Revisión de las técnicas de **inteligencia artificial aplicadas en seguridad informática**

Alisson B. Torres[1]
Corporación universitaria UNITEC
67151522@unitec.edu.co

Fredy G. Rendón[2]
Corporación universitaria UNITEC
67152518@unitec.edu.co

Juan F. Gutiérrez[3]
Corporación Universitaria UNITEC
Juan.gutierrez@unitec.edu.co

DOI: https://doi.org/10.21158/23823399.v7.n0.2019.2612

Fecha de recepción: 12 de marzo de 2020
Fecha de aprobación: 19 de junio de 2020

Cómo citar este artículo: Torres, A B.; Rendón, F. G.; Gutiérrez, J. F. (2019). Revisión de las técnicas de inteligencia artificial aplicadas en seguridad informática. *Revista Ontare, 8*, 97-115.
DOI: https://doi.org/10.21158/23823399.v7.n0.2019.2612

[1] Estudiante del programa de Ingeniería de Telecomunicaciones en la Corporación universitaria UNITEC.
ORCID: https://orcid.org/0000-0002-2503-4536
[2] Ingeniero en Telecomunicaciones, Técnico en mantenimiento de Hardware. **ORCID: https://orcid.org/0000-0002-1055-9532**
[3] Ingeniero electrónico de la Universidad Nacional de Colombia. Magister en Telecomunicaciones, de la Universidad Nacional de Colombia.
ORCID: https://orcid.org/0000-0001-8509-8075

RESUMEN

Gran parte de la vida de un ser humano está en constante interacción con sistemas que almacenan y transmiten información, con el fin de prestar algún servicio que optimice un proceso. El estudio de las diferentes políticas, herramientas y acciones que garanticen el buen uso de la información en sistemas informáticos —y, con frecuencia, en una organización— es por lo general el objetivo de la ciberseguridad. Las técnicas desarrolladas por la inteligencia artificial han empezado a aplicarse en una gran variedad de campos, en los cuales la identificación de patrones, el aprendizaje del entorno y la toma de decisiones son evidentemente necesarias. En este artículo se presenta una revisión bibliográfica de las diferentes técnicas de inteligencia artificial utilizadas en seguridad informática, con énfasis en sistemas de telecomunicaciones propiamente dichos. Los resultados obtenidos durante el estudio y la aplicabilidad de herramientas de control y prevención de comportamientos anómalos en sistemas de información basados en ciberseguridad han sido acogidos por las sociedades a nivel global, lo cual ha propiciado un crecimiento en la investigación y el desarrollo de inteligencias autónomas para el control y la manipulación de los datos, garantizando protección y almacenamiento. Por esto, ante la necesidad de contar con sistemas de almacenamiento seguros, se demuestra aquí la importancia de implementar técnicas basadas en inteligencia artificial, ya que es un mecanismo efectivo en la prevención y la reacción ante los inminentes riesgos, que permite cumplir con los lineamientos de la ciberseguridad: confidencialidad, integridad y disponibilidad.

Palabras clave: inteligencia artificial; seguridad informática; ciberseguridad; seguridad de redes; herramientas de seguridad informática; protección de datos.

Review of the artificial intelligence techniques **that are applied in computer security**

ABSTRACT

Much of a human being's life is in constant interaction with systems that store and transmit information to provide some service that optimizes a process. The study of the different policies, tools, and actions that ensure the proper use of the information in computer systems - and often in an organization - is generally the objective of cyber security. The techniques that have been developed by artificial intelligence are now being implemented in a wide variety of fields, in which identifying patterns, learning about the environment, and making decisions are a clear need. This article presents a literature review of the different artificial intelligence techniques that are used in computer security, specifically with emphasis on telecommunication systems. The results that were obtained during the study and the applicability of tools for the control and prevention of anomalous behavior in information systems that are based on cybersecurity have been accepted by societies at a global level, and this has led to a growth in the research and development of autonomous intelligence in view to control and manipulate data, guaranteeing protection and storage. For this reason, given the need for safe storage systems, this document demonstrates the importance of implementing techniques that are based on artificial intelligence, as they are an effective mechanism for preventing and reacting to imminent risks, which makes it possible to comply with cybersecurity guidelines: confidentiality, integrity, and availability.

