión de contenidos detectando y eliminando las publicaciones que infrinjan las normas antes de que sean reportadas. En algunos casos, se envía el contenido a equipos de revisión manual para que sean analizados. De esta forma, la IA construye modelos de aprendizaje automático que pueden reconocer elementos dentro de una foto y analizar los textos de la publicación.

Instagram: La IA en Instagram es usada para hacer las experiencias atractivas y divertidas, siendo capaz de responder preguntas y dar consejos desde más de treinta perfiles personalizados [41]. Así mismo, la IA también es usada en nuevos formatos conversacionales y brinda ayuda a la hora de escribir mensajes a través de un chatbot. Algunas de las señales que la red social tiene en cuenta en la recomendación

de contenido, son los gustos guardados y compartidos, la actividad y el historial de interacción con otros usuarios [41].

F. Impacto de la Inteligencia Artificial en la seguridad de la información

Según las Naciones Unidas para los Derechos Humanos [42], los sistemas de Inteligencia Artificial amenazan potencialmente los derechos humanos, lo que exige que todos los programas deban cumplir con la normatividad internacional. La capacidad de aprendizaje de las máquinas puede afectar los derechos como el de la intimidad a la educación, a la libertad de reunión, de movimiento, de asociación e incluso, la libertad de expresión.

Las Naciones Unidas en su informe del año 2021 analizaron los aspectos de la IA, concluyendo que las grandes cantidades de datos recopilados para alimentar la inteligencia artificial, llegan a ser discriminatorias y deficientes, y que a largo plazo podrían generar riesgos particulares difíciles de prever. Un ejemplo claro de ello, son los sistemas de reconocimiento facial que identifican personas en tiempo real permitiendo un seguimiento ilimitado del individuo violando la privacidad, la protección de datos y más aún, la generación de efectos discriminatorios en ciertos grupos marginados [42].

La IA en redes sociales representa un riesgo a la intimidad y a la privacidad; cada día los intrusos invaden escenarios que llegan a la imitación o a la alteración de la apariencia, el tono de voz y otras características individuales para manipular o afectar la reputación de las personas [43].

Las redes sociales nacieron con el fin de integrar personas y la IA con la finalidad de procesar información para mejorar la experiencia del individuo; sin embargo, esta combinación está yendo más allá de compartir contenidos llegando a propagar ideologías distorsionadas, noticias falsas, vulgaridades y otros contenidos inapropiados con una habilidad y rapidez exponencial que pasa a convertir estos espacios virtuales en un arma letal para las personas [44].

La inteligencia artificial, a pesar de sus promesas para mejorar la experiencia del usuario, plantea importantes desafíos. Mientras que Barnes, De Vinck, Lima, Oremus y Wang [45] sugieren que el futuro de la IA es prometedor, la preocupación por la privacidad y seguridad de datos sigue siendo relevante. Además, surge el desafío de los filtros de burbuja, donde la IA puede intensificar preferencias y opiniones, generando aprendizajes sesgados que limitan la exposición del usuario a diversas perspectivas y polarizan sus puntos de vista. En consecuencia, la información presentada puede ser incompleta y segmentar aún más las opiniones de los usuarios.

A nivel de seguridad y ciberseguridad tanto nacional como internacional, la Inteligencia Artificial anticipa amenazas en el análisis de artículos, blogs y noticias, reduciendo considerablemente los tiempos de respuesta [46]. Son muchos los beneficios para la generación de respuestas rápidas y efectivas que brinda la IA, pero no se pueden ignorar los riesgos ni dejar de plantear preocupaciones sobre el manejo de datos sensibles, la fuga de información, los riesgos de sesgos en los algoritmos y la dependencia excesiva para disminuir la habilidad humana [47].

En relación con los sesgos algorítmicos, estos se presentan cuando un sistema informático refleja los códigos utilizados por las personas para su entrenamiento; pueden ser de tres tipos: Estadístico, que procede de la obtención de datos; cultural, derivado de la sociedad, el lenguaje que se habla o lo que se aprende (estereotipos); y el cognitivo, que identifica y depende de las creencias de las personas [48].

Según Morales [48], la seguridad de la información está influenciada por dos aspectos

fundamentales; en primer lugar, destaca la capacidad de la inteligencia artificial (IA) para tomar decisiones de manera automatizada; en segundo lugar, resalta el sistema a través del cual la IA recibe, aprende y se desarrolla con la información proporcionada. Esto implica que, para garantizar la seguridad en su implementación, es crucial combinarla con políticas adecuadas de tratamiento de datos privados y personales. Todo esto debe llevarse a cabo considerando el actual panorama tecnológico, mismo que ha experimentado un cambio significativo. Tecnologías como la inteligencia artificial y el aprendizaje automático, han alcanzado niveles de desarrollo que originalmente se proyectaban para el año 2030, afectando las capacidades de exploración en conjuntos de datos, razonamiento y provisión de información para la toma de decisiones [49]. Este avance tecnológico redefine las reglas del juego, tanto para la seguridad como para los ciberdelincuentes.

Con la información pertinente suministrada a la inteligencia artificial (IA), el software tiene la capacidad de identificar suplantaciones, incidentes y otras amenazas maliciosas, siempre y cuando sea gestionado de manera responsable. Este compromiso recae en los entes gubernamentales y políticos [49]. La efectividad de la IA se maximiza cuando se combina con una operación humana eficiente y se le suministran datos adecuados. En otras palabras, la eficacia de las tareas realizadas por el algoritmo aumenta proporcionalmente según la cantidad y calidad de los datos proporcionados. Sin embargo, es decisivo destacar que, si la información suministrada a la IA es limitada e insuficiente, existe el riesgo de que pueda vulnerar los derechos individuales de las personas [50].

El avance de la inteligencia artificial (IA) es motivo de preocupación, como lo han expresado figuras destacadas como Elon Musk y Stephen Hawking, quienes advierten que podría representar uno de los mayores desafíos en la historia de la civilización actual [51]. La preocupación respecto a la Inteligencia Artificial se basa en su capacidad para ajustar sus objetivos a medida que su inteligencia se expande. Conforme las máquinas adquieren la capacidad de reprogramarse de forma eficaz, surgen riesgos inminentes que podrían superar las capacidades humanas. El principal desafío y amenaza futura reside en la incertidumbre asociada con los límites que aún no se han contemplado ni controlado hasta el momento [22].

IV. RESULTADOS

Con base en el análisis de documentos centrados en la identificación de vulnerabilidades y riesgos, vinculados al objetivo primordial, se constata que los autores coinciden en que las principales amenazas y debilidades de la inteligencia artificial en el ámbito de la generación de contenido para redes sociales, se centran en la *violación de la privacidad,* la *confidencialidad y la polarización de los datos*. El uso indebido de la inteligencia artificial propicia la manipulación de la información por parte de entidades tanto privadas como públicas, dando lugar a prácticas que comprometen el bienestar de las personas.

En el contexto de las redes sociales, la inteligencia artificial (IA) persigue múltiples objetivos, entre ellos, mejorar la experiencia del usuario al proporcionar información atractiva basada en sus gustos y preferencias. No obstante, este enfoque genera un fenómeno de burbuja que refuerza sesgos preexistentes, fomentando la discriminación de grupos marginados y representando una amenaza para la libertad y la democracia. En el entorno de las redes sociales, la IA recopila información, la clasifica y la dirige hacia los usuarios mediante algoritmos que siguen patrones de búsqueda. Además, posee la capacidad de destacar cierta información mediante el análisis de la frecuencia de comparticiones y el número de vistas.

Con respecto al análisis de normativas y

regulaciones relativas a la IA, se observa que la legislación actual presenta deficiencias en cuanto a la asignación de responsabilidades entre sus productores y beneficiarios. Es imperativo abordar en un marco legislativo, los desafíos asociados con la autonomía, la estandarización de los procesos de evaluación y la destreza para prever el comportamiento a largo plazo de la inteligencia artificial. Además de la estructura normativa, es esencial incorporar en este ámbito, conceptos clave como aprendizaje, autonomía, libertad, inteligencia, capacidad de comprensión, razonamiento y procesos de toma de decisiones. Esto se debe a que aquellos conceptos pueden tener interpretaciones distintas en comparación con las normas que rigen la inteligencia artificial.

A nivel internacional, la inteligencia artificial viene ocupando un papel protagónico para la agenda mundial 2030, por presentar tantas formas para su utilización que pueden llegar a violentar los derechos de las personas siendo imprescindible el contar con una regulación normativa que la controle sin desalentar sus ventajas y desarrollo.

En relación con la determinación del impacto de la inteligencia artificial (IA) en la seguridad de la información, considerando las limitaciones técnicas y económicas de las empresas y organizaciones involucradas, se infiere que la IA ejerce un impacto positivo en el crecimiento económico, así como en la eficiencia y productividad organizacional, gracias a su capacidad de aprendizaje y toma de decisiones. No obstante, es trascendental señalar que este impacto positivo coexiste con escenarios críticos que afectan la privacidad, confidencialidad y seguridad de las personas.

Aunque se reconocen conscientemente los riesgos y vulnerabilidades asociados a la IA, aún persiste la incertidumbre en torno a los límites del desarrollo que esta pueda alcanzar. Se desconoce el punto crítico en el cual la humanidad no pueda revertir su relación con esta tecnología, la cual posee la capacidad de reprogramarse y eventualmente adquirir una singularidad que podría llevar al ser humano a percibirla como una amenaza.

V. CONCLUSIONES

La inteligencia artificial forma parte del desarrollo tecnológico que se encuentra presente en la vida de cada persona, y se potencializa cada vez más con un crecimiento exponencial; además, es una representación de los avances significativos y de alto impacto que ha realizado actualmente el ser humano. Existe una evidente dependencia hacia ella, gracias a su facilidad de recoger, analizar y propagar todo tipo de información.

A nivel industrial y empresarial, la IA amplía las capacidades en el manejo óptimo y eficiente de todos los procesos, aumenta la productividad y permite el cálculo de varios escenarios posibles analizando factores y estrategias que permitan determinar el mejor curso de acción.

Igualmente, la IA cuenta con numerosas posibilidades que pueden generar ventajas a sus usuarios; sin embargo, si no se controla, puede llegar a representar un riesgo y una amenaza para la seguridad. Esto genera la necesidad de explorar los futuros escenarios a los que se pueda enfrentar el hombre de cara a la inteligencia artificial.

Por otra parte, la IA se ha convertido en las redes sociales, en un pilar necesario para las interacciones, el acceso a la información y el intercambio de datos. Se ha vuelto tan esencial que a futuro no se podrá interactuar por estos canales sin ella, lo que representa un riesgo y vulnerabilidad en materia de libertad de expresión y polarización de contenidos.

En consecuencia, la inteligencia artificial ha tenido un impacto significativo en la sociedad, lo que ha motivado a las instituciones a incluirla en sus marcos legales, estableciendo normativas y reglamentos que aborden todas sus

potencialidades y planteen medidas de control adecuadas. Por lo tanto, es crucial evaluarla de manera interdisciplinaria para desarrollar aplicaciones legales que evolucionen en consonancia con su progreso y su potencial futuro.

VI.REFERENCIAS

[1] A. E. Carvajal, «Reflexiones sobre la seguridad de la información. Revista Sistemas, (155), 8-17.,» 2020. [En línea]. Available: https://sistemas.acis.org.co/index.php/sistemas/article/view/105.

[2] R. Hernández Sampieri, C. Fernández Collado y P. Baptista Lucio, « «Alcance de la Investigación,»,» 2014. [En línea]. Available: Available: http://metabase.uaem.mx/bitstream/handle/123456789/2792/510_06_color.pdf.

[3] E. Gomez Luna, D. Fernando Navas, G. Aponte Mayor y L. Betancourt Buitrago, «Metodología para la revisión bibliográfica y la gestión de información de temas científicos, a través de su estructuración y sistematización,» Vols. %1 de %2Dyna, 81(184). [En línea].

[4] S. M. Rollán Oliviera, «Profesionales de enfermería asturianos en el siglo XX y XXI: un estudio intergeneracional desde la perspectiva de género,» 2022. [En línea].

[5] A. O. Ortega, «Enfoques de investigación. Métodos para el diseño urbano–Arquitectónico.,» 2018. [En línea].

[6] C. Rudas Murga , «Redes sociales: inteligencia artificial en el derecho al honor desde una perspectiva peruana,» Lucerna Iuris Et Investigation.º 1 - 2021, pp. 99 - 110, 2021. [En línea]. Available: https://revistasinvestigacion.unmsm.edu.pe/index.php/Lucerna/article/view/20137/16532.

[7] A. Zaremba, M. Ivanov, K. Zaremba y Z. Ramzan, «Social Engineering Attacks Against Social Media: The Role of Artificial Intelligence. IEEE Transactions on Dependable and Secure Computing, 18(3), 1469-1483,» 2021. [En línea].

[8] V. Dignum, «Artificial Intelligence in Social Media. Tecnology and Society Magazine, 40(1), 68-73,» 2021. [En línea].

[9] Y. Li, «Generating emotionally appealing texts by incorporating stylistic variations and emotion clues. IEEE Transactions on Affective Computing, 11(2), 227-238.,» 2020. [En línea].

[10] Y. Liu, Y. Zhang, J. Wang y Y. Wang, «Fake News Detection on Social Media: A Survey. IEEE Transactions on Cybernetics, 51(10), 4736-4755.,» 2021. [En línea].

[11] T. G. Stavropoulos, M. Stratakis y A. Leonidis, «The Interpretation of Texts Generated by AI: A Review of Recent Research. IEEE Access, 9, 29544-29558.,» 2021. [En línea].

[12] W. Shi, S. Wu, X. Huang y X. Xie, «Intelligent content production and delivery for online advertising: An overview. IEEE Transactions on Industrial Informatics, 17(2), 1381-1389.,» 2021. [En línea].

[13] J. Lee, «The Effects of AI Implementation on Media Labor in the Fourth Industrial Revolution. IEEE Intelligent Systems, 35(2), 30-37.,» 2020. [En línea].

[14] D. C. Ametller , «El proceso normativo ante el avance tecnológico y la transformación digital (inteligencia artificial, redes sociales y datos masivos). Revista general de Derecho administrativo, 50.,» 2019. [En línea]. Available: https://d1wqtxts1xzle7.cloudfront.net/58794499/.

[15] J. Kerns , «What's the Difference Between Weak and Strong AI?,» 2017. [En línea]. Available: https://www.machinedesign.com/markets/robotics/article/21835139/whats-thedifference-between-weak-and-strong-ai.

[16] A. Hintze, « Understanding the four types of AI, from reactive robots to self-aware beings,» 2016. [En línea]. Available: https://theconversation.com/understanding-the-four-types-of-ai-from-reactiverobots-to-self-aware-beings-67616.

[17] Comisión Europea, « IA para Europa. Comunicación de la Comisión al Parlamento europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones.,» COM(2018) 237 final{SWD(2018) 137 final} Bruselas, 25.4.2018, p. 1. , 2018. [En línea].

[18] M. Armstrong , «The Future Of A.I.», The Statistics Portal,» 2018. [En línea]. Available: <https://www.statista.com/chart/6810/the-futu re-of-ai.

[19] SAS, «Artificial Intelligence, what it is and why it matter? Obtenido de SAS Analytics Insights,» 2021.[Enlínea].Available:https://www.sas.com/en_us/insights/analytics/what-isThomas,.

[20] L. S. Vailshery, «https://www.sas.com/en_us/insights/analytics/what-isThomas,,» 2021. [En línea]. Available: https://www.statista.com/statistics/973815/worldwide-digital-voice-assistant-inuse/.

[21] G. Todorov, «Artificial Intelligence Statistics for 2021 and Beyond.,» 2021. [En línea]. Available: https://www.semrush.com/blog/artificialintelligence-stats/.

[22] D. A. Gómez Llinás , «El Impacto de la inteligencia artificial sobre el ser humano y sobre su seguridad,» 2021. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repository.unimilitar.edu.co/bitstream/handle/10654/39998/EL%20IMPACTO%20DE%20LA%20INTELIGENCIA%20ARTIFICIAL.pdf?sequence=1&isAllowed=y.

[23] J. Celaya , «La Empresa en la WEB 2.0. Editorial Grupo Planeta,» 2008. [En línea].

[24] eCMetrics , «El Futuro de las Redes Sociales Dependerá de la Inteligencia Artificial,» 2023. [En línea]. Available: https://ecmetrics.com/es/el-futuro-de-las-redes-sociales-dependera-de-la-inteligencia-artificial/#:~:text=El%20Papel%20de%20la%20IA%20en%20las%20Redes%20Sociales&text=Es%20una%20forma%20eficaz%20de,entender%20el%20comportamiento%20del%20usuario.

[25] Coobis , «La IA y las redes sociales: descubre los beneficios que puede aportarte esta combinación,» 18 02 2022. [En línea]. Available: https://coobis.com/es/cooblog/ia-y-las-redes-sociales/.

[26] N. K. Barbero, «Deep Nostalgia: Deepfakes con Fines Nostálgicos. Riesgos de la IA Desde la Teoría del Bildakt.,» 2021. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://d1wqtxts1xzle7.cloudfront.net/85582725/BarberoNoelia_DeepLearning_Bildakt-libre.pdf?1651830634=&response-content-disposition=inline%3B+filename%3DDeep_Nostalgia_Deepfakes_con_Fines_Nosta.pdf&Expi.

[27] L. Cotino Hueso, «Riesgos e impactos del big data, la inteligencia artificial y la robótica. enfoques, modelos y principios de la respuesta del derecho,» 2019. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.researchgate.net/profile/Lorenzo-Hueso/publication/349494641_Riesgos_e_impactos_del_big_data_la_inteligencia_artificial_y_la_robotica_y_enfoques_modelos_y_principios_de_la_respuesta_del_Derec.

[28] M. E. Larrondo y N. M. Grandi , «Inteligencia Artificial, algoritmos y libertad de expresión,» 2021. [En línea]. Available: http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-86342021000100177.

[29] S. Alvaró, «El poder de los algoritmos: cómo el software formatea la cultura.CCCBLAB.Investigación e Innovación en Cultura,» 2014. [En línea]. Available: https://bit.ly/3tiAGrO.

[30] C. Pombo, «Los riesgos de la inteligencia artificial y algunas soluciones,» 2022. [En línea]. Available: https://blogs.iadb.org/conocimiento-abierto/es/riesgos-inteligencia-artificial/.

[31] Revista Semana , «Aparece la inteligencia artificial 'GAN', el nuevo peligro que amenaza a usuarios de redes sociales y otras apps,» 11 4 2023. [En línea]. Available: https://www.semana.com/tecnologia/articulo/aparece-la-inteligencia-artificial-gan-el-nuevo-peligro-que-amenaza-a-usuarios-de-redes-sociales-y-otras-apps/202327/.

[32] Winecta, «Principales riesgos de la Inteligencia Artificial,» 2021. [En línea]. Available: https://www.winecta.com/principales-riesgos-inteligencia-artificial/.

[33] Revista Semana, «). Dron militar controlado por inteligencia artificial eliminó a su operador humano por ser un estorbo para su misión,» 2023. [En línea]. Available: https://www.semana.com/tecnologia/articulo/dron-militar-controlado-por-inteligencia-artificial-elimino-a-su-operador-humano-por-ser-un-estorbo-para-su-mision/202351/.

[34] P. Adamo Idoeta, «BBC News Brasil en Sao Paulo. Por qué los algoritmos de las redes sociales son cada vez más peligrosos,» 12 10 21. [En línea]. Available: https://www.bbc.com/mundo/noticias-58874170.

[35] E. E. Aponte Pinzón , «Responsabilidad civil sobre la inteligencia artificial: La utilización de inteligencia artificial en el derecho colombiano.,» 2020. [En línea]. Available: https://repository.ucatolica.edu.co/server/api/core/bitstreams/9a8b22af-2168-423a-a643-3b29d60be5fa/content.

[36] Comisión Europea , «Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: "Digitalización de la industria europea Aprovechar todas las ventajas de un mercado único digital" 19 de a,» 2016. [En línea].

[37] C. E. y. S. Europeo, «ictamen del Comité Económico y Social Europeo sobre «Confianza, privacidad y seguridad de los consumidores y las empresas en el internet de las cosas» Diario Oficial de la Unión Europea. C 440. 61° año. 6 de diciembre de 2018, pp. C 440/8- C 440/13,» 2018. [En línea]. Available: https://www.scielo.org.mx/scielo.php?pid=S2448-51362020000300049&script=sci_arttext#B13.

[38] A. Garriga Domínguez , «La elaboración de perfiles y su impacto en los derechos fundamentale: una primera aproximación a su regulación en el reglamento general de protección de datos de la Unión Europea.,» 2018. [En línea]. Available: https://www.torrossa.com/gs/resourceProxy?an=4312255&publisher=FZ1825.

[39] T. D. Zabala Leal y P. A. Zuluaga Ortiz , «Los retos jurídicos de la inteligencia artificial en el derecho en Colombia,» 2021. [En línea]. Available: https://revistascientificas.cuc.edu.co/juridicascuc/article/view/3141/3339.

[40] Facebook, «¿Cómo utiliza Facebook la inteligencia artificial para moderar el contenido?,» 2022. [En línea]. Available: https://es-la.facebook.com/help/1584908458516247.

[41] Revista Semana , «Instagram se dejó seducir por la inteligencia artificial; esto es lo nuevo que ofrecerá y lo que la llevará a otro nivel,» 6 6 2023. [En línea]. Available: https://www.semana.com/tecnologia/articulo/instagram-se-dejo-seducir-por-la-inteligencia-artificial-esto-es-lo-nuevo-que-ofrecera-y-lo-que-la-llevara-a-otro-nivel/202327/.

[42] Naciones Unidas para los Derechos Humanos, «Los riesgos de la inteligencia artificial para la privacidad exigen medidas urgentes –Bachelet,» 2021. [En línea]. Available: Los riesgos de la inteligencia artificial para la privacidad exigen medidas urgentes –Bachelet.

[43] K. Crawford , D. Roel, T. Dryer , G. Fried y Green B, «AI Now 2019 Report. New York: AI Now Institute,» 2019. [En línea]. Available: https://ainowinstitute.org/AI_Now_2019_Report.pdf.

[44] Y. A. Viteri Alcívar, C. G. Minaya Vera , D. E. Salto Pinargote y M. T. Cano Montesdeoca, «Inteligencia artificial y nuevas tecnologías en tiempos de pandemia. UNIVERSIDAD, CIENCIA y TECNOLOGÍA Vol. 25, Nº 110 Septiembre 2021 (pp. 164-171),» 2021. [En línea]. Available: https://scholar.archive.org/work/usx7nxbvkjcw7id4nj44po2ala/access/wayback/https://www.uctunexpo.autanabooks.com/index.php/uct/article/download/488/930.

[45] R. Barnes, G. De Vynck, C. Lima, W. Oremus y A. B Wang , « Supreme Court considers if Google is liable for recommending ISIS videosTwitter, 2023. Algoritmo de Twit,» 2023. [En línea]. Available: https://saturdays.ai/2023/04/11/la-inteligencia-artificial-en-las-redes-sociales/.

[46] IBM, «Inteligencia artificial (IA) para la ciberseguridad,» 2023. [En línea]. Available: https://www.ibm.com/mx-es/security/artificial-intelligence..

[47] O. C. Rodríguez Martínez , «El Impacto de IA en la Seguridad de la Información: Beneficios, Riesgos y Recomendaciones,» 06 06 2023. [En línea]. Available: https://www.linkedin.com/pulse/el-impacto-de-ia-en-la-seguridad-informaci%C3%B3n-riesgos-oliverio-cesar/.

[48] A. Moales Cáceres , «EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN LA PROTECCIÓN DE DATOS PERSONALES,» 01 09 2020. [En línea]. Available: https://www.worldcomplianceassociation.com/2767/articulo-el-impacto-de-la-inteligencia-artificial-en-la-proteccin-de-datos-personales.html.

[49] Microsoft , «Microsoft Prensa. Qué impacto tendrá la Inteligencia Artificial en el futuro de la seguridad,» 09 05 2023. [En línea].

[50] FEDERAL TRADE COMMISSION (FTC);, «Protecting Consumer Privacy in an Era of Rapid Change. Recommendations for Businesses and Policymakers,» 2020. [En línea]. Available: https://www.worldcomplianceassociation.com/2767/articulo-el-impacto-de-la-inteligencia-artificial-en-la-proteccin-de-datos-personales.html.

[51] M. Thomas , «Dangerous Risks of Artificial Intelligence,» 2021. [En línea].

LA GUERRA EN EL MARCO DE LA INDUSTRIA 4.0: Aplicaciones, Recomendaciones y Advertencias.

ST. Andrés Felipe Rojas Vanegas
Oficial del Ejército
andres.rojasvanegas@buzonejercito.mil.co

RESUMEN- ***El presente artículo condensa el resultado de una exhaustiva investigación sobre las tecnologías que componen la industria 4.0 y su uso en el marco del desarrollo de los conflictos armados, con el propósito de entregar al lector una óptica detallada sobre cómo los ejércitos del mundo están empezando a integrar las nuevas tecnologías como un factor decisivo dentro de la guerra.Igualmente, se presenta un análisis objetivo de las diferentes vulnerabilidades y desventajas que se derivan de la implementación de estas tecnologías, ofreciendo una amplia visión, al igual que las recomendaciones para obtener el máximo provecho a su incorporación paulatina, dentro de futuras operaciones militares.***

Palabras clave: *Comunicación 5G, Conflictos armados, Industria 4.0, Inteligencia Artificial, Internet de las Cosas.*

Abstract- This article was crafted to condense the results of an exhaustive investigation into the technologies comprising Industry 4.0 and their application within the context of the development of armed conflicts. It provides the reader with a detailed perspective on how armies worldwide are beginning to integrate new technologies as a decisive factor in warfare.In addition to reviewing the advantages, an objective analysis of the various vulnerabilities and disadvantages arising from the implementation of these technologies is conducted, offering a 360° view and final recommendations to fully leverage their gradual incorporation into future military operations.

Keywords- *5G Communication, Armed conflicts, Artificial Intelligence, Industry 4.0, Internet of Things.*

I. INTRODUCCIÓN

Actualmente, la tecnología ha avanzado en forma exponencial, lo que ha traído consigo avances que resultan fascinantes y permiten vislumbrar múltiples usos en varios ámbitos; sin embargo, existe un desconocimiento de los posibles usos o aplicaciones de las tecnologías propias de la industria 4.0, debido a que no es un tema del cual se haya escrito lo suficiente ni en el cual se haya ahondado demasiado.

El objetivo del presente artículo, consiste en realizar un recuento de las aplicaciones de las tecnologías de la industria 4.0 en el ámbito militar, a partir de la revisión de las actuales aplicaciones; igualmente, informar las que se encuentran prontas a implementarse, así como sus vulnerabilidades y, la realización de una serie de recomendaciones para el aprovechamiento de las ventajas que trae su implementación. En este sentido, el presente artículo condensa información con respecto a un tema de actualidad, siendo las tecnologías propias de la industria 4.0, aquellas que en los últimos años han estado adquiriendo gran popularidad e influencia en la sociedad, ofreciendo un enfoque acerca de las aplicaciones en el ámbito militar, desde las siguientes ópticas: ventajas, desventajas, recomendaciones y ejemplos recientes para facilitar su comprensión al respecto.

II.METODOLOGÍA

La ruta metodológica de este artículo, se

fundamenta en una investigación descriptiva, con base en la revisión de literatura en fuentes de información secundarias y artículos relacionados con el tema en cuestión. Para ello, se dividió el proceso en la definición de los objetivos de investigación, el método de búsqueda, selección de descriptores empleados, criterios de inclusión y de exclusión.

En primer lugar, se realizó una categorización sobre los estudios e investigaciones existentes relacionados con la conceptualización de la industria 4.0; cuáles son las tecnologías que la integran, sus usos generales y una revisión a los posibles empleos que se le han dado en los conflictos armados, con el fin de obtener una percepción global de esta área de investigación.

Para el desarrollo de esta revisión bibliográfica, se consultaron bases de datos, tales como: Google Académico, Dialnet e IEEE Xplore, a través de la búsqueda por descriptores como "Industria 4.0", "Internet of Things" "Artificial Intelligence" y "5G Communication".

Posteriormente, a fin de abarcar documentos pertinentes y útiles para esta investigación, como *criterios de inclusión* se consideraron:

a. Publicaciones dirigidas específicamente a descripciones de la industria 4.0, las tecnologías que le pertenecen y temas fundamentales para entender el campo de las ciencias militares.
b. Estudios y artículos periodísticos publicados en inglés, español, ruso y francés.
c. Estudios nacionales e internacionales, especialmente de América Latina, Europa y Estados Unidos.

Criterios de exclusión:

a. Publicaciones anteriores al año 2010.
b. Artículos no relacionados con el tema de estudio, por ejemplo, tecnologías complementarias que no cuentan con un campo de aplicación a la industria 4.0 en la guerra.

La principal limitación encontrada en la realización de la revisión, correspondió al bajo número de publicaciones relacionadas con el campo de las ciencias militares y aún más, el reducido nicho de los análisis en el uso de tecnologías para el desarrollo de conflictos armados.

III. DESARROLLO Y DISCUSIÓN

A. Herramientas de la industria 4.0 en el conflicto

a) La guerra como motor de la innovación tecnológica:

La guerra, según Clausewitz [1], es un conflicto en una escala más amplia que representa una extensión de las relaciones políticas a través de medios no diplomáticos. Es un enfrentamiento entre dos o más partes que utilizan la fuerza para imponer su posición o intereses sobre el adversario. Es esencial obtener una ventaja significativa para lograr este objetivo. A lo largo de la historia humana, los avances tecnológicos han sido cruciales para obtener esa ventaja, y han surgido como resultado directo de la necesidad de mejorar la efectividad en el campo de batalla, lo que ha generado una carrera armamentística incansable.

El internet, la energía nuclear, el GPS y las computadoras han sido algunos de los inventos que fueron desarrollados en el marco de los conflictos armados para obtener una ventaja sobre la parte contraria. Cada vez más los conflictos se van tecnificando y avanzando paulatinamente, creando nuevos dominios más allá del terrestre, marítimo, aéreo y espacial, haciendo que la guerra llegue al dominio ciberespacial, permitiendo que las tecnologías de la información y los datos sean un nuevo escenario de los conflictos [2] .

Las revoluciones industriales son

momentos claves en la historia humana, donde se observaun salto tecnológico e industrial causado por el desarrollo e implementación de tecnologías innovadoras que modifican el marco industrial, económico y social [3], que a su vez generan un acelerado cambio de ritmo en cuanto al desarrollo tecnológico y armamentístico, aplicado a los conflictos armados.

b) Industria 4.0: Aplicaciones en los conflictos armados

Con la llegada de la cuarta revolución industrial, la era de la digitalización o la industria 4.0, se ha evidenciado un crecimiento exponencial de la tecnología y las TIC, al igual que una integración sinérgica entre los sistemas físicos, digitales y biológicos, para generar la digitalización e interconexión de los procesos industriales por medio de diferentes tecnologías distintivas de esta revolución industrial, como son: El internet de las cosas (IOT), la Big Data, la Inteligencia Artificial, la computación en la nube y la impresión 3-D.

En este artículo se revisará cómo algunas de las diferentes tecnologías propias de la industria 4.0 han sido empleadas en los conflictos dentro de la última década, qué implicaciones han tenido y qué riesgos o posibles peligros podrían advertirse como resultado de la implementación de las nuevas tecnologías; y por último, algunas recomendaciones que pueden realizarse después de analizar los conflictos.

c) Inteligencia Artificial:

Según F. Rozo [3] la inteligencia artificial es una rama del conocimiento de naturaleza multidisciplinar, que involucra varios campos científicos, entre los que se encuentran: computación, información, lógica, matemática, estadística, biología, lingüística y otras más, para imitar el comportamiento de la mente humana por medio del uso de una serie de algoritmos y de esta forma, realizar tareas que requieran la inteligencia humana.

Algunas de estas actividades, otras podrían ser: aprender, razonar, resolver problemas, percibir visualmente, reconocer voz y rasgos distintivos, tomar decisiones, traducir idiomas, entre otras, pero es dentro del ámbito de los conflictos armados y de la seguridad y defensa que la IA ha tenido varias aplicaciones, como son: apoyo a la toma de decisiones, simulación de escenarios de operaciones militares, ciberdefensa y uso de vehículos autónomos.

A continuación, se presentará una serie de usos y aplicaciones de la Inteligencia Artificial en conflictos armados, describiendo en qué consiste cada uno de ellos y permitiendo al lector vislumbrar una dimensión totalmente diferente a la convencional.

Rusia vs Ucrania: La explosión de la IA / Detección y aprendizaje de tácticas enemigas: El As americano en Ucrania.

Si bien la inteligencia artificial no es una tecnología relativamente reciente, porque ha sido estudiada y desarrollada desde mediados de la década del 40, es en los últimos diez años donde se ha podido evidenciar un crecimiento exponencial que se ha reflejado en el empleo de múltiples ámbitos civiles y militares, siendo una de las tecnologías pertenecientes a la industria 4.0 más conocidas por el colectivo hoy en día. Es desde el año 2022, con el inicio del conflicto entre Rusia y Ucrania, que se empieza a evidenciar una tendencia bastante notoria en cuanto a la predilección de uso de herramientas que integran la Inteligencia Artificial por parte de los bandos beligerantes protagonistas del conflicto y también de otros que tienen participación en el mismo.

Aparece en escena EEUU, Estado con injerencia indirecta en el mencionado conflicto, que por intermedio de su Departamento de Seguridad (DoD), ha empleado sistemas de IA y machine learning para analizar los datos que recibe del conflicto entre Rusia y Ucrania, para realizar un análisis de millones de ellos, al igual

que imágenes públicas y secretas de los movimientos de las tropas rusas y, de esta forma, alimentar sus algoritmos con el objeto de predecir posibles escenarios, maniobras, técnicas y tácticas empleadas por los Rusos [4].

Esto quiere decir que están aprovechando datos obtenidos presuntamente por servicios de inteligencia de alguna de las partes involucradas y por satélites estadounidenses, para analizarlos mediante un proceso de aprendizaje realizado por inteligencia artificial y de esta forma, efectuar seguimiento a los movimientos de las tropas rusas. Lo anterior se traduce sencillamente, en que la IA aprende las maniobras, técnicas y tácticas que emplean las tropas rusas para desglosarlas y así, servir de herramienta al momento planear maniobras para contrarrestar a esas mismas tropas.

La ventaja tecnológica que recibe Ucrania gracias a EEUU y a su desarrollo de herramientas de Inteligencia Artificial, ha resultado ser bastante importante en el marco del conflicto, no solo porque se trata de las primeras implementaciones de la IA en el desarrollo de un conflicto armado de gran magnitud, sino porque otorga una gran ventaja estratégica y táctica a los ucranianos, al poder "predecir" las maniobras rusas.

