ANÁLISIS DE RIESGOS Y VULNERABILIDADES DE SEGURIDAD INFORMÁTICA APLICANDO TÉCNICAS DE INTELIGENCIA ARTIFICIAL ORIENTADO A INSTITUCIONES DE EDUCACIÓN SUPERIOR.

J.J. Castro-Maldonado[1,2,3], H.F. Villar-Vega[1], K. Marin-Ayala[1], K. Duarte-Herrera[1] y V. Giraldo-García[1]

[1] Grupo de Investigación en Gerencia y Aplicación de la Ciencia y la Tecnología-GIGAT, Centro de Servicios y Gestión Empresarial, Servicio Nacional de Aprendizaje SENA. Medellín-Colombia.
[2] Universidad Benito Juárez. Puebla-México.
[3] Institución Universitaria UNINPAHU. Bogotá-Colombia.

jcastrom@sena.edu.co; hvillar@sena.edu.co

Palabras clave: Seguridad Informática, Deficiencias, Riesgos, Vulnerabilidades.

RESUMEN

La seguridad informática se ha presentado como un instrumento primordial al momento de salvaguardar el activo más importante en las actuales organizaciones como son los datos y la información, debido a su valor dentro de una adecuada gestión del conocimiento. En ese sentido, las instituciones de educación superior deben manejar de forma responsable la información de los actores que en ella se interrelacionan, como son los estudiantes, docentes y personal administrativo. Este artículo tiene como objetivo principal presentar una investigación documental realizada para explorar las deficiencias, riesgos y vulnerabilidades en seguridad informática que poseen diferentes organizaciones, en especial las instituciones de educación superior. Este trabajo de investigación está enmarcado dentro de la corriente epistémica del positivismo, aplicando el método hipotético deductivo, con enfoque cualitativo, orientado a desarrollar un trabajo de investigación de corte exploratorio que propone abordar la situación sobre los métodos, técnicas y estrategias usadas para la identificación de las vulnerabilidades y riesgos informáticos como pilar de alcance transversal de toda organización, no solo en las áreas de tecnología sino también en áreas administrativas. Se pudo evidenciar, gracias al análisis documental, que la seguridad informática debe ser tenida en cuenta en las instituciones de educación superior tanto para resguardar información concerniente al funcionamiento de esta, como para concientizar a su comunidad en el manejo adecuado de la información personal que redunda en una adecuada cultura digital, y para ello se pueden usar diferentes estrategias, entre ellas las técnicas de inteligencia artificial para identificar amenazas o caracterizar vulnerabilidades.

01 INTRODUCCIÓN

El contexto actual en el cual nos hallamos inmersos se traslada al ciberespacio como medio para el intercambio de información, la interacción laboral, escolar y familiar generando mayor productividad, acceso a la información y un sin número de posibilidades, en donde el individuo navega para acceder a ellas. Sin embargo, existen personas que aprovechan las falencias en seguridad informática de los medios que transportan estos datos, como los computadores o celulares, para desarrollar todo tipo acciones digitales ilícitas como el robo de información e identidades, espionaje, secuestro del equipo, virus, entre otros.

Según un estudio adelantado por la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) y la policía Nacional de Colombia, entre 2017 y 2019 se reportaron 52.901 denuncias relacionadas con hurtos, concentrándose el mayor número de estas en crímenes a través de medios informáticos con 31.058 registros, seguido por robo de identidad con 8.037 casos, y se detalla que "*Bogotá fue la ciudad que más incidentes reportó (5.308), luego Cali (1.190) y Medellín (1.186)" [1]. Asimismo se indica que, en el país "los ataques por Malware crecieron un 612% y el monto pagado por rescate de información se ubicó entre los 32 millones y los 160 millones de pesos*", escenario ante el cual, Colombia es uno de los países más afectados por Ransomware (programa informático dañino que restringe el acceso a archivos y pide rescate para recuperarlos) en América Latina [1].

Este trabajo tiene por objetivo realizar una exploración sobre las vulnerabilidades y riesgos informáticos a los que se encuentran expuestos los actores de las instituciones educativas.