Keywords: artificial intelligence; computer security; cybersecurity; network security; computer security tools; data protection.

Revisão das técnicas de inteligência artificial **aplicadas em segurança informática**

RESUMO

Grande parte da vida de um ser humano está em constante interação com sistemas que alojam e transmitem informação, com o fim de prestar algum serviço que otimize um processo. O estudo das diferentes políticas, ferramentas e ações que garantam o bom uso da informação em sistemas informáticos — e, com frequência, em uma organização — é em geral o objetivo da cibersegurança. As técnicas desenvolvidas pela inteligência artificial têm começado a aplicar-se numa grande variedade de campos, nos quais a identificação de padrões, a aprendizagem do meio e a tomada de decisões são evidentemente necessárias. Neste artigo apresenta-se uma revisão bibliográfica das diferentes técnicas de inteligência artificial utilizadas em segurança informática, com ênfase em sistemas de telecomunicações, propriamente ditos. Os resultados obtidos durante o estudo e a aplicabilidade de ferramentas de controle e prevenção de comportamentos anômalos em sistemas de informação baseados em cibersegurança têm sido acolhidos pelas sociedades a nível global, o que tem propiciado um crescimento na pesquisa e no desenvolvimento de inteligências autônomas para o controle e a manipulação dos dados, garantindo proteção e armazenamento. Por isto, ante a necessidade de contar com sistemas de armazenamento seguros, se demonstra aqui a importância de implementar técnicas baseadas em inteligência artificial, já que é um mecanismo efetivo na prevenção e na reação ante os iminentes riscos, o que permite cumprir com os delineamentos da cibersegurança: confidencialidade, integridade e disponibilidade.

Palavras-chave: inteligência artificial; segurança informática; cibersegurança; segurança de redes; ferramentas de segurança informática; proteção de dados.

Passage en revue des intelligences **artificielles spécialisées dans la sécurité informatique**

RÉSUMÉ

La majeure partie de la vie d'un être humain se passe en interaction constante avec des systèmes stockant et transmettant des informations permettant la fourniture de service d'optimisation de processus. La cybersécurité analyse les différentes politiques, outils et actions garantissant l'utilisation adéquate des informations des systèmes informatiques. Les techniques développées par l'intelligence artificielle ont ainsi commencé à être mises en place dans différents domaines d'activité où l'identification des modèles, l'apprentissage de l'environnement et la prise de décision sont d'une nécessité vitale. Cet article pase en revue les différents types d'intelligence artificielle utilisés en sécurité informatique mettant l'accent sur les systèmes de télécommunications eux-mêmes. Les résultats obtenus lors de l'investigation, l'applicabilité des outils de contrôle et de prévention des comportements anormaux dans les systèmes d'information basés sur la cybersécurité ont été salués par le secteur entrepreneurial, conduisant à une forte croissance de la recherche et développement en intelligence artificielle appliquée au contrôle et à la manipulation des données, tout en garantissant la protection de leur stockage. Pour cette raison, et compte tenu de la nécessité impérieuse de posséder des systèmes de stockage sécurisés, il est primordial de mettre en œuvre des techniques basées sur l'intelligence artificielle dans la mesure où il s'agit de mécanismes efficients de prévention et de réaction aux risques imminents tout en respectant les fondements de la cybersécurité á savoir la confidentialité, l'intégrité et la disponibilité.

Mots clés: intelligence artificielle; sécurité informatique; cyber-sécurité; sécurité Internet; outils de sécurité informatique; protection des données.

1. Introducción

Con el surgimiento de la humanidad aparece la información y con ella distintas formas destinadas a su almacenamiento. En la actualidad, la información es aún uno de los objetos con más valor para la colectividad y las organizaciones, en especial en la toma de decisiones (Rocha, 2011).