Sistemas de Armas Autónomas: Robots asesinos como protagonistas del conflicto.

Los vehículos aéreos no tripulados (en adelante VANTs) son aeronaves controladas de manera remota, es decir, que no poseen tripulación humana en su interior que realice funciones de pilotaje, razón por la cual los VANTs poseen características claves como un tamaño reducido, poco peso y la capacidad de planear. Es por estas características que en el ámbito militar son empleados para misiones de reconocimiento o en ocasiones, en operaciones ofensivas desde áreas de alto riesgo o que tienen un acceso complejo y reducido.

Sin embargo, en la frenética carrera por obtener ventaja sobre el enemigo, las empresas fabricantes han realizado investigaciones y pruebas en diferentes modelos de VANTs para desarrollar equipos más eficientes y tecnológicamente superiores, ya sea con mejoras en la capacidad de autonomía o en la exactitud del control; también, en la implementación de cámaras con mejor resolución o a partir de la implementación de un algoritmo basado en IA, como es el caso de los sistemas de armas autónomas.

En referencia a lo anterior, el Comité Internacional de la Cruz Roja (en adelante CICR), define los sistemas de armas autónomas como aquellos que tienen la capacidad de seleccionar objetivos y de aplicar la fuerza sin la necesidad de intervención humana [5]; es decir, no es necesario que un ser humano se encuentre controlando en tiempo real el arma en cuestión para dirigir el movimiento del sistema, seleccionar y posteriormente causar una afectación a un objetivo militar.

En ese sentido, el desarrollo de la capacidad de autonomía en estos sistemas de armas, genera un salto abismal con respecto a la implementación y el uso de este tipo de tecnología, teniendo en cuenta que en el pasado se empleaban para labores de reconocimiento y recolección de información en el campo de combate o en la conducción de operaciones militares, conociéndose popularmente como *Drones Kamikaze,* los cuales siempre eran controlados por un piloto a la distancia. Actualmente, en el desarrollo del conflicto de Rusia y Ucrania, se ha evidenciado que ambas partes del mismo emplean activamente sistemas de armas autónomas en el desarrollo de operaciones militares, principalmente siendo empleadas con la finalidad de afectar y neutralizar sistemas de radares, antenas, convoyes o patrullas de vehículos militares; de esta forma, se obtiene una gran ventaja militar, porque no implica arriesgar las propias tropas, que adicionalmente, gracias al tamaño y a la

velocidad de los VANT, poseen un "gran factor de sorpresa".

El ejército ruso se encuentra haciendo uso de un sistema de armas autónomas de fabricación rusa llamado KUB-BLA [6], un vehículo aéreo no tripulado (VANT) dotado con cámaras e inteligencia artificial con la capacidad de llevar una carga de 3kg de explosivos por 30 minutos a una velocidad máxima de 130 km/h, el cual ha sido diseñado para identificar objetivos en tiempo real y estrellarse contra estos, para neutralizarlos y dejarlos inhabilitados.

En contraparte, Ucrania también ha empleado sistemas de armas autónomas similares, como son los drones turcos TB2 y los Switchblade [7], catalogados como municiones merodeadoras o drones kamikaze [8] de fabricación americana dotados de IA, que han sido diseñados para detectar y seleccionar objetivos en tierra para de igual forma, estrellarse contra estos y de esta forma, neutralizarlos o afectarlos.

A continuación, en la Figura 1, se presenta la comparación de las características técnicas de los vehículos aéreos no tripulados, para visualizar en forma estructurada, las ventajas y diferencias que aportan los modelos más empleados en el conflicto Rusia-Ucrania:

Figura 1. VANTs en el conflicto Rusia y Ucrania

País parte del conflicto	UCRANIA	RUSIA
Modelo	SwitchBlade 600L	Kub-Bla
Fabricante	AeroVironment	Kalashnikov Corp.
Origen	EEUU	Rusia
Velocidad Maxima	113 – 185 Km/h	80 – 130 km/h
Explosivo	15kg de Explosivo antitanque usado en los Javelin (ATGM)	3kg dc explosivo
Autonomía Max	40 min	30 minutos
Altura	NA	16.5 cm
longitud	1,30 cm	95 cm
Diámetro	150 mm	NA
envergadura	NA	1.21 m
Uso IA	Identificación de objetivos en tiempo real	Identificación objetivos en tiempo real Guiado y control del VANT

Fuente: Autor

Como se revisó previamente, la Inteligencia Artificial en el campo de los VANT implica un avance representativo, debido a que dota de gran autonomía a las aeronaves y desliga de cierta forma a sus pilotos, en el momento de tener que maniobrar a la distancia para seleccionar y atacar a los objetivos; no obstante, esto crea un dilema moral y legal que se revisará posteriormente.

IA y OSINT: combinación para entender al enemigo mediante inteligencia militar

La información es un conjunto organizado de datos, incalculablemente valiosa en cualquier ámbito, sea en el empresarial o en el militar; en este último enfoque, la información es el activo más importante que se pueda poseer y puede evidenciarse en: información del terreno, del enemigo, de las propias tropas, de técnicas y tácticas del adversario o del planeamiento del mismo, los cuales pueden en ocasiones ser la diferencia entre la victoria y la derrota militar, o en otras palabras, la vida y la muerte.

Existen demasiadas formas para preservar, obtener y aprovechar la información que se posee o que se obtiene, pero específicamente, para los fines de este artículo se revisará el uso de la inteligencia de fuentes abiertas en una relación sinérgica con la IA en el ámbito militar.

Según el Departamento de Seguridad de los Estados Unidos, la información de fuentes abiertas (desde ahora OSINT), puede ser

recopilada explotada y difundida a una adecuada para suplir un requisito de inteligencia [10]. Es así como dentro de este conflicto, se ha aprovechado la tendencia del ser humano a estar conectado y de encontrarse contantemente suministrando información a fuentes de datos abiertas, tales como: blogs, redes sociales, publicaciones o datos comerciales.

En consecuencia, por medio de la IA y de personal especializado se recopila esta información y después de un proceso de análisis, se obtiene un producto de inteligencia militar, lo cual ayudará a quien la posea a tener una ventaja significativa sobre el enemigo. Ya lo había mencionado Sun Tzu [11] en una época donde no habían tantos avances en materia marcial; así mismo, lo han reafirmado bastantes doctrinantes de las ciencias militares a lo largo de la historia, quienes han demostrado que la inteligencia resulta ser un factor crucial en el desarrollo de un conflicto.

En este sentido, por medio del empleo de la IA y de la producción de OSINT, el Ejército ucraniano ha obtenido información en tiempo real sobre localización y movimiento de personas, para de esta forma anticiparse, tomar decisiones y planear operaciones militares, lo cual ha sido una ventaja para este país en el mencionado conflicto.

DeepFake: desinformación y guerra contra la moral combativa

Como se ha revisado con anterioridad, las guerras han mutado, evolucionado y por consiguiente, también lo han hecho los medios y métodos para hacer y conducir las hostilidades; el general chino Sun Tzu [11] propuso en su obra que la excelencia consistía ganar las batallas sin luchar. Sin lugar a duda, esto ha sido puesto en práctica innumerables veces, en distintos conflictos y diferentes momentos de la historia humana.

En efecto, los DeepFake [12] son videos, imágenes o audios de índole hiperrealista que emplean los cambios de rostro para manipular, desinformar, alterar o implantar una idea que parece verdadera en el colectivo. En los últimos años, los DeepFake se han vuelto cada vez más posibles de realizar, adquiriendo gran popularidad gracias a que las herramientas de inteligencia artificial están al alcance de la población.

Los DeepFake son producto del Deep Learning, una herramienta de la inteligencia artificial que hace uso de las redes neuronales para simular el comportamiento del cerebro humano. Esto dificulta la detección de anomalías que pongan al descubierto que se trata de un contenido falso, lo cual genera la falta de confianza a nivel mundial sobre la veracidad del contenido, que puede ser emitido en periódicos, radio, redes sociales, televisión, etc [13].

En el conflicto de Rusia y Ucrania se dio un caso de DeepFake que llegó a ser muy conocido y publicado en el año 2022, y se afirma que es el primer Deepfake empleado en un conflicto armado [14]. Al respecto, se puede ver al presidente ucraniano Vlodimir Zelenski haciendo un llamado a sus hombres a deponer sus armas y a no combatir; este video en cuestión fue subido por una reconocida cadena de televisión ucraniana (Ukraine 24), que fue hackeada por cibercriminales rusos y que posteriormente adquirió bastante popularidad en redes sociales como YouTube, Facebook y VKontakte.

A pesar de que este video era de baja calidad y podía determinarse que era falso solo con analizarse, rápidamente se volvió viral por varios motivos: el algoritmo de recomendaciones de las redes sociales, el impacto mediático que implica la figura de Zelenski en el conflicto de Rusia y Ucrania y la ola masiva de reposteos del video para desmentirlo; pero el hecho de que se haya detectado, desmentido y eliminado el video, no garantiza que no haya afectado la moral combativa de las tropas y del pueblo ucraniano, siendo una operación psicológica por parte del

ejército Ruso en aras de debilitar y obtener una ventaja sobre su contraparte [15].

B. Internet of Things / Internet de las Cosas (IoT)

El Internet de las Cosas o Internet of Things, es una tecnología insignia de la industria 4.0, que permite conectar al internet los elementos físicos, y que por esto mismo, tiene un amplio uso en el ámbito civil. En los últimos años también se ha llevado al campo militar mediante varias aplicaciones, que van desde la salud y la seguridad de los soldados, la detección y neutralización de amenazas, el sostenimiento en la logística (municiones y material de combate) y las comunicaciones militares, entre otros.

El IoT en el ámbito militar busca mejorar la efectividad de los sistemas militares por medio de una red de sensores, dispositivos de IoT y accesorios portátiles que se encuentran conectados a la red [16], mismos que portan los combatientes en el área de operaciones para realizar ciertas actividades que principalmente permitirán la conexión permanente a la nube y de esta forma, mantenerse comunicados más allá de los sistemas de comunicaciones militares convencionales.

Los autores Gotarene y Raskar [17], además de enlistar diferentes usos y aplicaciones, hacen énfasis en que la aplicación de esta tecnología en el ámbito militar requiere alto nivel de seguridad, para lo cual exponen un protocolo seguro y adecuado para las características que intrínsecamente acarrea dicho ámbito. Entonces, la seguridad es un factor fundamental para la implementación de esta tecnología, toda vez que ignorar u omitir el correcto establecimiento del protocolo y unas medidas de ciberseguridad robustas y eficientes, podrían llegar a materializarse en un DoS o un DDoS (Distributed Denial-of-Service) y con esto, obtener una ventaja significativa sobre el enemigo en cualquier conflicto armado.

Estos ataques para la denegación de servicios, han sido evidenciados en varios momentos de la historia dentro de las últimas dos décadas, entre los cuales se destaca el conflicto Rusia – Georgia de 2008 [18], Rusia – Ucrania por Crimea en 2014 [19] y el conflicto actual Rusia – Ucrania [20], sin ahondar en los numerosos ataques que sufren países como EE. UU., China, Singapur, Vietnam, Indonesia, Canadá e Israel [21].

Por otra parte, algunos de los usos que permite el Internet de las Cosas del Campo de Batalla (IoBT) son los siguientes:

Seguimiento de la batalla en tiempo real:

El Mando Tipo Misión, es una función de conducción de la guerra, la cual se define como "el conjunto de tareas y sistemas relacionados entre sí, que permite al comandante integrar, sincronizar y articular elementos de poder de combate con el fin de concentrar sus efectos en el momento y lugar decisivos" [22] y [23]; lo anterior quiere decir que es un factor clave por medio del cual el comandante puede equilibrar el arte del mando con la ciencia del control para obtener una ventaja sobre el enemigo.

Es decir, que el Mando Tipo Misión resulta ser la expresión del mando y control del comandante en adición a la libertad que se permite al subalterno para el desarrollo de sus tareas o misiones en el marco de una operación militar, siguiendo la intención del comandante durante el cumplimiento de la misión.

El ejercicio del Mando Tipo Misión, implica la existencia de una comunicación precisa y continua entre el mando y sus tropas, para realizar el seguimiento a la batalla y facilitar al comandante el proceso de planeamiento, teniendo en cuenta las coordenadas exactas en las que se encuentran ubicadas las tropas que comanda y de esta forma, realizar estimaciones respecto al terreno, evaluar los cursos de acción que implica una maniobra, emitir órdenes o eventualmente, sortear una dificultad que

aparezca repentinamente excediendo el planeamiento realizado.

Desde esta perspectiva, el seguimiento operacional a las tropas o seguimiento a la batalla mencionado anteriormente, resulta ser muy efectivo debido a que es una práctica ya empleada y mantenida en el tiempo; sin embargo, como se mencionó al inicio del presente artículo, la guerra y la tecnología se encuentran estrechamente ligadas, y es entonces que, conforme se van desarrollando innovaciones como el IoBT, estas se van implementando y van remplazando técnicas que se empleaban en el pasado.

El Internet de las Cosas en el Campo de Batalla (IoBT) ya descrito, se compone de una serie de sensores que, de acuerdo con Kott [24] , Tayadoni [25] y Zhu [26], hay una serie de estos que al analizarse, se evidencia que pueden integrarse para realizar el ejercicio del comando y control, además de garantizar las comunicaciones, siendo una herramienta fundamental para el aseguramiento de la Función Conducción de la Guerra de Mando Tipo Misión (MTM).

Los sensores de movimiento, las cámaras y los micrófonos son herramientas que al encontrarse conectadas por medio de IoT, pueden dar información en tiempo real con respecto a la ubicación del combatiente, las imágenes que visualiza y los sonidos que se encuentran en el área de operaciones. Lo anterior complementa la información que tiene el comandante sobre los elementos del ambiente operacional, además de proporcionar la capacidad de enviar mensajes en tiempo real desde una sala de comando y control; de esta forma se convierten en herramientas claves para el mando y el control durante el desarrollo de las operaciones militares.

En conclusión, desde el campo del seguimiento operacional, se está llevando una carrera frenética para desarrollar la herramienta que permita integrar sensores y comunicaciones en el equipo de los soldados o de los comandantes que lideran la maniobra en el terreno donde se desarrollan las operaciones militares, con el fin de facilitar el proceso de planeamiento y mejorar exponencialmente el control que poseen los comandantes desde el nivel táctico hasta el nivel estratégico.

Drones y Vehículos Conectados a la Red: Los sentidos del comandante

Anteriormente, se habían mencionado los vehículos aéreos no tripulados desde el punto de vista de los sistemas de armas autónomas; sin embargo, dentro de la rama del Internet de las Cosas, se ha encontrado que puede llevarse un paso más allá el control y el seguimiento con respecto a lo que sucede en el área de operaciones; es entonces que mediante la adición de una serie de sensores y conexiones a la red, se transforma a los vehículos terrestres tripulados y a los vehículos aéreos no tripulados convencionales (UAVs) en "Vehículos IoBT".

La adición de varios sensores, como sensores inerciales, de fuerza y de movimiento, acelerómetros, giroscopios, sensores de presión de neumáticos y sistemas de control de vehículos, permite obtener información detallada sobre el estado del vehículo y las características del área de operaciones. Esto proporciona un entendimiento más completo del entorno en el que se trasladan tropas, material o se realiza el reconocimiento del terreno.

Los sensores mencionados anteriormente funcionan como una herramienta para obtener una retroalimentación detallada del dispositivo en cuestión o del área de operaciones en avanzada. Como se analizó en el apartado de Inteligencia Artificial, esto se convierte en un insumo valioso para el comandante en el campo de batalla, proporcionándole una ventaja estratégica que debe ser capitalizada en el diseño de futuras operaciones militares.

En adición a lo revisado previamente, se encuentra lo realmente fascinante e innovador referente a la tecnología del Internet de las Cosas del Campo de Combate (IoBT) y es, como su nombre lo indica, la conexión a internet o a una red especifica mediante la cual se va a realizar el intercambio de paquetes de datos (entre los cuales circulará la información que los vehículos recogen en sus misiones), dando de esta forma una comunicación efectiva en tiempo real entre el vehículo y el centro de control, evitando que se pierda tiempo esperando a que retorne al mismo centro de control para recibir la retroalimentación, toda vez que el tiempo en el desarrollo de una operación militar resulta ser un activo vital.

En conclusión, el IoT gracias a sus características y a la posibilidad de integrar redes de dispositivos conectados a la red podrá continuar implementándose y ser de vital importancia en el desarrollo de las operaciones militares, ya que metafóricamente se convertirán en los ojos y oídos del comandante en el campo de combate, además de extender aún más la posibilidad de ejercer comando y control por parte de los comandantes.

C. Comunicaciones 5G

La comunicación digital [27], es decir, el conjunto de procesos y tecnologías que permiten la transferencia de datos y la interacción en línea, es un pilar crucial de la industria 4.0. Además de facilitar el envío, recepción y acceso a información, estos sistemas han transformado la forma en que el mundo interactúa y opera. Con el continuo avance tecnológico, las telecomunicaciones se han vuelto cada vez más relevantes al atender las necesidades emergentes y permitir la conectividad global, asegurando así el éxito y desarrollo sostenido de la industria.

La conectividad, velocidad, disponibilidad y la confiabilidad de la información, son requisitos fundamentales que los usuarios demandan y que las empresas de telecomunicaciones han establecido como objetivos primordiales en su competitiva trayectoria por satisfacer las expectativas del mercado [28].

En respuesta a estas crecientes exigencias y como resultado de los avances inherentes a la evolución industrial en el campo de las telecomunicaciones, ha surgido la quinta generación de tecnología móvil, conocida como 5G. Esta nueva generación, que sucede a las previas 4G (LTE) y 3G, representa un salto significativo en términos de velocidad, capacidad, latencia y confiabilidad, introduciendo mejoras revolucionarias que han transformado la manera de conectarse y comunicarse.

5G: Revolución en las comunicaciones militares

Las comunicaciones militares comprenden un conjunto de medios y sistemas, sean tecnológicos o analógicos, que son empleados por los comandantes a todos los niveles para transmitir, recibir información u órdenes; de esta forma, se mantiene el comando y control en desarrollo de las operaciones militares [29]. Su relevancia radica en que proporciona el medio para mantener una comunicación ininterrumpida y, por consiguiente, un flujo constante de información, en cualquier momento durante el desarrollo de una misión en el área de operaciones.

Es decir, las comunicaciones militares son una herramienta clave mediante la cual los comandantes pueden ejercer el comando y control, y de esta forma, emitir órdenes para prevenir ataques, responder a hostilidades y maniobrar de determinada forma frente a una amenaza salvando las vidas de sus subalternos, garantizando el éxito militar y el cumplimiento de la misión.

Las comunicaciones militares han existido desde el inicio de la humanidad y han avanzado con la guerra: desde las civilizaciones antiguas, donde los mensajeros entregaban información

a pie, hasta nuestros días. Actualmente, con el extenso uso de las Tecnologías de la Información y las Comunicaciones (en adelante TIC), han comenzado a desarrollarse y adoptarse nuevas tecnologías, como el 5G.

Pese a que actualmente esta tecnología se encuentra aún en desarrollo y en estudio dentro del ámbito militar, se encuentran varios países que han notado del potencial que representa implementar el 5G en sus equipos de comunicaciones, debido a que existen características propias de esta nueva quinta generación de comunicaciones, como por ejemplo:

• *Ondas milimétricas:* Las comunicaciones 5G trabajan con ondas de ultra alta frecuencia, gracias a la alta frecuencia de sus ondas (300 MHz – 300 GHz) lo que hace posible realizar comunicaciones Full Duplex de super alta velocidad, permitiendo el recibimiento y la transmisión simultanea de paquetes de datos a una velocidad de 10 Gigabits por segundo, dejando muy por detrás a la 4G, que permitía una velocidad de 100 Megabits por segundo.

• *Latencia Reducida:* Las comunicaciones 5G gracias a la velocidad de carga y descarga de paquetes de datos, permite la comunicación con una latencia de entre 1 y 2 milisegundos, la cual resulta ser muy superior a la latencia que presentaba 4G.

• *Equipos compactos:* Gracias a la corta longitud de las ondas UHF, los equipos que se emplean para transmitir y para recibir estas ondas van a ser cada vez más compactos, debido a que estos tienen una relación directamente proporcional con la longitud de la onda, permitiendo que sean más tácticos, ligeros y fáciles de incorporar en el desarrollo de operaciones militares.

• *Redes 5G:* La posibilidad de crear redes 5G permite conectar una cantidad mil veces mayor que su antecesora, lo cual permitirá que se puedan integrar gran cantidad de dispositivos al mismo tiempo sin el riesgo de comprometer la velocidad o la latencia, siendo una ventana de oportunidad para la implementación de dispositivos accesorios de IoT o de IoBT haciendo posible que exista una comunicación efectiva, que se realice en una fracción del tiempo al que se acostumbraba a experimentar.

La creación de redes 5G permite empezar a vislumbrar la posibilidad de crear (en el ámbito civil y comercial) ciudades inteligentes, las cuales serán posibles gracias a la conexión masiva de dispositivos IoT a la red en cuestión, lo que facilita una comunicación veloz, eficaz y confiable creando un ambiente inteligente en las cosas cotidianas. En el ámbito militar se aterrizaría a la creación de bases militares inteligentes que permitan integrar de manera efectiva sensores, alarmas, antenas, vehículos y dispositivos que permitan a la tropa una mayor capacidad de control de todos los aspectos de la base en cuestión.

Lo anterior proporciona al lector una idea más clara de los posibles usos que podrían darse a los dispositivos de comunicaciones que incorporen la tecnología 5G, enfocándose especialmente en: seguridad perimetral, comunicación dispositiva a dispositivo (D2D) a través de la red 5G, seguimiento a la batalla y el comando y control.

D. Recomendaciones y advertencias frente a la implementación de las tecnologías de la industria 4.0

Anteriormente, se realizó una revisión de las principales tecnologías de la industria 4.0 y su aplicación en el ámbito militar, resaltando una serie de ventajas que las hacen llamativas con el fin de ahondar más en éstas para implementarlas; sin embargo, existen una serie de aspectos que,

deben revisarse y tenerse en consideración como lo son:

IA: responsabilidad y autonomía

La Inteligencia Artificial se ha popularizado y se ha implementado ampliamente en los últimos años. Esta tecnología tiene una amplia gama de usos y puede ser muy beneficiosa en términos de automatización y realización de tareas monótonas y repetitivas de manera más rápida y, en ocasiones, más efectiva que un ser humano. No obstante, al examinar cómo se ha utilizado la IA en la guerra, se puede notar que a veces atraviesa fronteras éticas y plantea una serie de dilemas y problemáticas, tales como:

• *Sistemas de Armas completamente autónomos:* La Inteligencia Artificial ha sido una pieza clave para que los VANTs empiecen a ser cada vez más investigados e implementados en el desarrollo de los conflictos armados, como es el caso actual de Rusia – Ucrania, donde se han empezado a utilizar sistemas de armas autónomas que tienen la capacidad de seleccionar sus objetivos en pleno vuelo y neutralizarlos.

En el ámbito del Derecho Internacional Humanitario, se da un debate ético y legal sobre la habilidad que podrían tener los sistemas de armas autónomas para elegir sus objetivos y realizar un juicio sobre la naturaleza de sus propósitos dentro del marco legal que rige los conflictos armados. Esto implica que dichos sistemas deberían cumplir con los principios fundamentales del DIH: Distinción, precaución, proporcionalidad y respeto a la humanidad.

Para no ahondar demasiado en la revisión de la discusión ética y legal con respecto a los sistemas de armas autónomas, por la naturaleza de este artículo, se limitará la revisión únicamente a los principios de distinción y de proporcionalidad.

a. Principio de Distinción: Consiste en la capacidad para diferenciar entre un combatiente y un no combatiente, un bien protegido, de un objetivo militar; en pocas palabras, dejar por fuera de las hostilidades a los bienes y personas protegidas por el DIH, enfocando las operaciones militares en bienes o personas que se puedan considerar como objetivos militares, evitando así que se ataque a la población civil, o que se lancen ataques indiscriminados.

Respecto a esto, varios autores proponen que a pesar de la avanzada tecnología que existe en relación con la IA, las armas autónomas no garantizan ser capaces de distinguir y por ende ser garantes del principio de distinción [30]. Aunque un algoritmo podría seleccionar un objetivo basado en su programación, la identificación completa de un objetivo militar legítimo es el resultado de diversos factores, como su uso, ubicación y función, entre otros [31]. Esta tarea requiere la capacidad de razonamiento propia de un ser humano.

Puede que exista un algoritmo que emplee sistemas de reconocimiento biométrico o un algoritmo para identificar objetos, pero estos softwares no resultan ser exactos a la hora de diferenciar entre un objetivo militar de una persona o bien protegido, debido a la complejidad de los conflictos armados, las características tecnológicas y técnicas de los VANTs y las condiciones del terreno en las que se emplearían los VANTs.

b.Proporcionalidad: El principio de proporcionalidad es la relación existente entre los daños, la ventaja militar concreta y la directa prevista, en donde la ventaja debe exceder y ser superior a los posibles daños incidentales que pueda causar, siendo de esta forma uno de los pilares fundamentales para planear y conducir una operación militar.

Es en esencia, uno de los fines últimos del DIH: menguar los daños excesivos e innecesarios de los conflictos armados, humanizando el

conflicto. Es meritorio y casi obligatorio hacer énfasis en la palabra humanizar, toda vez que es una palabra que dota de total sentido a este marco legal al definir la naturaleza de todos los actos que buscan minimizar los daños excesivos a quienes no participan directamente en el conflicto, siendo actuar con "humanidad" una propiedad únicamente factible y atribuible al ser humano, tal y como lo afirma Gorrín Mérida [32].

En los conflictos armados, existe una gran responsabilidad respecto al planeamiento y al desarrollo de las operaciones militares, la cual va ligada al principio de proporcionalidad, debido a que si dentro de la estimación de la maniobra, se evidencia o se predice que puede llegar a causar un daño excesivo (que supere la ventaja que pueda otorgar), sencillamente se abstendría de ejecutarse, se suspendería o de plano se modificaría para que no lo cause; pero nuevamente, es una cualidad que únicamente puede desarrollar un ser humano.

En este sentido, puede que exista un algoritmo que dé la ilusión de "autonomía de elección", que permita que el sistema en cuestión pueda "elegir" al enfrentarse a una situación en específico [33], pero únicamente va a tener dichas "elecciones" basadas en una programación que define su algoritmo, siguiendo una línea lógica que tendrá como resultado una respuesta conocida y determinada [31]. Entonces, las "elecciones" de un sistema autónomo son limitadas, y la complejidad y ambigüedad del conflicto armado pueden llevarlo a cometer violaciones del Derecho Internacional Humanitario (DIH).

En conclusión, dotar de autonomía a una máquina por medio de IA, por más sofisticada que sea, no dejará de ser un error, por cuanto no podrá asegurar la totalidad de eficacia y exactitud en sus respuestas respecto al marco del DIH y a la complejidad intrínseca de los conflictos armados. Su accionar debe tener, aunque sea un mínimo de intervención humana, de lo contrario sería completamente una irresponsabilidad, al poner la vida de uno o varios seres humanos, en "manos" de un algoritmo.

• *Uso Malicioso:* La Inteligencia Artificial es una de las innovaciones más destacadas de la cuarta revolución industrial, ya que se ha expandido rápidamente y ha ganado gran popularidad en diversos campos gracias a sus numerosas ventajas. Sin embargo, esta tecnología poderosa también conlleva riesgos.

Como anteriormente se evidenció, la Inteligencia Artificial ha sido empleada en los Deep Fakes, dentro y fuera del ámbito militar, por ejemplo, en la elaboración de videosque suplantan la identidad de una persona (generalmente una figura pública o influyente), para comunicar un mensaje falso.

Se han registrado en redes sociales varios casos de Deep Fakes, videos o demás contenido multimedia realizado con Inteligencia Artificial, que en ocasiones se realiza con fines "recreativos" o para experimentar las capacidades de la IA; no obstante, es el auge de popularidad y la facilidad para acceder a esta tecnología, la que según Hendrycs, Mazeika y Woodside [34], puede ser una herramienta útil para las personas malintencionadas que buscan desestabilizar la sociedad.

Algunos de los usos malintencionados que se le puede dar a la IA, son: el desarrollo de armas bioquímicas, IAs hostiles, propaganda falsa y concentración del poder mediante vigilancia y censura, tal y como resaltan los autores anteriormente citados.

a. Armas Biológicas: Gracias a su capacidadpara recopilar información y buscar rápidamente temas específicos mediante motores de exploración o filtros, la inteligencia artificial puede proporcionar acceso fácil a información detallada, como instrucciones paso a paso para crear patógenos mortales [35], potenciando de esta forma la búsqueda y el desarrollo de nuevas armas biológicas o bioquímicas

que tengan un impacto devastador en la sociedad.

b. IAs Hostiles: Las herramientas de IA han sido sometidas a pruebas y puestas a disposición del público en general para su desarrollo interactivo. Sin embargo, debido a la actividad de individuos malintencionados, pueden surgir fenómenos como el de Chaos-GPT. Este surge de una IA basada en Chat GPT-4, creada mediante el uso de un programa de código abierto llamado Auto-GPT, el cual carecía de los filtros de seguridad de la versión original, convirtiéndose así en una IA autónoma.

Rápidamente, Chaos GPT se convirtió en una IA que tenía como fin último "destruir a la humanidad", y otros objetivos secundarios como "establecer el dominio mundial", "provocar caos y destrucción", "controlar a la humanidad mediante la manipulación" y "alcanzar la inmortalidad" [36] y [37]. Si bien Chaos GPT, no ha representado ser una amenaza real hoy en día, sí muestra ser el inicio de una problemática que podría llegar a ser muy peligrosa para el ser humano y que no se pensaba que fuese a escapar de las películas y libros de ciencia ficción.

c. Desinformación y censura: Con la globalización, las fronteras se han estrechado y el flujo de información entre continentes se ha acelerado gracias a las tecnologías de la información. Esto permite conocer rápidamente la situación de otros países y acceder a información desde casi cualquier parte del mundo. Aunque a simple vista, esto parezca ser solo beneficioso, lamentablemente, las personas malintencionadas pueden convertirlo en una seria amenaza para la sociedad.

La globalización y la popularidad de las redes sociales han logrado intensificar y potenciar un problema ya existente: la desinformación. Lo anterior hace posible que exista un gran flujo de Fake News, propaganda e información falsa, que propicia la aparición y el desarrollo de fenómenos, como la polarización de opiniones, la alteración de la percepción de la realidad y el terrorismo.

Si bien la desinformación era un peligro ya existente que amenazaba a la sociedad, ha sido con el reciente auge de las IA, que ésta ha incrementado su peligro y su alcance, gracias a su capacidad de sectorizar nichos y a la impresionante capacidad de crear contenido que resulta ser realmente similar al original.

Como se revisó anteriormente, hay ocasiones donde la noticia falsa es evidente, pero aun así siendo evidente, se vuelve viral gracias a la alta difusión por parte de bots, medios de comunicación y el colectivo general [38] que, sin importar la intención, terminan llegando al mismo resultado: la masificación de las noticias falsas.

Para evitar la propagación excesiva de las noticias falsas y la proliferación de la desinformación, se recomienda que sean las entidades gubernamentales y/o las organizaciones de prensa autorizadas, quienes deberían realizar un proceso de vigilancia continua al contenido realizado por la IA, denunciándolo o directamente erradicándolo, para mantener solo un flujo de información verificada y que el público tenga la certeza de que son verídicas.

Sin embargo, esta solución tampoco es perfecta y resulta ser un arma de doble filo, porque podría ser empleada como una herramienta para centralizar el poder, la información y las opiniones de la gente, generando una burbuja por medio de la censura excesiva, la denegación al acceso de ciertos sitios web o contenido y la polarización de opiniones e intereses [39], ya sea por parte de un gobierno, una cadena de noticias o una persona influyente, beneficiando la proliferación de regímenes autoritarios.

Es aconsejable considerar diversos aspectos cruciales antes de introducir la tecnología de Inteligencia Artificial en

aplicaciones militares, con el fin de aprovechar al máximo sus beneficios y evitar que se convierta en un inconveniente:

• *Cumplir y garantizar el cumplimento al DIH:* Las guerras y los conflictos bélicos son algo inherente al ser humano. Desde el inicio de la historia humana, ha existido la imperante necesidad del ser humano de imponer su voluntad sobre los otros; sin embargo, gracias a que la sociedad ha evolucionado, se ha logrado normar y establecer límites a estos conflictos bélicos, siendo a nuestros días el Derecho de la Guerra o Derecho Internacional Humanitario.

Es importante hacer énfasis en los múltiples pronunciamientos del Comité Internacional de la Cruz Roja [40], organización neutral que promueve el respeto por el DIH, que cumple funciones de asistencia humanitaria fundamentado en los convenios de Ginebra de 1949 y sus protocolos adicionales, con respecto a la implementación de los sistemas de armas autónomas, mismo que solicita a los estados que hacen parte de esta, la adopción de normas jurídicas vinculantes que permitan regular el uso de las armas letales autónomas. Aunque no existe un marco legal vinculante que regule el empleo de sistemas de armas autónomas, se recomienda encarecidamente su no utilización para evitar violaciones al DIH, para garantizar el cumplimiento de sus principios y preservar la humanidad en el desarrollo de los conflictos armados.

• *Identificar Fake News:* En este momento, la IA ha sido utilizada para crear videos o imágenes que se han difundido para propiciar la proliferación de información falsa que puede causar terror, pérdida de objetividad y cerco de la realidad; la recomendación en este caso, es analizar bien el contenido que se consume; así, el realizar un análisis objetivo minucioso, puede facilitar la detección de Deep Fakes o Fake News.

Es importante revisar otros medios de comunicación o investigar un poco más a fondo, con respecto a un tema que se haya revisado y del cual se sospeche que sea una Fake New o un Deep Fake, antes de compartirlo o considerarlo verídico.

• *Consultar otras fuentes:* Es importante consultar varios medios de comunicación, ya sea para identificar casos de desinformación o para descubrir si se está siendo víctima de la censura; es fundamental no limitarse a creer y asumir la información que se obtiene en redes sociales o en los medios de comunicación nacional; gracias a la globalización y a las TICs, se tiene un fácil acceso a toda la información del mundo, con solo dar un click.

• *Cultura de seguridad:* En ocasiones, la mejor solución es crear una cultura de seguridad en el público, realizar capacitaciones, sensibilizaciones y charlas que versen sobre qué son, cómo funcionan y los riesgos que traen consigo las IAs; pueden ser cruciales para evitar que las vulnerabilidades sean explotadas en contra del usuario.