02 METODOLOGÍA

La presente investigación se basó en el uso de una técnica cualitativa, donde los datos cualitativos corresponden a las variables que se centran en contextos situacionales y estructurales; mediante un proceso inductivo, en el que se utiliza inicialmente las premisas para llegar a la conclusión general, es decir, a partir de la observación de los hechos y fenómenos se logran establecer conclusiones, es decir, aplica a la indagación de eventos que causan estos fenómenos sociales utilizando el análisis y la comprobación [2]. El tipo de investigación utilizada es exploratoria, en donde se presenta los diferentes rasgos y características de los fenómenos relevantes que intervienen en la investigación, en ese sentido, se realizó una revisión bibliográfica de artículos vigentes desde el año 2017 hasta el 2021, exceptuando algunos que por su aporte en la investigación y que no estaban dentro de este intervalo de tiempo se tuvieron en cuenta.

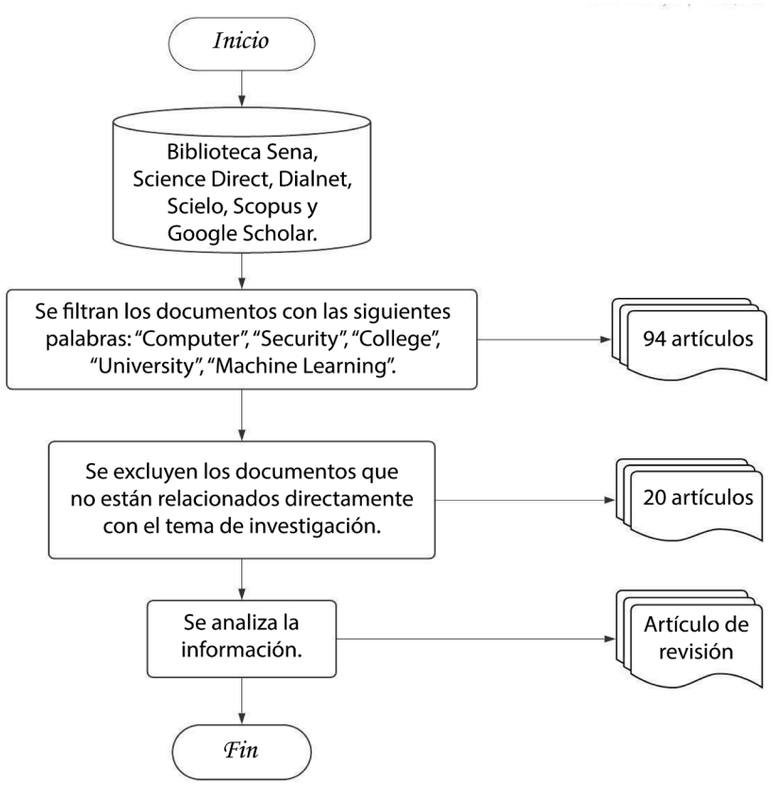

Figura 1. Diagrama de flujo del proceso de la revisión sistemática. Fuente: Elaboración propia.

A partir de un proceso de revisión sistémica de información [3], se consultaron documentos referentes al tema empleando palabras clave como "Computer", "Security", "College", "University", "Machine Learning", entre otras. Esta revisión se hizo en bases de

datos como Biblioteca Sena, Science Direct, Scielo, Scopus y Google Scholar donde se encontraron 94 artículos. Por medio de un análisis de los artículos encontrados, se excluyeron los que no estaban relacionados directamente con el tema de investigación, también se estudió y analizó el potencial impacto que tuviese respecto a la educación, seguridad informática e inteligencia artificial específicamente, como conector a resaltar en la investigación. En el proceso de búsqueda se tomaron como base 20 artículos donde se evidencia el abordaje en cada uno de ellos de los temas a analizar dentro de la investigación (Educación, Seguridad Informática, *Machine Learning*) desde una mirada reflexiva y de exploratoria conceptual, como se puede visualizar en la figura 1. Como resultado de la búsqueda se hallaron artículos científicos y trabajos de grado a nivel de pregrado y posgrado que podrían adaptarse como estrategia descriptiva relevante a nuestro trabajo.