La seguridad de la información inició en el interior de organizaciones que incrementaron los procesos informatizados, en los cuales los administradores y analistas técnicos eran quienes buscaban las falencias de seguridad e intentaban solucionarlas de la manera que les fuese posible. No se contaba con un entendimiento claro acerca del tratamiento y la seguridad de la información, lo que ocasionaba que durante este desarrollo se aumentara la facilidad con la que se transmitía la información por medio de procesos automáticos que permitieron el uso de internet como plataforma de sus movimientos de información. De esta manera, se logró fluidez en las comunicaciones interpersonales, en las intersucursales, en las transacciones o en el flujo digital de todo tipo o nivel de importancia. No obstante, esto dejó muchos datos expuestos a terceros no autorizados en sus sistemas.

Lo anterior hizo notorio la falta de un servicio profesional que detectara movimientos inusuales, que atacara imitando al intruso y permitiera así evaluar de manera real las condiciones de seguridad para que, de existir brechas en el sistema, fuera posible solucionarlas de forma preventiva, reactiva y correctiva.

A diario las organizaciones se enfrentaban a todo tipo de amenazas relacionadas o dirigidas a la información. A partir de esto, muchos especialistas de seguridad informática estudiaron y practicaron métodos de intrusión en su información y fue entonces cuando empezaron a ofrecer sus servicios a las organizaciones a modo de proveedor o contratante.

A mediados de la década de los noventa del siglo XX, en conjunto con los inicios del *ecommerce,* se integraban poco a poco a la red pequeñas y medianas empresas —e incluso el público en general—, y aparecen malware mucho más sofisticados. Se publicaban nuevas técnicas de intrusión o explotación de vulnerabilidades y no existía una correcta capacitación sobre la administración de los servidores y su seguridad.

Debido a la ausencia de una plataforma educativa que formalizara la seguridad informática aparece entonces un comportamiento inusual con los recursos compartidos. Los jóvenes de todo el mundo entraban a internet a divertirse con los sistemas informáticos de sus países, engañando de esta manera a las centrales telefónicas y, al mismo tiempo, intercambiando información con sus pares del otro lado del mundo. De allí salen los mejores profesionales de seguridad para ese entonces, así como intrusos cibernéticos (Tori, 2008).

A nivel global, las tecnologías de la información y la comunicación se convierten en los motores de desarrollo y progreso, evidenciando en ellas mejoras en los procesos y las aplicaciones estratégicas de la sociedad. El mundo se convirtió de manera progresiva en protagonista de su propia evolución con el apoyo de internet y a medida que se desarrollaba era cada vez más necesaria la interacción con este, de modo que las personas se convierten en generadoras de contenido virtual. Este progreso presenta nuevas perspectivas y, así como en la vida real se deben brindar seguridades a los activos adquiridos, también deben proporcionarse a la información que se administra de manera digital (Rocha, 2011).

Tabla 1. Línea de tiempo seguridad informática

LÍNEA DE TIEMPO SEGURIDAD INFORMÁTICA		
AÑO	**EVENTO**	**DESCRIPCIÓN**
1981	Se generan los primeros correos SPAM	IBM con el primer servidor de lista, generó los primeros spams, las guerras de listas y los primeros trolls.
1983	Primer virus Informático	Surge en seminario de Seguridad Informática, realizado en la Universidad de California del Sur.

1988	Primeros ataques	Permiten conocer las vulnerabilidades de la RED.
1993	Nuevos métodos *Hackig*	*Sniffing* (rastreo) y *spoofing* (suplantación).
1998	SQL IJECTION	Consultas y comandos a través de SQL
1999	Virus Melisa	Primer virus en Windows, se propagaba a través de correos electrónicos.
2001	Proyecto OWASP	Un código abierto dedicado a determinar y combatir las causas que hacen que el *sofware* sea inseguro.
2005	Implementación normas ISO-IEC	Contiene las mejores prácticas en seguridad de la información para los sistemas de gestión.
2008	Virus Conficker	Intrusión en la red con afectación y control sobre los sistemas operativos.
2010	Espia Stuxnet	Roba información y reprograma sistemas, ocultando los cambios realizados en este.
2011	SLAAC	Ataque IPV6, de autoconfiguración de direcciones sin estado.

Fuente. Elaboración propia.