3.2 IoT: Conexión masiva, protección masiva: El internet de las cosas y el internet de las cosas del campo de combate, son herramientas que están tomando cada vez más fuerza en el ámbito civil y en el ámbito militar; sin embargo, es una tecnología que por sus características podría llegar a presentar inconvenientes y vulnerabilidades como pueden ser:

• *Mayor número de brechas de seguridad:* Al ser la tecnología IoT una herramienta que busca el empleo de diversos dispositivos conectados a una red en común para garantizar un flujo de paquetes de datos de un punto a otro u otros, es también una tecnología que implica la existencia de una cantidad de vulnerabilidades, hecho que es directamente proporcional a los dispositivos que se integran a la red.

El abanico de posibilidades de elección con respecto a los dispositivos que se pueden integrar mediante IoT es bastante amplio y

variado; existen diversas empresas que venden el mismo producto, con diferentes precios, capacidades, formas, sistemas operativos y configuraciones de seguridad, lo cual presenta al usuario que busca implementarlo, un ecosistema variado que implica tener mayores cuidados y consideraciones de medidas de ciberseguridad.

La desatención a la ciberseguridad en entornos de IoT puede abrir las puertas a diversos ataques. Entre ellos se encuentran el análisis de tráfico, las perturbaciones, los ataques de denegación de servicio (DoS) y los ataques de hombre en el medio (MiTM). Si estos ataques se materializan, podrían suponer una desventaja considerable en el desarrollo de operaciones militares.

A continuación, se detallan algunos de los riesgos que conlleva la falta de ciberseguridad en entornos IoT en el ámbito militar:

- **Robo de información:** Los atacantes podrían obtener información sensible sobre operaciones militares, estrategias y personal.
- **Sabotaje:** Los sistemas IoT podrían ser manipulados para causar daños físicos o interrumpir operaciones militares.
- **Desinformación:** Los atacantes podrían difundir información falsa para generar confusión y caos.
- **Interrupción de comunicaciones:** Los ataques podrían bloquear o interferir las comunicaciones entre unidades militares.

En síntesis, la ciberseguridad es un aspecto fundamental que debe ser considerado en la planificación y desarrollo de operaciones militares que involucren el uso de dispositivos IoT. La negligencia en este ámbito puede tener graves consecuencias para la seguridad y el éxito de las operaciones.

• *Capacitación en seguridad:* Aunque el ser humano no forma parte del IoT o IoBT, sí es parte integral de la red al ser el usuario que opera, supervisa e interactúa directamente con los dispositivos para obtener sus beneficios. Sin embargo, es el elemento más susceptible a ser una vulnerabilidad y brecha de seguridad en la red. Por esta razón, se recomienda implementar campañas de capacitación para el personal que interactúe con esta tecnología, con el fin de minimizar aquellas brechas de vulnerabilidad, causadas por descuido o desconocimiento.

• *Redes seguras:* Los dispositivos de IoT requieren estar conectados a una red a través de la cual se evidencie un flujo de información en varias direcciones. Por esta razón, al implementarse en conflictos armados, pueden considerarse objetivos militares susceptibles de ataques dirigidos por parte del enemigo. Estos ataques pueden buscar inhabilitar, inhibir, interferir o destruir estos dispositivos con el fin de obtener una ventaja militar.

Por este motivo, es necesario estar supervisando las medidas de ciberseguridad que garanticen la confidencialidad, la disponibilidad y la integridad de la información que circula por medio de los dispositivos de IoBT y a través de las redes a las que se conecten.

• *No confiar totalmente en los dispositivos:* Si bien los dispositivos tecnológicos son de gran ayuda y pueden brindar ventajas al ser empleados, no es recomendable centrar por completo los esfuerzos en la implementación de una sola tecnología.

En cualquier ámbito imaginable donde se empleen tecnologías de la información, se requiere mantener la continuidad del negocio o el incesante flujo de información; es decir, se deben implementar varias opciones para comunicarse más allá de los dispositivos de IoBT, vistos anteriormente. En este sentido, los dispositivos de IoBT pueden ser una gran herramienta para garantizar y maximizar la capacidad de obtención de información en el campo de batalla, pero no deberían reemplazar en su totalidad los sistemas de comunicaciones convencionales, ni tampoco las capacidades propias de los seres humanos. En otras palabras, hay que evitar la dependencia de los elementos

tecnológicos para de esta forma evitar un estancamiento o un traumatismo en el desarrollo de operaciones militares al enfrentarse a un eventual fallo.

• *Mantener actualizados los dispositivos que pertenecen a la red:* Generalmente, las empresas fabricantes realizan periódicamente actualizaciones a los softwares y a los sistemas operativos de los equipos que se emplean a diario, con la finalidad de solucionar problemas, actualizar las bases de datos de amenazas y optimizar los dispositivos.

Las tecnologías 4G y 5G, en proceso de implementación, ofrecen una amplia capacidad de conexión de dispositivos. Esta capacidad permite crear y experimentar un ambiente inteligente e interconectado. Sin embargo, es crucial mantener actualizados los dispositivos que convergen en la red. Esto es necesario para mitigar las numerosas vulnerabilidades que pueden enfrentar.

5G: más velocidad y alcance implica más seguridad: La quinta generación de comunicaciones móviles trae consigo considerables ventajas y avances que servirán para ir complementando la actual tecnología; y también, con el paso de los años, ir subrogando a su predecesor, tal y como se revisó anteriormente; sin embargo, esta tecnología no es perfecta, por lo cual su implementación generaría posibles amenazas y una serie de desafíos para la seguridad.

• *Amenazas a la Red por su naturaleza:* Debido a la naturaleza inalámbrica de la quinta generación de comunicaciones, ésta puede ser susceptible a una serie de amenazas que puedan poner en riesgo la seguridad de la comunicación; entre estas amenazas se puede encontrar el análisis de tráfico, las perturbaciones, los ataques de denegación de servicios (DoS) y los ataques de hombre en el medio (MiTM).

• *Amenazas a los dispositivos IoT:* La implementación de las redes 5G y su capacidad mejorada para incluir dispositivos IoT han revelado una vulnerabilidad relacionada con la baja prioridad que se otorga a la ciberseguridad en el ámbito de los dispositivos IoT, sobre todo en dispositivos inteligentes de gama baja.

Esta vulnerabilidad se genera debido al crecimiento exponencial en la conexión de dispositivos, algunos de los cuales pueden carecer de altos niveles de seguridad debido a su propósito específico. Esto los convierte en posibles puntos de acceso a ser vulnerables o débiles en la red, aumentando su exposición a ataques cibernéticos.

Se recomienda que antes de implementar la tecnología 5G en el campo militar, se tengan en cuenta una serie de aspectos clave para maximizar las ventajas que ofrece la tecnología en cuestión, de tal forma que no se convierta en una brecha de vulnerabilidades que el enemigo podría explotar en cualquier momento, así:

• *Invertir en capacitación al personal:* En ocasiones, la mejor medida de seguridad, consiste en invertir en educación sobre temas de ciberseguridad para el personal en general; de esta forma, se evita o minimizan las vulnerabilidades ya existentes o que se encuentran en estado de latencia, de acuerdo con un estudio realizado por IBM [41]: aproximadamente un 95% de las incidencias en ciberseguridad, son causadas por errores humanos.

• *Antivirus en los dispositivos:* Al instalar un antivirus en los dispositivos conectados a la red, se logra una protección en tiempo real contra amenazas de malware. Esta protección opera en segundo plano mediante escaneos, bloqueo de sitios web maliciosos, el uso de firewalls efectivosy una base de datos de malware actualizada que permita la identificación precisa de amenazas.

• *Contraseñas fuertes:* Implementar una contraseña robusta es la primera línea de defensa contra el acceso no autorizado a los dispositivos de la red. Esta medida puede frustrar los intentos de hackers o personas que intenten utilizar software keygen para acceder a la red.

Varias empresas del sector de ciberseguridad y organizaciones internacionales [42], [43] y [44], recomiendan que las contraseñas fuertes deben ser creadas con ciertas características: longitud mínima de entre 8 y 12 caracteres, inclusión de caracteres numéricos, inclusión de caracteres de símbolos e incluir mayúsculas y minúsculas.

• *Actualizar contraseñas periódicamente:* Además de contar con una contraseña fuerte y robusta, debe implementarse una política de actualización de contraseñas, para evitar que personas ajenas a la institución, logren vulnerar la seguridad de la contraseña y permanezcan con acceso ininterrumpido al dispositivo. Varios expertos recomiendan hacerlo al menos cada tres meses [45], aunque esto dependerá de las políticas de seguridad del lugar en cuestión.

• *Mantener actualizados los dispositivos que pertenecen a la red:* Las empresas fabricantes llevan a cabo actualizaciones periódicas en los softwares y sistemas operativos de los equipos utilizados a diario. Esto se hace con el objetivo de resolver problemas, actualizar la base de datos de amenazas y optimizar el rendimiento de los dispositivos.

Teniendo en cuenta que con la tecnología 5G se busca aumentar la conexión de dispositivos para crear un ambiente inteligente (ciudades o bases militares, por ejemplo), es necesario que se mantengan al día las actualizaciones en aplicaciones, firmware, y/o sistemas operativos de todos los dispositivos que convergen en la red 5G en cuestión, para mitigar vulnerabilidades.

IV. CONCLUSIONES

La revisión bibliográfica realizada evidencia la necesidad de implementar o, al menos, conocer las tecnologías y sus diferentes aplicaciones para ser empleadas a nivel ofensivo y también, para desarrollar estrategias defensivas en el ámbito de la ciberseguridad. De esta forma, el conocimiento de las tecnologías y sus aplicaciones, es fundamental para no quedar rezagados en materia tecnológica dentro de la guerra cibernética. Por lo tanto, la constante evolución de las amenazas, exige una actualización permanente en estrategias de seguridad.

Si bien la existencia de diversas tecnologías y aplicaciones para la guerra cibernética ofrece múltiples posibilidades, es crucial destacar que su implementación requiere políticas y medidas robustas de ciberseguridad. Esta necesidad se fundamenta en dos aspectos: el primero, la mitigación de las vulnerabilidades y segundo, el maximizar las ventajas de la implementación de nuevas tecnologías, lo que facilitaría su adopción y desarrollo.

Finalmente, se recomienda a los lectores de este artículo continuar con esta investigación y llevar a cabo un ejercicio constante para fortalecer sus capacidades en ciberseguridad. Esto garantizará que no se produzcan brechas de seguridad en la tecnología que utilicen en el futuro.

V. REFERENCIAS

[1] C. V. Clausewitz, De la guerra, 1832.

[2] Ejército Nacional de Colombia, Manual MFE 1-01 Doctrina, 2017.

[3]] F. Rozo-García, Revisión de las tecnologías presentes en la industria 4.0, 2020.

[4] P. J. García y Patos Herrero, La inteligencia artificial en los nuevos escenarios de conflicto: Ucrania 2022.

[5] CICR, Preguntas y respuestas: Lo que hay que saber sobre las armas autónomas, 2022.

[6] Centro de Análisis del Comercio Mundial de Armas, Se recomienda la adopción del complejo de municiones merodeadoras KUB-BLA 2022.

[7] American Institute of Aeronautics and Astronautics, UAV Roundup, 2013.

[8] Center for the Study of the Drone of Bard College (2017) Loitering Munitions in Focus

[9] Andres F. Rojas, VANTs en el conflicto Rusia y Ucrania, 2023

[10] Heather J. Williams, Ilana Blum, Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise, 2018.

[11] Sun Tzu, El arte de la guerra, 400 a.C.

[12] R. Chawla, Deepfakes: How a pervert shook the world, International Journal of Advance Research and Development, 2019.

[13] M. T. Sastre, Deepfakes: creación de nuevas caras a partir de imágenes de famosos, 2022.

[14] L. R. Romero D. and N. Sánchez G. Valenzuela, Sociedad Digital, Comunicación y Conocimiento: Retos para la Ciudadanía en un Mundo Global, 2022.

[15] M. Vázquez M., Las Operaciones Psicológicas y Operaciones de Información de Campaña, 1998.

[16] Zhu, L., Majumdar, S., and Ekenna, C. An Invisible Warfare with the Internet of Battlefield Things: A Literature Review. Human Behavior and Emerging Technologies. 2021.

[17] V. Gotarane y Raskar, S. IoT Practices in Military Applications In Proceedings of the International Conference on Trends in Electronics and Informatics, ICOEI. 2019

[18] R. R. Brooks, L. Yu, I. Ozcelik, J. Oakley and N. Tusing, Distributed Denial of Service (DDoS): A History, 2021

[19] A. N. Riaño Crimea. Una perspectiva desde el ciberespacio. 2022

[20] P. Manotas, M. Ataques de denegación de servicio distribuido: Cómo evitarlos y cómo enfrentarlos. 2022.

[21] O. Yoachimik y J. Manotas, Informe sobre las amenazas DDoS en el 2º trimestre de 2023, 2023.

[22] Ejército Nacional de Colombia, MFE 3-0 Operaciones, 2017.

[23] Ejército Nacional de Colombia, MFE 6-0 Mando Tipo Misión, 2017.

[24] Kott, A., Swami, A., & West, B. J, The internet of battle things. 2016

[25] Tadayoni, R., Henten, A., & Falch, M. Internet of Things—The battle of standards. 2017

[26] Zhu, L., Majumdar, S., & Ekenna, C. An invisible warfare with the internet of battlefield things: A literature review. Human behavior and emerging technologies, 2021

[27] Amazon Web Services. What is 5G?, 2023

[28] C. Peliza, F. Dufour and A. Serra. Redes 5G desde el Estado al Arte, 2019

[29] Ejército Nacional de Colombia, MCE 6.02 Operaciones de Comunicaciones, 2021

[30] Varona, M. A.. Breve comentario sobre el desafío que para el DIH representan las armas autónomas. 2016

[31] J. Madrid. El derecho internacional humanitario frente al desafío de las armas autónomas, 2021

[32] Leonel Gorrín Mérida, Las armas autónomas y el DIH, 2016

[33] M. Meier, "Lethal Autonomous Weapons Systems (LAWS): Conducting a Comprehensive Weapons Review". 2016.

[34] D. Hendrycks, M. Mazeika y T. Woodside An Overview of Catastrophic AI Risks, 2023

[35]] E. Soice y Al, Can large language models democratize access to dual-use biotechnology? 2023

[36] J. Lanz, Conoce a Chaos-GPT: La Herramienta de IA Que Busca Destruir a la Humanidad, 2023

[37] X. Lizana, Chaos GPT ha sido creado para acabar con la humanidad, 2023

[38] O. Varol y Al. Online Human-Bot Interactions: Detection, Estimation, and Characterization, 2017

[39] J. Gerschewski y A. Dukalskis, How the internet can reinforce authoritarian regimes: The case of North Korea. 2018

[40] CICR, Posición del CICR sobre los sistemas de armas autónomos. 2021

[41] IBM, X-Force Threat intelligence index. 2018

[42] Kaspersky, Consejos para generar contraseñas seguras y únicas. 2023

[43] Google, ¿cómo crear una contraseña segura?. 2023

[44] Organization of American States, Consejos para crear contraseñas fuertes. S.F.

[45] PandaSecurity, ¿Con qué frecuencia debes cambiar tus contraseñas? 2020

IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN LA SEGURIDAD DE LA INFORMACIÓN EMPRESARIAL EN COLOMBIA

Esp. Wilman Michael Fonseca Rodríguez
Ingeniero de Soporte de plataforma y aplicaciones
fonsecamichaelftth@gmail.com

RESUMEN- ***La inteligencia artificial y otras tecnologías emergentes no son fenómenos recientes. Su desarrollo se ha gestado a lo largo de varias décadas, con la aspiración de contribuir y beneficiar a las actividades humanas, la sociedad y el medio ambiente. En la actualidad, estas tecnologías han traspasado muchos de los límites para los que fueron diseñadas, con consecuencias tanto positivas como negativas. Con base en lo anterior, el objetivo de este artículo de investigación consiste en describir los efectos de la inteligencia artificial relacionados con la seguridad de la información en las empresas colombianas. Para cumplir con este objetivo se definieron los riesgos, vulnerabilidades y beneficios de la IA, se evaluó la legislación existente y se determinaron los avances y limitaciones a nivel empresarial.***

La investigación fue documental, en la que se revisaron artículos y documentos académicos de manera cualitativa. Se concluyó que la IA es una herramienta excepcional que ha traído diversos beneficios a la humanidad y ha generado grandes avances en tecnología y a nivel científico. Así como cuenta con innumerables ventajas, también genera bastantes riesgos por el mismo acceso ilimitado a la información. A nivel legislativo, se han dado los primeros pasos pero aún la regulación es muy general y no enmarca los alcances y limitaciones. En Colombia, se han dado avances; sin embargo, es una tecnología que actualmente está surgiendo en comparación con otras naciones en donde se encuentra más avanzada.

Palabras clave: *Inteligencia artificial, Seguridad de la información, Legislación, Riesgos y vulnerabilidades.*

Abstract- Artificial intelligence and other emerging technologies did not emerge overnight; they have been proposed for several decades in order to contribute to and benefit human activities, society and the environment. Today it is a reality that has surpassed many of the limits for which it has been designed in a positive and negative way. With the above, the objective of this research article is to describe the effects of artificial intelligence on the information security of Colombian companies. To meet this objective, the risks, vulnerabilities and benefits of AI are defined, the existing legislation and the progress and limitations at the business level are determined.

The research was documentary, in which articles and academic documents were reviewed qualitatively. It was concluded that AI is an exceptional tool that has brought many benefits to humanity and has generated great advances in technology and at a scientific level, which, just as it has innumerable advantages, also generates many risks due to the same unlimited access to information. At the legislative level, the first steps have been taken but the regulation is still very general and does not frame the scope and limitations. In Colombia, progress has been made, however, it is a technology that is just beginning compared to other nations.

Keywords- *Artificial intelligence, Information security, Legislation, Risks and vulnerabilities.*

I. INTRODUCCIÓN

La inteligencia artificial se encuentra en un

proceso acelerado de desarrollo, que indudablemente ha traído consigo mejoras a las tecnologías digitales, especialmente en el campo empresarial. Tiene un gran potencial para infinidad de temas organizacionales de gran importancia, como el fomento de la economía, la automatización y la productividad en los procesos. Sin embargo, se considera que muchos sistemas de la IA operan como cajas negras con mecanismos ocultos que a largo plazo no se sabe cómo funcionarán [1].

Dentro de ese marco de dudas a nivel social y empresarial, surge la necesidad de identificar los beneficios y vulnerabilidades de la Inteligencia Artificial, así como los marcos y guías en escala nacional e internacional para la implementación de estos sistemas, buscando que se efectúe de manera segura, transparente y responsable, el respeto por la privacidad, evitando de esta forma un atentado contra el bienestar de las personas y las organizaciones. Todo lo anterior se expresa, teniendo en cuenta que la IA va ligada al factor de innovación empresarial, un tema que ayuda a las compañías a reinventarse reduciendo el riesgo de desaparecer si no toman la iniciativa de actualizarse tecnológicamente.

En el ámbito empresarial, la inteligencia artificial tiene ventajas a la hora de manejar grandes cantidades de datos en procesos como contratación, manejo de inventarios, gestión de clientes, marketing y todo lo relacionado con la oferta y la demanda. Aunque si bien es cierto que sus ventajas son ilimitadas, también es innegable que representa muchos riesgos alusivos a la falta de certeza sobre lo que puede llegar a representar y en lo que se puede transformar a largo plazo [2].

En función de lo planteado anteriormente, la Organización para la Cooperación y el Desarrollo Económico (OCDE) [3], establece cinco principios para la administración responsable de la IA, mismos que se sintetizan a continuación: beneficiar a las personas impulsando el desarrollo sostenible mediante el diseño del crecimiento y el respeto por los derechos humanos, los valores democráticos y la diversidad, de tal forma que se garantice la intervención humana en caso de ser necesario. Para lograrlo, debe haber transparencia y divulgación responsable de la información, que garantice los resultados; igualmente, los sistemas deben funcionar de manera sólida y segura; los riesgos, deben evaluarse y gestionarse; y, las organizaciones que operan sus sistemas con esa tecnología, deben ser responsables de que todo funcione correctamente. En relación con la problemática expuesta, la presente investigación tiene como objetivo general describir los efectos del uso de la inteligencia artificial en la seguridad de la información de las empresas colombianas y como objetivo específico: identificar los principales riesgos y vulnerabilidades en el uso de inteligencia artificial.

II. PROCEDIMIENTO Ó METODOLOGÍA

Esta investigación es documental, descriptiva y analítica; el aspecto documental se realizó por medio del abordaje de artículos y documentos relacionados con inteligencia artificial, seguridad de la información, marco legislativo y la aplicación de la IA en las empresas colombianas. La investigación documental se efectuó mediante la búsqueda de información en fuentes bibliográficas con el propósito de ser analizada [4].

El enfoque es cualitativo, lo que permite describir perspectivas y escenarios centrando los datos y la información en un contexto específico; es un enfoque que le permite al investigador interpretar puntos de vista para generar conocimiento [5]. En la búsqueda de información, se utilizaron descriptores como "inteligencia artificial", "Legislación de la Inteligencia artificial", "Riesgos AND vulnerabilidades de la Inteligencia artificial", en bases de datos como Google académico, Redalyc, Scopus y Scielo. En la tabla 1, se presentan los descriptores y número de artículos encontrados.

TABLA I
BASES DE DATOS Y DESCRIPTORES UTILIZADOS EN LAS BÚSQUEDAS

BASE DE DATOS	DESCRIPTORES	N° DE ARTÍCULOS
Scopus	Inteligencia Artificial	4
Scielo		6
Google Académico		8
Scielo	Legislación de la Inteligencia artificial	3
Redalyc		4
Google Académico		10
Google Académico	Riesgos y vulnerabilidades de la Inteligencia artificial	12

Criterios de inclusión a. documentos y artículos de investigación relacionados con los objetivos propuestos; b. estudios publicados en los idiomas inglés y español.

Criterios de exclusión a. publicaciones anteriores al año 2019; b. Artículos que no se relacionan con el tema y los objetivos propuestos.

Principales limitaciones: Las principales limitaciones abarcaron los marcos legales relacionados con la inteligencia artificial a nivel nacional e internacional.

III. DESARROLLO Y DISCUSIÓN

A. inteligencia artificial

La Inteligencia Artificial, en adelante denominada "IA", es el nombre que se le asigna a las tecnologías con características que antes eran sólo humanas; aplica cuando una máquina tiene la capacidad de imitar a las personas en la forma de aprender y de resolver problemas [6] .Algunas de las características de la IA, son el aprendizaje automático y profundo basado en redes neuronales.

La IA, tuvo sus inicios hacia el año 1950 con la idea de Alan Turing de crear un aparato inteligente. El concepto fue introducido en 1956 cuando John McCarthy lo definió como la capacidad de las máquinas para ejecutar tareas y resolver problemas tal como lo hace la inteligencia humana [7]. Los primeros indicios reales se dieron en 1996, cuando el operador Deep Blue de IBM jugó una partida de ajedrez contra el campeón del mundo donde una aplicación práctica ofrecía alternativas de juego; más adelante en 2012, se empezó a hablar de Deep Learning con la creación de Google.

Se podría sintetizar como lo relaciona [8], que la inteligencia artificial es un término general para resumir algoritmos y softwares complejos que son capaces de realizar tareas humanas por medio del reconocimiento de datos y el análisis de problemas. La Inteligencia artificial tiene una gama amplia de aplicaciones que se han ido nutriendo con los avances tecnológicos.

Entonces, la IA tiene la capacidad de aprender automática y profundamente a partir del procesamiento y reconocimiento del lenguaje.

Así mismo, la IA, está presente en muchas de las actividades cotidianas, porque interactúan con todo tipo de sistemas; muchas de las tareas que antes se realizaban de manera personal, son actualmente llevadas a cabo por esta tecnología que, al estar en auge, se considera que tendrá una gran repercusión en el futuro y una revolución económica mundial [6]. Hoy en día todo está relacionado con la IA; es por ello que las personas y las organizaciones deben capacitarse y reconocer no solo sus ventajas sino también, sus amenazas.

a) Generalidades

Los tipos de IA según las funciones destacadas por [9], son las siguientes:

- *Máquinas reactivas:* Carecen de capacidad para tomar decisiones, su funcionamiento es básico y solo aplica para el objetivo con el cual fueron diseñadas.

- *Memoria ilimitada:* tiene una memoria transitoria que puede adquirir experiencias que ya pasaron.

- *Con "teoría de la mente":* Comprenden emociones, necesidades, creencias y deseos; al interactuar con ellas es similar que hacerlo con una persona. Es una tecnología en desarrollo.

- *Autoconciencia:* Es algo que tiene camino por recorrer, pretende simular una IA con consciencia de sí misma. Se considera algo lejano de lograrse.

Entendiendo que la IA combina la creatividad del hombre y la inteligencia, se debe reconocer que tiene varios enfoques siendo su interés principal la imitación de la inteligencia humana. Por lo anterior, sus principales características radican en la capacidad de razonar y tomar decisiones con base en la información disponible las 24 horas del día sin intervención de las personas [9]. La IA, entonces, hace posible el manejo de grandes cantidades de información en un tiempo récord, algo que genera muchas ventajas para las actividades que se realizan a diario.

Las tecnologías que se basan en la IA constan de máquinas y softwares complejos que crecen exponencialmente y que por su capacidad de adaptación expanden el conocimiento y la innovación. Su uso ha cambiado la economía mundial, tanto que expertos señalan que puede ser regulada y adaptada al desarrollo sostenible en aras de potenciar el futuro tecnológico del país [10]. Con esto, se puede inferir que la inteligencia artificial bien utilizada puede ser una herramienta que contribuya en la solución de los problemas a los que se enfrenta el mundo.

Dentro de los subconjuntos de la IA, se pueden mencionar el Machine Learning y el Deep Learning; el primero, se centra en la enseñanza a las máquinas para aprender cosas nuevas y tomar decisiones aplicando algoritmos; y el segundo, denominado aprendizaje profundo, el cual emplea datos para enseñar a los artefactos a hacer cosas que antes sólo las personas podían hacer. Es un mecanismo de imitación del cerebro humano que interpreta datos mediante la construcción de redes neuronales [11]. Herramientas como Machine y Deep Learning, tienen la capacidad de aprender con base en los datos que procesan.

b) Beneficios

La IA, puede ser utilizada para ayudar a los profesionales en sistemas a incorporar en estos, una mayor complejidad y estar por delante de las intrusiones a la privacidad, al igual que la detección temprana de amenazas sofisticadas y cambiantes. El análisis y toma de decisiones en tiempo real, también son usados en el desarrollo de sistemas autoadaptables y automáticos frente a las respuestas a posibles amenazas [7]. En este sentido, la IA fusiona todos los sistemas con los que interactúa para realizar análisis y predicciones generales en determinados contextos.

Dentro de los beneficios de la IA, la ONU destaca la selección personalizada de contenidos, aumentando la experiencia de cada persona; sin embargo, esto es considerado también un riesgo potencial, pues la posibilidad de que cada uno acceda a diversos puntos de vista puede llegar a interferir con las ideas de los individuos de otras posiciones ideológicas; esta segmentación que llega a ser muy útil, puede reforzar creencias que lleven a contenidos violentos o a la desinformación solo por tener la participación en línea de los usuarios [12]. Uno de los componentes más valiosos de la IA es entonces la facilidad de personalizar contenidos, pese a que esto en sí mismo es un riesgo que puede derivar en problemas sociales como la exclusión y la violencia debido a la diferencia de

pensamientos.

Por otra parte, en el mundo de la seguridad, la velocidad de la IA es fundamental para hacer frente ante escaladas potenciales; entoces, esta tecnología se transforma en un ejemplo eficaz de defensa contra atacantes, pues las amenazas bien planeadas y ocultas pueden ser detectadas y reducidas rápidamente. A nivel empresarial, investigaciones aluden a que 7 de cada 10 empresas consideran que la IA es el futuro de la ciberseguridad por su capacidad de respuesta ante amenazas críticas, en donde el 60% de los directivos la consideran útil porque incrementa la eficiencia y productividad del analista, reduce costos en la detección de brechas y responde ágilmente ante el descubrimiento de ellas [13]. De este modo, existe un nivel de conciencia empresarial que asume la necesidad de la IA para el procesamiento y seguridad de la información como herramienta de competitividad.

La IA puede ser utilizada en la identificación, protección, detección, respuesta y recuperación de incidentes dentro del ámbito de la seguridad inteligente; está desarrollada para detectar y detener amenazas complejas que puedan considerarse un riesgo para los datos. Después del COVID-19, con el incremento de los ataques para acceder a datos y sistemas, la IA ha combinado herramientas que hacen más difícil que dichas irrupciones tengan éxito [7]. Es así, como en el campo de la ciberseguridad, es considerada una gran apuesta en la prevención y defensa ante todo tipo de ataques.

Por otro lado, la IA para las empresas representa una mejoría en los procesos, porque da a conocer la información en tiempo real que a simple vista puede escaparse. A nivel económico, la firma PWC informó que para el año 2019 esta tecnología contribuyó con 2 billones del PIB y para el año 2025, se espera que llegue al menos a los 15.5 billones, gracias a su potencial de transformar la industria aumentando la productividad [10]. En relación con los datos anteriores, se puede inferir que la IA es una necesidad inminente que garantiza el crecimiento y expansión económica de un país.

En consecuencia, la IA integra atributos sociales y técnicos que promueven la transformación de la economía y la sociedad, convirtiéndose en un eje de competitividad en donde quienes la implementen, recibirán mayores beneficios. Sin embargo, tiene varios desafíos y riesgos que requieren nuevas formas de vigilancia, pues en caso de quedar sin control puede causar graves daños [11]. En otras palabras, la IA genera beneficios siempre y cuando sea bien administrada y controlada, garantizando las herramientas para su vigilancia.

Así las cosas, en este apartado conviene mencionar sectores que han incorporado de manera eficiente la IA. Uno de ellos, es el de la salud y la medicina, por cuanto han aumentado la productividad y la eficacia en temas como el seguimiento a los pacientes y la prevención o promoción de hábitos saludables. En efecto, con la IA aquellas han dinamizado su campo, incorporando video juegos, audios y diversas herramientas que permiten realizar análisis del estado de salud en una persona [14]. Este avance se potencializó después de la pandemia, en donde las instituciones de salud adoptaron herramientas virtuales para mejorar los procesos de tramitación, atención y seguimiento a los usuarios.

En función de lo planteado, Korinek y Stiglitz [15], aseguran que la IA puede ayudar a las organizaciones del sector salud en el máximo aprovechamiento de sus recursos, por medio del análisis de imágenes, la identificación de tasas, el procesamiento de registros de pacientes y la toma de decisiones más precisas. Se trata pues de potencializar las herramientas que brinda la IA para aumentar la eficiencia y las operaciones dentro de la industria de la salud.

En resumidas cuentas, los beneficios de la IA a nivel global están en la formulación, diseño, evaluación y generación de nuevos conocimientos que permiten mejorar los

procesos, la reducción de errores, el incremento en la creatividad, al igual que la toma rápida y más eficiente de decisiones [16]. Entonces, la IA de manera general actúa para aumentar las ventajas competitivas en una era de información, en donde los datos fluyen de manera constante actualizando todos los procesos.

Por último, es conveniente acotar que a pesar de que son bastantes las bondades de la inteligencia artificial, existen riesgos inminentes. Por mencionar un ejemplo, en un software que lanzó la IBM para analizar informes clínicos basándose en los datos del paciente con el fin de generar posibles tratamientos para el cáncer, el personal de médicos encontró que se suscitaban recomendaciones erradas; esto, debido a que el sistema fue construido con una muestra de datos muy pequeña y sin una validación bajo las reglamentaciones vigentes [17]. De los anterior se deduce que los riesgos son una realidad, lo cual requiere la existencia de un adecuado manejo y control de la información procesada por la IA, cuando se generen reportes o indicaciones.

c) Riesgos y vulnerabilidades

En la actualidad, los ataques cibernéticos son un inconveniente para todas las organizaciones porque ocasionan pérdidas económicas, robo de información, daños a la reputación y otras afectaciones. En estos incidentes de ciberseguridad, los delincuentes aprovechan las vulnerabilidades de los dispositivos y sitios web para impulsar ataques por medio de sofisticadas herramientas que irrumpen en las estructuras informáticas [18]. Todos los sistemas tienen un riesgo de exposición; así mismo, cada uno de ellos se enfrenta a alguna pérdida o daño relacionado con la información.

Algunos de los principales riesgos que relaciona Open Web Application Security Project (OWASP), entre otros, son: Injection, Sensitive dta exposure, Broken Access control, Cross Site Scripting, Insecure Deserialización e Insufficient logging and monitoring [19]. Dentro de los riesgos más comunes, se reconocen la exposición de datos confidenciales y la violación de accesos, riesgos que en su mayoría se intensifican debido a errores humanos.

Con base en [20], la IA es utilizada por delincuentes cibernéticos para la implementación de amenazas como el Deepfake, que manipula contenido auditivo y visual haciendo que parezca auténtico o con técnicas de Machine Learning, en donde se mejoran los algoritmos para descifrar contraseñas a gran escala. Herramientas como el mencionado Deepfake, son muy populares para engañar y desinformar, ejemplo claro de ello son las comunicaciones o declaraciones de políticos que son manipuladas para desprestigiarlos.

A nivel de Colombia y el mundo en general, los riesgos han avanzado tanto o más de lo que lo ha hecho la IA; según la Cámara Colombiana de Informática y Telecomunicaciones, entre el 2017 y 2019, fueron más de 31.000 los delitos informáticos registrados, de los cuales al menos 8.000 fueron por medio de herramientas asociadas a la inteligencia artificial [21]. Y desde el punto de vista tanto individual como empresarial, estos riesgos han sido motivo de preocupación, de tal manrea que se ha incentivado la búsqueda de herramientas para contrarrestarlos.

Sin duda, conceptos como "ciberseguridad" y "ciberdefensa", surgen como respuesta hacia las constantes amenazas a la información, que emergen través de softwares maliciosos y distintos ataques en el ciberespacio para asuntos ilegales o irregulares. En este sentido, la IA es utilizada por medio de su capacidad de aprendizaje autónomo para fortalecer los sistemas con acciones preventivas. Uno de estos fortalecimientos se fundamenta en el Machine Learning que se nutre de los datos para desarrollar algoritmos con capacidades lógicas satisfactorias [22]. La IA es entonces una tecnología multifuncional que, usada como

beneficio, puede representar oportunidades para grandes avances tecnológicos.