03 RESULTADOS Y DISCUSIONES

La búsqueda de los documentos dentro de las principales bases de datos inició principalmente con los conceptos de "Computer" "Security" "College" "University" y "Machine Learning", entre otros, a través de la ecuación de búsqueda: Computer AND Security AND College OR University AND Machine Learning.

A partir de estas consultas, se seleccionaron artículos publicados en un periodo de cinco años. Luego, se llevaron a cabo las respectivas visualizaciones, con el fin de encontrar las relaciones entre las palabras clave mencionadas anteriormente, donde se evidencian conexiones entre los procesos de educación, el *Machine Learning* y la seguridad informática, a partir de elementos asociados al tema de ciberseguridad, poniendo en evidencia la importancia de las vulnerabilidades y riesgos informáticos en los procesos formativos en las instituciones de educación superior, además, de su relación con técnicas de inteligencia artificial . Esto se puede ver en la figura 2.

Figura en la página 51.

En ese sentido, se encontró que la palabra *Machine Learning* es la palabra más común dentro los artículos, trabajos y estudios consultados, toda vez, que el concepto de *Machine Learning* está relacionado fuertemente con otros conceptos como son *Big data*, seguridad, privacidad. Así mismo, se tiene en cuenta que la palabra "sistemas de aprendizaje" es bastante repetitiva en los trabajos hallados y que está a su vez tienen relación con *Malware, Network Security, Learning Systems,* etc. Con todo esto, se puede identificar que, a nivel mundial, se están trabajando conceptos de *Machine Learning* relacionados a la seguridad informática orientados hacia procesos formativos, que es la temática principal del trabajo exploratorio de investigación que se está ejecutando, como se ve en la figura 3.

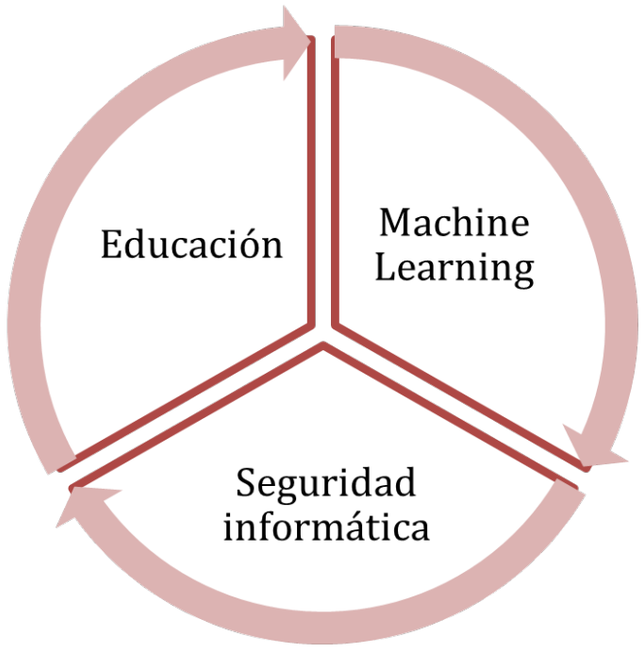

Figura 3. Conceptos conexos a la investigación exploratoria.
Fuente: Elaboración propia.

Se procedió a abordar cada uno de estos conceptos identificados en el análisis cienciométrico a partir de la situación actual de nuestro contexto, iniciando con un diagnóstico muy somero de la situación actual de la seguridad informática en Colombia. Posteriormente, se analizó el estado de la formación en seguridad en las instituciones de educación superior (IES). Seguidamente, se socializaron diferentes estrategias o acciones de ciberseguridad que se implementan en las IES. Finalmente, se comentaron algunas aplicaciones que implementan técnicas de inteligencia artificial en el campo de la seguridad informática.