Dadas las nuevas amenazas para los datos, que han evolucionado de manera paralela con el constante crecimiento de la tecnología y todo lo que concierne a la seguridad informática, se empieza a definir una necesaria búsqueda dirigida a mitigar los riesgos y reducir la probabilidad de que estos se materialicen, ocupándose hasta hoy de generar buenas prácticas destinadas a garantizar sistemas de información seguros y confiables, con base en la implementación del uso de la inteligencia artificial como generadora de herramientas de control tanto a nivel de *hardware* como de *software*; pues existen intrusos que pueden perjudicar el sistema operativo, las aplicaciones instaladas o, simplemente, tomar el control del equipo afectado.

Se establecen políticas o parámetros que garantizaron el libre y abierto acceso a la información, tecnologías seguras utilizadas a fin de proteger los activos de cualquier organización, lo cual la Unión Internacional de Telecomunicaciones o UIT entiende como «ciberseguridad» (2016). La ciberseguridad garantiza que se almacenen y mantengan las propiedades

de seguridad de los datos en una organización, permite que el acceso a los sistemas no sea vulnerable a ataques, intrusiones o indisponibilidades presentes por el ciberentorno que afecten la integridad y confidencialidad de los datos (UIT, 2010).

En la actualidad se ha buscado la manera de encontrar alternativas de protección y refuerzo del ciberentorno, en especial mediante el uso de tecnologías avanzadas, autónomas y con dominios técnicos y cognitivos con los que se logren solucionar problemas en tiempos reducidos; se habla, entonces, del uso de la inteligencia artificial o IA, concebida como un insumo crucial para el progreso y la robustez de la ciberseguridad.

La inteligencia artificial estudia y analiza el comportamiento humano en aspectos de comprensión, percepción, resolución de problemas y toma de decisiones, lo cual, al replicarse en un computador, permite que se creen aplicaciones de IA que, principalmente, simulan actividades intelectuales del hombre. Bajo estos parámetros, los sistemas de IA tratan datos numéricos con algoritmos heurísticos o clásicos que permiten abordar problemas sin solución.

Tabla 2. Línea de tiempo inteligencia artificial

LÍNEA DE TIEMPO INTELIGENCIA ARTIFICIAL		
AÑO	**EVENTO**	**DESCRIPCIÓN**
1936	Turing	Base a la noción de algoritmo. Teoría de los autómatas y calculabilidad.
1943	Primer computador	Condujo al verdadero nacimiento de la IA, ENIAC maquina de programa grabado.
1950	Test de Turing	Ejercicio comparativo en respuesta de la acción humana vs. máquina.
1956	Nacimiento IA	Aparece por primera vez el término IA.
1970	Heurística	Enumeración inteligente de soluciones a través de reglas optativas.
1975	Boom IA	Se establecen las bases de la IA. Representación de conocimientos, sistemas expertos y robótica.

1980	IA y Economía	Crecimiento notable de las investigaciones en países industrializados.
1990	Comunicación Hombre-Máquina	Interfaces inteligentes, interfaces multiagentes y la IA distribuida.
2000	El futuro	Computación cuántica.

Fuente. Elaboración propia.

En el presente artículo se realiza una revisión bibliográfica general sobre la ciberseguridad, planteando, finalmente, cómo este campo de estudio se relaciona con el uso y la aplicabilidad de la inteligencia artificial, basados en las diferentes normas que la regulan. De esta manera, este trabajo pretende ofrecer una inducción bibliográfica para la investigación, la cual guíe el estudio de la inteligencia artificial y su integración en la seguridad informática, así como la presentación de las normas relevantes para el momento de empelar estrategias de ciberseguridad.

2. Normatividad

La Asamblea Mundial de Normalización de las Telecomunicaciones o AMNT define en su resolución la situación actual frente a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación (TIC) y la contribución del UIT-T para la solidez de esta.

De igual forma, sugiere que todas las comisiones de estudio del UIT-T continúen con la evaluación de las recomendaciones existentes, en especial, las definidas sobre señalización y protocolos de telecomunicaciones, refiriéndose a la necesidad de fortalecer la protección frente a grupos malintencionados e interferir destructivamente en su implementación en la infraestructura mundial de información y las telecomunicaciones, en el propósito de que se elaboren recomendaciones sobre nuevas estrategias de seguridad (UIT, 2008).