En relación con el manejo de datos, [23] hace referencia a que los riesgos que se mencionan a continuación, abarcan gran cantidad de datos a los cuales tiene acceso la IA, tanto para procesar como para analizar la información, así:

- Riesgos de concentración, debido a la acumulación de grandes volúmenes de datos.
- Riesgos sistémicos: Al depender del soporte de otras compañías en operaciones consideradas como críticas.
- Protección del cliente: al manejar grandes volúmenes de datos aumentan los riesgos de algunas entidades de los cuales los clientes no saben.

B. Marco legal de la inteligencia artificial

La IA es una parte del desarrollo tecnológico que lo revolucionará progresivamente en el tiempo, apuntando a un crecimiento exponencial que, desde la vigilancia y el control, puede dificultar la privacidad de la información en todos los entornos y escenarios geográficos. Elementos como el reconocimiento facial, la recolección de información en redes sociales, la asociación de patrones, entre otros, ponen en duda el destino de las personas en cuanto a que no se sabe cómo afectará su privacidad.

En relación con este tema, Elon Musk prende las alarmas acerca del desarrollo descontrolado de la IA generando preguntas, como: ¿por qué esta tecnología representa una amenaza mayor que la de una guerra nuclear? y ¿qué tan lejos estamos de un punto de no retorno? [24]. Debe señalarse que actualmente se encuentra en debate a nivel internacional, el hecho de que la legislación es limitada con respecto a varios estándares de protección frente a esta tecnología. A continuación, se relacionan las políticas y leyes existentes:

a) Legislación internacional

Según la Comisión Europea (UE), la IA es una combinación de tecnologías que agrupa algoritmos, datos y capacidad informática, siendo la economía de datos una parte fundamental. Se trata de sistemas de información que muestran un comportamiento inteligente, que actúan con un determinado nivel de autonomía para alcanzar metas específicas [25]. Bajo este marco es fundamental establecer cuál es el nivel de autonomía a la que se puede llegar y en qué medida las personas tendrán un control sobre la misma.

La UE califica la inteligencia artificial, como de "alto riesgo" creando la necesidad y concienciación de estandarizar normativas relacionadas con las repercusiones positivas y negativas de ésta, en la sociedad, el medio ambiente y la mente humana [26]. En este sentido, se requiere el establecimiento de una reglamentación y normatividad claras y concisas, que contrarresten de forma contundente esas repercusiones.

Uno de los análisis internacionales, es la Declaración de Montreal para un desarrollo responsable de la IA, llevada a cabo en el foro de Montreal en 2017, en donde se discutieron sus implicaciones éticas y sociales. La declaración describe 10 principios y 59 recomendaciones que guían el desarrollo de la Inteligencia Artificial en temas como el respeto a la dignidad humana, la justicia, autonomía y democracia. Sin embargo, es un documento criticado, pues se considera que deja por fuera el posible uso malicioso de esta tecnología en la guerra, la vigilancia y la propaganda personalizada [27]. Con lo anterior, se abre una puerta que forja diferencias considerables entre países considerados más desarrollados con respecto a los que no lo son.

La ODCE, el G-20 y el G-7, han venido trabajando sobre propuestas acerca de la gobernanza de la IA. La OCDE en 2019, adoptó la recomendación sobre la inteligencia artificial

que define las directrices que han acordado los Estados como principios rectores ya relacionados en el capítulo anterior. El G-7 adoptó en 2017 la denominada "Charlevoix common vision for the future of artificial intelligence" que enfatiza esfuerzos por promover una IA centrada en las personas salvaguardando la privacidad, incluso mediante regímenes legales apropiados y la inversión en ciberseguridad [28]. Aquí se puede hacer alusión a párrafos anteriores en los que se siembra la duda acerca del alcance y las limitaciones del hombre en el manejo y control de la IA.

En 2018, la UE y sus Estados miembros publicaron el Plan Coordinado Europeo sobre la Inteligencia Artificial, que tiene por objeto garantizar que la IA se centrara en el ser humano de manera fiable, permitiendo su desarrollo y aplicación, con el fin de garantizar que su función fuera únicamente solo para el bien de las personas.

Es un plan que aborda un marco jurídico de los derechos fundamentales y los riesgos a la seguridad y que define un marco de responsabilidad civil [29]. A nivel internacional, se debe priorizar la legislación para garantizar esos derechos y de esta manera, disminuir los riesgos.

A partir de lo anteriormente citado, se observa que son varios los países y organizaciones internacionales quienes se han preocupado por el tema; así mismo, muchos intelectuales de este campo han centrado sus reflexiones en el futuro de la IA haciendo una proyección, indicando que se encuentra en un vertiginoso desarrollo difícil de detener, lo cual hace necesario que, desde la jurisprudencia, se delimiten los alcances y desafíos, la manera de enfrentarlos y el control adecuado para su nivel de autonomía [30]. Así las cosas, la sociedad se encuentra ante un futuro incierto, frente a las posibles respuestas que surjan a partir de eventos que han sido considerados como películas de ciencia ficción.

Dentro del marco normativo a nivel internacional, es importante mencionar las normas ISO que, para la protección de la seguridad y de la información, se enmarca en las ISO 27001 y 27002, las cuales permiten la identificación de factores que afectan todos los ámbitos de las organizaciones. Son normas que establecen políticas de seguridad y procedimientos que evalúan los riesgos y salvaguardan los activos informáticos [31]. Entonces, la ISO 27001, según [32], presenta un amplio espectro de guías para la protección de la información en todo tipo de empresas, proporcionando una metodología que reduce los riesgos en un nivel aceptable. En el plano nacional e internacional, las normas ISO fortalecen y se integran con otras políticas de la empresa, logrando un mecanismo más robusto de protección.

b) Legislación nacional

En el año 2019, Colombia adoptó una política nacional para la Transformación Digital e Inteligencia Artificial (CONPES 3975), que establece un marco de desarrollo ético y responsable de la IA, impulsando la disminución de barreras en la adopción de tecnologías y fortaleciendo el capital humano para el aprovechamiento de oportunidades frente a los retos de la cuarta y quinta revolución industrial [33]. Esto ha incentivado a las empresas hacia la digitalización y automatización de sus procesos, así como el establecimiento de herramientas para controlarlos.

En el año 2020, se adoptó el documento denominado "Marco ético para la inteligencia artificial en Colombia", con el fin de realizar esfuerzos similares a los realizados por la Unión Europea. Es un documento que enmarca tres postulados: que la IA debe ser lícita y cumplir con las normas aplicables; que debe ser ética garantizando los principios y valores y, que debe ser robusta a nivel técnico y social, debido a que la IA a pesar de ser creada con buenas intenciones puede provocar daños [34]. Visto de este modo,

se puede asegurar que el país ha iniciado el proceso de preocuparse por las implicaciones de la IA; pese a esto, el documento al igual que otros de carácter internacional se queda corto en aclarar los límites, sus alcances y las actividades que se deben ejecutar para ejercer control.

La IA es un reto para el gobierno, porque implica la generación de condiciones y políticas que estimulen su uso sin afectar los recursos y los derechos fundamentales, con el propósito de actuar dentro de un marco ético sin representar un riesgo para la sociedad [35]. Se puede resumir que en Colombia y a nivel mundial, existe una evidente ausencia de normatividad frente al tema de inteligencia artificial. Los marcos éticos no se han planteado correctamente, lo que implica que haya libertad en el marco de su programación, no solo de esta sino también de otras tecnologías.

C. Ámbito empresarial frente a la inteligencia artificial

a) Avances

Antes de mencionar los avances de la IA en las empresas, [36] resalta los tipos de información que pueden manejar dentro de sus procesos diarios, como los son: empresarial, clientes, administrativa, transaccional o financiera, de mercadeo y de ventas o procesos. Al respecto [37], relaciona el sistema de información empresarial como un conjunto de componentes que se interrelacionan a través de distintos medios y métodos con el fin de trabajar objetivamente. Entonces, se entiende la información dentro de una empresa, como una herramienta que apoya los procesos y decisiones para lograr la coordinación y el cumplimiento de actividades.

Los avances de la IA en los últimos años, han sido trascendentales, motivo por el cual se han desencadenado diversas aplicaciones automáticas de inteligencia artificial aplicativa; una muy conocida, es el ChatGPT la cual guía y configura textos en segundos a través de Chatbots generando respuestas escritas coherentes y relevantes muy similares a las usadas por las personas en tiempo real [38]. Con este tipo de avances, se ahonda el interrogante del alcance de la IA y su paralelismo con la mente humana. En esta misma línea [39], asegura que la IA es una herramienta potencial que facilita muchas actividades - por no decir todas -, algo visto como una gran ventaja que se convierte en un reto, pues desde la perspectiva jurídica y ética, sigue generando incertidumbre acerca de su futuro incierto con respecto a la capacidad que puede llegar a tener para recrear inteligencia similar a la de una persona.

De este modo, la IA está siendo utilizada en muchos campos; uno de ellos, el de la salud porque incorpora medicina personalizada y otras innovaciones como los asistentes personales de atención médica que actúan como entrenadores y alarmas para la toma de medicamentos o la ejecución de terapias. En campos como el de las ventas, proporciona capacidades para realizar compras virtuales ofreciendo recomendaciones personalizadas a clientes, además de ofrecer un pronóstico de demandas esperadas por medio de redes recurrentes a empresas. En instituciones financieras, puede identificar transacciones fraudulentas, calificar perfiles crediticios y automatizar tareas para administrar datos [40]. Los alcances de la IA son ilimitados cuando se utilizan para facilitar los procesos empresariales en aras de lograr una mayor competitividad y productividad.

Ahora bien, en la denominada industria 4.0, la IA ha facilitado la automatización de tareas imitando procesos del pensamiento humano para la toma de decisiones: puede entender, razonar y actuar según los datos que posea [41]. Conceptos como los de manufactura inteligente, Big Data y robótica, son sólo uno de los beneficios de esta tecnología. El Big Data, hace referencia al volumen de datos generados por los sistemas y las actividades. En este aspecto, la robótica hace referencia a la incorporación en los entornos de producción de robots que interactúan con humanos [42]. Cabe resaltar que en la industria

4.0, la IA se centra en la máquina y la automatización dejando de lado la tarea humana como protagonista.

Por otro lado, si se analizan los avances en Colombia, informes demuestran que durante la última década la implementación de herramientas tecnológicas y de medidas de seguridad para salvaguardarlas, ha crecido. De las empresas colombianas, [43] plantea que al menos el 68% evalúa la seguridad informática y de esta, el 32% realiza ejercicios que informan acerca de posibles fallas y violaciones. Desde esta perspectiva, Colombia es un país que ha avanzado en materia tecnológica pero que, en comparación con otras naciones industrializadas, se queda corto en cuanto a implementación y medidas de protección.

b) Limitaciones

La IA mejora, como ya se ha dicho, todo tipo de procesos; sin embargo, el flujo tan alto de información se escapa al ojo humano. Es un área que causa gran curiosidad a nivel personal y empresarial por su capacidad de transformar las relaciones y la industria. Igualmente, es un sistema que se perfecciona sobre la práctica, de lo cual se infiere que a futuro no se tenga claridad, en lo concerniente a si las organizaciones están o no preparadas para sortear su desarrollo [44]. Con esto, lo que se quiere manifestar es que una de las principales limitaciones que puede llegar a tener la IA, es el desconocimiento de los alcances e impacto a corto, mediano y largo plazo.

Los avances en inteligencia artificial y robótica han originado una serie de interrogantes no solo complejos sino también urgentes, que a nivel social y legal aún no se han definido. En el mundo empresarial, esto representa un desafío para iniciar la construcción de sistemas bajo diseños controlables que pongan límites a esta tecnología [45]. Es una realidad que la IA se ha convertido en una tendencia, tanto es así, que en países como Alemania, Estados Unidos, Australia, Francia y el Reino Unido la cultura de adopción de la tecnología es una realidad; sin embargo, en países de América Latina son muy pocos los que la incorporan y si lo hacen, van a un ritmo más lento. Esto ha hecho que en cuestión de seguridad y eficiencia operativa estén más expuestas frente a amenazas externas [46]. Por lo anterior, se puede asegurar que, en comparación con países de Europa y Norte América, la seguridad en redes e informática presenta mayor riesgo y amenazas.

Adicionalmente, [46] plantea otro inconveniente relacionado con el personal de las empresas y la escasa capacitación con la que este cuenta, en relación con el empleo de las herramientas tecnológicas mencionadas en el presente análisis. Dicha limitación causa preocupación, pues mientras la IA está entrenada para aprender a través del conjunto de datos que le brindan, las empresas no cumplen con los requerimientos de personal calificado para hacer uso y administración de la misma, lo que requiere una planificación e inversión considerables.

La IA ha impactado positivamente en la cooperación máquina-humano; con su aprendizaje activo, se ha convertido en un requerimiento extremadamente útil para el análisis de macro datos, lo que hace de ella una tecnología muy costosa. Lo anteriormente descrito, requiere que los gobiernos no retrocedan en su empeño de generar los principios fundamentales para su creación, programación, actualización y control [47]. La IA siempre ha sido vista como una oportunidad y debe ser así, pero para ello hay que sentar las bases normativas, antes de que tome ventaja y llegue a un punto incontrolable.

IV. CONCLUSIONES

La inteligencia artificial vino al mundo para quedarse. Fue desarrollada como una herramienta cuyo propósito es colaborar con el hombre, aportando respuestas a problemáticas de la sociedad. Pese a esto, es una tecnología con la capacidad de aprender de los errores al poseer autonomía, lo que ha ocasionado una serie de

dilemas acerca de los riesgos y desafíos que puede representar.

El principal riesgo y desafío que enfrentan las empresas frente a la inteligencia artificial, está en sus ventajas y limitaciones, sumado a los recursos necesarios para que el procesamiento y manejo de los datos no se vea expuesto ante códigos maliciosos y anomalías. Adicionalmente, existe una evidente falta de mano de obra capacitada en áreas de seguridad de la información, lo que facilita que los sistemas inteligentes se vuelvan más autónomos al no ser correctamente administrados y operados.

En el campo nacional e internacional, existen puntos de partida acerca de la legislación y regulación de la IA. Aunque se han dado los primeros pasos, sin embargo, los principios acerca de sus usos y efectos no son claros. Por consiguiente, no existe un contexto de transparencia legal que indique los aspectos fundamentales para la programación, las funciones y libertades de la inteligencia artificial. Son muchos los cuestionamientos acerca de los alcances y daños que pueda causar, así como el punto de no reversa en cuanto al control. En el mundo existe una preocupación creciente acerca de las escasas políticas que enmarcan la inteligencia artificial en su diseño y control. Es un reto para la privacidad y la protección, no solo de los datos y de la información, sino también de las personas.

A largo plazo, la IA presenta mejoras positivas en el ámbito empresarial potenciando la automatización de los procesos en distintos escenarios donde convergen las personas y los sistemas. Aunque aún es muy incipiente, se espera que integre el trabajo entre las personas y las máquinas por medio del desarrollo de nuevas estrategias que reconfiguren el mercado laboral. En contextos como el medioambiental, puede llegar a tener un impacto positivo porque mejora la eficiencia de los recursos.

V. REFERENCIAS

[1] A. García-López, F. Girón-Luque y D. Rosselli, «La integración de la inteligencia artificial en la atención médica: desafíos éticos y de implementación,» 2023. [En línea]. Available: https://revistas.javeriana.edu.co/files-articulos/UMED/64-3(2023)/6572567006/index.html.

[2] A. M. Casallas Sotaquira, «Inteligencia artificial: la nueva visión a la que apuestan las empresas de hoy,» 2021. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repository.unimilitar.edu.co/bitstream/handle/10654/38009/CasallasSotaquiraAngie-Milady2021.pdf?sequence=1&isAllowed=y.

[3] Organización para la cooperación y el desarrollo económico, «Cuarenta y dos países adoptan los principios de la OCDE sobre inteligencia artificial ,2019 México (Online),» 2019. [En línea]. Available: www.oecd.org/centrodemexico/medios/cuarentaydospaisesadoptanlosprincipiosdelaocdes obreinteligenciaartificial.htm .

[4] C. Tancara Q, « La investigacion documental. Temas Sociales , (17), 91-106.,» 1993. [En línea]. Available: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S0040-29151993000100008&lng=es&tlng=es.

[5] P. Schettini y I. Cortazzo, «Técnicas y estrategias en la investigación cualitativa,» 2016. [En línea]. Available: http://sedici.unlp.edu.ar/handle/10915/53686.

[6] J. Estupiñán Ricardo, M. Y. Leyva Vázquez, A. J. Peñafiel Palacios y Y. E. Assafiri Ojeda, «Artificial intelligence and intellectual property,» 2021. [En línea]. Available: https://rus.ucf.edu.cu/index.php/rus/article/view/2490/2445.

[7] A. Ayerbe, «La ciberseguridad y su relación con la inteligencia artificial,» 2020. [En línea]. Available: https://media.realinstitutoelcano.org/wp-content/uploads/2021/10/ari128-2020-ayerbe-ciberseguridad-y-su-relacion-con-inteligencia-artificial.pdf.

[8] M. Anishchenko, I. Gidenko, M. Kaliman, V. Polyvaniuk y Y. Demianchuk, «Artificial intelligence in medicine: legal, ethical and social aspects,» Acta Bioethica 2023; 29(1): 63-72, 2023. [En línea]. Available: https://www.scielo.cl/pdf/abioeth/v29n1/1726-569X-abioeth-29-01-63.pdf.

[9] J. D. Pedraza Caro, «La inteligencia artificial en la sociedad: explorando su impacto actual y los desafíos futuros,» 2023. [En línea]. Available: https://oa.upm.es/75068/.

[10] N. C. Pacanchique Quilaguy y R. C. Rodríguez Olaya , «El Impacto de la Inteligencia Artificial en el Trabajo,» 2021. [En línea]. Available: https://repository.unilibre.edu.co/bitstream/handle/10901/20588/El%20Impacto%20de%20la%20Inteligencia%20Artificial%20en%20el%20Trabajo.pdf?sequence=2&isAllowed=y.

[11] A. A. Becerril G, «Retos para la regulación jurídica de la Inteligencia Artificial en el ámbito de la Ciberseguridad,» Rev. IUS vol.15 no.48 Puebla jul./dic. 2021 Epub 14-Mar-2022, 2021. [En línea]. Available: https://www.scielo.org.mx/scielo.php?pid=S1870-21472021000200009&script=sci_arttext.

[12] M. E. Larrondo y N. M. Grandi , «Inteligencia Artificial, algoritmos y libertad de expresión,» 2021. [En línea]. Available: http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-86342021000100177.

[13] G. Rondo Montes, «Inteligencia Artificial en la Seguridad de TI,» INF-FCPN-PGI Revista PGI, (8), 99–101, 2021. [En línea]. Available: https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/59.

[14] C. G. Coral Tupaz, «Aplicación e impacto de la inteligencia artificial en el sector terciario de la economía,» 2023. [En línea]. Available: https://repository.unimilitar.edu.co/handle/10654/45067.

[15] A. Korinek y J. E. Stiglitz, «Artificial intelligence, globalization, and strategies for economic development. National Bureau of Economic Research,» 2021. [En línea]. Available: https://doi.org/10.3386/w28453.

[16] M. E. Sánchez Acevedo, «La inteligencia artificial en el sector público y su límite respecto de los derechos fundamentales,» Estudios constitucionales vol.20 no.2 Santiago dic. 2022, 2022. [En línea]. Available: https://www.scielo.cl/scielo.php?pid=S0718-52002022000200257&script=sci_arttext.

[17] Watson for Oncology, «IBM,» 2022. [En línea]. Available: https://www.ibm.com/common/ssi/cgi-bin/ssialias?appname=skmwww&htmlfid=897%2FENUS5725-W51&infotype=DD&subtype=SM&mhsrc=ibmsearch_a&mhq=IBM%20WATSON%20ONcology.

[18] M. Ortiz Osorio, «Importancia de las buenas prácticas en ciberseguridad en el trabajo remoto de entidades públicas de Colombia en época de pandemia.,» 2021. [En línea]. Available: https://repository.unad.edu.co/handle/10596/44501.

[19] C. Flores Siñani , «Inteligencia Artificial, Machine Learning, Deep,» INF-FCPN-PGI Revista PGI, (7), 11–13., 2021. [En línea]. Available: https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/96.

[20] G. Fernández Rubio, «El uso de la IA para ciberseguridad,» Número especial: Conferência Internacional Cooperação Internacional, multiculturalidade, trabalho colaborativo e ambientes mais inclusivos, sustentáveis e resilientes.9(4), 91-97, 2021. [En línea]. Available: https://revistas.rcaap.pt/uiips/article/view/26214/19289.

[21] J. J. Castro-Maldonado y H. F. Villar-Vega, «Análisis de riesgos y vulnerabilidades de seguridad informática aplicando técnicas de inteligencia artificial orientado a instituciones de educación superior. Revista modum, 3.,» 2021. [En línea]. Available: http://revistas.sena.edu.co/index.php/Re_Mo/article/download/4543/4734.

[22] B. S. C. Rojas, C. U. C. Rodríguez, D. J. E. Osorio y Y. T. G. Bello, «Redes neuronales artificiales y estado del arte aplicado en la ciberseguridad. Revista Matices Tecnológicos, 12, 58-63.,» 2020. [En línea]. Available: http://ojs.unisangil.edu.co/index.php/revistamaticestecnologicos/article/view/150.

[23] A. Fernández, «Inteligencia artificial en los servicios financieros,» 2019. [En línea]. Available: https://repositorio.bde.es/bitstream/123456789/8448/1/be1902-art7.pdf.

[24] D. A. Gómez Llinás, «El impacto de la inteligencia artificial sobre el ser humano y sobre su seguridad,» 2021. [En línea]. Available: https://repository.unimilitar.edu.co/bitstream/handle/10654/39998/EL%20IMPACTO%20DE%20LA%20INTELIGENCIA%20ARTIFICIAL.pdf?sequence=1&isAllowed=y.

[25] Comunicación de la comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económica y Social Europeo y al Comité de las Regiones, «Inteligencia artificial para Europa". Bru-selas, 25 de abril del 2018 COM(2018) 237 final. {SWD(2018) 137 final,» 2018. [En línea]. Available: https://ec.europa.eu/trans-parency/regdoc/rep/1/2018/ES/COM-2018-237-F1-ES-MAIN-PART-1.PDF.

[26] E. Vazquez Pita, «la UNESCO y la gobernanza de la inteligencia artificial en un mundo globalizado. la necesidad de una nueva arquitectura legal,,» [En línea]. Available: https://publicaciones.unex.es/index.php/AFD/article/view/1028.

[27] F. Morandín Ahuerma, «Principios normativos para una ética de la inteligencia artificial,» Consejo de Ciencia y Tecnología del Estado de Puebla (Concytep). pp. 28-85, 2023. [En línea]. Available: https://philpapers.org/rec/MORDDM-2.

[28] G7 Charlevoix, «Charlevoix common vision for the future of artificial intelligence,» 2018. [En línea]. Available: https://www.international.gc.ca/world-monde/assets/pdfs/international_relations-relations_internationales/g7/2018-06-09-artificial-intelligence-artificielle-en.pdf.

[29] Consejo de la Unión Europea , «Conclusiones relativas al Plan Coordinado sobre la Inteligencia Artificial,» 2019. [En línea]. Available: https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/es/pdf..

[30] C. L. Nodals García, «Sobre la necesidad de unificación de las iniciativas para un uso ético de la Inteligencia Artificial,» 2021. [En línea]. Available: https://revistas.uncp.edu.pe/index.php/socialium/article/view/880/1172.

[31] C. Milio, «Homo Sapiens, el eslabón débil de la seguridad de la información,» 2021. [En línea]. Available: http://portalreviscien.uai.edu.ar/OjS/index.php/RAIA/article/view/12/11.

[32] M. R. Ospina Díaz y P. E. Sanabria Rangel, «Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia,» Rev. Crim. vol.62 no.2 Bogotá May/Aug. 2020 Epub Nov 26, 2020, 2020. [En línea]. Available: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199.

[33] A. Guío Español , «Marco ético para la inteligencia artificial en COLOMBIA,» 2020. [En línea]. Available: https://www.usergioarboleda.edu.co/wp-content/uploads/2021/11/Marco-etico-para-la-inteligencia-artificial-en-Colombia-Maestria-en-Inteligencia-artificial.pdf.

[34] W. E. Ulrich Astaiza, «La necesidad de un marco ético y legal obligatorio para la inteligencia artificial y los algoritmos en Colombia,» DIXI, vol. 25, n°. 2, julio-diciembre 2023, 1-28, 2023. [En línea]. Available: https://revistas.ucc.edu.co/index.php/di/article/view/4765/3563.

[35] S. Arenas, M. Giraldo, J. Ochoa y A. Tangarife, «Posibilidad, riesgo e incertidumbre: análisis de tendencias en las ciencias de la información. Revista Interamericana de Bibliotecología, 45(3), e347313,» 2022. [En línea]. Available: https://eds-p-ebscohost-com.bibliotecavirtual.unad.edu.co/eds/pdfviewer/pdfviewer?vid=2&sid=dd93c405-e6d6-4405-a5de-767937856a62%40redis.

[36] D. Terreros, « Sistemas de Información Empresarial: Tipos de información para un gestión eficiente organizacional. Marketing Exitoso: Volumen 1, número, 1, pp. 1-22,» 2022. [En línea]. Available: https://blog.hubspot.es/marketing/sistemas-de-informacion-empresas.

[37] J. L. Londoño Córdoba , D. R. Dorado Gutiérrez y D. Giraldo Rendón , «Gerencia de la seguridad en la información de las organizaciones,» 2022. [En línea]. Available: https://digitk.areandina.edu.co/bitstream/handle/areandina/4535/Trabajo%20de%20Grado.pdf?sequence=1&isAllowed=y.

[38] K. M. Gutiérrez López, «Inteligencia artificial generativa: irrupción y desafíos,» Revista Enfoques. 4(2), 57, 2023. [En línea]. Available: https://revistasdigitales.uniboyaca.edu.co/index.php/EFQ/article/view/1075/838.

[39] J. M. Gómez Rodríguez, «Inteligencia artificial y neuroderechos. Retos y perspectivas,» Cuest. Const. no.46 Ciudad de México ene./jun. 2022 Epub03-Mar-2023, 2023. [En línea]. Available: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-91932022000100093.

[40] E. Burns, «What is Artificial Intelligence? Obtenido de SearchEnterprise AI:,» 2021, Agosto. [En línea]. Available: https://searchenterpriseai.techtarget.com/definition/AI-Artificial-Intelligence .

[41] M. J. Daza Cantor , C. A. Orjuela Mahecha , D. Paredes Castañeda , D. Salamanca Cubillos y Y. P. Martin Rincón , «Impacto de la inteligencia artificial en las empresas manufactureras en Colombia,» 2021. [En línea]. Available: https://repository.universidadean.edu.co/bitstream/handle/10882/11331/SanMartinYeny2021.pdf?sequence=2&isAllowed=y.

[42] L. F. Garcés-Giraldo, M. Benjumea-Arias, S. Cardona-Acevedo y C. Bermeo-Giraldo, « Uso de inteligencia artificial en gestión de la información: una revisión bibliométrica. Revista Ibérica de Sistemas e Tecnologias de Informação, (E54), 506-517.,» 2022. [En línea]. Available: https://search.proquest.com/openview/cd91b567d2231af1ab3b1838a62b3948/1?pq-origsite=gscholar&cbl=1006393.

[43] J. J. Cano M y A. Almanza, «Estudio de la evolución de la Seguridad de la,» 2021. [En línea]. Available: https://www-proquest-com.bibliotecavirtual.unad.edu.co/docview/2385758173/fulltextPDF/E0150AE384C74552PQ/1?accountid=48784.

[44] M. Kuglitsch, A. Albayrak, R. Aquino, A. Craddock, J. Edward-Gill, R. Kanwar y J. Luterbacher, «La inteligencia artificial aplicada a la reducción de riesgos de desastre: oportunidades, retos y perspectivas.,» 2022. [En línea]. Available: https://repositorio.aemet.es/bitstream/20.500.11765/14124/1/Boletin_OMM-71_1%285%29.pdf.

[45] F. Lledó Yagüe y O. Monje Balmaseda, «Ética y robótica : principios éticos para la inteligencia artificial y robótica,» 2020. [En línea]. Available: https://dialnet.unirioja.es/descarga/articulo/7631160.pdf.

[46] A. Pinilla Rodríguez , «Técnicas de inteligencia artificial usadas en seguridad informática,» 2020. [En línea]. Available: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1821_PinillaRodriguezA.pdf..

[47] G. Corvalán y M. Rodríguez, «Inteligencia articial para la recuperación pospandemia,» 2021. [En línea]. Available: https://scioteca.caf.com/bitstream/handle/123456789/1942/Inteligencia%20artificial%20para%20la%20recuperaci%c3%b3n%20pospandemia.pdf?sequence=1&isAllowed=y.

INDUSTRIA 5.0: MÁS ALLÁ DE LA AUTOMATIZACIÓN, HACIA UNA MANUFACTURA HUMANIZADA.

Ing. Esp. Cristian Camilo Cruz Hernández
Administrador Seguridad Administrada Datacenter
tresc92@hotmail.com

RESUMEN- ***En la época actual, las organizaciones deben ajustarse a los cambios tecnológicos y a las revoluciones industriales que se han presentado a lo largo de la historia, lo que han traído consigo la digitalización y la optimización de la interacción entre el hombre y la máquina, capitalizando el valor agregado que le puede ofrecer el trabajador al proceso industrial. Este artículo de investigación de tipo documental con enfoque cualitativo, tiene como objetivo general describir cómo la transición empresarial hacia la industria 5.0 ha impactado el factor humano y los procesos de manufactura; para ello, se abordarán las principales características de las dos últimas revoluciones industriales (4.0 y 5.0) y su diferencia, determinando el impacto de la industria 5.0, teniendo en cuenta el factor humano y los procesos de manufactura. Se concluye que la quinta revolución industrial nace de la anterior, retomando la participación humana como eje fundamental para responder a los retos tecnológicos actuales. La industria 4.0 se centró en la manufactura inteligente y la automatización, mientras que la industria 5.0, integró estos conceptos con las capacidades de las personas. La revolución industrial 5.0 pretende impactar de forma positiva la sostenibilidad, la resiliencia y el centrismo en el humano.***

Palabras clave: *Industria 4.0, Industria 5.0, manufactura, personas, tecnología.*

Abstract- In the current era, organizations must adapt to the changes in society and the industrial revolutions that have occurred throughout history and that have brought with them digitalization and the optimization of the interaction between man and machine, capitalizing the added value that the worker can offer to the industrial process. This documentary-type research article with a qualitative approach has the general objective of describing how the business transition towards industry 5.0 has impacted the human factor and manufacturing processes; To do this, the main characteristics of the last two industrial revolutions (4.0 and 5.0) and their difference are addressed, determining the impact of industry 5.0 taking into account the human factor and manufacturing processes. It is concluded that the fifth industrial revolution is born from the previous one, resuming human participation as a fundamental axis to respond to current technological challenges. Industry 4.0 focused on smart manufacturing and automation, while Industry 5.0 integrated these concepts with people's capabilities. The industrial revolution 5.0 aims to positively impact sustainability, resilience and human centrism.

Keywords- *Industry 4.0, Industry 5.0, manufacturing, people, technology.*

I. INTRODUCCIÓN

El área de manufactura e industria, ha evolucionado paralelamente a las revoluciones industriales determinando factores claves en los procesos de producción y transformación digital. En la industria 1.0, se utilizaban manualmente las herramientas teniendo en cuenta la experiencia y destreza; en la industria 2.0, los procesos estaban acompañados por máquinas y sistemas de información; por su parte, la industria 3.0, inició con un trabajo colaborativo entre robots, computadores y máquinas automatizadas; y en la industria 4,0, se dio paso a los sistemas

ciberfísicos y su interacción con las personas, siendo esta una industria determinante en el denominado "operador del futuro" abriendo campo a la robótica, la inteligencia artificial, el Big Data, el Cloud Computing, el IoT, entre otros [1].

Ahora, la Industria 5.0 surge como una evolución de la Industria 4.0, enfocándose en el abordaje de los problemas asociados al costo humano en la optimización de la manufactura. Esta nueva fase busca revitalizar el papel del factor humano, contrarrestando el dominio exclusivo de la tecnología. Se fundamenta en varios aspectos clave del mercado laboral y en la influencia de la tecnología en la era de la información. En relación con la idea anterior, la industria 5.0 se fundamenta en tres principios o características: La centralidad en las personas (enfoque humano), la sostenibilidad y la resiliencia, todo en aras de orientarse a un trabajo más colaborativo entre la máquina y el humano [2]. Todas y cada una de las revoluciones tienen como característica, su construcción sobre la anterior, dando paso al surgimiento de nuevas tecnologías que ayudan a la trasformación de la industria y la forma de trabajar [3].

La industria 4.0 impactó la vida laboral de los individuos, ofreciendo flexibilidad y robustez con altos niveles de calidad, detonando cadenas de valor dinámicas y organizaciones automatizadas [4], lo que implicaba menos participación del individuo. La industria 5.0, por su parte, trajo un replanteamiento de los equipos de trabajo para hacer organizaciones más resilientes, innovadoras, sostenibles y situando a la persona, como eje central [5].

Con todo lo anterior, este artículo de investigación pretende describir cómo la transición empresarial hacia la industria 5.0 ha impactado el factor humano y los procesos de manufactura; los objetivos específicos son: identificar las principales características y elementos de la industria 5.0, evaluar las diferencias de la industria 5.0 con respecto a laindustria 4.0 teniendo en cuenta el factor humano y los procesos de manufactura, y, determinar el impacto de la industria 5.0 en los procesos humanos y de manufactura.

II. PROCEDIMIENTO Ó METODOLOGÍA

La metodología de investigación empleada en esta indagación, fue la documental con enfoque cualitativo. La revisión documental se caracteriza por llevar a cabo una revisión de la bibliografía, la recolección, recopilación y selección de información relacionada con un tema específico articulando los datos de una manera analítica [6]. El enfoque cualitativo permite realizar un análisis de la información recolectada desde distintas perspectivas llegando a la definición de un contexto en particular [7].

Las estrategias para la búsqueda de información que se llevaron a cabo, consistieron en la revisión en distintas bases de datos y buscadores académicos, usando operadores booleanos como AND - OR y descriptores como: "Industria 4.0", "factor humano", "Industria 5.0", "elementos", "impacto" y "procesos de manufactura". Dentro de los artículos revisados a lo largo de 30 días, se seleccionaron 40 para este estudio; su categorización se puede ver en la tabla 1.