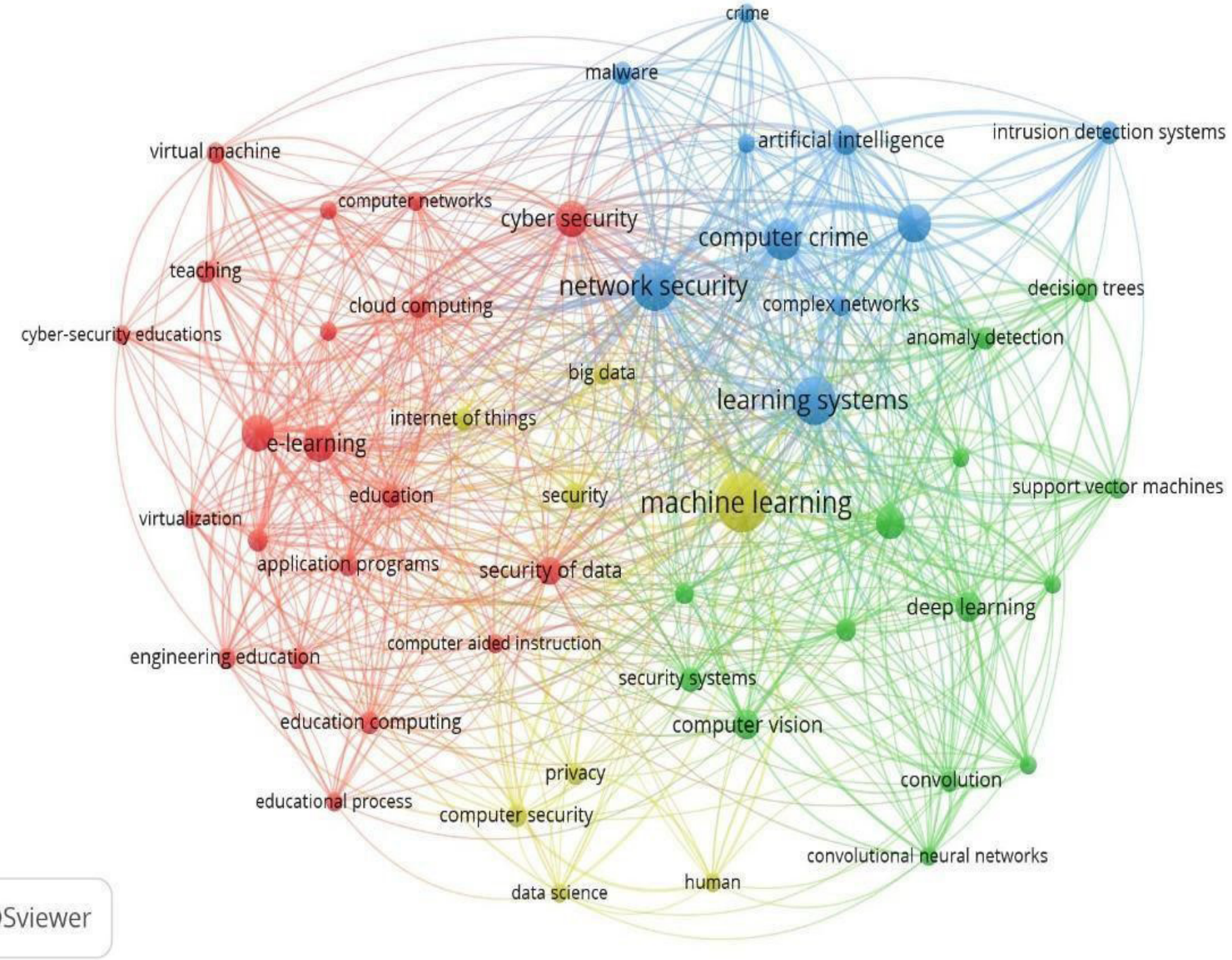

Figura 2. Mapa de Relación de palabras conexas a las ecuaciones de búsqueda.
Fuente: Elaboración propia con apoyo del Software VOSviewer®.