La normatividad UIT-T X.1205 plantea una definición de ciberseguridad utilizada por los diferentes entes de control y la normatividad en el sector de las telecomunicaciones. Realiza una sustentación frente a las diversas amenazas de seguridad que vulneran la estabilidad en una organización y sobre cuál es la afectación a las capas de la red que provocan inestabilidad y brechas para posibles riesgos de intrusión y ataque por parte de organismos externos.

Adicionalmente, esta normatividad da a conocer los principios y los sistemas de protección a la red al tratar las estrategias de gestión de riesgos, así como resalta de manera continua la importancia de la utilización de herramientas robustas y eficaces dentro de una organización.

Las normas de seguridad cibernética determinarán por la forma en que se aplican cuándo y cómo los infractores deben rendir cuentas. Esto significa que es fundamental que los gobiernos sean proactivos y colaboradores a la hora de contribuir y evaluar las normas de seguridad cibernética, así como determinar cómo hacer que sean efectivas y aplicables (Dignum, 2017).

3. Inteligencia artificial y la seguridad de la información

La inteligencia artificial, en la actualidad, afecta en distintas medidas la cotidianidad del mundo, pues su implementación modifica de diferentes maneras nuestro entorno. A fin de asegurar que los sistemas desarrollados se mantengan con los valores humanos se requieren métodos que incorporen principios éticos y que aborden preocupaciones sociales. El crecimiento tecnológico y los avances científicos cada vez alteran más la forma de vida y reorganizan los grupos de valores, así como generan nuevos productos y servicios, lo cual hace que estos avances se trabajen desde varios frentes.

Los líderes empresariales entienden las ventajas competitivas actuales y cómo mejorarlas con las tecnologías emergentes; los responsables políticos y las sociedades empiezan a tener una comprensión más clara de cómo la tecnología da forma a la economía global, y sobre cómo invertir en nuevas

formas de educación e infraestructura, pues este cambio disruptivo afecta las ventajas comparativas. Las entidades legislativas y reguladoras gestionan nuevas capacidades biológicas y la protección de derechos, así como la privacidad de los ciudadanos; los gobiernos crean, entonces, un entorno social en el cual las personas siguen prosperando incluso cuando todos estos avances afectan sus vidas (Manyika et al., 2013). Son estos impactos los medidos durante el desarrollo del potencial sistematizado que es la IA.

Por otra parte, la seguridad informática cuenta con tres principios fundamentales: confidencialidad, integridad y disponibilidad. Estos sustentan y son la base de cualquier sistema que se implemente, pues a partir de esto la seguridad informática se vuelve indispensable para cualquier tipo de organización, dado que frente a muchos casos no es posible estimar el valor de la información (Pfleeger y Pfleeger, 2003). En este sentido, la inteligencia artificial ha tenido una gran participación en la implementación para diferentes áreas de seguridad informática, como, por ejemplo, su utilización en redes mediante la detección de intrusos y bloqueos de correos no deseados, análisis forense, antivirus, etc., lo cual ha permitido que sistemas generales operen de manera automática, adaptativa y proactiva (Cohen, 2007).

Los sistemas expertos —basados en inteligencia artificial— manejan problemas mediante un modelo computacional de razonamiento humano, sin embargo, la mayoría de estos sistemas se someten a continuos mantenimientos con el fin de obtener un buen desempeño (Weiss y Kulikowski, 1991). El desarrollo de estos sistemas inteligentes se realiza con base en el aprendizaje automático y la teoría conexionista, ya que ambos aplican conjuntos de datos sintéticos que poseen porcentajes de ruido de características y utilizan diferentes técnicas representativas, como, por ejemplo, un análisis discriminante en línea, un algoritmo de clasificación de árbol o una herramienta de red neuronal. Así, se estudian en diversas formas los datos, previamente analizados, de modo que se obtienen resultados que confirman la aplicabilidad del mismo análisis para un conjunto de datos del mundo real (Nolan, s. f.).