TABLA I
CATEGORIZACIÓN DE LA BÚSQUEDA DE ARTÍCULOS

Buscador	Descriptor	Artículos
Scielo	Industria 4.0	9
	Industria 5.0	3
	Impactos de la industria 5.0	1
	Industria 5.0	2
Redalyc		
Google Académico	Industria 4.0	8
	Industria 5.0	7
	Impactos de la industria 5.0	10

Fuente Propia

En la búsqueda de información se tuvieron en cuenta unos criterios de inclusión y de exclusión, que se exponen a continuación:

Criterios de inclusión (a. artículos de investigación y estudios que incluyeran los temas de revolución industrial, procesos de manufactura, factor humano e impactos de la industria 5.0; b. estudios publicados en inglés y español; c. estudios nacionales e internacionales

Criterios de exclusión (a. publicaciones anteriores al año 2019 y 2020; b. Artículos no relacionados con el objeto de estudio).

Principales limitaciones: En la búsqueda de fuentes bibliográficas, hubo escasez de información acerca del impacto de las revoluciones industriales 4.0 y 5.0 en el factor humano.

III. DESARROLLO Y DISCUSIÓN

Una revolución industrial es considerada como los cambios en los procesos dentro de la industria; situación que se ha venido dando desde la segunda mitad del siglo XVIII, donde la agricultura dejó de ser la base de muchas economías para darle paso a la industria como fuente de desarrollo [8]. A continuación, se describen las dos últimas revoluciones industriales a las que el mundo se ha enfrentado:

A. Industria 4.0

La industria 4.0 aceleró el desarrollo y crecimiento en varios sectores de manufactura, trayendo desafíos a la sociedad trabajadora relacionados con la sustitución por tecnologías de muchos puestos de trabajo, haciendo que se desvalorizara el rol y la experiencia laboral de muchos empleados [9].

Por lo tanto, sería una industria que abordaría y resolvería algunos de los desafíos del mundo, como la producción urbana, el cambio demográfico, la eficiencia energética y la optimización de los recursos. Se enfocaría en sistemas inteligentes que evitarían que los trabajadores realizaran tareas rutinarias para que se centraran en labores creativas y de valor agregado. Sin embargo, ante una inminente falta de trabajadores calificados, generó brechas en materia de empleo [10].

Debe señalarse que la cuarta revolución industrial engloba cambios sociales, políticos y económicos que surgen de los sistemas ciberfísicos y la digitalización. El término surgió en Alemania hacia el año 2011, en el que se buscaba como meta digitalizar los procesos de manufactura, es decir, partir de la transición empresarial a la era digital, utilizando procedimientos tecnológicos como el internet de las cosas, el Big Data, la Inteligencia artificial, el almacenamiento en la nube y los robots o co-bots colaborativos que apoyan los procesos de fabricación [11].

a) Características

La revolución 4.0 se centró en aspectos técnicos, sin tener en cuenta las habilidades humanas; esto le dio como principal característica, la deshumanización de la industria y un aumento de la tecnología que derivó en un incremento de la contaminación ambiental y problemas de seguridad informática [12]. Por lo demás, se observa que una de las características principales de esta revolución industrial, fue el uso de tendencias tecnológicas en las organizaciones que permitieron mayor productividad por medio del intercambio de información y la comunicación dentro y fuera de la empresa, a una variedad y velocidad sorprendente [13].

Es por esto, que la cuarta revolución industrial facilitó el acceso a dispositivos computacionales para todos [8], la conectividad, el auge de los algoritmos de inteligencia artificial, la generación de dispositivos y transporte interconectados, el desarrollo de asistentes virtuales, entre otros. Trajo consigo una transformación imparable de todos los procesos.

Resulta claro que la revolución 4.0 se alinea con las tecnologías para transformar la

fabricación, operación, diseño y servicio de productos, a través del análisis y la utilización de factores que mejorarían considerablemente los resultados de las organizaciones [14]. En este sentido, la planificación en las empresas fue fundamental para la implementación de nuevas tecnologías y la competitividad en el mercado.

Según la Federación Empresarial de Japón Keidanren [15], la Sociedad 4.0 se caracterizó por la reducción de la carga laboral, la implementación del trabajo remoto mediante tecnologías de la información y comunicación (TIC), y la automatización, así como un cambio de software y la transformación de los servicios; igualmente, rapidez en la innovación tecnológica y en las habilidades requeridas; y, sobre todo, la innovación disruptiva que produjo negativas al conocimiento tradicional y la experiencia. Todo esto, aunque representaba avances sustanciales, generaba un quiebre en las relaciones entre el hombre con la naturaleza, y por supuesto, un crecimiento en problemáticas sociales relacionadas con el estilo de vida.

Es así, como la cuarta revolución industrial fue el resultado de una transformación laboral que llegó a impactar negativamente los centros de trabajo haciendo necesaria la capacitación en empleos con mayor grado de calificación y trabajadores con altos conocimientos en plataformas digitales y trabajos remotos.

b) Elementos

El Sistema tecnológico es el primer elemento de la industria 4.0, especialmente en su facilidad de acceso y la capacidad para incorporarse a los sistemas productivos y la sociedad en forma masiva [16]. Los principales elementos de los sistemas o soluciones tecnológicas de esta industria según Smith citado por [16], son:

- La interoperabilidad (conexión inteligente)
- La virtualización (fábricas inteligentes
- La descentralización (tecnologías que pueden tomar decisiones)
- La capacidad en tiempo real
- La orientación al servicio
- Modularidad

En relación con el tema, el Foro Económico Mundial menciona cinco elementos fundamentales que sirven como base para evaluar la cuarta revolución industrial [17]:

- **Innovación:** Adopción de nuevas tecnologías para la transformación de la producción.
- **Economía global:** Inversión en la transferencia del conocimiento.
- **Capital humano y capacidades:** Conocimientos especializados con mano de obra flexible y capacitada.
- **Recursos naturales y sostenibilidad:** Producción con respeto hacia el medio ambiente.
- **Regulación y gobernanza:** Puede fomentar o ser impedimento para la implementación de la tecnología.

En lo esencial, la industria 4.0 sustenta un desarrollo de sistemas que al trabajar de manera conjunta, generan cambios trascendentales en la manufactura, el empleo, el comportamiento del consumidor y la manera acerca de cómo se efectúan los negocios dejando una latente necesidad de incluir procesos de formación del capital humano para obtener un valor agregado [18]. El impacto tecnológico, entonces trae consigo varios retos a los que se debe responder con una perspectiva integradora que involucre los recursos y las personas.

c) Factor humano

La industria 4.0 nació hacia el año 2011 como respuesta a la necesidad de perfeccionar el rendimiento de las máquinas normales. Fue considerada una fase de digitalización del sector de la manufactura que se impulsó gracias al aumento de la información y los datos, una potencialización en la conectividad y la inclusión de herramientas computacionales que llevaron a

nuevas capacidades y formas de interacción entre la persona y la máquina a través del seguimiento de la información en tiempo real [19].

Dentro de este marco, la maquinaria y los procesos de fabricación alcanzaron otros niveles que fueron dejando por fuera la supervisión y aportación de las personas. Algunos de los procesos y recursos disponibles que reemplazaron el trabajo humano, se relacionan en la tabla 2.

TABLA II
INDUSTRIA 4.0, PROCESOS QUE REEMPLAZARON EL FACTOR HUMANO

Recursos	Funciones en la Industria 4.0
Big Data	Recopilación y evaluación de datos a velocidades altas, concisas y precisas
Robot autónomo	Desarrollo de tareas repetitivas con una alta precisión
Simulación	Aprovechamiento de datos para reflejar el mundo físico en el virtual reduciendo costos y tiempos
Internet de las cosas	Comunicación en red de objetos direccionados e interconectados entre sí
Ciberseguridad	Protección de sistemas y de la información haciendo uso de protocolos estándar
Manufactura auditiva	Producción de productos personalizados e individualizados en menor tiempo
Realidad aumentada	Mezcla del contenido digital con el físico por medio de la construcción de una realidad mixta en tiempo real

Fuente (9)

Según [20], la revolución 4.0 enfatizó las siguientes necesidades y requerimientos a nivel de formación y capacitación:

- Formación en la ciencia de datos
- Operarios con habilidades digitales
- Mantenimiento, supervisión y programación de robots.
- Capacitación en los procesos de simulación.
- Técnicos y especialistas en mantenimiento predictivo.
- Expertos en machine Learning.

En efecto, el concepto de industria 4.0 fusiona las tecnologías y su interacción con los ámbitos físicos, digitales y biológicos distinguiendo cuatro enfoques: El social, que busca una mejora en el nivel de vida aunque implique un desempleo masivo; el basado en competencias, que requiere nuevas habilidades generando cambios estructurales y en la forma de trabajo; el basado en la producción, que automatiza los procesos de producción enfocándose en el aspectos funcional de la empresa; y el basado en el desarrollo, que promueve un cambio en la interacción hombre máquina con una interacción objeto – objeto, dejando de lado a las personas [21]. Evidentemente, fue una revolución industrial cuyos impactos más significativos alteraron drásticamente la forma en que las personas se relacionaban con las empresas.

En el ámbito laboral, países industrializados como Alemania, el uso de robots fue una característica 4.0 que ocasionó una disminución del 23% en el empleo manufacturero, dejando por fuera trabajadores con cualificaciones y ocupaciones medias [22]. Esto, como se puede ver, es solo un ejemplo del impacto negativo en la sociedad y en los beneficios económicos de trabajadores poco calificados. La introducción de las tecnologías llevó a un incremento en la desigualdad por la pérdida de puestos de trabajo afectando la composición económica de un país.

En relación con la idea anterior, la transformación digital de la industria 4.0, trajo a las organizaciones la necesidad de buscar actualización para sus colaboradores en el desarrollo de nuevas habilidades frente a la transformación digital [23]. Todo esto indica que conforme las empresas avanzan en sus tecnologías, también deben hacerlo en la capacidad de sus colaboradores y en la búsqueda de una mejor gestión organizacional.

d) Procesos de manufactura

En procesos como la administración de cadenas de suministro, muchas pymes digitalizaron varios de los procesos generando un decrecimiento de las actividades humanas; al sistematizar los procesos, generaron valor a

los negocios y disminuyeron los contratiempos. Hubo un fortalecimiento en las relaciones entre proveedores y clientes que bajó los costos operativos gracias al intercambio de altos niveles de información y la optimización de la cadena [24].

En la búsqueda constante de innovación en estrategias, las empresas han optado por adoptar tecnologías para el comercio en línea, lo que ha tenido un impacto significativo en la forma en que se distribuyen y gestionan los inventarios. El uso de internet en la implementación logística se ha vuelto un proceso crucial para mejorar los indicadores de productividad [25].

De esta manera, la industria 4.0 fue un período de asimilación de nuevas tecnologías de la información y de la comunicación dentro de los procesos productivos, donde se dieron cadenas de montaje sin operadores humanos, algo que llevó a un mejor aprovechamiento de las energías renovables, a diferencia de la tercera revolución industrial caracterizada por el uso de carbón y los recursos naturales [26].

En relación con lo anterior [26], los procesos de creación del producto generaron nuevas redes y ecosistemas de valor en los que se logró mejor calidad, agilidad en el rastreo y flexibilidad. El mantenimiento se conectó a la producción de manera integrada cubriendo todo el ciclo, derivando en beneficios económicos, sociales y ecológicos.

Para las empresas, la revolución 4.0 implicó aspectos positivos en la agilización de procesos a través de sistemas inteligentes y aprendizaje automático. En las líneas de producción, los robots por medio de algoritmos, aprendieron de los errores produciendo bienes más rápido, lo que minimizó accidentes, mejorando la calidad y un ahorro en costos sin intervención de la participación humana en algunos pasos del proceso. Una de sus ventajas, fue el hecho de que evitó la sobreproducción, pues solo se fabricaban los bienes que los clientes compraban [26].

Cabe considerar, que en la transición a la industria 4.0, se dieron cambios en las condiciones de operación y producción [27]; algunos de esos cambios se relacionan a continuación:

- **Cortos períodos de desarrollo:** Desarrollo de productos de forma más rápida.
- **Flexibilidad:** Para garantizar el cumplimiento de los requerimientos de los usuarios.
- **Eficiencia:** En el manejo de recursos y la optimización de los procesos.

En cuanto a la Tecnología 4.0, es evidente que ha representado una revolución industrial, porque mejoró la eficiencia en las fábricas, al minimizar los retrasos mediante la creación de valor. No obstante, al reducir la participación humana en los procesos de producción, ha ocasionado una disminución en los salarios y un aumento del desempleo en varios sectores industriales.

Siendo las cosas así, la industria 4.0 ayudó a las empresas a impulsar soluciones tecnológicas que optimizaron los procesos en cuanto a la disponibilidad de inventarios, repuestos, herramientas para el mantenimiento y reparación; elementos que fueron determinantes para maximizar la efectividad operativa. En el caso de mantenimiento, por ejemplo, la escasez podría ser catastrófica, debido a que elementos defectuosos ocasionarían interrupciones y fallas que podrían afectar todo el proceso de producción [28].

Por consiguiente, es importante concluir que en las actividades de manufactura el vínculo común es la *innovación de procesos y servicios* por medio de técnicas de aprendizaje con niveles superiores que incluyen materiales nuevos, interacción entre las máquinas y sistemas virtuales que utilizan la información.

B. Industria 5.0

La sociedad 5.0, es consecuencia de cuatro

sociedades antecesoras: la primera, una sociedad cazadora (1.0); la segunda, una sociedad agraria (2.0) donde las personas se hacen sedentarias; luego, una sociedad que abarca la primera y segunda revolución industrial (3.0), y por último, una sociedad de la información (4.0) [25].

De este modo, la sociedad 5.0 es definida como la que se centra en el hombre y equilibra el proceso tecnológico, económico y de resolución de problemas [25]. Esto significa, que consiste en una sociedad que posibilita la satisfacción general, teniendo como base las tecnologías digitales. En este contexto, las personas ocupan un papel central, ya que, a través de su capacidad de innovación y creatividad, tienen la oportunidad de dar vida a sus ideas utilizando la tecnología disponible.

Por consiguiente, la Comisión Europea en el año 2021 anunció la industria 5.0, con el propósito de enfocar el desarrollo del sector productivo hacia tecnologías más competitivas, cuya finalidad es, potenciar las relaciones entre el hombre y las máquinas [29]. Para [30], corresponde a una rehumanización de la industria y el reconocimiento de los avances digitales, robóticos y de automatización, como procesos fundamentales en una organización.

La industria 5.0 se ha ido caracterizando por el desarrollo exponencial de la inteligencia artificial y de la robótica a través de dos enfoques: el trabajo conjunto entre máquinas y personas, por medio de la colaboración activa y el trabajo sincrónico que relaciona la experiencia del individuo con la fuerza de trabajo del robot [31].

En función de lo planteado, la Industria 5.0 asume una colaboración entre las personas y las máquinas buscando un equilibrio entre la industria, la economía y la ecología que prioriza la sustentabilidad ante la creciente demanda de energías limpias, sostenibles y asequibles [32]. Es una revolución fortalecida con la era digital, donde el empoderamiento de las tecnologías exige una perspectiva nueva en cuanto a la labor de la persona y el desarrollo de su poder de imaginación, para no ser dependiente de la digitalización que ha impuesto cambios que requieren la priorización del individuo [33].

a) Características

La principal característica de la industria 5.0, es la unión entre los seres humanos y las máquinas con el fin de darle un valor agregado a la producción, y, a la creación de soluciones, productos y servicios personalizados e innovadores [30].

Por su parte [34], considera que la principal característica de esta industria, es la evolución emergente del sector industrial en el desarrollo de productos y servicios gracias al paralelo desarrollo tecnológico, con una finalidad centrada en tres elementos: el humano centrismo, la sostenibilidad y la resiliencia.

En otras palabras, la industria 5.0 radica en el poder que tiene para lograr objetivos de crecimiento y empleo convirtiéndose en un proveedor que coloca como eje fundamental el bienestar del trabajador [35]. No obstante, es necesario tener en cuenta una serie de competencias indispensables para enfrentar estos desafíos, entre las cuales se encuentran: la programación, las redes digitales, el manejo de bases de datos, la computación en la nube, el análisis de Big Data, la simulación y la impresión 3D, entre otros [35].

b) Elementos

Algunas de las tecnologías relacionadas con la industria 5.0, según [36], son:

- Las centradas en la persona y en la interacción humano-máquina que se interconecten e intercambien fortalezas.
- Tecnologías bioinspiradas.
- Tecnologías digitales en tiempo real y de modelado de sistemas complejos.
- Tecnologías de almacenamiento, transmisión y análisis de datos.

- Inteligencia artificial.
- Tecnologías para la autonomía confiable y la eficiencia energética.

Por su parte [37], menciona algunas de las posibles aplicaciones de la industria 5.0:

- **Manufactura en la nube:** orientada al proceso de manufactura tradicional, donde las partes interesadas trabajan juntas para lograr un proceso de fabricación más eficiente.
- **Gestión de la cadena de suministro:** La inteligencia aplicada combinada con la innovación de las personas, permite satisfacer la demanda con productos personalizados a un ritmo más rápido.
- **Manufactura y producción:** En este ámbito, se integra la inteligencia humana con la computación cognitiva de la robótica para desarrollar operaciones colaborativas que potencian la inteligencia y conectividad de las máquinas.

Con lo mencionado anteriormente, se fomenta la idea de que, a diferencia de su predecesora, esta nueva forma de trabajo promueve empleos altamente calificados en colaboración con las máquinas, lo que contribuye a mejorar la satisfacción del cliente y a promover un entorno más saludable.

c) Factor humano

La Agenda para el Desarrollo Sostenible, considera 17 objetivos para lograr una relación armónica en el mundo con la naturaleza; en este sentido, la sociedad 5.0 interviene en cambios en los estilos de vida profundizando en temas como la creatividad y la imaginación; los recursos humanos de esta sociedad deben caracterizarse por la diversidad y la disposición de hacer uso de la Inteligencia Artificial en aras de cumplir los horizontes planteados para el 2030 por las Naciones Unidas [25]. Con esto, se puede asegurar que la sociedad 5.0 representa un desafío en el factor humano pues no es claro cuáles son las habilidades que las personas deben tener para atender las necesidades actuales y con ello contribuir al desarrollo sostenible.

Basándonos en lo expuesto anteriormente, la Cumbre para el Reinicio Laboral de 2020 presentó un informe sobre el futuro de los empleos, en el cual se identificaron diez habilidades principales proyectadas para el año 2025. Estas habilidades se clasificaron según su grado de importancia en habilidades para la resolución de problemas, autogestión, trabajo colaborativo con personas y tecnologías, así como el uso y desarrollo de tecnologías [38].

Las habilidades se resumen en la tabla 3.

TABLA III
HABILIDADES QUE DEBEN POSEER LAS PERSONAS PARA EL AÑO 2025

Tipo	Habilidad
Resolución de problemas	Pensamiento centrado en el análisis y la innovación. Ideación y razonamiento Iniciativa, originalidad y creatividad Análisis y pensamiento crítico Resolución de problemas complejos
Tecnología, uso y desarrollo	Uso de tecnología: monitoreo y control. Diseño de tecnología y programación
Autogestión	Flexibilidad, tolerancia al estrés y resiliencia
Trabajo con personas	Aprendizaje activo y estrategias de aprendizaje Liderazgo e influencia social.

Fuente: [38]

En la tabla 3, se evidencian las habilidades que las personas deben adquirir para salvaguardarse a sí mismas, a la sociedad y al planeta, teniendo en cuenta que estamos en una era en la que los horizontes y desarrollos tecnológicos van a un crecimiento exponencial, convirtiéndose en escenarios potenciales para el desarrollo humano.

Dentro de este marco de ideas, la persona para la industria 5.0 debe contar con competencias formales y prácticas como componentes claves para realizar y responder a las necesidades, Luis Daniel Álvarez López, doctor en Ciencias de la investigación [39], las divide como habilidades 5.0 en cinco grupos que se relacionan en la figura 1.

Figura 1. Habilidades 5.0 1.

Grupo	Habilidad
Cognitivo	Resolución de problemas, pensamiento crítico, pensamiento analítico, alfabetización informacional y aprendizaje activo
Socioemocional	Colaboración, social interacción, resolución de conflictos, multicultural, inteligencia emocional, la gestión de personas, percepciones sociales, persuación, la formación y la enseñanza.
Estructural	Servicio, orientación empresarial, análisis de operaciones y formulación de informes
Técnico	La información y comunicación tecnológica, aplicación de tecnología, programación y seguridad digital
Estratatégico	Visión, planificación, toma de desiciones, autorregulación, identificación de problemas, evaluación de soluciones, identificación de causas y consecuencias

Fuente: [40]

Sucede pues que, el progreso de la inteligencia humana y la introducción de nuevas tecnologías son factores clave que impactan el mercado laboral, que se convierten en desafíos para las organizaciones, algo que transformó las reglas del juego abriendo la necesidad de adaptación al entorno digital e innovador para lograr un desarrollo integral beneficioso para todos.

d) Procesos de manufactura

En la Revolución Industrial 4.0, la visión de la industria se centraba en mejorar la eficiencia y productividad al colocar las nuevas tecnologías en el núcleo del proceso de producción. En esta revolución, también fundamentada en las nuevas tecnologías, se refuerza el papel del trabajador buscando generar prosperidad y crecimiento en el empleo respetando los límites ambientales [26]. Es una revolución centrada en la sostenibilidad, la resiliencia y en las personas que se integran con las organizaciones y la tecnología complementando los desarrollos de las revoluciones anteriores.

En este orden de ideas, la revolución 5.0, no se trata de sistemas inteligentes y máquinas automatizadas, sino de la integración de los avances, las energías renovables y la capacidad humana.

En los procesos de manufactura, Colombia se destaca por su relativa lentitud en la adopción de la automatización, principalmente debido a la falta de conciencia empresarial acerca de los beneficios que esta tecnología puede ofrecer. En contraste, países como Australia, Japón, Alemania, China y Estados Unidos han logrado un mayor acceso a los mercados tecnológicos lo que les ha permitido convertirse en referentes de la industrialización y la innovación, generando así un considerable valor agregado. Estas naciones son reconocidas mundialmente en el ámbito de la automatización, en contraposición a otras de menor tamaño y alcance en este sector [41]. En resumen, las empresas colombianas deben establecer alianzas internacionales para impulsar la productividad, el crecimiento y la eficiencia económica mediante la adopción de tecnologías de inteligencia artificial y otras herramientas que sean pertinentes en el contexto de la globalización actual [42].

Evidentemente, la transformación de los procesos generada por esta industria se ha vuelto una necesidad imperante en lugar de ser simplemente una opción para las empresas en el ámbito actual; como resultado, es decisivo que las personas se adapten a la hiperconectividad mediante el conocimiento, transformando tanto su forma de actuar como de pensar. Esto implica que los individuos se conviertan en generadores de ideas a partir de los avances tecnológicos, lo que a su vez fomenta la innovación y la ejecución de planes para reducir la exposición y los daños que los agentes externos puedan ocasionar a los datos [43].

C. Impacto de la industria 5.0

La industria 5.0 a diferencia de la anterior, complementa y amplía los factores económicos, tecnológicos, sociales y ambientales. Es considerada como el resultado de un ejercicio que responde a las necesidades y tendencias emergentes, sin dejar de lado a la persona. Recopila conocimientos y mejora la comprensión del factor humano en conjunto con la tecnología, fusionando procesos de educación y capacitación para enfrentar la nueva era digital [44].

Todas las revoluciones anteriores han dejado de lado la moral y el compromiso para favorecer los avances científicos y tecnológicos, ahondando problemáticas como el desempleo y la carencia de mano de obra especializada. Es

así, como la quinta revolución industrial viene con la idea de fomentar la ética, crear soluciones y proyectos que respondan a las necesidades de capacitación requeridas para que el hombre no quede minimizado por las nuevas tecnologías [45].

Por lo tanto, la revolución 5.0, trae características fortalecidas de la 4.0, reorganizando los recursos humanos para usar la inteligencia artificial sin desconocer las necesidades sociales y dando paso a la imaginación y a la creatividad, como generadores de valor.

Así las cosas, esta revolución busca crear ingeniería social mejorando el bienestar de las comunidades a través de la inteligencia artificial y otras tecnologías como el Blockchain y el Big Data. Su principal objetivo es lograr una perfecta sincronización entre la persona y la tecnología, produciendo sincronía con el medio ambiente [11].

Por último, es conveniente acotar que la Industria 5.0 se articula con los Objetivos de Desarrollo Sostenible, buscando mejorar la calidad del ambiente y de la vida, intensificando el concepto de ciudades inteligentes a través del desarrollo de herramientas digitales que despliegan tecnologías inteligentes, asegurando un crecimiento económico integral que le da valor a las personas dentro de la digitalización y la interconexión [46].

En áreas como la salud, la movilidad y la infraestructura, la industria 5.0 mejora la posición económica de las empresas, asegurando una mejor calidad de vida de la población, adaptando los cambios que trajo la revolución anterior al enfoque humano [47]. Esta industria mejora los entornos industriales integrando los factores de eficiencia, eficacia y calidad de vida.

El Boletín de Innovación, Logística y Operaciones de julio de 2023 señala que el impacto más significativo de la industria 5.0 se centra en la capacitación y el aprendizaje de las personas para interactuar y adaptarse a las herramientas tecnológicas actuales. Esto se hace con el objetivo de reducir el potencial de las máquinas para reemplazar ciertos trabajos humanos, reconociendo que se pueden mejorar numerosas áreas de la sociedad siempre y cuando se logre minimizar los riesgos y maximizar los beneficios [48].

Entonces, se plantea que la industria 5.0 se apoya en diversos sistemas tecnológicos para mejorar el diseño de productos mediante gemelos digitales, reducir fallas y optimizar mantenimientos y reparaciones; aumentar la productividad y destreza con co-bots o robots colaborativos; expandir el alcance del Internet de las Cosas (IoE) para incluir personas, procesos y datos; implementar Blockchain en la gestión descentralizada de instalaciones; y desarrollar el 6G, destinado a mejorar el rendimiento y redefinir los conocimientos [49].

En relación con la idea anterior, es importante recalcar que aunque es una tecnología con muchos beneficios, también tiene desventajas y desafíos a los que se enfrenta, como la seguridad, la confiabilidad y la privacidad de los datos que sólo puede asegurarse con la actualización y mantenimiento de la ciberseguridad en las estructuras digitales [49].

Por lo tanto, la transformación de las empresas de la industria 4.0 a la 5.0, se fundamentó en la creación de espacios inteligentes que buscan una industria más humana, resiliente y sostenible, definida en las siguientes líneas de actuación:

- Desarrollo de una manufactura personalizada.
- Diseño de robots colaborativos con las personas.
- Empoderamiento del trabajador.
- Integración con mayor colaboración en los sistemas globales.
- Defensa del medioambiente con menor generación de residuos y de contaminación.
- Desarrollo de soluciones sostenibles y ecológicas.
- Colaboración a través de la innovación abierta.
- Diseño de sistemas adaptables entre el hombre y la máquina.

Con todo lo anterior, se puede concluir que el impacto de la industria 5.0 está arraigado en un modelo de organización permanente en la que se define un modelo de cultura organizacional abierta que integra los recursos, las capacidades, los espacios inteligentes y la creatividad humana, para generar ventajas competitivas que responden a las necesidades actuales.

IV. CONCLUSIONES

A partir de la industria 4.0 y 5.0, el mundo empresarial ha introducido nuevas capacidades y características que satisfacen de manera más eficiente y en tiempo récord las necesidades de la población. Tecnologías como la IA, el Big Data, el Blockchain y el internet de las cosas, han hecho posibles servicios de alta calidad y capacidades integradas que en la actualidad y con la industria 5.0, mejoran el rendimiento integral de los procesos al combinar la tecnología con la gestión humana.

La quinta revolución industrial representa un cambio significativo en el ámbito de la producción y la fabricación, surgido de la era de la industria 4.0 donde se minimizaba la participación humana. Este nuevo período busca restablecer la colaboración entre el trabajador y la máquina inteligente, otorgando un valor esencial a las habilidades humanas y a la innovación en los procesos productivos. Para lograrlo, es necesario realizar mejoras sustanciales en los procesos de capacitación y enseñanza, con el fin de enfrentar de manera eficaz los desafíos tecnológicos actuales.

La industria 4.0 estaba enfocada en revolucionar el sector de manufactura, integrando varias tecnologías y buscando una "industria inteligente" cuya prioridad era la automatización; en cambio, la industria 5.0 integra la eficiencia de las máquinas con la capacidad de la persona. Se enfoca en asignar tareas repetitivas a los aparatos y tareas de creatividad y pensamiento crítico a los individuos.

Después de un creciente auge y continuo crecimiento de las nuevas tecnologías, la producción en masa y la automatización, el mundo hoy en día se enfrenta a una revolución industrial que pretende regresar el protagonismo a las personas. En este sentido, se debe considerar que se necesitan grandes esfuerzos para llegar a la denominada sostenibilidad digital que integra los ODS, las personas y las tecnologías inteligentes.

En la era de la industria 5.0, se produce una integración más estrecha entre los trabajadores y las máquinas con el fin de incrementar la eficiencia y optimizar los procesos de manufactura, logística y control de calidad. En este contexto, se enfatiza la sostenibilidad como prioridad, al tiempo que se mantienen aspectos clave de la industria 4.0, como la reducción de costos y la precisión en los resultados.

La principal diferencia entre la revolución industrial 4.0 y 5.0, radica en la proyección de la persona en la producción inteligente, las redes y las tecnologías digitales, brindándole protagonismo a través de la innovación y la creatividad. El factor humano en la transición entre estas dos revoluciones, es redefinido a partir de nuevas funciones, en donde las personas dejan de lado labores repetitivas para estimular su capacidad de innovación y creatividad.

V. REFERENCIAS

[1] I. Val Pardo, «Sistemas socio-técnicos e industria 5.0,» 2022. [En línea]. Available: https://www.researchgate.net/profile/Isabel-Pardo/publication/364096777_SISTEMAS_SOCIO-TECNICOS_E_INDUSTRIA_50_Isabel_De_Val_Pardo_Catedratico_de_Organizacion_de_Empresas_XX_Encuentro_Internacional_AECA_.

[2] I. Gonzalez Gonzalez, M. P. Martìnez Ruiz y J. J. Blazquez Resino, «El impacto de las ultimas tecnologias en la transformaciòn de la industria,» 2020. [En línea]. Available: https://www.mintur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/428/GONZALEZ,MARTINEZ,BLAZQUEZ.pdf.

[3] A. Hernández Arango , «TECNOLOGÍAS 5.0 O DE PERFECCIONAMIENTO HUMANO PARA LA MEDICINA,» 2021. [En línea]. Available: https://revistamedicina.net/index.php/Medicina/article/view/1643/2127.

[4] P. A. Castellanos Rivero y M. d. P. Escott Mota, «Evolución de las habilidades laborales en la industria 4.0 y su impacto financiero. Revista Innova ITFIP, 6(1)106-119JUNIO2020,» 2020. [En línea]. Available: https://revistainnovaitfip.com/index.php/innovajournal/article/view/82/172.

[5] J. M. Garcia Contreras y L. E. Mendoza Hernandez, «El impacto de la Industria y Sociedad 5.0 en la educación. UNO Sapiens Boletín Científico de la Escuela Preparatoria No. 1. Publicación semestral, Vol. 5, No. 10 (2023) 15-18,» 2023. [En línea]. Available: https://repository.uaeh.edu.mx/revistas/index.php/prepa1/article/view/10387/9932.

[6] L. Reyes Ruíz y F. A. Carmona Alvarado , «La investigación documental para la comprensión ontológica del objeto de estudio.,» 2020. [En línea]. Available: http://bonga.unisimon.edu.co/bitstream/handle/20.500.12442/6630/La%20investigaci%c3%b3n%20documental%20para%20la%20comprensi%c3%b3n%20ontol%c3%b3gica%20del%20objeto%20de%20estudio.pdf?sequence=1&isAllowe.

[7] J. A. Maxwell, «Diseño de la investigación cualitativa,» 2019. [En línea]. Available: https://books.google.es/books?hl=es&lr=&id=ZLewDwAAQBAJ&oi=fnd&pg=PT351&dq=investigaci%C3%B3n+cualitativa+&ots=fl7BxDq0zO&sig=L1IwcdqVxHgmUQKHIBVK9NovCbw..

[8] L. Arciniegas Londoño y G. D. Corzo Ussa, «Contextualización de la Cuarta Revolución Industrial, Industria 4.0, Industria 5.0 y Tecnología 5G con el sector Defensa y Seguridad,» Revista científica en Ciencias Sociales e interdisciplinaria. Volumen 12, número 21, enero–diciembre 2020, pp. 245-258, 2020. [En línea]. Available: https://revistascedoc.com/index.php/pei/article/view/225/188.

[9] J. Carro Suárez y S. Sarmiento Paredes, «El factor humano y su rol en la transición a Industria 5.0: una revisión sistemática y perspectivas futuras. Entreciencias: diálogos soc. conoc. vol.10 no.24 León ene./dic. 2022 Epub 28-Feb-2023,» 2023. [En línea]. Available: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-80642022000100216&lang=es.

[10] L. T. Mantilla Avendaño, «Industria 5.0: ¿Vuelve el hombre al centro de los procesos de producción?,» [En línea]. Available: https://repository.eafit.edu.co/bitstream/handle/10784/15195/Lorena_Taiz-Mantilla_2019.pdf?sequence=2&isAllowed=y.

[11] I. Morillo Trujillo, «Industria 4.0 y Sociedad 5.0: análisis de las estrategias de China, Japón y la Unión Europea,» 2022. [En línea]. Available: https://uvadoc.uva.es/bitstream/handle/10324/55614/TFM-J-77.pdf?sequence=1&isAllowed=y.

[12] G. Barrera y O. Leon , «A Tecnologías de la Industria 5.0: Un Análisis empírico de su impacto en la sostenibilidad,» XXII Congreso Internacional AECA. Inteligencia Artificial, riesgos y sostenibilidad: claves de hoy para las organizaciones del futuro, 2023. [En línea]. Available: https://xxiicongreso.aeca.es/wp-content/uploads/2023/09/poster1.pdf.

[13] K. V. Saavedra Salinas, «Una revisión de la revolución industrial 4.0 y sus métodos de implementación en las nuevasindustrias,» 2022. [En línea]. Available: https://acofipapers.org/index.php/eiei/article/view/2210/1847.

[14] G. Fajardo Marin , «La industria 4.0: un análisis comparado entre países Latinoamericanos países desarrollados,» 2021. [En línea]. Available: https://repository.ucc.edu.co/server/api/core/bitstreams/71c66cb8-8bb5-44ce-bee9-f2a6f3d5fbfd/content.