3.1 LA SEGURIDAD INFORMÁTICA EN COLOMBIA

Colombia no tiene las medidas necesarias para enfrentar o manejar las amenazas en la seguridad de la información. En la cuarentena preventiva impuesta por la COVID19 hubo un incremento significativo del ciberdelito contra estados, organizaciones e individuos. Por lo tanto, se deben promover políticas de seguridad en el país para proteger la información de los ciudadanos y entidades, asimismo, administrar la información, proteger los dispositivos que están conectados a la red, identificar las barreras y procedimientos de acceso a los datos y establecer niveles de acceso adecuados, entre otros [4]. La seguridad informática tiene un impacto positivo en los datos e información a nivel mundial, y permite enfrentar y prevenir los ciberataques en nuestros equipos de trabajo.

Se hicieron análisis con estadísticas acerca de la última década sobre la situación de ciberseguridad y cómo esto ha sido difícil de manejar en los gobiernos, organizaciones y en la sociedad [5], ya que a medida que evoluciona la tecnología, aumenta la densidad digital por lo que nos convertimos en una sociedad cada día más digital. Por lo tanto, no es suficiente solo conocer el concepto de seguridad informática, sino empezar a crear herramientas o métodos que nos permitan estar seguros en nuestro espacio de trabajo [6].

Se puede notar que con el cambio de las nuevas tecnologías de la información y la comunicación (TIC) van apareciendo nuevas amenazas, a partir de las cuales las empresas toman decisiones y empiezan a actuar de modo que puedan prevenir y minimizar los ataques cibernéticos, por lo cual se tienen en cuenta las diferentes formas de protección, actualizando y mejorando los softwares de seguridad [7]. En ese sentido, Mitxelena X, Guzmán Flórez C y Angarita Pinzón contemplan, que por la digitalización de los procesos se ha incrementado la competitividad de las organizaciones, razón por la cual, es importante tener la prevención necesaria para asegurar nuestra información [8,9]. Asimismo, es importante fortalecerse en el campo del saber de seguridad informática, toda vez, que entre más interacciones digitales haya, mayor será la probabilidad de ser afectados por un ciberdelito.

Las empresas han reflejado su preocupación respecto a los ataques recibidos en contra de sus negocios, y de su integridad. De acuerdo con la memoria anual de *Symantec* (ISTR), en donde se realizó un estudio en 157 países, se logró observar que nuestro país está en un lugar preocupante y no tiene estrategias necesarias para enfrentar estos ataques [10]. Esto se puede evidenciar con el aumento de los ataques malintencionados a los medios de comunicación oficiales de algunos estamentos de nuestro gobierno [11], por lo que se exhorta urgentemente a crear un modelo completo para resolver estos problemas. La auditoría forense podría ser la herramienta que se necesita para resolver dichos problemas, [12] dado que permite detectar fraudes, autores y posibles cómplices, permitiendo ayudar a solucionar estos ciberdelitos junto a una persona especializada.

3.2 LA FORMACIÓN EN SEGURIDAD INFORMÁTICA

Hace algún tiempo la seguridad informática se convirtió en un tema de mucha importancia en el ámbito tecnológico y empresarial, toda vez, que las empresas, entidades o instituciones son las que se ven más afectadas, debido a que la mayoría del tiempo están accediendo a internet, descargando datos o archivos que pueden convertirlos en un blanco fácil para los ciberataques. Uno de los lugares con más víctimas de robo de información son las instituciones de educación superior [13], debido a que sus instalaciones no cuentan con la seguridad informática adecuada para prevenir este tipo de situaciones. Si comparamos esta postura frente a otras instituciones o industrias, nos daremos cuenta de que estas tienen el menor desempeño, por lo que se vuelven un objetivo fácil para los ciberdelincuentes al momento de obtener datos. Por eso, es fundamental idear un plan para tener más profesionales en el área de seguridad informática que ayuden o socialicen cómo se puede prevenir ataques informáticos y proteger los datos y sistemas ante estas amenazas.

La formación en seguridad informática es necesaria en las actuales organizaciones enmarcadas dentro de la industria 4.0 que van desde procesos de manufactura, pasando por comercio, hasta llegar a organizaciones que prestan servicios, toda vez, que utilizan dispositivos conectados a internet para desarrollar de buena forma sus procesos. Por tanto, la formación de las personas que intervienen en ellas es vital, debido a que estos grupos de trabajo son los que pueden implementar acciones que ayuden a salvaguardar la información y tomar conciencia sobre este activo intangible, vital en las actuales organizaciones para su adecuada gestión del conocimiento a través de planes de seguridad informática.