3.1 Técnicas

Estos sistemas aplicados con base en inteligencia artificial han pasado por estudios previos en los que se realiza una comparación del aprendizaje a partir de algoritmos (Nolan, 2002). Así, por ejemplo, Shavlik Mooney y Towell (1991) estudiaron la diferencia entre el algoritmo de aprendizaje inductivo 1D3, el perceptrón —algoritmo de red neuronal básica— y el aprendizaje neural de propagación hacia atrás; en este estudio utilizaron cinco conjuntos de datos del mundo real y analizaron el rendimiento cuando se insertó ruido en estos.

Weiss y Kapouelas (1989) realizaron un estudio comparativo de los métodos de clasificación de reconocimiento de patrones estadísticos, redes neuronales y aprendizaje automático para cuatro conjuntos de datos. En estos se enfatizó en el análisis del rendimiento resultante de las redes neuronales (Nolan, 2002).

La magnitud de los sistemas mencionados cuenta con datos que se encuentran expuestos a distintos ataques producidos por vulnerabilidades del mismo entorno, pues es allí donde las alternativas de la inteligencia artificial y la evolución de esta presentan mejoras a la seguridad informática por medio de la detección de intrusos, virus o cualquier hecho malintencionado sobre las redes computacionales (Hernández, De la Rosa y Rodríguez, 2013).

En todos los casos, la inteligencia artificial busca la optimización y detección más eficaz de intrusiones, razón por la cual son variadas las técnicas de IA que se han implementado en sistemas informáticos, lo que ha permitido reducir el esfuerzo humano por construir sistemas detectores de intrusos y mejorar el rendimiento de estos (Frank, 1994).

Los sistemas de detección de intrusos (IDS) cuentan con aplicaciones de inteligencia artificial en diferentes áreas. Se ha desarrollado un enfoque utilizando razonamiento basado en casos que miden de forma indirecta el ataque de un cibercriminal. Los resultados revelaron que el razonamiento basado en casos tiene el potencial de utilizarse en investigaciones forenses y de seguridad al identificar el atacante.

Se plantea la implementación de un sistema basado en casos (SBC) con un IDS Short que contiene un sistema de reglas, en el cual se proponen las limitaciones con las que cuenta el propio sistema, como, por ejemplo, las alertas que brinda, y cómo el SBC puede utilizarse a la manera de una sofisticada técnica que mejora las dificultades del sistema de seguridad y permite así la detección de los comportamientos anómalos, resúmenes y la detección de escaneos (Hernández *et al.*, 2013).

Entre las técnicas más conocidas de inteligencia artificial aplicadas a los IDS se encuentran la máquina de vectores de soporte (SVM), redes neuronales artificiales (ANN), regresión multivariada adaptativa utilizando *splines* (MARS) y programas genéticos lineales (LGP).

La SVM utiliza algoritmos para la calificación de textos mediante modelos de aprendizaje automático, como, por ejemplo, el correo *spam*, uno de los más serios problemas de seguridad en razón a su capacidad de consumo de los recursos que requiere al ser procesado. Este método presenta una de las alternativas más eficientes y aprobadas para la solución de este problema mediante el uso de las técnicas de inteligencia artificial. Se han realizado análisis de la complejidad para la detección de estos problemas y se estudian varias técnicas funcionales sobre la observación. La SVM detecta daños sobre la categorización de textos, lo que permite realizar un filtrado de *spam*. Así, *email classification using examples* o ECUE utiliza un sistema de razonamiento basado en casos, indexados por semántica y latente —razonamiento basado en instancias— que permite una calificación del mensaje (Méndez, Fdez-Riverola, Díaz y Corchado, 2007).

Por otra parte, Heroic es una herramienta de ciberseguridad basada en inteligencia artificial. Se encarga de la protección contra cualquier tipo de amenaza utilizando una plataforma descentralizada contra vulnerabilidades, en especial las provenientes de P2P o *peer to peer*. Esta aplicación basada en *blockchain* permite mayor protección de la información consignada, además, almacena una cantidad de registros referentes a un «bloque» vinculándose con una serie de bloques en orden estratégico, de modo que genera un código único, visto como huella digital (Heroic.com., 2018). Así protege la información consignada contra el robo de identidad y monitoriza la web a fin

de detectar y destruir las amenazas en tiempo real, disponiendo de una línea profesional conocida como EPIC o de protección empresarial de información y credenciales, la cual descubre, remedia y previene vulnerabilidades de terceros que involucran credenciales a proveedores o clientes que acceden a una organización.