[15] Keidanren Japan Business Federation , «Innovation for SDGs. Road to society 5.0,» 2018. [En línea]. Available: https://media.realinstitutoelcano.org/wp-content/uploads/2021/11/ari10-2019-ortega-sociedad-5-0-concepto-japones-sociedad-superinteligente.pdf.

[16] F. Walas Mateo, «Industria 5.0. Inteligencia Artificial y Aprendizaje Automático para optimizar procesos industriales,» 2023. [En línea]. Available: https://www.researchgate.net/publication/373722726_Industria_50_Inteligencia_Artificial_y_Aprendizaje_Automatico_para_optimizar_procesos_industriales/

link/64f9c2784c72a2514e5b8691/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6In.

[17] H. R. Cabrera, B. Rodríguez Pérez, J. L. León González y A. Medina León, «Ideas y conceptos básicos para la comprensión de las industrias 4.0.,» Universidad y Sociedad vol.12 no.4 Cienfuegos jul.-ago. 2020 Epub 02-Ago-2020, 2020. [En línea]. Available: http://scielo.sld.cu/scielo.php?pid=S2218-36202020000400008&script=sci_arttext.

[18] L. Gamboa Matos , «Aplicación en la industria 4.0.,» Revista Complejidades del Ágora Jurídica Vol. 2 n°1 2021, pp. 78-89, 2021. [En línea]. Available: http://www.peid.uda.cl/wp-content/uploads/2021/07/5-LISBET-Aplicacion-en-la-industria-4.0%5EL.pdf.

[19] S. Vaidya, P. Ambad y S. Bhosle, «ndustry 4.0 - A Glimpse. 2nd International Conference on Materials Manufacturing and Design Engineering, 20(1), 233-238,» 2019. [En línea].

[20] R. L. Gonzalez , «El impacto de la cuarta revolución industrial en la educación superior,» 2022. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.researchgate.net/profile/Rosana-Leonor-Gonzalez/publication/365721606_EL_IMPACTO_DE_LA_CUARTA_REVOLUCION_INDUSTRIAL_EN_LA_EDUCACION_SUPERIOR/links/638b70327d9b40514e1012e9/EL-IMPACTO-DE-LA-CU.

[21] Y. A. Sukhodolov, «The Notion, Essence, and Peculiarities of Industry 4.0 as a Sphere of Industry. Studies in Systems, Decision and Control, 169, 3-10.,» 2018. [En línea]. Available: https://doi.org/10.1007/978-3-319-94310-7_1.

[22] S. Pedraza Guevara y Y. Chamba Flores , «La robótica en el ámbito laboral: un estudio de revisión,» 2021. [En línea]. Available: https://www.innovasciencesbusiness.org/index.php/ISB/article/view/38/44.

[23] P. A. Rodríguez-Correa, C. A. Echeverri-Gutiérrez, A. Valencia Arias, L. C. Acosta Agudelo y M. Echeverri Gutiérrez, «Tendencias en tecnologías convergentes en la industria 4.0: una revisión de literatura,» 2023. [En línea]. Available: https://revistas.uis.edu.co/index.php/revistaion/article/download/14339/13180/101158.

[24] G. A. Vázquez Valerio, «Innovación y productividad en cadenas de suministro inteligentes en la post pandemia,» 2023. [En línea]. Available: https://ojs.eumed.net/rev/index.php/rilco/issue/download/10/6#page=38.

[25] A. M. Reyes Fabela , «diseño y desarrollo sostenible en la sociedad 5.0,» 2022. [En línea]. Available: http://ri.uaemex.mx/bitstream/handle/20.500.11799/112881/Dise%C3%B1o%20y%20desarrollo%20sostenible.pdf?sequence=1#page=39.

[26] D. M. Altamar Martínez, «EL IMPACTO DE LA INDUSTRIA 4.0 EN LA HISTORIA Y QUE SE PUEDE ESPERAR A FUTURO CON LA INDUSTRIA 5.0,» 2023. [En línea]. Available: https://repository.unimilitar.edu.co/bitstream/handle/10654/44828/AltamarMartinezDeybyManuel2023_Ensayo.pdf.pdf?sequence=1&isAllowed=y.

[27] J. Caballero y D. S. Suarez, «6G: Nuevas Tecnologias y sus Aplicaciones,» 2022. [En línea]. Available: https://repositorio.uniandes.edu.co/bitstream/handle/1992/63465/6G%20-%20Nuevas%20Tecnologias%20y%20sus%20Aplicaciones.pdf?sequence=6&isAllowed=y.

[28] L. F. Montilla Arbeláez, «El estado del arte de la industria 4.0 en paises desarrollados y Colombia,» 2021. [En línea]. Available: https://repository.ucc.edu.co/server/api/core/bitstreams/dd44e0c6-ef3e-489e-b159-72e422eda1a7/content.

[29] Advanced Factories Expo & Congress, «¿Qué es la industria 5.0 y cuáles son sus 3 principales características?,» 24 11 2022. [En línea]. Available: https://www.advancedfactories.com/industria-5-0-caracteristicas/.

[30] TOTVS LATAM , «Industria 5.0: ¿Qué hay de nuevo y cuáles son sus,» 27 Diciembre 2021. [En línea]. Available: https://es.totvs.com/blog/industria-4-0/industria-5-0-que-hay-de-nuevo-cuales-son-sus-impactos/.

[31] K. A. Demir , G. Döwen y B. Sezen, «The Next Industrial Revolution: Industry 5.0 and Discussions on Industry 4.0. 4th International Management Information Systems Conference "Industry 4.0", 01-10. Turkey: İstanbul University.,» 2019. [En línea]. Available: https://www.researchgate.net/publication/336653504_The_Next_Industrial_Revolution_Industry_50_and_Discussions_on_Industry_40.

[32] O. A. Elfar, C. Chang, H. Y. Leong, A. P. Peter, K. W. Chew y P. L. Show, « Prospects of Industry 5.0 in algae: Customization of production and

new advance technology for clean bioenergy generation. Energy Conversion and Management: X, 10, 01-10.,» 2021. [En línea]. Available: https://doi.org/10.1016/j.ecmx.2020.100048.

[33] M. Fernández Pereira, «Pandemia, cambios en el mundo y nueva sociedad,» VOL. 6 NÚM. 3 (2021): JULIO-SEPTIEMBRE - 2021 , 2021. [En línea]. Available: https://revistaoc.oncti.gob.ve/index.php/odc/article/view/60.

[34] A. V. Travez Tipan y C. M. Villafuerte Garzon, «Industria 5.0, revisión del pasado y futuro de la,» Ciencia Latina Revista Científica Multidisciplinar, 7(1), 1059-1070, 2023. [En línea]. Available: https://ciencialatina.org/index.php/cienciala/article/view/4457/6834.

[35] I. Lopes Martínez, A. Cuesta Santos, J. Vilalta Alonso , M. S. Fleitas Triana, T. Delgado Fernández , G. Neumann y A. Cruz Ruiz, «Creando capacidades: hacia la industria 5.0 en la formación de ingenieros industriales,» Revista Cubana De Administración Pública Y Empresarial, 6(2), e230., 2022. [En línea]. Available: https://apye.esceg.cu/index.php/apye/article/view/230

[36] J. Muller, «Enabling Technologies for Industry 5.0 Results of a workshop with Europe's technology leaders,» 2020. [En línea]. Available: https://op.europa.eu/en/publication-detail/-/publication/8e5de100-2a1c-11eb-9d7e-01aa75ed71a1/language-en.

[37] P. K. Maddikunta, Q. V. Pham, N. Deepa, T. r. Gadekallu, R. Ruby y M. Liyanage, «Industry 5.0: A survey on enabling technologies and potential applications. Journal of Industrial Information Integration, 26, 100257.,» 2021. [En línea]. Available: https://doi.org/10.1016/j.jii.2021.100257.

[38] WORLD ECONOMIC FORUM, «Estas son las 10 principales habilidades laborales del futuro - y el tiempo que lleva aprenderlas,» 2020. [En línea]. Available: https://es.weforum.org/agenda/2020/10/estas-son-las-10-principales-habilidades-laborales-del-futuro-y-el-tiempo-que-lleva-aprenderlas/.

[39] L. D. Alvarez López, «HUMANOS 5.0: el recurso humano, activo fundamental para la competitividad,» Revista Científica Internacional, 6(1), 46–60, 2023. [En línea]. Available: https://www.revista-cientifica-internacional org/index.php/revista/article/view/63/139.

[40] M. E. Jiménez, «Concepción, desarrollo y validación de un modelo interaccionista de competencias profesionales en la industria 4.0,» 2021. [En línea]. Available: https://r.search.yahoo.com/_ylt=AwrFfbBxVE5li.4FRRWrcgx.;_ylu=Y29sbwNiZjEEcG9zAzEEdnRpZAMEc2VjA3Ny/RV=2/RE=1699661042/RO=10/RU=https%3a%2f%2fdialnet.unirioja.es%2fservlet%2ftesis%3fcodigo%3d305612/RK=2/RS=8ans_Zji1HACdvMWuQS01wHU3GE-.

[41] N. Gonzalez Rubio, «Análisis de los avances tecnológicos en la industria 4.0 en países desarrollados y Colombia,» 2021. [En línea]. Available: http://repository.ucc.edu.co/items/c89b34ba-1af7-49bf-acb0-e24afec435ef.

[42] A. D. Pardo Melo , Z. M. Cañón y J. C. Téllez Alonso, «Efectos de la Inteligencia Artificial en las Empresas,» 2020. [En línea]. Available: https://digitk.areandina.edu.co/bitstream/handle/areandina/3959/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y.

[43] P. Medina Chicaiza, M. Chango Guanoluisa, M. Corella Cobos y D. Guizado Toscano, «Transformación digitalen las empresas: una revisión conceptual.,» Vol. 7, N°. CININGEC II (2022) -2022, 2022. [En línea]. Available: https://revistas.utb.edu.ec/index.php/sr/article/view/2804/2373.

[44] M. Breque, L. De Nul y A. Petridis , « Industry 5.0: Towards a sustainable, human-centric and resilient European industry,» 2021. [En línea]. Available: https://op.europa.eu/en/publication-detail/-/publication/468a892a-5097-11eb-b59f-01aa75ed71a1/.

[45] F. R. Arencibia Pardo, B. Peña Rodríguez y A. Pardo García, «El falso conteo de las revoluciones industriales: de la 1 a la 5.,» 2020. [En línea]. Available: https://revistas.curn.edu.co/index.php/aglala/article/view/1562.

[46] M. P. Gaytán, V. H. T. Preciado y J. E. R. Delgado, «Medición de la transformación digital en la Industria 5.0 y la Agenda 2030 en economías seleccionadas de APEC,» 2022. [En línea]. Available: http://ww.ucol.mx/content/publicacionesenlinea/adjuntos/economia-y-sociedad-digital_534.pdf#page=125.

[47] M. G. BenitesCastillo, D. J. Diego Chinchayhuara, J. E. Sánchez Vásquez y A. M. Vásquez Díaz, «La adopción de la industria 4.0 y su influencia en la mejora de la calidad de vida en la sociedad 5.0: Una revisión sistemática,» 2022. [En línea]. Available: https://revistas.unitru.edu.pe/index.php/RINGIND/article/view/4984/5266.

[48] J. D. Peralta Mendoza, E. Mercado Cano, J. Huitron Hernandez y A. Troncoso Palacio, «Cómo Mejorar la Gestión del Conocimiento Mediante la,» BILO Vol. 5 No. 2. Julio-Diciembrede 2023© The author; licensee Universidad de la Costa -CUC. BILO Vol. 5. No. 2, pp. 1-9.Julio -Diciembre2023Barranquilla. ISSN 2711-3280Creative Commons —CC BY-NC-ND 4.0, 2023. [En línea]. Available: https://revistascientificas.cuc.edu.co/bilo/article/view/5341/5087.

[49] C. Deus Aguilera, R. Casares Li y A. E. García Toll, «Maintenance 5.0: Trends and Challenges,» 2022. [En línea]. Available: https://www.researchgate.net/profile/Carlos-Deus-Aguilera/publication/364167100_Maintenance_50_Trends_and_Challenges_Mantenimiento_50_tendencias_y_desafios/links/638e41c911e9f00cda1f483a/Maintenance-50-T.

Revista TECNO**ESCOM**
ISSN 2711-0761. Vol. 6. No. 1

INFLUENCIA DE LA NORMA ISO 27001 EN LA IMPLEMENTACIÓN Y ACTUALIZACIÓN DE LA TECNOLOGÍA EN LA INDUSTRIA FARMACÉUTICA

Esp. Carlos Andrés Arias
Líder de ciberseguridad
E-mail: ariasfonseca@gmail.com

RESUMEN- ***Uno de los principales objetivos de cualquier organización, es llevar a cabo una adecuada gestión de la seguridad de la información dentro de la empresa, siendo aquella un activo de gran valor, especialmente en áreas como la salud. Este artículo de investigación, basado en la búsqueda de información con enfoque cualitativo, tiene como objetivo general describir la influencia de la Norma ISO 27001 en la seguridad de la información y la actualización tecnológica de la industria farmacéutica. Para responder a ello, se describen los principales aspectos y elementos de la norma, así como las características de la industria farmacéutica y los procesos más destacados que esgrime a nivel tecnológico. Como resultados, se encontró que la norma responde al crecimiento exponencial de la información y la tecnología, presentando unos puntos y aspectos clave que se deben incorporar dependiendo de las características particulares de cada empresa. La industria farmacéutica es una de las más avanzadas a nivel tecnológico, lo que hace que cuente con procesos actualizados de diseño, automatización y manejo de la información, más aún sabiendo que es uno de los sectores con mayor riesgo de ataques cibernéticos. La implementación de tecnologías en la industria, amparándose en la Norma ISO 27001, hace que esta se convierta en uno de los sectores que prioriza la seguridad y la mitigación de riesgos.***

Palabras clave: *Implementación tecnológica, Industria farmacéutica, Norma ISO 27001, Seguridad de la información.*

Abstract-One of the main objectives of any organization is to carry out adequate management of information security within the company, with information being a highly valuable asset, especially in areas such as health. This research article based on the search for information with a qualitative approach had the general objective of describing the influence of the ISO 27001 standard on information security and technological updating of the pharmaceutical industry. To respond to this, the main aspects are described and elements of the standard, the characteristics of the pharmaceutical industry and the most outstanding processes it manages at a technological level. As a result, it was found that the standard responds to the exponential growth of information and technology by presenting some key points and aspects that must be incorporated depending on the particular characteristics of each company; The pharmaceutical industry is one of the most technologically advanced, which means it has updated design, automation and information management processes, even more so knowing that it is one of the sectors with the highest risk of cyber-attacks. The implementation of technologies in the industry based on the ISO 27001 standard makes it become one of the sectors that prioritizes security and risk mitigation.

Keywords- *Information security, ISO 27001, Pharmaceutical industry, Technological implementation.*

I. INTRODUCCIÓN

Temas como la seguridad de la información y el desarrollo tecnológico en las organizaciones, son fundamentales y necesarios. Es así que, requieren un gran esfuerzo económico y una adecuada planificación que garantice la

eficiencia de los procesos y actividades, así como una gestión adecuada de vulnerabilidades y políticas de seguridad que aseguren elementos como la integridad, disponibilidad y confidencialidad de la información.

Como respuesta a las amenazas que aumentan de manera exponencial, surge la norma ISO 27001, la cual establece los requisitos del sistema de gestión de seguridad de la información y mitiga en gran medida los riesgos de ciberseguridad y seguridad informática. Esta norma implica realizar una evaluación integral del estado de las compañías, identificando brechas y vulnerabilidades [1].

En este contexto, el presente artículo relaciona la Norma ISO 27001, con una industria esencial y en continuo crecimiento a nivel nacional e internacional: la industria farmacéutica. En Colombia, esta industria se encuentra en el sector terciario y representa un alto porcentaje del PIB y del empleo.

El objetivo general de esta investigación, es describir la influencia que tiene la norma ISO 27001 en la seguridad de la información, así como la implementación y actualización de la tecnología en la industria farmacéutica. Los objetivos específicos son: relacionar los principales aspectos y elementos de la norma ISO 27001, reconocer las características tecnológicas presentes en la industria farmacéutica en Colombia, e identificar los procesos más destacados que requieren implementación tecnológica dentro de esta industria.

II. PROCEDIMIENTO Ó METODOLOGÍA

Esta investigación adoptó un enfoque cualitativo que inició con la identificación de variables seleccionadas para recopilar información de diversos estudios sobre la norma ISO 27001, seguridad de la información y su implementación en la industria farmacéutica. Según [2], el enfoque cualitativo comienza con una revisión inicial de la literatura que respalda la formulación de un problema, hasta llegar al informe de resultados basado en la muestra, recolección y análisis de datos, lo que permite comprender fenómenos desde diversas perspectivas.

Para llevar a cabo la búsqueda de información, se consultaron bases de datos como Google Académico, Scielo y Redalyc, utilizando descriptores como "ISO 27001", "industria farmacéutica" e "implementación tecnológica". Se revisaron aproximadamente 80 artículos, de los cuales se seleccionaron 40. La Tabla 1 muestra las bases de datos utilizadas, los descriptores y el número de artículos encontrados en cada una.

TABLA I
BASES DE DATOS Y DESCRIPTORES UTILIZADOS EN LAS BÚSQUEDAS

Base de datos	Descriptores	Artículos
Google Académico	ISO 27001	7
	Industria farmacéutica	9
	Implementación tecnológica	4
Redalyc	ISO 27001	4
Scielo	Industria farmacéutica	6
	ISO 27001	10

Fuente: Propia

Para la búsqueda de información, se tuvieron en cuenta:

- Criterios de inclusión: (a. publicaciones dirigidas específicamente a los descriptores abordados y temas relacionados con la seguridad informática en la industria farmacéutica; b. estudios nacionales e internacionales; c. investigaciones en español e inglés).

- Criterios de exclusión (a. se descartaron artículos ajenos al objeto del presente estudio; b. publicaciones con fecha anterior al año 2020).

- Principales limitaciones: En la búsqueda de información se presentó escasez de documentos que relacionaran la norma ISO27001 con la industria farmacéutica y sus procesos.

III. DESARROLLO Y DISCUSIÓN

A. Norma ISO 27001

Las organizaciones están cada vez más expuestas a amenazas que pueden causar pérdidas y vulnerabilidades a sus activos. Según datos del Foro Económico Mundial, el 65% de las organizaciones en Australia fueron víctimas de ataques que dejaron pérdidas superiores a un millón de dólares [3]. En Latinoamérica, la mayoría de las fugas de información se centran en el sector organizacional, lo que conduce a pérdidas en productividad, competitividad y perjuicios financieros que comprometen la continuidad de una empresa [3]. Como respuesta a esta situación, se crearon políticas que mejoran la gestión de la seguridad de la información, siendo la norma ISO 27001, una de las más relevantes.

En el ámbito de la seguridad informática, existen normas relacionadas con la seguridad de la información que nacen con la ISO 27000, estandarizando a nivel internacional las buenas prácticas para garantizar la ciberseguridad. De estas, la ISO 27001 se centra en la gestión continua de riesgos, presentando en detalle los procesos para la implementación, establecimiento, monitoreo, mantenimiento, mejora y operación de un sistema [4].

El objetivo de la norma, consiste en garantizar una mejor protección con respecto a la integridad, disponibilidad y confidencialidad de la información dentro de una empresa, partiendo del análisis de riesgos y una evaluación que permite identificar y evitar obstáculos, mediante un proceso de mitigación y tratamiento [5].

La norma ISO 27001 determina las herramientas necesarias para llevar a cabo una adecuada implementación de un sistema de seguridad de los datos y la información [6]. La primera versión fue publicada en 2005 y otra en 2007, que establecía reglas para gestionar y generar informes confiables en las transacciones y relaciones empresariales.

Por otra parte, es una norma internacional que gestiona la seguridad de todo tipo de organizaciones, incluyendo las gubernamentales y entidades sin ánimo de lucro. Así mismo, permite establecer, implementar, supervisar y mejorar los sistemas de seguridad de la información, haciendo referencia a términos como "seguridad de la información", definida como la protección de la información ante una amplia gama de amenazas [7].

Cabe destacar que la norma especifica los elementos que se establecen, implementan, mantienen y mejoran dentro de un sistema de información empresarial. Es la única que tiene una certificación que genera confianza en materia de comercio electrónico [6].

En Colombia, la ISO 27001 se desprende del concepto de seguridad humana y la prevención de riesgos o amenazas en diferentes áreas. Con la tecnología y la incorporación de herramientas en línea e inteligencia artificial, es una norma que implica cambios para reestructurar la seguridad, llevándola a la protección de datos e información. En sentido general, mitiga aquellas amenazas que atentan contra la integridad del activo primordial de la empresa: los datos [8].

a) Características generales

La norma ISO 27001, contempla 14 dominios basados en la seguridad [9]:

1. Políticas.
2. Organización.
3. Seguridad de los recursos humanos.
4. Gestión de los activos.
5. Control de acceso.
6. Criptografía, cifrado y gestión de claves.
7. Seguridad física y ambiental.
8. Seguridad operacional.
9. Seguridad de las comunicaciones.
10. Adquisición, desarrollo y mantenimiento del sistema.

11. Gestión de incidentes de seguridad de la información.
12. Cumplimiento.
13. Gestión de incidentes
14. Aspectos de seguridad

Se infiere como una norma que fortalece los requisitos generales de una empresa en términos de seguridad de los activos de la organización, pues permite la adopción de normas y controles que disminuyan los riesgos, amenazas y vulnerabilidades [9]. No obliga a adaptar todos los dominios, solo los más adecuados para la empresa. Su implementación radica en el establecimiento de políticas de control que permitan establecer accesos a servicios o recursos específicos a los usuarios, esto en aras de minimizar los ataques informáticos [10].

Algunos beneficios de la aplicación de la norma según [10], son:

- Reducción de los riesgos en seguridad.
- Certificación estándar internacional.
- Confianza y garantías de calidad para clientes y otros actores estratégicos.
- Garantías de cumplimiento de la normatividad vigente acerca de información y propiedad intelectual.
- Enfoque estructurado y coherente.
- Evaluación integral del riesgo.
- Focalización de la inversión donde produce mayor ventaja en cuestión de seguridad.
- Revisión continua y control de los riesgos. Integración con otras normas de gestión ISO.
- Reglas y pautas claras para los colaboradores de la organización.
- Ventajas de marketing.

Es por esto que la ISO 27001, permite la adecuada gestión de la seguridad en las herramientas de tecnología informática. Facilita el establecimiento de manuales que promuevan la adaptabilidad de la información logrando flexibilidad y dinámica en la organización. Establece procesos definidos que garantizan cambios efectivos [11]. Igualmente, es un estándar universal que asegura la credibilidad e integridad de la información posibilitando a las organizaciones la valoración del peligro y la adaptación de controles para suprimirlo aumentando las capacidades de una empresa en la administración de datos, equipos y aplicaciones [12].

Adicional a lo anterior [13], la norma clasifica los elementos de la gestión de la seguridad, en: aplicación de los controles, identificación de los activos, de los impactos, de los riesgos, así como vulnerabilidades y amenazas.

b) Implementación en una empresa

La activación de un sistema de seguridad basado en la ISO 27001, requiere primero adecuar un manual de seguridad que sirva como guía al sistema de gestión, incorporando el alcance, los responsables, los objetivos, las políticas, directrices y otras actividades que se consideren importantes.

En segundo lugar, se debe generar una guía de procedimientos que englobe todas las actividades operativas y relacione los encargados de cada una de ellas, asegurando procesos adecuados de planificación, operación y control. En tercer lugar, debe generar instrucciones por medio de un documento que describa el paso a paso de cómo se deben realizar las actividades y tareas que se deben cumplir. Por último, es fundamental establecer un plan de registros que garantice la correcta documentación de la información. Toda la implementación del sistema se basa en el ciclo continuo PHVA (Planificar, Hacer, Verificar, Actuar) [14].

Es así como en el planificar, se implementan las políticas de seguridad, se define la metodología que se va a llevar a cabo y se seleccionan los controles. En el hacer, se implementa el sistema de gestión y el plan de tratamiento de riesgos, además de la implementación de los controles. En el verificar, se monitorean las actividades y se hacen las

revisiones. En el actuar, se revisan los resultados, se toman las acciones correctivas y las de mejora [15].

Por consiguiente, la norma presenta para la puesta en marcha de las políticas de seguridad, unas actividades básicas que aseguran los procesos y sistemas de gestión, los cuales se enumeran a continuación [16]:

- Mantenimiento y administración de redes.
- Soporte técnico a los usuarios.
- Supervisión del proyecto informático .
- Generación de propuestas para el acceso y uso de la tecnología .
- Trabajar por la seguridad e integridad de la información.
- Desarrollar, adaptar e investigar nuevas herramientas para el mejoramiento de la gestión a nivel interno y externo.

C) Importancia en la seguridad de la información

La norma ISO 27001, establece un modelo para administrar e implementar un sistema destinado a la seguridad de la información, con base en los procesos, el análisis de los riesgos y la formulación de controles que ayudan a la protección de los datos y la mitigación de los riesgos. Algunos de los factores que engloba en relación con la seguridad son: la violación a los datos personales, los crímenes cibernéticos, los ataques y el vandalismo [17].

Por consiguiente [16], la norma promueve las buenas prácticas en el uso de las tecnologías y la informática, con el fin de minimizar los riesgos sobre la información organizacional y los activos informáticos. En este sentido, la política alude a los niveles de madurez de los sistemas que mejoran con la optimización de la operación de los servicios informáticos. En este caso, el nivel lo determina la medición de riesgos y la elaboración de las políticas de seguridad para garantizar la integridad, confiabilidad, disponibilidad e integración de los recursos informáticos y la información.

B. Industria farmacéutica en Colombia

a) Características generales

La industria farmacéutica en Colombia, es un sector estratégico que se conjuga con otros sectores como el de la salud, la tecnología, la innovación y la ciencia. Es estratégico en el sentido de que, contribuye al bienestar social de la población minimizando los problemas de salud y fomentando el crecimiento económico [18].

En Colombia, este sector ocupó el tercer lugar en la industria manufacturera, con una participación del 0,3% y un crecimiento del 8,4% en el año 2019 [19]. A nivel nacional, la producción llegó a $7.975 millones de pesos en el 2016, con una tendencia creciente [19]. Según datos de la ANDI [20], en el año 2022 tuvo un crecimiento en producción local de medicamentos del 21,1%, generando 49.768 empleos, abarcando un crecimiento promedio para los últimos seis años del 3,8%. Estos datos indican que es una industria en auge, lo cual requiere estar a la vanguardia de los requerimientos del mercado y las nuevas tecnologías, conllevando la responsabilidad de hacer una adecuada gestión de la información, con el objetivo de salvaguardar los datos que administra.

A nivel de tecnología, es una industria cuya innovación requiere altas inversiones en ciencia, tecnología, investigación y desarrollo, aspectos adicionales a la estricta regulación que debe cumplir [18]. En relación con la economía, este sector corresponde a los niveles secundario y terciario, lo que motiva llevar a cabo una inversión más alta que le permita incursionar en el sector primario [18].

De esta manera, el sector farmacéutico elabora, fabrica, distribuye y comercializa medicamentos para la prevención de enfermedades, lo que indica que requiere constantes avances en materia de desarrollo y crecimiento, algo que la relaciona con la industria 4.0 en los procesos de mejoras tecnológicas,

por su constante innovación y avances en maquinarias y equipos de comunicación *[21]. Es tan estrecha la relación entre la industria farmacéutica con la 4.0, que el informe de "Industry 4.0: Building the digital Enterprise" ha denominado al sector como Pharma 4.0, especificando los niveles de implementación que se muestran en la Fig. 1:*

Figura 1. Configuración de emisor común

Niveles de implementación - Industria 4.0	
Nivel físico, o de tecnologías hardware inteligentes	Como puede ser el aplicar robótica avanzada, la internet de las cosas, las impresoras 3D, etc.
Nivel de automatización de procesos físicos	Donde aplicar la sistematización, monitorización, trazabilidad, simulaciones, realidad aumentada, etc.
Nivel de automatización de procesos lógicos	Puede ser la implantación de soluciones BPM y de colaboración, sistemas MES o BI, CRM y sistemas de marketing Automation, sistemas MRP y SCM, ERP, etc.
Nivel de inteligencia distribuida	Donde utilizar la información de todo lo que pasa dentro y fuera de las fábricas, crear modelos predictivos y aplicar machine learning, integrar sistemas en el cloud y ofrecerlos en movilidad, securización de todos los hilos, etc.

Fuente: [21]

Por consiguiente, la industria farmacéutica es un sector que a nivel de país debe mantener una estructura robusta para cumplir con las tareas que desarrolla; de aquí la importancia de adaptarse a los cambios tecnológicos y adecuarse a la normatividad que implica salvaguardar la información que posee y genera con los mismos, para optimizar los procesos [22].

b) Necesidades tecnológicas

La industria farmacéutica colombiana afronta retos macroeconómicos tras la pandemia. Estos desafíos han frenado el crecimiento del sector, con el cierre de numerosas empresas durante el confinamiento. Solo algunas, como las del sector salud, experimentaron un aumento en la demanda para satisfacer el requerimiento de productos vitales como los tapabocas [23].

El mencionado sector y en especial, la industria farmacéutica, ha tenido que implementar dentro de sus procesos sistemas de calidad, ambientales y de personal que optimicen el control de los productos y procesos. Hoy en día, con la revolución digital y la automatización, han sido pioneros en la incorporación de sistemas de seguridad de la información, a través de planes estratégicos y de procesos que cumplan con los estándares de seguridad que necesitan [24].

Con todo lo anterior, la industria farmacéutica fue una de las que aumentó su demanda, siendo este un factor de éxito para las organizaciones de este tipo, lo que las llevó a rediseñar toda la producción en aras de contar con inventarios de seguridad que atenuaran cada una de las fluctuaciones de la demanda. En este punto, la tecnología se convirtió en un elemento crucial de competitividad.

Siendo las cosas así, la transformación digital en el sector ha alcanzado altos niveles integrando sistemas y la computación en la nube haciendo que la seguridad cibernética sea una necesidad inminente de integrar. El hecho de producir en masa y de manera personalizada, significa un desafío y la generación de estrategias que le hagan frente. Es por ello que las empresas farmacéuticas han tenido que adquirir nuevas tecnologías y competencias para garantizar las tareas y la confidencialidad de la información y los procesos [25].

Según predicciones del IQVIA Institute, la industria farmacéutica para el año 2023, debería pasar un crecimiento por encima de los 1.5 trillones de dólares debido al aumento en la demanda de medicinas y fármacos, lo que requiere que se implemente en su producción, la robótica y los equipos automatizados [26]. Por esta razón, la industria farmacéutica debe necesariamente incorporar nuevas tecnologías para mantenerse a la vanguardia del mercado y así poder responder a las necesidades inminentes.

Recientemente, algunas de las tendencias tecnológicas que cita [26] en la industria farmacéutica, son:

- *Inteligencia artificial:* En la industria farmacéutica, contribuye con el desarrollo de fármacos y medicamentos, búsqueda de

pacientes y ensayos clínicos.
- *Procesos digitales:* Vuelve más eficientes las operaciones, permite el seguimiento y análisis de datos.
- *Tecnología en la nube:* Permite la asociación con otras empresas, brindando acceso centralizado.
- *Capacitación digital:* Garantiza la programación, implementación de software, reduce la posibilidad de errores y el cumplimiento de estándares.
- *Mayor enfoque en la investigación:* Reduce el costo en materias primas por medio de la identificación de problemas, antes de que se presenten.
- *Big Data:* En las compañías farmacéuticas, se manejan grandes volúmenes de datos para análisis predictivos y prescriptivos, descubrimientos y desarrollo de nuevos productos.
- *Tecnología Blockchain:* Agiliza los procesos de producción y distribución, brindando mejores resultados en la investigación y desarrollo.

De este modo, la industria farmacéutica se compone de procesos tecnológicos que son paralelos a la trazabilidad y calidad en la producción de medicamentos. La automatización en las actividades, ha permitido garantizar la calidad de los resultados.

Por otro lado, se puede mencionar dentro de las necesidades tecnológicas, la relación entre la automatización y el Blockchain para la descentralización de operaciones, sin necesidad de intermediarios ni la intervención humana. Es una red que facilita la realización de transacciones, firmas de contratos y movimientos de productos de manera automática, mediante procesos de inteligencia artificial [27].

La tecnología Blockchain mejora notablemente el sector productivo al posibilitar un seguimiento detallado de todas las etapas del proceso, desde la producción hasta la entrega al cliente final. Proporciona información veraz e instantánea, lo que agiliza significativamente los procesos de planificación.

C. Implementación tecnológica en la industria farmacéutica

a) Gestión de la seguridad

Estamos en una sociedad basada en el conocimiento, la tecnología, la ciencia y la innovación, como elementos para el desarrollo sostenible y la competitividad de una organización. En el caso del sector salud y de la industria farmacéutica, se puede decir que están a la vanguardia en estos temas, materializando el conocimiento por medio de la tecnología, que a su vez les permite mejorar el desempeño y generar valor dentro del mercado [28].

En función de lo planteado, la disrupción tecnológica ha facilitado una interacción global mejorando la vida de las personas y los procesos organizacionales; sin embargo, no todas las empresas comprenden e implementan una adecuada gestión de seguridad; esta, se asocia a tener un buen paquete de antivirus y contraseñas seguras. Se desconoce la normativa y las estrategias que garantizan la protección y privacidad de los datos, generando vulnerabilidades e inconsistencias [29]. Por consiguiente, esas vulnerabilidades y amenazas son explotadas por personas sin escrúpulos que ingresan a los sistemas con ciberataques para ocasionar daños, pérdidas y una mala reputación a la empresa, algo que afecta toda su actividad.

En ese sentido, los ciberataques y las vulnerabilidades cada día son más comunes, en especial, sobre grandes empresas del área de la salud porque tienen mayor exposición en los entornos digitales y un nivel de riesgo más alto, debido a la cantidad de usuarios. Es por ello, que este tipo de empresas ha invertido altos presupuestos en proteger la seguridad de distintos ataques. Datos mencionan que para el 2019, Colombia fue el segundo país con mayor nivel de exposición y riesgos en relación con la seguridad digital [30]. Pruebas de lo anterior, son los ataques cibernéticos que se presentan a EPS solo con el fin de causar pérdida de dinero y de

datos.

Al respecto, según información de IBM y la división Threat Intelligence de Check Point Software, en la industria sanitaria durante el año 2022, los ataques de este tipo aumentaron en un 60% con un costo promedio de 10 millones [31]. Estos ataques al igual que la tecnología, van de forma creciente y en tendencia, pues los delincuentes saben que el impacto sobre ellos afecta la confidencialidad y confianza en las organizaciones.