Igualmente, el desarrollo de nuevas tecnologías ha permitido incursionar hacia otra áreas de formación, orientadas a la seguridad informática como lo es la informática forense [12], que ofrece, a través de competencias adquiridas, robustecer parámetros de ciberseguridad de las empresas por medio de auditorías forenses para identificar o reaccionar ante cualquier ciberataque que afecte el normal desempeño de sus operaciones.

Como se puede ver, es necesario contar con personal capacitado que puedan identificar amenazas y prevenir riesgos informáticos, además, de democratizar estos conceptos, con el fin de que puedan llegar a diferentes organizaciones y personas que estén en continua interacción con las redes o medios informáticos.

3.3 CIBERSEGURIDAD EN LAS UNIVERSIDADES

Para lograr un buen empleo de la ciberseguridad en todos los contextos sociales, es necesario una constante capacitación, inicialmente, de todos los actores que intervienen en las instituciones de educación superior, en procura de que estos sean apropiados por la mayor cantidad de personas dentro de los diferentes ámbitos de la sociedad, toda vez, que estos conceptos son transversales actualmente a cualquier actividad económica que se esté practicando.

En ese sentido, las universidades o instituciones de educación superior (IES) deben realizar un papel protagónico en la implementación, tanto de una cultura de la ciberseguridad y aplicación de políticas orientadas al fortalecimiento de competencias en las personas como en la identificación, desarrollo y aplicación de tecnologías que contribuyan a favorecer o fortalecer los sistemas de prevención de ataques informáticos por parte de los ciberdelincuentes [14].

En ese orden de ideas, Roque Hernández y Juárez Ibarra (2018) realizan un estudio sobre la concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios, en él se pudo evidenciar que inicialmente los estudiantes contaban con muy bajas competencias en temas relacionados a la seguridad informática desde sus datos personales, y que es posible que estas competencias se puedan fortalecer a través de la concientización de ellos, por medio de programas que evidencien la importancia de técnicas muy básicas para salvaguardar nuestra información [15].

Asimismo, Rojas Mirquez y Sánchez Moreno (2013) realizan un trabajo de investigación sobre la seguridad informática en el uso de la red social de Facebook en estudiantes entre 11 a 17 años. En él se pudo identificar que, en efecto, los estudiantes tienen una alta vulnerabilidad a delitos informáticos como el Ciberbullying que se materializan a través de amenazas como el acoso de usuarios, desinformación por parte de padres, estudiantes y docentes, infiltración, ingeniería social y publicación de contenido malintencionado, entre otros [16].

En coherencia, dentro de las diferentes alternativas que se tienen para abordar el estado de la seguridad informática en las organizaciones, están los planes integrales de actividades enmarcados dentro estándares de seguridad. Estos parten desde un diagnóstico para identificar el estado actual de este tema en la organización, hasta una encuesta aplicada a expertos para probar la eficiencia del plan propuesto, consolidando los resultados en la percepción de mejora de la seguridad informática de la organización [17].

Como se puede evidenciar, en las IES gran parte de los estudiantes no actúan como usuarios digitales responsables, aun cuando pasan la mayor parte del día conectados a la red, aunado a que son los que más carecen de conocimientos sobre el tema, por lo que son más propensos a ser víctimas de crackers o robos informáticos.

3.4 APLICACIONES DE TÉCNICAS DE INTELIGENCIA ARTIFICIAL EN EL CAMPO DE LA SEGURIDAD INFORMÁTICA

Los diferentes campos de la Inteligencia Artificial (IA) han incursionado en diferentes saberes desde el comercio hasta la salud, debido a su alta aplicabilidad para poder describir fenómenos, predecir comportamientos y segmentar características dentro de los individuos de estudio. En ese sentido, la aplicación de la IA dentro de la seguridad informática, ha tenido importantes avances desde el punto de vista de la detección de riesgos a través de las caracterización de factores y su impacto en los activos de las organizaciones, hasta la identificación de vulnerabilidades por medio de la segmentación de los individuos por medio de la determinación de sus comportamientos e interacciones en la red.