Las métricas de seguridad actuales, normalmente, están enfocadas en medir vulnerabilidades, individuales y no muchas consideran sus efectos combinados. Este modelo presenta la aplicación de redes dinámicas bayesianas, las cuales llevan a cabo un conocimiento aplicable a un sistema estándar de puntuaciones CVSS (*Common Vulnerability Scoring System*), que trabaja suponiendo que las amenazas pueden poseer una vulnerabilidad que varía con el tiempo y con mayor velocidad por ser las redes un entorno dinámico.

Dentro de los múltiples sistemas de redes que existen, las bayesianas se utilizan en este caso con el propósito de modelar los pasos de un ataque potencial atómico a la red. Cada uno de los vértices representa una propiedad única de violación del estado de seguridad y a cada arista le corresponde una explotación de una o más vulnerabilidades expuestas; el peso de estas indica la probabilidad de explotar una vulnerabilidad (Liu y Man, 2005).

Algunas organizaciones utilizan como estrategia para fortalecer la seguridad la conformación de los centros de operaciones de ciberseguridad o CSOC, los cuales ayudan a prevenir —por medio de pruebas de seguridad y revisión de controles de seguridad—, a detectar —monitoreo continuo y hallazgo de amenazas—, a responder —gestión, contención y recuperación efectiva— y a predecir futuras brechas de seguridad. Aplicaciones como B-Secure, LogRhythm e Invotecsa, entre otras, utilizan esta estrategia con la finalidad de aplicarse en organizaciones basadas en inteligencia artificial como insumo para robustecer la ciberseguridad tanto a nivel local como en el ciberentorno (B-Secure, s.f.).

¿Llegará el día en el que las aplicaciones tengan la autonomía para tomar decisiones? Si bien este es uno de los cuestionamientos que se generan frente a la adaptación de herramientas basadas en inteligencia artificial, son más las ventajas reflejadas en el funcionamiento y la seguridad que implica

el manejo de todo tipo de datos y los riesgos frente a la posibilidad de un descontrol en la administración de los sistemas informáticos para cualquier aplicación.

Mantener un sistema operativo seguro requiere del manejo de buenas prácticas para la seguridad de la información, a su vez, una implementación de aplicaciones de IA que cumplan los lineamientos necesarios dirigidos a la detección, reacción y prevención de riesgos que pretenden afectar en diferentes medidas los datos y al usuario dueño de estos, de manera que impacten de forma global las organizaciones. Por lo anterior, es evidente la necesidad de abordar con mayor énfasis la investigación y el estudio de la inteligencia artificial y su aplicabilidad en la seguridad informática, en el propósito de la mejora de procesos informáticos.

4. Conclusiones

El crecimiento de los datos, la facilidad del acceso a la información y la evolución tecnológica han sido los factores elementales para el desarrollo de sistemas que sean capaces de almacenar, analizar y decidir —a partir de conjuntos de datos propiamente agrupados que determinan comportamientos— estados y entornos, generando así aprendizaje automático y programado. Los resultados obtenidos durante el estudio y la aplicabilidad de herramientas de control y prevención de comportamientos anómalos en sistemas de información basados en ciberseguridad han sido acogidos por las sociedades a nivel global, lo cual ha permitido la maximización en la investigación y el desarrollo de inteligencias autónomas que hacen posible el control y la manipulación de los datos, garantizando su protección y almacenamiento.

El tratamiento de la información de cualquier nivel supone el uso de lineamientos normativos establecidos por los entes de control pertinentes, a nivel mundial y nacional, lo cual permite de manera reglamentaria la implementación de nuevas tecnologías que utilicen inteligencia artificial a fin de controlar la seguridad de los datos. Estos lineamientos se encuentran en continua interpretación debido a la evolución que exige la ciberseguridad.