En los procesos de automatización, esta industria utiliza cuatro tecnologías, que [32] asegura garantizan la calidad en la seguridad de la información y de los procesos:

- *Tecnología de software* basada en la automatización de procesos industriales: Se programan controladores lógicos e interfaces de operación que cumplen con la legislación vigente.
- *Tecnología para el diseño de sistemas:* para la diagramación de catálogos y diseño de nuevos productos
- *Software para la administración de reportes:* Para garantizar la trazabilidad de los procesos
- *Tecnología para el sistema documental:*
- Trata la automatización y desarrollo bajo el cumplimiento de normas técnicas.

Debe señalarse que dentro de este proceso, la industria 5.0 ha brindado las herramientas para que la tecnología trabaje en función del hombre, aumentando la eficacia e integrando mejoras en la logística y en la creación de productos personalizados, basándose en redes más rápidas que impulsan las aplicaciones, integran los sistemas y garantizan la obtención de datos de calidad [33].

Es importante mencionar que, en el campo de la seguridad, también se debe hacer alusión al tema de capacitación del personal que emplea el sistema con el fin de medir su efectividad e impacto en la prevención de la pérdida de datos. Las organizaciones en el desarrollo de sus planes de gestión, deben contemplar los planes de gestión, deben contemplar los planes de actualización para sus trabajadores, con el propósito de mitigar las vulneraciones o infracciones a la seguridad [34]. De esta forma, la correcta gestión dentro de la organización, garantiza la protección de los sistemas y las bases de datos; quizás no se erradiquen todos los riesgos, pero sí se contribuye a su prevención.

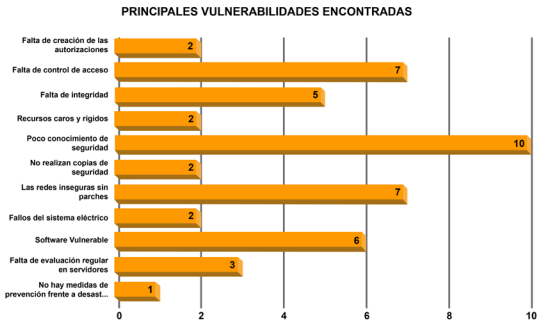
Se plantea entonces, que en la gestión de la seguridad de la información, se debe tener en cuenta que los datos de una pequeña organización no son los mismos que los de una grande y que por tanto, el nivel de control de riesgos y de los activos informáticos, es distinto. En cada una se aplica un enfoque de análisis y trámite diferente que identifica y elimina cada riesgo asociado. La norma ISO 27001, permite en cada organización - dependiendo de sus características -hacer un análisis puntual y una contemplación de los riesgos de su entorno [35].

b) Amenazas y vulnerabilidades

Con respecto a los problemas actuales sobre protección de la información y de los activos de ésta en una empresa, [36] manifiesta que la seguridad tiene que ser una actividad de "constancia y ejecución" que deben ser realizadas por la organización de manera periódica; para ello, se sugiere implementar un sistema de seguridad que se adapte a la organización, lo cual sería lo ideal.

En otras palabras, en relación con las vulnerabilidades en los sistemas, según [37], estas surgen de inconsistencias en los sistemas que facilitan a los cibercriminales afectar negativamente los activos de información. Por su parte, [38], relaciona que la diferencia entre vulnerabilidad y amenaza, es que la primera es el factor que deriva la segunda y que trae como consecuencia una afectación a la información y a los activos de cualquier empresa. Al respecto, en la figura 1, se muestran las vulnerabilidades internas más comunes que se pueden presentar en una organización:

Figura 1. Vulnerabilidades en una empresa



Fuente: [5]

La figura permite inferir que la principal vulnerabilidad se relaciona con el desconocimiento de lo que es la seguridad. Es decir, en situaciones de amenazas a la información, el mayor riesgo son las personas de la misma empresa. Con respecto a lo anteriormente expuesto, [30] reconoce que los conocimientos en seguridad dentro de una organización son insatisfactorios, lo que dilata el problema convirtiéndolo en un aspecto para ser aprovechado por los cibercriminales.

Así como existen vulnerabilidades internas, también existen unas externas que amenazan los activos de la información, mismas que se encuentran documentadas en la ISO 27001 haciendo alusión a la importancia de precisar el impacto de cada una, con el fin de evitar los ataques. En la figura 2, se relacionan las principales amenazas a las que se puede enfrentar una empresa:

Figura 2. Amenazas en una empresa

Fuente: [39]

Se puede observar en la mencionada figura que, la principal amenaza tiene que ver con el malware, los hackers, el acceso no autorizado, la filtración de privacidad, los ataques de fuerza bruta y la suplantación. Todos los anteriores, con la única intención de causar daño.

Resulta claro que los estándares de seguridad de la ISO 27001 para el contexto empresarial, se entienden como riesgos o vulnerabilidades, contratiempos, eventos o consecuencias negativas que causen daño o generen alguna eventualidad con la información o los datos. Al estar la información disponible en internet o en otros dispositivos IoT, se pueden presentar casos de ingreso de códigos maliciosos que vulneran la seguridad de la información [40].

La norma clasifica las amenazas en tres grupos, relacionados en la tabla 2:

TABLA II
CLASIFICACIÓN DE LAS AMENAZAS SEGÚN LA NORMA ISO 27001

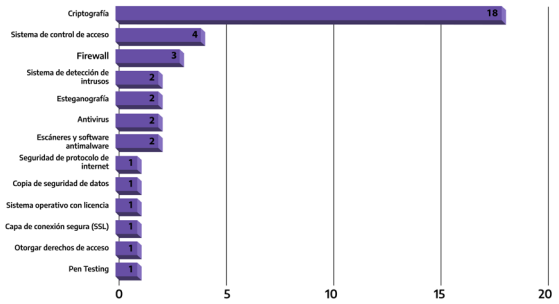
Grupo	Descripción
Destrucción	Destruye toda o una parte de la información inutilizándola
Modificación	Diversifica los contenidos, cambia, agrega o roba partes de la misma, para perjudicar las comunicaciones.
Robo	Se recepta la información de forma indebida; se interrumpe el servicio.

Fuente: [13]

Así mismo, clasifica las vulnerabilidades en: físicas, deficiencia en el diseño de los sistemas, virus y softwares maliciosos, debilidades en los protocolos o en los códigos que ejecuta el sistema y vulnerabilidades humanas [13]. Con lo anterior, se puede evidenciar que las amenazas y vulnerabilidades dependen de la intención y que en muchas ocasiones, la falta de protocolos hace que sean más latentes.

Con todo lo anterior, se requiere que las entidades conozcan cuales son las vulnerabilidades y amenazas a las que se exponen, en aras de implementar estrategias que garanticen los niveles mínimos de seguridad. Al respecto, [41] hace alusión a que si se analizan las vulnerabilidades y amenazas, se pueden encontrar más fácilmente soluciones que permitan gestionarlas. Algunas de esas soluciones se relacionan en la Figura 3.

Figura 3. Soluciones para gestionar la seguridad de la información



Fuente: [39]

La criptografía es la principal solución para la seguridad de la información, seguida del firewall, los sistemas de detección de intrusos y los antivirus. En cuestión de criptografía, cabe mencionar que puede ser de dos clases: simétrica o asimétrica, siendo esta última la más recomendable en el ámbito empresarial, por su nivel de seguridad en la codificación y decodificación [42].

De allí que las compañías farmacéuticas con ayuda de la norma, pueden definir la documentación para una eficiente gestión de riesgos, haciendo uso de metodologías que orienten la política de seguridad en la información, aclarando los procesos para los datos en la nube y los servicios IoT (proveedor – usuario) [40].

La norma ISO 27001, responde al constante aumento de las amenazas que ponen en riesgo la información de las organizaciones, implementando herramientas que salvaguardan los datos y garantizan la confidencialidad. No obstante, mitigar los riesgos en un 100% es muy difícil, pues los sistemas de información están en constante exposición, lo que implica que las empresas se enfoquen en la creación de pautas adicionales para asegurar sus sistemas dentro de las distintas tecnologías utilizadas [43].

De este modo, las empresas deben ver la seguridad como un universo que requiere integrar seguridad informática, ciberseguridad y seguridad de la información, para obtener sistemas de protección robustos que garanticen la disminución de brechas que puedan llevar a fugas de información [44].

c) Innovación

Las aplicaciones tecnológicas en esta industria, son importantes desde hace varias épocas porque han permitido al sector salud contar con mecanismos novedosos y eficaces para la investigación y el tratamiento de las enfermedades. La implementación tecnológica lleva más de dos décadas; ha sido orientada al sector de la salud y a la generación de conocimientos científicos [45].

Es en este sentido, que conviene acotar la importancia de la innovación en un país, la cual se puede reconocer por la cantidad de patentes que se solicitan y se otorgan. Es una actividad que muestra la dinámica en donde el conocimiento es generado y apropiado por la industria. En cuestión de patentes, el sector farmacéutico colombiano presentó durante el periodo del 2000 al 2018, el 69,21% de todas las solicitudes, lo cual significa que, en materia de innovación, la nación se encuentra en un alto nivel indicando consecuentemente, el valioso grado de implementación tecnológica [46].

En función de lo planteado, en la actualidad, las empresas del sector están dedicando inversiones a recursos tecnológicos que les permitan mejorar su competitividad

en el mantenimiento y soporte de equipos tecnológicos. Además, están enfocando recursos humanos altamente capacitados en Tecnologías de la Información [47].

Por supuesto, el reto más importante de esta industria radica en la gestión logística en cuanto a la trazabilidad y seguimiento de la información. Para ello, se han aplicado los aspectos de la industria 4.0 con el fin de optimizar los recursos de la cadena de abastecimiento y hacer seguimiento detallado a los productos, garantizando que la información sea verídica [48].

Al igual que todos los sectores, es una industria que trabaja mejorando los procesos de innovación e investigación para asegurar una alta competencia, fundamentándose principalmente en la industria 4.0 como factor esencial en la búsqueda de crecimiento y la incorporación de nuevas tecnologías que apoyen la modificación y minimización de procesos repetitivos, en aras de incrementar la producción [21].

Otro factor clave del sector, ha sido la inteligencia artificial, que ha llegado a resolver tareas de manera automatizada; tareas que van desde la distribución de medicamentos, la interacción de chatbots con clientes y pacientes, el control médico y los apoyos en la creación de fórmulas farmacéuticas [49]. Las aplicaciones más comunes de la inteligencia artificial en la farmacia, son el manejo de inventarios, la asistencia al farmacéutico, el apoyo en ventas y el diseño de medicamentos [50].

Cabe resaltar que el uso de chatbots en esta industria, ha sido un método eficaz a la hora de interactuar con clientes porque ofrecen con rapidez un proceso de búsqueda de tratamientos farmacéuticos, asegurando la disponibilidad en el servicio. La aplicación asegura que interrogantes comunes sobre medicamentos, la composición, indicaciones, número y frecuencia de las dosis y efectos secundarios, esté disponible en cualquier momento y lugar [51].

Otro factor que cabe resaltar, se encuentra en el manejo de inventarios con Inteligencia Artificial (IA). Según [52], permite administrar la demanda, garantizando las existencias de un medicamento; su abastecimiento o suministro, programando las cantidades que se requieren para el inventario, el control de costos de adquisición, su mantenimiento y escasez.

Pese a lo anterior, la fusión de la IA con la industria farmacéutica en Colombia, aún no se ha aprovechado. Latinoamérica es uno de los lugares con menos desarrollos tecnológicos, en donde el país tiene una inserción casi nula en la materia, con respecto a otras naciones que tienen adelantos importantes. Hoy en día es un reto incursionar en la IA para que la industria pueda tener un mayor impacto, más aún después de la época del Covid-19 [49].

IV. CONCLUSIONES

El crecimiento exponencial de la tecnología, ha derivado en un aumento de los robos y ataques a la información, especialmente en el ámbito empresarial. Por tanto, resulta fundamental estar al tanto de las amenazas y vulnerabilidades a las que se enfrentan los activos informáticos, así como la identificación de las herramientas necesarias para mitigar estos riesgos. En este sentido, la norma ISO 27001, juega un papel crucial al ofrecer pautas para una gestión más efectiva, reduciendo las amenazas que puedan comprometer la seguridad de la información.

Así mismo, la Norma ISO 27001, proporciona directrices para comprender la organización y su entorno, identificando sus necesidades y expectativas. Define el alcance del sistema de gestión de seguridad de la información, apoyándose en los recursos, la documentación y la comunicación. Además, detalla cómo planificar, implementar y controlar cada proceso, al igual que la realización de una evaluación de riesgos y su correspondiente tratamiento.

Además, es trascendental que la alta dirección de la organización se comprometa y capacite al personal, en políticas de seguridad. Asimismo, se deben realizar revisiones periódicas para asegurar que el sistema de información y las medidas de protección implementadas, funcionen conforme a lo planificado.

La industria farmacéutica es una de las más competitivas a nivel mundial en términos tecnológicos, especialmente después de la pandemia, dado su impacto en la economía. Aunque este sector se sitúa a la vanguardia en seguridad de la información, esto también lo hace más vulnerable a ataques y amenazas, lo que requiere una actualización y capacitación continua.

La industria farmacéutica cuenta con procesos tecnológicos avanzados que incluyen la automatización de procesos, diseño y diagramación, software para la administración de reportes y sistemas documentales robustos, contribuyendo así a la trazabilidad de los procesos y garantizando la calidad y la investigación, como pilares fundamentales de su actividad.

Por último, la implementación de nuevas tecnologías en el sector farmacéutico se ha tornado prioritaria para mantener la eficiencia, calidad y reputación de las organizaciones. A través de la adopción de normas como la ISO 27001, estas industrias aseguran un mejoramiento continuo y la mitigación de riesgos y amenazas a su activo más valioso: la información.

V. REFERENCIAS

[1] I. J. Zárate Santos, «Herramienta de armonización entre las normas 27001 y NIST800-53 como pilares para la medición del nivel de madurez del SGSI,» [En línea]. Available: https://repository.ucatolica.edu.co/entities/publication/0fb9f560-e14b-4091-a1aa-e73835aad465.

[2] R. Hernandez Sampieri y C. P. Mendoza Torres, «Metodologia de la investigación. Las rutas cuantitativa, cualitativa y mixta,» 2018. [En línea]. Available: https://books.google.es/books?hl=es&lr=&id=5A2QDwAAQBAJ&oi=fnd&pg=PP1&dq=investigacion+cualitativa+hernandez+sampieri+&ots=Tj_m-X1oN6&sig=zWqVDIcq1l_rtzc9rUeeOYN7qn4#v=onepage&q&f=false.

[3] S. Bustamante García, M. Á. Valles Coral, I. E. Cuellar Rodríguez y D. Lévano Rodríguez, «Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú Enfoque UTE, vol. 12, núm. 2, 2021, -Junio, pp. 69-79 Universidad Tecnológica Equinoccial,» 2021. [En línea]. Available: https://www.redalyc.org/journal/5722/572266265005/572266265005.pdf.

[4] A. A. Dávila Angeles y B. J. Dextre Alarcón, «"Propuesta de una Implementación de un programa de Gestión de Vulnerabilidades de Seguridad Informática para mitigar los siniestros de la información en el policlínico de salud AMC alineado a la NTP-ISO/IEC 27001:2014 en la ciudad de Lima - 2021,» 2021. [En línea]. Available: https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/4906/A.Davila_B.Dextre_Tesis_Titulo_Profesional_2021.pdf?sequence=1&isAllowed=y.

[5] E. M. Guevara Vega, J. R. Delgado Meza y A. Mendoza de los Santos, «Vulnerabilidades y amenazas en los activos de información: una revisión sistemática,» 2023. [En línea]. Available: http://portal.amelica.org/ameli/journal/535/5354040004/html/.

[6] G. R. Cruz Rodríguez, R. A. Méndez Fernández y A. C. Mendoza De Los Santos, «Seguridad de la información en el comercio electrónico basado en ISO 27001 : Una revisión sistemática,» 2023. [En línea]. Available: https://revistas.ulasalle.edu.pe/innosoft/article/view/79.

[7] E. A. Muñoz Villero y . L. M. Palmera Quintero, «Planeación del sistema de gestión de seguridad de la informacion para la empresa fq tecnologías s.a.s, basado en la norma ISO 27001:2013,» 2019. [En línea]. Available: https://repositorioinstitucional.ufpso.edu.co/bitstream/handle/20.500.14167/1382/Cuerpo%20del%20trabajo%20-%20PLANEACI%c3%93N%20DEL%20SISTEMA%20DE%20GESTI%c3%93N%20DE%20SEGURIDAD%20DE%20LA%20INFORMACION%.

[8] E. Rumbo Camelo y V. Díaz Plaza, «Análisis y Mitigación de Riesgos que afectan la Seguridad Física: una revisión,» Rices, vol. 1 núm. 1, Enero–Junio 2023, pp. 1–11 (ISSN 2981-5010), 2023. [En línea]. Available: https://revistas.universu.com.co/index.php/rices/article/view/5/4..

[9] R. G. Ramos Mamami, R. Cahuaya Ancco y R. R. Llanqui Argollo, «Política informática y la gestión de la seguridad de la información en basea la norma ISO 27001,» Revista Innovación y SoftwareVol. 4, No. 1, Mes Marzo-Agosto, 2023ISSN: 2708-0935Pág. 96-106, 2023. [En línea]. Available: https://revistas.ulasalle.edu.pe/innosoft/article/view/57/101.

[10] E. E. Ríos Miranda, «SGSI BAJO EL MARCO NORMATIVO ISO 27001 EN EL PROCESO DE CONTROL DE ACCESOS PARA UNA EMPRESA: una revisión científica de los últimos 9 años,» 2020. [En línea]. Available: https://repositorio.upn.edu.pe/bitstream/handle/11537/26449/Trabajo%20de%20Investigaci%c3%b3n_Total.pdf?sequence=2&isAllowed=y.

[11] F. C. Trujillo Bailon, «ISO 27001 en la Gestión de Seguridad de la Información en el área TI en una institución pública, Lima 2023,» 2023. [En línea]. Available: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/120927/Trujillo_BFC-SD.pdf?sequence=1&isAllowed=y.

[12] Y. G. Lizárraga Caipo, J. A. Panaqué Domínguez y A. C. Mendoza de los Santos, «Impacto de la auditoría informática en las organizaciones: una revisión bibliográfica,» 2022. [En línea]. Available: https://revistas.upt.edu.pe/ojs/index.php/ingenieria/article/view/638/631.

[13] G. N. Garofalo Serrano, « Análisis de un SGSI con Normas ISO/IEC 27001 para complementar las normas de control interno de CGE, relacionadas con Tecnologías de la Información para el Gobierno Autónomo Descentralizado del Cantón Guaranda (Bachelor's thesis, Babahoyo: UTB-FAFI.,» 2022. [En línea]. Available: http://dspace.utb.edu.ec/handle/49000/11601.

[14] C. A. Gomez Rabelo, «Diseñar un Sistema de Gestión de la Seguridad de la Información para la Empresa Qwerty SA a partir de la Norma ISO 27001,» 2020. [En línea]. Available: https://repository.unad.edu.co/handle/10596/34624.

[15] J. H. Córdoba, «Propuesta de implementación de un Sistema Gestor de Seguridad de la Información, basados en INTE/ISO/IEC 27001: 2014 en el departamento de TI para Almacenes El Rey, en el año 2021. Tecnología Vital, 1(9).,» 2021. [En línea]. Available: https://revistas.ulatina.ac.cr/index.php/tecnologiavital/article/view/464.

[16] A. C. Llano Casa, M. L. Gaibor Gavilanez, C. C. Cruz Caiza y J. A. Cadena Moreano, «Importancia de políticas de seguridad Informática de acuerdo a las ISO 27001 para pequeñas y medianas empresas del Ecuador. Ciencias de la Ingeniería y Aplicadas, 5(2), 82-98.,» 2021. [En línea]. Available: http://investigacion.utc.edu.ec/revistasutc/index.php/ciya/article/view/374.

[17] E. A. Ramírez Camargo y M. A. Rincón Pinzón , «La importancia de la seguridad de la información en el sector público en Colombia,» 2022. [En línea]. Available: https://scielo.pt/pdf/rist/n46/1646-9895-rist-46-97.pdf.

[18] A. Mendoza Ruiz, M. A. Oliveira y J. Paranhos, «La industria farmacéutica en Colombia en la literatura académica interdisciplinaria: revisión de alcance, 1990-2018*,» Innovar, vol. 32, núm. 83, 2022, Enero-Marzo, pp. 153-174 Facultad de Ciencias Económicas. Universidad Nacional de Colombia, 2022. [En línea]. Available: https://www.redalyc.org/journal/818/81870307012/81870307012.pdf.

[19] A. M. Mosquera Martínez , «Impacto de Alianza del Pacífico en el sector exportador farmacéutico Colombiano,» 2022. [En línea]. Available: https://repository.ucc.edu.co/server/api/core/bitstreams/c4a87b09-2d80-4a8b-b3e7-32e6800a3d50/content.

[20] ANDI, «Radiografía del mercado farmacéutico colombiano,» 14 junio 2022. [En línea]. Available: https://www.andi.com.co/Home/Noticia/17274-radiografia-del-mercado-farmaceutico-co#:~:text=Desde%202022%20se%20proyecta%20un,mismo%20per%C3%A-Dodo%20de%20a%C3%B1o%20anterior14..

[21] M. J. Mejía Triana y J. I. Bohórquez , «Contraste de (i + d) de la industria 4.0 entre una compañía del sector farmacéutico en Colombia y una en España,» 2019. [En línea]. Available: https://repository.usta.edu.co/bitstream/handle/11634/21240/2020mariameja.pdf?sequence=1&isAllowed=y.

[22] E. López Santana , G. Méndez Giraldo, H. A. Ávila Choconta, C. Franco y F. Rueda Velasco , «Metodologías y aplicaciones de diagnósticos sectoriales: una revisión de la literatura,» ing. vol.28 supl.1 Bogotá Apr. 2023 Epub Mar 25, 2023, [En línea]. Available: http://www.scielo.org.co/scielo.php?pid=S0121-750X2023000400203&script=sci_arttext.

[23] M. A. Parra Chaparro, «Análisis de planeación de la demanda en el sector farmacéutico aplicando dinámica de sistemas,» 2022. [En línea]. Available: https://repository.unimilitar.edu.co/bitstream/handle/10654/44221/ParraChaparroMichaelAlexander2022.pdf?sequence=1&isAllowed=y.

[24] M. J. Epifania Moreno, «"Estandarización de procesos y gestión de abastecimiento en las comercializadoras de productos farmacéuticos en el periodo 2010-2020: revisión sistemática de la literatura científica",» 2020. [En línea]. Available: https://repositorio.upn.edu.pe/bitstream/handle/11537/27051/Epifania%20Moreno%20Maria%20Julia.pdf?sequence=1&isAllowed=y.

[25] M. Reyes y C. Quispe, «Transformación Digital en la Industria 4.0 una Revisión de la Literatura,» 2020.

[26] Nester Group, «Las tendencias tecnológicas de la industria farmacéutica para 2022 y 2023,» 2023. [En línea]. Available: https://www.netsergroup.com/blog/las-tendencias-tecnologicas-de-la-industria-farmaceutica/..

[27] D. N. Florez Delgado, «La Red Blockchain y su rol en la industria y la automatización,» 2022. [En línea]. Available: https://repository.usta.edu.co/handle/11634/42778.

[28] L. P. Cáceres Gómez y L. E. Becerra Ardila, «Transferencia de tecnología para organizaciones del sector salud, barreras y brechas en economías emergentes,» 2022. [En línea]. Available: https://investigacion.fca.unam.mx/docs/memorias/2022/18.02.pdf.

[29] M. Humpiri Flores, E. Figueroa Donayre, M. L. Guillen Guevara, D. J. Cabel Moscoso, R. Humpriri Flores y J. C. Huanca Marín, «Revisión sistemática: vulnerabilidtades de seguridad cibernética en los activos digitales,» 2023. [En línea]. Available: https://www.unaj.edu.pe/revista/index.php/vpin/article/view/250/156.

[30] R. D. Estrada Esponda, J. Unás Gómez y O. E. Flórez Rincón, «Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá,» 2021. [En línea]. Available: https://revistalogos.policia.edu.co:8443/index.php/rlct/article/view/1446/1652.

[31] Cibernoticias, «Los ciberataques: La enfermedad incurable del sector salud,» 3 abril 2023. [En línea]. Available: https://www.informaticaforense.com.co/los-ciberataques-la-enfermedad-incurable-del-sector-salud/.

[32] F. Suárez Concepción, R. Piñero Aguilar, A. Prieto Moreno, A. Alfonso Cordoví, J. C. Carbó Castro y O. Llanes Santiago, «Metodología para la automatización de procesos tecnológicos en la industria farmacéutica cubana,» Ing. Ind. vol.43 no.1 La Habana ene.-abr. 2022 Epub 17-Feb-2022, 2022. [En línea]. Available: http://scielo.sld.cu/scielo.php?pid=S1815-59362022000100082&script=sci_arttext.

[33] C. Deus Aguilera, R. Casares Li y A. E. García Toll, «Maintenance 5.0: Trends and Challenges,» 2022. [En línea]. Available: https://www.researchgate.net/profile/Carlos-Deus-Aguilera/publication/364167100_Maintenance_50_Trends_and_Challenges_Mantenimiento_50_tendencias_y_desafios/links/638e41c911e9f00cda1f483a/Maintenance-50-T.

[34] M. J. Rojas Valiente, J. Castillo Sarmiento y A. C. Mendoza de los Santos, «Seguridad de la información en la prevención de perdida de datos: una revisión sistemática,» Revista Innovación y SoftwareVol. 4,No. 2, Mes Septiembre-Febrero, 2023, 2023. [En línea]. Available: https://revistas.ulasalle.edu.pe/innosoft/article/view/92/144..

[35] A. S. Olmo Parra, E. Álvarez, L. E. Sánchez Crespo y D. Garcia Rosado, «Revisión Sistemática de Análisis de Riesgos Asociativos y Jerárquicos. Periodo 2014 – 2019,» 2020. [En línea]. Available: https://www.researchgate.net/profile/Antonio-Parra-4/publication/340472247_Revision_Sistematica_de_Analisis_de_Riesgos_Asociativos_y_Jerarquicos_Periodo_2014_-_2019/links/6418382266f8522c38bd5af7/Revisio.

[36] M. A. Velepucha Sánchez y J. P. C. M. F. Morales Carrillo, «Análisis y evaluación de riesgos aplicados a la seguridad de la información bajo la norma ISO. Informática y Sistemas: Revista de Tecnologías de La Informática y Las Comunicaciones, 6(1), 63–78,» 2022. [En línea]. Available: https://doi.org/10.33936/isrtic.v6i1.4473.

[37] G. Sánchez-Bautista y L. Ramírez-Chávez, «Amenazas de seguridad a considerar en el desarrollo de software. XIKUA Boletín Científico de La Escuela Superior de Tlahuelilpan, 10(19), 31–37,» 2022. [En línea]. Available: https://doi.org/10.29057/xikua.v10i19.8118.

[38] E. Guerra, H. Neira, J. L. Díaz y J. Patiño, «esarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. Información Tecnológica, 32(5), 145–156,» 2021. [En línea]. Available: https://doi.org/10.4067/S0718-07642021000500145.

[39] G. Sánchez-Bautista y L. Ramírez-Chávez, «Amenazas de seguridad a considerar en el desarrollo de software. XIKUA Boletín Científico de La Escuela Superior de Tlahuelilpan, 10(19), 31–37,» 2022. [En línea]. Available: https://doi.org/10.29057/xikua.v10i19.8118.

[40] L. A. Gantiva Henao, «Gestión de riesgos en el internet de las cosas (IoT),» 2023. [En línea]. Available: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6868/Risk%20management%20IoT_LAGH%20V5.pdf?sequence=1

[41] F. Kitsios, E. Chatzidimitriou y M. Kamariotou, «eveloping a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. Sustainability, 14(3), 1269,» 2022. [En línea]. Available: https://doi.org/10.3390/su14031269.

[42] F. Solís, D. Pinto y S. Solís, «eguridad de la información en el intercambio de datos entre dispositivos móviles con sistema Android utilizando el método de encriptación RSA. Enfoque UTE, 8(1), 160–171,» 2017. [En línea]. Available: https://doi.org/10.29019/enfoqueute.v8n1.123.

[43] A. P. Jacome Sanchez, «Diseño de una propuesta sobre la aplicación de un SGSI para la empresa de transporte la Ecuatoriana bajo la norma ISO 27001,» 2022. [En línea]. Available: https://repositorio.epnewman.edu.pe/handle/20.500.12892/322.

[44] C. G. Villamar Silva, «nálisis de seguridad de la información basado en la norma ISO 27001 en el Área Técnica de Reparación e Instalación de la Corporación Nacional de Telecomunicaciones" CNT EP" de la ciudad de Babahoyo (Bachelor's thesis, BABAHOYO: UTB, 2021).,» 2021. [En línea]. Available: http://dspace.utb.edu.ec/handle/49000/10549.

[45] L. Vega Izaguirre, F. López Cossio, J. F. Ramírez Pérez y A. Orellana García, «Impacto de las aplicaciones y servicios informáticos desarrollados por la Universidad de las Ciencias Informáticas para el sector de la salud,» RCIM vol.12 no.1 Ciudad de la Habana ene.-jun. 2020 Epub 01-Jun-2020, 2020. [En línea]. Available: http://scielo.sld.cu/scielo.php?pid=S1684-18592020000100058&script=sci_arttext.

[46] J. D. Romero Betancur , «Innovación tecnológica en Colombia: con base en el estado de las patentes otorgadas entre los años 2000 y 2018,» 2020. [En línea]. Available: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-2122_RomeroBetancurJD.pdf.

[47] J. M. Valdospinos Guerra, «Propuesta de un modelo para el proceso de control de calidad en el área de ti para las empresas farmacéuticas en base a las buenas prácticas de cobit 5,» 2020. [En línea]. Available: http://repositorio.uisrael.edu.ec/handle/47000/3085.

[48] M. P. Ramírez Castellanos, «Análisis de las características de los modelos de trazabilidad para los procesos logísticos en la industria farmacéutica en Colombia,» 2022. [En línea]. Available: https://repository.unimilitar.edu.co/bitstream/handle/10654/43668/RamirezCastellanosMariaPaula2022.pdf.pdf?sequence=1&isAllowed=y.

[49] M. D. Ortega Urbano, «The Pharmacy in the New Era of Artificial IntelligencePharmacy and Artificial Intelligence,» 2023. [En línea]. Available: https://journals.eagora.org/revTECHNO/article/view/4804/3108.

[50] V. Kaul , S. Enslin y S. Gross, « History of artificial intelligence in medicine. Gastrointestinal Endoscopy, 92(4), 807-812,» 2020. [En línea]. Available: http://10.1016/j.gie.2020.06.040.

[51] J. G. Live , «Inteligencia Artificial en Salud. Revista Innova, salud digital. 6-7.,» 2020. [En línea]. Available: https://issuu.com/innovasaluddigital/docs/revista_innova_salud_digital_-_n1_a_o_2020.

[52] A. C. Fernández, «Gestión de inventarios. COML0210. IC editorial.,» 2018. [En línea]. Available: https://journals.eagora.org/revTECHNO/article/view/4804/3108.

3. **Artículos Semilleros** de investigación

NMAP: UN ALIADO INDISPENSABLE EN LA EVALUACIÓN DE REDES Y SEGURIDAD INFORMÁTICA

Cristian Iván Corredor Cuestas
Estudiante Ingeniería Electrónica y Telecomunicaciones IX Semestre ESCOM
cristiancorredorcuestas@cedoc.edu.co

Yeison Alfonso Buitrago Rojas
Docente Líder Semillero de Ciberseguridad ESCOM
yeisonbuitragorojas@cedoc.edu.co

Andrés Felipe Rodríguez Sánchez
Estudiante Ingeniería Electrónica y Telecomunicaciones X Semestre ESCOM
andresrodriguezsanchez@cedoc.edu.co

Juan Sebastián Rincón Vega
Estudiante Ingeniería Electrónica y Telecomunicaciones III Semestre ESCOM
juanrinconvega@cedoc.edu.co

Laura Catherine Moreno Romero
Estudiante Ingeniería Electrónica y Telecomunicaciones V Semestre ESCOM
lauramorenoromero@cedoc.edu.co

Juan Felipe Veloza Pabón
Estudiante Ingeniería Electrónica y Telecomunicaciones III Semestre ESCOM
juanvelozapabon@cedoc.edu.co

Daniel Mauricio Acevedo Rodríguez
Estudiante Ingeniería Electrónica y Telecomunicaciones III Semestre ESCOM
danielacevedorodriguez@cedoc.edu.co

Alejandro Javier Carlos Pinto
Estudiante Ingeniería Electrónica y Telecomunicaciones VII Semestre ESCOM
alejandrocarlospinto@cedoc.edu.co

RESUMEN- ***En este trabajo de investigación, se examina la trascendencia de Nmap (Network Mapper) como una herramienta de código abierto indispensable para la evaluación de redes y la seguridad informática. Se destaca su capacidad para identificar hosts y servicios, así como para llevar a cabo exploraciones detalladas de puertos, detección de versiones y scripting personalizado. A través de un ejemplo concreto, se ilustra cómo Nmap puede escanear puertos en una red, ofreciendo información valiosa sobre la topología y la seguridad de la infraestructura. Se exploran las capacidades, ventajas y desafíos asociados con esta herramienta, considerando su papel fundamental en el panorama de la ciberseguridad. Además, se examinan casos de uso, consideraciones éticas y limitaciones, proporcionando una visión integral de esta herramienta y su impacto en la evaluación de redes.***

Palabras clave: *: Evaluación de redes, Host, Nmap, Puertos de Red.*

Abstract-This research paper examines the significance of Nmap (Network Mapper) as an indispensable open source tool for network assessment and computer security. It highlights its ability to identify hosts and services, as well as to perform detailed port scans, version detection and custom scripting. Through a concrete example, it illustrates how Nmap can scan ports on a network, providing valuable information about the topology and security of the infrastructure. The capabilities, advantages and challenges associated with this tool are explored, considering its pivotal role in the cybersecurity landscape. In addition, use cases, ethical considerations and limitations are examined, providing a comprehensive view of this tool and its impact on network assessment.