Dentro de las principales ramas de la IA que actualmente se aplican para aportar en la identificación de vulnerabilidades de seguridad informática, se tiene el *Machine Learning* o aprendizaje de máquinas, el cual, dentro de sus fortalezas permite generar modelos que predicen el comportamiento de un fenómeno y hacer segmentaciones para identificar características similares entre comportamientos de las poblaciones o muestras tenidas en cuenta para los estudios.
En ese sentido, se presenta a continuación una serie de trabajos enmarcados en la aplicación de herramientas de la IA en el desarrollo de actividades de seguridad informática.

En coherencia, Carvajal Montealegre (2015) presentó el desarrollo de árboles de decisión para modelar el comportamiento de incidentes, apoyado desde el uso de la pro-

gramación genética. En él se pudo identificar los diferentes perfiles de los incidentes, con el fin de minimizar el porcentaje de ocurrencia de estos. Igualmente, la implementación de los árboles de decisión para presentar los resultados de la programación genética, mostró ser una muy buena técnica para su posterior implementación en desarrollos WEB. En este trabajo, la implementación de algoritmos y visualizaciones enmarcados dentro de la IA, mejoró la rapidez en los procesamientos de los datos a través de la minería de datos y su fácil interpretación para futuras aplicaciones [18].

Asimismo, Azán Basallo et al. (2016) propusieron la utilización de la lógica difusa para emplearla en la etapa de análisis de auditorías de seguridad informática a los sistemas gestores de bases de datos, y de esta manera, manejar los términos lingüísticos con la cual se evalúa el riesgo de la seguridad de la información [19].

En concordancia, Gil Vera y Gil Vera (2017) desarrollaron un modelo de simulación que permite evaluar el nivel óptimo de seguridad que deben tener las organizaciones considerando aspectos relacionados con la reducción del riesgo y la obtención de beneficios empresariales; para la realización de este modelo, los autores utilizaron la técnica de simulación basado en dinámica de sistemas [20].

La IA y la Seguridad Informática están actualmente muy ligadas, debido a la gran cantidad de procesos en ciberseguridad que se pueden automatizar gracias a la implementación de técnicas como el Machine Learning. Durante varios años, el centro de la implementación de las acciones de seguridad informática estaba enfocada en la experticia del humano, no obstante, esto traía consigo algunas desventajas propias de la persona, como el cansancio a medida que transcurren las horas realizando una actividad repetitiva o estar sentado por largos periodos de tiempo al frente de un ordenador. Es por ello que aparece una gran alternativa como lo es la IA, que permite elaborar algoritmos con base a los datos recolectados de antiguos incidentes, y de esta forma puede pronosticar, con cierto porcentaje de error, los futuros ataques dentro de la organización mitigando el impacto de estos [21].

04 CONCLUSIONES

La implementación de las tecnologías y específicamente los sistemas informáticos en diferentes labores o procesos de las organizaciones, gracias a la implementación de las técnicas del Internet de las cosas industrial (IoT), entre otros, han propiciado escenarios virtuales vulnerables que los ciberdelincuentes están aprovechando para cometer distintos delitos como el Ransomware, que afecta de forma directa los activos intangibles de las empresas como lo es la información.

De acuerdo con los hallazgos encontrados en los textos citados en el presente trabajo, se puede evidenciar la falta de apropiación y aplicación de conductas favorables de seguridad informática en el entorno educativo de los estudiantes sin importar el nivel académico. Por ende, diferentes IES están implementado programas o acciones que permitan, inicialmente, realizar un diagnóstico sobre estos conocimientos para posteriormente implementar programas o planes que fortalezcan las competencias dentro de los estudiantes y demás integrantes de la comunidad académica, en temas relacionados a la prevención de ciberataques o delitos informáticos en contra de la información personal o institucional.

Igualmente, se puede notar el auge que está teniendo actualmente la implementación de técnicas de inteligencia artificial dentro de la seguridad informática como herramienta eficaz para la obtención de modelos que permitían identificar las vulnerabilidades o riesgos informáticos a los que pueda estar expuesta una organización, y de esta forma, mitigar los impactos de los ciberataques a que haya lugar.