Debido a la cantidad de información digital que actualmente se genera es necesario contar con sistemas de almacenamiento seguros que garanticen la integridad, la calidad y la trasmisión de los datos, de lo contrario se exponen a ataques o intrusiones presentes en el entorno cibernético, lo cual ocasiona indisponibilidad y afectación. En razón a lo anterior surge la necesidad de implementar técnicas basadas en inteligencia artificial para la mejora continua en materia de seguridad de la información, pues es un mecanismo efectivo en la prevención y la reacción ante los inminentes riesgos, que permite cumplir con los lineamientos de la ciberseguridad: confidencialidad, integridad y disponibilidad.

Referencias

B-Secure. (2019). *Centro de Operaciones de Ciberseguridad-CSOC*. Recuperado de https://bit.ly/34roQli

Cohen, E. (2007). *Information and beyond: Part I.* California: Informing Science Press.

Dignum, V. (2017). Responsible artificial intelligence: designing AI for human values. *ITU Journal: ICT Discoveries, Special Issue*(1), 1-8. Recuperado de https://bit.ly/31qpnSo

Frank, J. (1994). Artificial intelligence and intrusion detection: current and future directions. Texto presentado en 17th *National Computer Security Conference.* Baltimore, Maryland, EE.UU., 22-23 de octubre.

Hernández, A.; De la Rosa, J.; Rodríguez, O. (2013). Aplicación de técnicas de inteligencia artificial en la seguridad informática: un estudio. *Revista Iberoamericana de Inteligencia Artificial*, 16(51), 65-72. DOI: https://doi.org/10.4114/intartif.vol16iss51

Heroic.com. (Febrero de 2018). *Cybersecurity powered by artificial intelligence and the blockchain.* Recuperado de https://bit.ly/2EdwYLG

Liu, Y.; Man, H. (2005). Network vulnerability assessment using Bayesian networks. E*n Proceedings of SPIE.* 5812, 61-70. DOI: https://doi.org/10.1117/12.604240

Manyika, J.; Chui, M.; Bughin, J.; Dobbs, R.; Bisson, P.; Marrs, A. (2013). *Disruptive technologies: advances that will transform life, business, and the global economy.* San Francisco: McKinsey Global Institute.

Méndez, J. R.; Fdez-Riverola, F.; Díaz, F.; Corchado, J. M. (2007). Sistemas inteligentes para la detección y filtrado de correo spam: una revisión. *Inteligencia Artificial, Revista Iberoamericana de Inteligencia Artificial,* 11(34), 63-81.

Nolan, J. R. (2002). *Computer systems that learn: an empirical study of effect of noise on the performance of three classification methods. Expert Syst. Appl.*, 23, 39-47. DOI: https://doi.org/10.1016/S0957-4174(02)00026-X

Pfleeger; C. P.; Pfleeger, S. P. (2003). *Security in computing* (4a ed.). Nueva Jersey: Prentice Hall.

Rocha, C. (2011). La seguridad informática. *Revista Ciencia EMI,* 4(5), 26-33. DOI: https://doi.org/10.29076/issn.2528-7737vol4iss5.2011pp26-33p

Shavlik, J. W.; Mooney, R. J.; Towell, G. G. (1991). Symbolic and neural learning algorithms: an experimental comparison. *Machine Learning*, 6(2), 111-144. DOI: https://doi.org/10.1007/BF00114160

Tori, C. (2008). *Hachking ético.* Rosario: Autoedición. Recuperado de https://bit.ly/3glzY5n

UIT (2008). *Aspectos generales de la ciberseguridad. ITU X.1205.* Recuperado de https://bit.ly/2EsRiIG

UIT (Unión Internacional de Telecomunicaciones). (2010). *Ciberseguridad.*

UIT (Unión Internacional de Telecomunicaciones). (2016). *Resolución 50 – Ciberseguridad.* Hammamet, Túnez. Recuperado de https://bit.ly/31p1lr5

Weiss, S. M.; Kapouleas, I. (1989). An empirical comparison of pattern recognition, neural nets, and machine learning classification methods. En Sridharan, N. (Ed.) IJCAI-89: *Proceedings of the Eleventh International Joint Conference on Artificial Intelligence.* (781-787). San Mateo, CA: Morgan Kaufman.

Weiss, S.; Kulikowski, C. (1991). *Computer systems that learn.* California: Morgan Kauman.