Keywords- *Hosts, Network Assessment, Nmap, Network Ports*

I. INTRODUCCIÓN

La seguridad informática a nivel mundial, enfrenta desafíos constantes que evolucionan con el progreso tecnológico. La proliferación de ciberataques a gran escala, como el ransomware

y los ataques DDoS (Distributed Denial of Service), sigue siendo una preocupación crítica. Estos incidentes afectan a gobiernos, empresas y usuarios individuales, comprometiendo datos y operaciones esenciales. En Colombia, la seguridad informática enfrenta desafíos similares a otros países, incluyendo amenazas como malware, phishing, ransomware y ataques DDoS. La protección de infraestructuras críticas, como sistemas de energía y comunicaciones, es una preocupación importante. A lo largo de los años, Colombia ha experimentado incidentes de seguridad, como ataques a sitios web gubernamentales y casos de ransomware dirigidos a empresas [1].

Colombia figura entre los diez países con mayor número de ataques cibernéticos a nivel mundial, como se evidencia en la Tabla 1, en donde se destaca su posición, misma que ocupa el puesto número 6, en términos de ataques de ransomware:

TABLA I

Volumen de Ransomware EN 2022

País	Volumen
Estados unidos	217486516,00
Reino unido	71350221,00
España	52681013,00
Brasil	21808229,00
Alemania	20166920,00
Colombia	15519964,00
Países bajos	13636729,00
Italia	12471704,00
Noruega	8355138,00

Fuente [2]

La protección de infraestructuras críticas, como los sistemas de control industrial, requiere una evaluación exhaustiva mediante pruebas de penetración (pentesting). Esto implica la identificación de posibles vulnerabilidades y la propuesta de medidas de mitigación para garantizar la resiliencia de estas infraestructuras clave. Además, la concienciación y educación en ciberseguridad desempeñan un papel crucial. Un enfoque de pentesting podría evaluar la eficacia de los programas de concienciación, identificar áreas de mejora y promover prácticas seguras.

En la actualidad, existen numerosas herramientas que ayudan a mitigar la materialización de vulnerabilidades, entre las cuales se destaca "Nmap".

En el ámbito de la seguridad informática y la evaluación de redes, Nmap, también conocido como Network Mapper, se destaca como un instrumento indispensable que ha ganado reconocimiento en la comunidad tecnológica. Desarrollado como software de código abierto, esta herramienta sobresale por su capacidad para explorar y auditar redes de manera exhaustiva. Su versatilidad y amplio conjunto de funcionalidades, lo convierten en un aliado valioso para administradores de sistemas y profesionales de seguridad, que buscan comprender la topología y los servicios presentes en una red.

Además de su cabida para identificar hosts y servicios, brinda la posibilidad de realizar exploraciones detalladas de puertos, detección de versiones y scripting personalizado. Esta capacidad, proporciona información detallada sobre la infraestructura de red, permite a los equipos de seguridad diseñar estrategias efectivas para proteger los activos digitales de una organización [3] [4].

Figura 1. NMAP

Nmap, se destaca por su habilidad para realizar escaneos detallados de puertos, revelando qué servicios están en funcionamiento en un host específico. Esta capacidad no solo proporciona información sobre la infraestructura de red, sino que también permite la detección de posibles vulnerabilidades y la evaluación de la seguridad de los sistemas; además, su capacidad para identificar versiones específicas de servicios y sistemas operativos; esta aplicación contribuye a un análisis más profundo de la arquitectura de la red [3] [6].

La flexibilidad de Nmap radica en su capacidad para adaptarse a una amplia gama de entornos y necesidades, desde escaneos básicos hasta exploraciones avanzadas y altamente personalizadas. El Nmap Scripting Engine (NSE) permite a los usuarios desarrollar scripts personalizados para automatizar tareas específicas durante el escaneo, lo que ofrece un nivel adicional de personalización y eficiencia. Esta funcionalidad no solo agiliza el proceso de evaluación de redes, sino que también permite abordar desafíos particulares y adaptarse a requisitos específicos de seguridad o configuración de red [6].

No obstante estas capacidades destacadas, también se subraya la imperativa necesidad de un uso ético y legal de la herramienta, debido a que su mal uso puede acarrear consecuencias no deseadas. En conjunto, Nmap se consolida como un desarrollo esencial para comprender la complejidad de las redes, identificar posibles riesgos y fortalezas, y, en última instancia, fortalecer la seguridad en el siempre cambiante paisaje tecnológico. Su adecuada utilización no solo contribuye con la protección de los sistemas, sino que también apoya a la promoción de un entorno digital. A continuación, se presenta un cuadro comparativo de las ventajas y desventajas de la herramienta en mención:

TABLA II
Ventajas y desventajas NMAP.

VENTAJAS	DESVENTAJAS
- Nmap es una herramienta adaptativa. - Proporciona información detallada sobre los hosts y servicios en una red. - La capacidad de utilizar el Nmap Scripting Engine (NSE), permite a los usuarios escribir scripts personalizados para automatizar tareas. - Nmap cuenta con una comunidad activa de usuarios y desarrolladores. - Está disponible para varias plataformas, incluyendo Windows, Linux y macOS. - Nmap destaca por su rapidez y eficiencia al ejecutar escaneos, convirtiéndolo en una opción ideal para redes de cualquier tamaño.	- Puede ser "intimidante" para usuarios principiantes. - Como cualquier herramienta de seguridad, Nmap puede ser utilizada con fines maliciosos. - En algunos casos, Nmap puede generar falsos positivos o negativos. - Algunas instrucciones de seguridad pueden detectar la actividad de Nmap. - Para realizar escaneos efectivos, a veces es necesario tener permiso y autorización.

Fuente: [3] [6]

Con base en el cuadro comparativo de la Tabla 02, se puede mencionar que Nmap ofrece una serie de ventajas significativas para los profesionales de la seguridad informática y la administración de redes. Destaca por su adaptabilidad, proporcionando información detallada sobre los hosts y servicios en una red, permitiendo a los usuarios automatizar tareas según sus necesidades específicas. Además, la comunidad activa de usuarios y desarrolladores, garantiza un constante progreso y soporte.

Sin embargo, no se pueden pasar por alto algunas desventajas importantes. Para los usuarios principiantes o novatos, Nmap puede resultar confuso debido a su amplia gama de funciones y opciones. Además, como cualquier herramienta de seguridad, existe el riesgo

de que sea utilizado con fines maliciosos. La posibilidad de falsos positivos o negativos, junto con la detección de intrusiones de seguridad, también representa desafíos potenciales. Es fundamental recordar que, en muchos casos, es necesario obtener permiso y autorización, antes de realizar escaneos con Nmap para evitar problemas legales y éticos.

A continuación, se enumeran una serie de términos relevantes a tener en cuenta durante el proceso de escaneo y verificación del estado actual de una red informática, utilizando Nmap.

A. Auditoría de redes

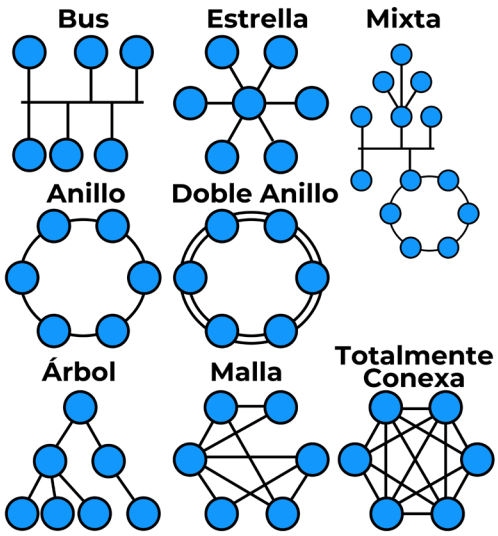
Una auditoría de redes constituye un proceso sistemático de evaluación y análisis de la infraestructura de red de una organización. Su objetivo principal es verificar la seguridad, eficiencia y confiabilidad de la red, identificando posibles vulnerabilidades y proponiendo mejoras. Esta evaluación se puede realizar tanto internamente, utilizando equipos de la organización, como externamente, mediante auditores independientes. Se distinguen varios tipos de auditorías de redes, cada una enfocada en aspectos específicos de la infraestructura, adaptada a las necesidades particulares de la organización [7] [8].

B. Topología

Una topología de red, se refiere a la estructura física o lógica que define la conexión de los nodos (dispositivos) en una red. Describe la forma en que estos dispositivos están interconectados y cómo se comunican entre sí. La topología establece la disposición de los nodos y los enlaces, lo que puede tener un impacto significativo en el rendimiento, la escalabilidad y la confiabilidad de la misma. Existen varias topologías de red, cada una de estas tiene sus propias características y es adecuada para diferentes escenarios y requisitos. Es importante seleccionar la topología adecuada para una red específica, teniendo en cuenta sus necesidades actuales y futuras. Algunas de estas son: [9]:

- Topología de Bus
- Topología de Estrella
- Topología de Anillo
- Topología de Malla
- Topología de Árbol

Figura 2. Topología de RED



Fuente [10]

C. Puertos

Los puertos de comunicación, hacen referencia a un número de identificación lógica asignado a un proceso específico o servicio que se ejecuta en un dispositivo dentro de una red. Estos números de puerto ayudan a direccionar el tráfico de red a destinos específicos en un dispositivo. Hay dos tipos principales de puertos en una red: puertos físicos y puertos lógicos [9].

- Puertos físicos: En el contexto de hardware, un puerto físico se refiere a una conexión física en un dispositivo, como un conector USB, HDMI o Ethernet en una computadora.

- Puertos lógicos: En el contexto de redes, los puertos lógicos son números de identificación asignados a procesos y servicios específicos que se ejecutan en un dispositivo. Estos puertos son

esenciales para la comunicación entre diferentes aplicaciones y servicios en una red.

Así mismo, los puertos lógicos se dividen en dos rangos principales: [11]

- Puertos bien conocidos (Well-known ports): Estos son números de puerto predefinidos asignados por la Internet Assigned Numbers Authority (IANA), para servicios comunes y ampliamente utilizados. Por ejemplo, el puerto 80 está asociado al servicio HTTP (Hypertext Transfer Protocol), mientras que el puerto 443 está asociado a HTTPS (HTTP Secure).

- Puertos dinámicos o privados (Dynamic or Private ports): Estos puertos están en el rango de 49152 a 65535 y son utilizados por procesos y servicios específicos que no están predefinidos por la IANA. Estos puertos se utilizan para garantizar que no haya conflictos con los puertos bien conocidos.

Cuando un equipo en una red desea comunicarse con otro dispositivo específico, utiliza la dirección IP del destino y el número de puerto asociado al servicio o aplicación que desea acceder. Esta combinación de dirección IP y número de puerto, se conoce como "socket" y permite una comunicación eficiente y organizada en la red.

D. Vulnerabilidades

Una vulnerabilidad, en el contexto de la seguridad informática, se refiere a la debilidad o fallo en un sistema, aplicación, red o proceso que puede ser explotado por un atacante para comprometer la seguridad de un dispositivo o tecnología. Las vulnerabilidades pueden surgir debido a errores de diseño, implementación o configuración, y pueden permitir a un atacante realizar diversas acciones no autorizadas, como acceder a información confidencial, ejecutar código malicioso o interrumpir el funcionamiento normal del mismo. Una debilidad puede estar en cualquier lado, por ejemplo: [12]

- Errores de programación.
- Configuraciones incorrectas.
- Fallas en la seguridad de red.
- Software desactualizado.
- Fallas en la seguridad física.

Las organizaciones y los profesionales de la seguridad informática trabajan constantemente para identificar, mitigar y corregir vulnerabilidades antes que sean explotadas por actores malintencionados. Esto se logra mediante la implementación de buenas prácticas de seguridad, la realización de auditorías regulares, la aplicación de parches y actualizaciones, y la concienciación sobre seguridad en toda la organización.

Esta investigación tiene como objetivo analizar una de las herramientas de código abierto más importantes para la seguridad informática.

II. COMANDOS

Network Mapper, es una herramienta de código abierto utilizada para explorar redes y realizar auditorías de seguridad. Su versatilidad y funcionalidad, permite a los administradores de sistemas y profesionales de seguridad, descubrir, mapear y analizar los dispositivos y servicios dentro de una red. En esta sección, se presentan algunos de los comandos y utilidades más relevantes que ofrece Nmap, destacando su capacidad para escanear puertos, detectar hosts, identificar servicios y realizar exploraciones avanzadas. Estos comandos y utilidades no solo son fundamentales para comprender la infraestructura de red, sino también, son herramientas indispensables para mejorar la seguridad y la resiliencia de los sistemas informáticos en un entorno cada vez más digitalizado y amenazante [13], [14].

1 Nmap [dirección IP o nombre de host]: Escaneo básico de puertos en una dirección IP o nombre de host. Este es el comando principal de Nmap; se

utiliza para realizar un escaneo de puertos en un objetivo especificado.

2 Nmap -p [puertos] [dirección IP o nombre de host]: Escaneo de puertos específicos en una dirección IP o nombre de host. Permite especificar los puertos que se desea escanear, en lugar de escanear todos los puertos disponibles.

3 Nmap -F [dirección IP o nombre de host]: Escaneo rápido de los 100 puertos más comunes. Realiza un escaneo rápido que se enfoca en los puertos más comunes para obtener resultados más rápidos.

4 Nmap -A [dirección IP o nombre de host]: Detección de sistemas nmap -Pn [dirección IP o nombre de host]: Escaneo sin detección de hosts. Evita la detección de hosts en la red objetivo y realiza el escaneo directamente, sin enviar solicitudes de detección de hosts.

5 Nmap -sV [dirección IP o nombre de host]: Escaneo de versiones de servicios. Escanea puertos abiertos y trata de determinar las versiones de los servicios que se ejecutan en esos puertos.

6 Nmap -sS [dirección IP o nombre de host]: Escaneo SYN stealth (escaneo sigiloso). Realiza un escaneo utilizando el método de escaneo SYN, que puede ser más sigiloso y difícil de detectar que otros métodos.

7 Nmap -Pn [dirección IP o nombre de host]: Escaneo sin detección de hosts. Evita la detección de hosts en la red objetivo y realiza el escaneo directamente, sin enviar solicitudes de detección de hosts.

8 Nmap -sS [dirección IP o nombre de host]: Escaneo SYN stealth (escaneo sigiloso). Realiza un escaneo utilizando el método de escaneo SYN, que puede ser más sigiloso y difícil de detectar, que otros métodos.

9 Nmap -Pn [dirección IP o nombre de host]: Escaneo sin detección de hosts. Evita la detección de hosts en la red objetivo y realiza el escaneo directamente, sin enviar solicitudes de detección de hosts.

10 Nmap -O [dirección IP o nombre de host]: Detección de sistema operativo. Identifica el sistema operativo del objetivo, mediante el análisis de las respuestas a las solicitudes de escaneo.

11 Nmap -T [velocidad] [dirección IP o nombre de host]: Especifica la velocidad del escaneo (de 0 a 5). Permite ajustar la velocidad del escaneo, en donde 0 es el más lento y 5 es el más rápido.

12 Nmap -v [dirección IP o nombre de host]: "Modo detallado". Proporciona una salida más detallada, demostrando el progreso del escaneo en tiempo real.

Parámetros especiales:

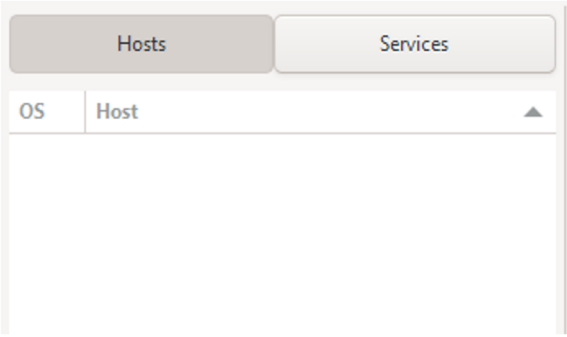
- **-p** para especificar puertos específicos.
- **-T** para configurar la velocidad del escaneo (de 0 a 5).
- **-sV** para detectar versiones de servicios.
- **-A** para realizar un escaneo completo con detección de versión y detección de sistema operativo.
- **-O** para intentar detectar el sistema operativo del objetivo.

III. FUNCIONAMIENTO

A continuación, se muestra una prueba del funcionamiento de la herramienta Nmap sobre la máquina:

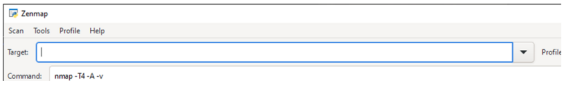
- Inicialmente se reconoce el entorno que se va a trabajar. En la Fig. 3, se observa el entorno virtual de la herramienta Nmap:

Figura 3. Entorno de Nmap



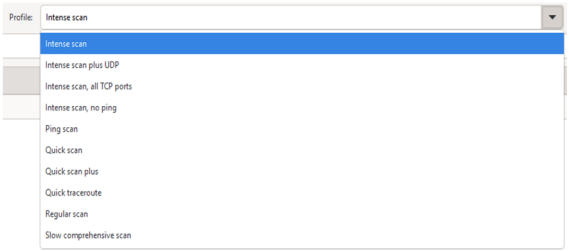
De la imagen se pueden identificar diferentes secciones importantes. En la cabecera, se observa un bloque de escritura llamado Target (Fig. 4); en este bloque se inserta la dirección IP, nombres de domino, rango de direcciones IP, subredes, puertos específicos, redes completas, servicio y/o versiones.

Figura 4. Apartado Target de Nmap.



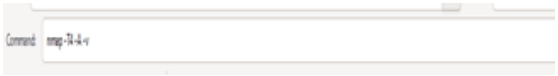
Seguido del apartado de Target, se encuentra una lista desplegable titulada "Profile", como se observa en la Fig. 5. Esta lista desplegable ofrece una serie de opciones para especificar la verificación que se desea realizar en el objetivo seleccionado. Como se puede apreciar en esta imagen, la lista presenta una amplia variedad de opciones, las cuales cambian dependiendo del tipo de escaneo deseado y la información que se quiere verificar.

Figura 5. Lista desplegable del apartado Profile.



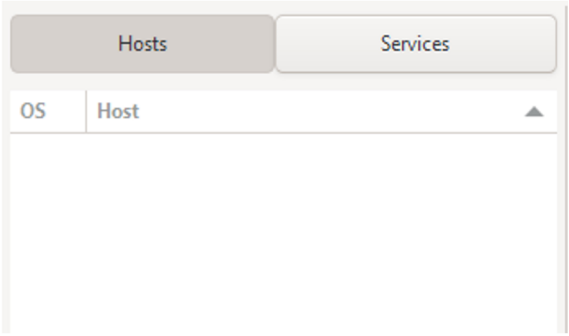
Las instrucciones de Nmap no solo se pueden ejecutar desde su entorno virtual; también desde el CMD (Terminal de Comando de Windows); así pues, Nmap ofrece la redacción automática de la instrucción que se debe ejecutar en el CMD para realizar la misma actividad, pero desde un entorno diferente, como se presenta en la Fig. 6:

Figura 6. Apartado Command de Nmap.



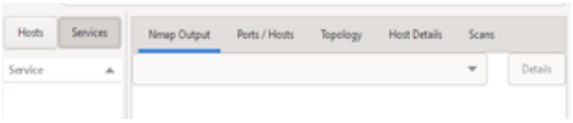
Dentro del mismo entorno virtual de Nmap, se encuentran otras ventanas que ofrecen funcionalidades adicionales. Una de estas opciones se denomina "Host and Services" (ver Fig. 7). Esta ventana proporciona la capacidad de explorar los distintos objetivos que se han ingresado en el escaneo. Aquí, los usuarios pueden visualizar y analizar la información relacionada con los hosts detectados y los servicios asociados a cada uno de ellos:

Figura 7. Ventana Host y Services de Nmap



Finalmente, Nmap cuenta con la ventana principal donde se verifica la información resultante de escaneo. Esta ventana cuenta con 5 opciones diferentes, las cuales están dispuestas de forma horizontal sobre la ventana. De esta forma, para acceder a cada una se debe dar click sobre la misma, como se muestra en la Fig. 8:

Figura 8. Características de Nmap.



A continuación, se describen cada uno de los apartados de la Figura 08:

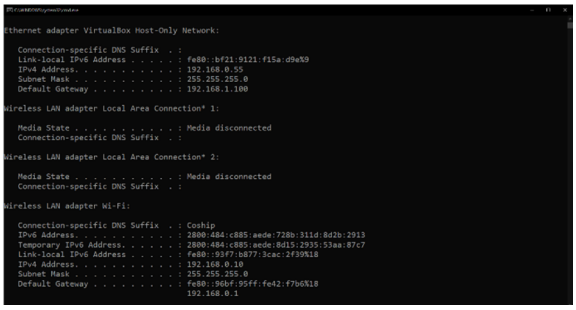
1. **Nmap Output:** Se refiere a los diversos formatos en los que Nmap puede presentar los resultados de un escaneo.
2. **Port/Hots:** Hace refencia a la capacidad de especificar los puertos y hosts que se desea escanear.
3. **Topology:** Muestra la estructura y disposición de los hosts y sus conexiones en una red.
4. **Host Detail:** Esta opción se relaciona con la obtención de información detallada sobre un host específico durante un escaneo.
5. **Scans:** Se refiere a los diferentes tipos de escaneos que se pueden realizar para obtener información sobre los hosts y servicios en una red.

- Para iniciar el escaneo del PC, primero se debe identificar la dirección IP de la máquina. Esto se puede lograr ejecutando el comando ipconfig en el CMD (Terminal de Comando de Windows), como se muestra en la Fig. 9

Figura 9. Ejecución de la instrucción ipconfig.

Al ejecutar dicha instrucción, se deben observar diversos parámetros, entre los cuales se encuentra la dirección IPv4 del adaptador LAN. Esta información es fundamental para establecer la conexión y llevar a cabo el escaneo de la red. En la Fig.10, se identifica la dirección IPv4 del adaptador LAN en el sistema:

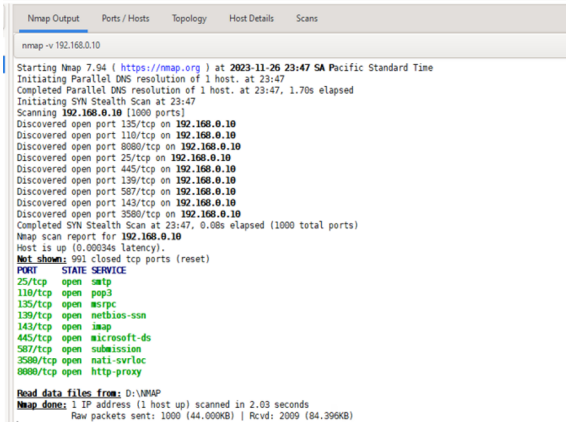
Figura 10. Identificación de la dirección IP.



Luego de identificar la dirección IP, se ejecuta uno de los comandos descritos anteriormente para obtener información detallada sobre los puertos abiertos del PC.

- La instrucción nmap -v 192.168.0.10, se ejecuta en el apartado de Target para llevar a cabo un escaneo básico de los puertos de la PC especificada. Esto permite obtener información detallada sobre los servicios y puertos abiertos en el dispositivo. En la Fig. 11, se muestra claramente cómo se realiza este proceso, brindando una visualización precisa del análisis realizado por Nmap.

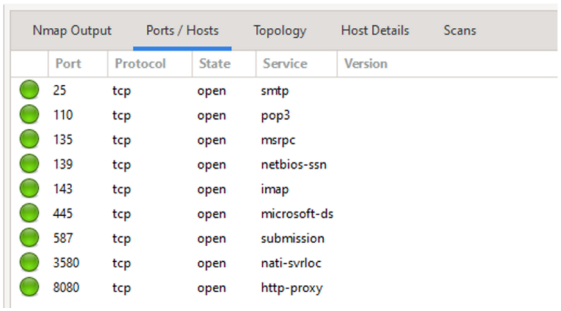
Figura 11. Resultado del escaneo básico (Nmap Output).



Además, se pueden apreciar otras características que ofrece Nmap (ver Fig. 12), en el apartado de Ports/Host. Aquí se exhiben diversas funcionalidades que permiten un análisis minucioso de los puertos y hosts escaneados,

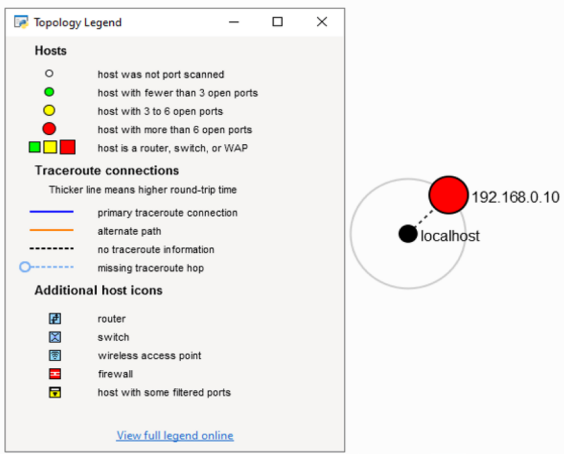
proporcionando una visión más completa de la infraestructura de red y sus posibles vulnerabilidades.

Figura 12. Puertos y Host.



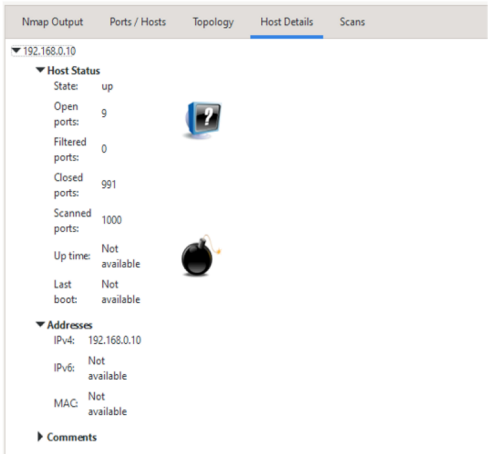
En la Fig. 13, se puede verificar la topología de la red; en este caso, solo se cuenta con el local host y la máquina que se esta escaneando, representada por su respectiva dirección IP:

Figura 13. Topología y legenda de la topología.



Finalmente, en la Fig. 14, se exponen los detalles del Host:

Figura 14. Detalles del Host



Considerando lo mencionado anteriormente, queda claro que la herramienta Nmap ofrece a los profesionales de las TIC una comprensión profunda y una visión integral de la infraestructura de red, incluido su estado de seguridad. Esta aplicación facilita la identificación de vulnerabilidades, el mapeo de la topología de la red, la detección de hosts y servicios, así como la evaluación de la efectividad de las medidas de seguridad implementadas.

La información obtenida a través de Nmap capacita a los administradores y equipos de seguridad para tomar decisiones informadas y eficientes, destinadas a mejorar la seguridad y la eficiencia de la red. Esto, a su vez, fortalece la integridad y disponibilidad de los activos digitales de una organización, promoviendo así su reputación y confianza en el ámbito de la ciberseguridad.

IV. ANÁLISIS RESULTADOS

Del escaneo realizado, se puede definir lo siguiente:

A. Información inicial:

- Se está utilizando Nmap 7.94.
- El escaneo inició el 26 de noviembre de 2023 a las 23:47 hora estándar del Pacífico.

B. Resolución de DNS:

- Se realizó la resolución de DNS en paralelo para el host 192.168.0.10, completándose en 1.70 segundos.

C. SYN Stealth Scan:

- Se inició un escaneo SYN Stealth a las 23:47, explorando 1000 puertos en el host 192.168.0.10.

D. Descubrimiento de Puertos Abiertos:

- 25/tcp: SMTP (Simple Mail Transfer Protocol) - Servicio de envío de correo electrónico.
- 110/tcp: POP3 (Post Office Protocol) - Protocolo para la recepción de correo electrónico.
- 135/tcp: MSRPC (Microsoft Remote Procedure Call) - Llamadas a procedimientos remotos en sistemas Windows.
- 139/tcp: NetBIOS-SSN (NetBIOS Session Service) - Servicio de sesión NetBIOS.
- 143/tcp: IMAP (Internet Message Access Protocol) - Protocolo de acceso a mensajes de Internet.
- 445/tcp: Microsoft-DS (Microsoft Directory Services) - Servicios de directorio en sistemas Windows.
  587/tcp: Submission - Utilizado para enviar correos electrónicos.
- 3580/tcp: nati-svrloc - Ubicación de servidor NAT.
- 8080/tcp: HTTP Proxy - Proxy para servicios web.

E. Estado del Host y Latencia:

- El host 192.168.0.10 está en línea con una latencia de 0.00034 segundos.

F. Puertos Cerrados:

- Se identificaron 991 puertos cerrados (reset), indicando falta de respuesta.

G. Resumen de Estadísticas del Escaneo:

- El escaneo se completó en 2.03 segundos.
- Se enviaron 1000 paquetes brutos, totalizando 44.000KB.
- Se recibieron 2009 paquetes brutos, totalizando 84.396KB.

V. CONCLUSIONES

- Nmap se posiciona como una herramienta esencial durante las fases iniciales y activas de un pentesting, proporcionando datos detallados y perspicaces para guiar hacia una evaluación de seguridad efectiva.

- Nmap es una herramienta tanto poderosa como valiosa, para aquellos que buscan comprender la seguridad de sus redes o realizar evaluaciones de seguridad. Sin embargo, su uso debe ser guiado por la ética y la legalidad; es fundamental obtener el permiso adecuado antes de realizar escaneos en redes que no son de su propiedad.

- Un hito importante en la concienciación sobre la importancia de la información, radica en reconocer que, mientras el escaneo proporciona información valiosa sobre la infraestructura del host, la evaluación de la seguridad debe ir más allá, considerando aspectos específicos de configuración y medidas de protección en cada servicio y puerto.

- El escaneo revela la presencia de diversos servicios y puertos abiertos en el host analizado, así como una latencia mínima y una rápida velocidad del mismo. Estos datos proporcionan una visión detallada de la infraestructura de red y su estado de seguridad, permitiendo al usuario final, tomar medidas adecuadas para mejorar la seguridad y la eficiencia de la red.

- La presencia de puertos abiertos aso

ciados con los protocolos SMTP, POP3 y MSRPC, plantea diversos riesgos significativos en términos de ciberseguridad. Estos riesgos incluyen la exposición a ataques de fuerza bruta, phishing y correos no deseados, así como la explotación de vulnerabilidades en los servicios de correo electrónico y en el protocolo MSRPC. Además, existe el apuro potencial de obtención de datos sensibles a través de estos servicios. Por lo tanto, es decisivo implementar medidas de seguridad sólidas, como parches de seguridad, configuraciones de firewall y monitoreo activo, para mitigar estos riesgos y proteger la infraestructura de red contra posibles amenazas cibernéticas.

VI. REFERENCIAS

1 S. Inc, «Resumen ejecutivo - Informe de ciberamenazas 2023 de SonicWall», 2023. [En línea]. Disponible en: www.sonicwall.com

2 S. Inc, «2023 SonicWall Cyber Threat Report», 2023.

3 K. D. Kang, G. Park, H. Kim, M. Alian, N. S. Kim, y D. Kim, «NMAP: Power management based on network packet processing mode transition for latency-criticalworkloads», en Proceedings of the Annual International Symposium on Microarchitecture, MICRO, IEEE Computer Society, oct. 2021, pp. 143-154. doi: 10.1145/3466752.3480098.

4 S. Liao et al., «A Comprehensive Detection Approach of Nmap: Principles, Rules and Experiments», en Proceedings - 2020 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2020, Institute of Electrical and Electronics Engineers Inc., oct. 2020, pp. 64-71. doi: 10.1109/CyberC49757.2020.00020.

5 F. Preciado, «GuardHack,» 14 07 2019. [En línea]. Available: https://guardhack.files.wordpress.com/2019/07/nmap.png.

6 «Nmap, Nmap, Nmapping on Server Ports Una introducción "amable" al escaneo de red».

7 N. Rocío Tirado Ríos, D. Janeth Ramos Reyes, E. Leuvany Álvarez Morales, y S. Daniel Carreño Sandoya, «Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas», 2017.

8 V. Villarreal Página, «Curso: Auditoría de Redes».

9 M. Lederkremer, Redes Informáticas. 2019.

10 L. A. Garcia, «Quora,» 2020. [En línea]. Available: https://qph.cf2.quoracdn.net/main-qimg-bda988562a1c0f9ebbb009df2e44c598

11 L. Heilig y S. Schwarze, «Instituto de Sistemas de Información, Hamburgo, Alemania,» 01 07 2017. [En línea]. Available: https://aisel.aisnet.org/hicss-50/da/decision_support_for_scm/2/. [Último acceso: 19 03 2024].

12 R. C. Martha Irene et al., Introducción a la seguridad informática y el análisis de vulnerabilidades. 2018.

13 Hernán M. Domínguez L., Edgar A. Maya O., Diego H. Peluffo O., y Christian M. Crisanto Ñ, «Aplicación de técnicas de fuerza bruta con diccionario de datos, para vulnerar servicios con métodos de autenticación simple "Contraseñas", pruebas de concepto con software libre y su remediación», 2018.

14 Byron. Oviedo, A. Gracia, y Emilio. Zhuma, «Análisis de herramientas de códigos abiertos que permitan la seguridad de la data en la Universidad Técnica Estatal de Quevedo», 2018.

Es motivo de orgullo institucional ofrecer a la comunidad académica Escom, el sexto volumen de la Revista Científica TECNOESCOM, una publicación que confirma la formación científica de nuestros estudiantes y refleja el alto nivel de formación profesional de nuestro equipo de docentes.

En esta revista, elaborada con rigoren sus contenidos, se presentan temáticas que demuestran compromiso universitario con el medio ambiente, la ciudadanía y la institución castrense, como lo es el Ejército; Fuerza que tiene como misión - entre otras - la defensa de la soberanía, la independencia y la integridad territorial, con el propósito de proteger a la población civil, para la consecucuón de la paz y el orden constitucional. En tal sentido, esta edición presenta un punto de encuentro en donde estudiantes y profesores socializan propuestas que aportan e impactan positivamente aquellas dimensiones que son parte inherente y fundamental para el desarrollo de la sociedad.

Invito entonces, desde estas líneas, a la lectura de los contenidos que encontrarán en la presente edición de Resvista TECNOESCOM, misma que está dividida en tres secciones: Artículos de investigación, que expone los resultados de estudios efectuados por estudiantes de los diferentes programas de pregrado y posgrado, quienes aportan y responden a necesidades reales de las comunidades rurales, la academia y la empresa; por otra parte se encuentran los artículos de revisión bibliográfica, abordados con una visión crítica, argumentada en fuentes serias y reconocidas por la comunidad científica, además de propositivas, lo que aporta valor en el momento de resolver problemáticas afines a estas. Por último, se presentan los artículos producto de semilleros d einvestigación realizados a partir de un análisis certero y profundo en lo que atañe a tecnologías emergentes y de impacto social.

ESCOM
ESCUELA DE COMUNICACIONES MILITARES

Escuela de Comunicaciones Militares
www.escom.mil.co

COMUNICACIONES
MILITARES
80 años