05 AGRADECIMIENTOS

Los autores agradecen el apoyo del SENA, del grupo de investigación GIGAT, y de los semilleros MERLIN y REDTIS que participaron en este proyecto, aportando con sus ideas y haciendo que este trabajo pueda ser impulsado.

06 REFERENCIAS

[1] Ceballos López A, CR (RA) Bautista García F, Mesa Guzmán L, Argáez Quintero C, TC Durán Santos A, MY Miranda Herrera F, CT Acevedo Nieto R, TE Prada Roa W, IT Ruiz Leal J and PT Santos Rocha H 2019 Informe de las Tendencias del Cibercrimen en Colombia 2019-2020 (Bogotá)

[2] Comte A and Mill. J S 2017 Distancias epistemológicas Acheronta 78
[3] Kitchenham B 2004 Procedures for Performing Systematic Literature Reviews
[4] Ospina Díaz M R and Sanabria Rangel P E 2020 Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia Rev. Crim. 62 199–217
[5] Gavino Ramos M S 2018 Ciberseguridad en la actividad organizacional de la era digital (Universidad Nacional Federico Villarreal)
[6] Cano M. J J and Rocha A 2019 Ciberseguridad y ciberdefensa. Retos y perspectivas en un mundo digital RISTI - Rev. Iber. Sist. e Tecnol. Inf. 2019
[7] Gutiérrez Toro D L 2020 Amenazas cibernéticas y su impacto en las organizaciones del sector industrial y servicios de Colombia en la última década (Universidad Nacional Abierta y a Distancia)
[8] Mitxelena X 2020 Euskadi 2025 - Sin ciberseguridad no hay futuro Ekon. Rev. vasca Econ. 98 194–227
[9] Guzman Flores C A and Angarita Pinzon C A 2017 Protocolos para la mitigación de ciberataques en el hogar. Caso de estudio: Estratos 3 y 4 de la ciudad de Bogotá (Universidad Catolica de Colombia)
[10] Valoyes Mosquera A 2019 Ciberseguridad en Colombia Semin. SIA 1–12
[11] Arias Torres N A and Celis Jutinico J A 2015 Modelo experimental de ciberseguridad y ciberdefensa para Colombia (Universidad Libre)
[12] Caamaño Fernández E E and Gil Herrera R de J 2020 Prevención de riesgos por ciberseguridad desde la auditoría forense: conjugando el talento humano organizacional NOVUM, Rev. Ciencias Soc. Apl. 10 61–80
[13] Security Scorecard 2018 2018 Education Cybersecurity Report (New York City)
[14] Anchundia Betancourt C E 2017 Ciberseguridad en los sistemas de información de las universidades Dominio las Ciencias 3 200–17
[15] Roque Hernández R V and Juárez Ibarra C M 2018 Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios PAAKAT Rev. Tecnol. y Soc. 8 1–13
[16] Rojas Mirquez M A and Sánchez Moreno N P 2013 Evaluación de la seguridad informática en el uso de la red social facebook entre menores de 11 a 17 años frente a la problemática del Ciberbullying en el Colegio “A” en la localidad de ciudad Bolívar en Bogotá (Universidad Piloto de colombia)
[17] Liñán Salinas E 2008 Plan de seguridad informática en la Escuela Universitaria de Posgrado de la Universidad Nacional de Federico Villareal (Universidad Wiener)
[18] Carvajal Montealegre C J 2015 Extracción de reglas de clasificación sobre repositorio de incidentes de seguridad informática mediante programación genética Tecnura 19 109
[19] Azán Basallo Y, Martínez Sánchez N and Estrada Senti V 2016 La lógica difusa para la evaluación del riesgo de seguridad informática a bases de datos Rev. Control. Cibernética y Autom. Vol. III, 5
[20] Gil Vera V D and Gil Vera J C 2017 Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas Sci. Tech. 22
[21] Kaspersky 2021 La IA y el machine learning en la ciberseguridad: cómo determinarán el futuro.