ESTADO ACTUAL DE LA CIBERSEGURIDAD APLICADA A SISTEMAS DEFENSIVOS Y OFENSIVOS A PARTIR DE INTELIGENCIA ARTIFICIAL

LEONARDO ENRIQUE CASALLAS RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

ESTADO ACTUAL DE LA CIBERSEGURIDAD APLICADA A SISTEMAS DEFENSIVOS Y OFENSIVOS A PARTIR DE INTELIGENCIA ARTIFICIAL

LEONARDO ENRIQUE CASALLAS RODRIGUEZ

Trabajo de Monografía para optar por el título:
Especialista en Seguridad Informática

Director de Monografía:
Ing. EDGAR MAURICIO LOPEZ ROJAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

DEDICATORIA

Este trabajo es dedicado todas y cada una de las personas que a través de su apoyo me han servido de impulso para poder llegar a culminarlo. Son mi esposa, mis hijos, mis padres y en muchos casos mis amigos los que me hacen ver que muchas cosas son posibles, es solo un paso más para alcanzar mis metas y desarrollarme tanto intelectualmente como personalmente.

CONTENIDO

LISTA DE FIGURAS

GLOSARIO

ACTIVO: Un activo es un recurso con valor que alguien posee con la intención de que genere un beneficio futuro.
AGENTE: Es un programa sencillo que actúa para otro software o para un usuario.
AMENAZA: Hace referencia al riesgo que un objeto o circunstancia pueda infligir daño contra un sistema.
APRENDIZAJE: Proceso de adquisición del conocimiento de algo por medio de la experiencia, en especial de los conocimientos necesarios para aprender algún arte u oficio.
ARTIFICIAL: Que no ha sido hecho por la naturaleza sino por parte del ser humano.
AUTÓNOMO: Que trabaja por sí mismo, tiene la propiedad de tomar decisiones.
BOT: Es un programa que tiene la habilidad de realizar tareas de manera automática.
CHATBOT: Se refiere a bot especializados en mantener conversaciones.
CIBER-ATAQUE: Es cualquier tipo de acción dirigida dañar o tomar control de un sistema informático.
DISPOSITIVO: Es un objeto que hace parte de un sistema más complejo y que cumple una función específica dentro de ese sistema.
ENTORNO: Conjunto de circunstancias que rodean una cosa o persona y que influyen en su estado o desarrollo.
EMULAR: Se refiere a imitar un comportamiento procurando que se realice de igual manera.
ENTRADA: Se refiere a la información que se recibe y sirve como estímulo de un sistema.
ÉTICA: Conjunto de valores que definen el comportamiento humano en sociedad.
HUMANOIDE: Se considera que tiene un aspecto físico muy parecido al de un ser humano.
INFORMACIÓN: Es un conjunto organizado de datos procesado que tiene un significado y que es relevante para el sistema que lo contiene o hace uso de él.
MÁQUINA: Es un objeto que se compone por un conjunto de piezas que es usada para cumplir con una tarea determinada.
PERÍMETRO: Se refiere a la delimitación de la línea defensa contra posibles amenazas.
PROBLEMA: Es el planteamiento de una pregunta por medio de la cual se busca hallar una respuesta a partir de algunos datos conocidos.
PROCESAMIENTO: Es la habilidad de poder acumular, manipular datos por medio de tareas generando información relevante para un sistema informático.
ROBOT: Se trata de una entidad ya sea virtual o física diseñada para cumplir una tarea específica de manera automática.
SALIDA: Se refiere respuesta entregada por parte de un sistema a un estímulo recibido.

VULNERABILIDAD: Es el riesgo que un sistema u objeto tiene de sufrir daños ante amenazas físicas o virtuales.

RESUMEN

En este estudio monográfico se realiza una contextualización sobre la inteligencia artificial sus principales conceptos y como actúa el aprendizaje sobre los sistemas que se basan en esta tecnología, esto se realiza basándose en la documentación que se recopila a través de fuentes documentales y los repositorios de información públicos. Se explica también su interacción con la seguridad informática y como los conceptos propios de la inteligencia artificial son aplicados en el desarrollo de aplicaciones en la rama de la ciberseguridad haciendo énfasis en los avances de los sistemas defensivos y ofensivos que son utilizados para proteger o vulnerar la información de las personas y organizaciones.

PALABRAS CLAVE: APRENDIZAJE AUTOMÁTICO, CIBERSEGURIDAD, HACKER ÉTICO, INTELIGENCIA ARTIFICIAL, SEGURIDAD INFORMÁTICA.

ABSTRACT

In this monographic study has present a contextualization on artificial intelligence, the main concepts and how learning acts on the systems that are based on this technology, this is done based on the documentation that is collected through documentary sources and information public repositories. It also explains their interaction with computer security and how the concepts of artificial intelligence are applied in the development of applications in the cybersecurity line, the advances of defensive and offensive systems that are used to protect or violate information of people and organizations.

KEY WORDS: MACHINE LEARNING, CIBERSECURITY, ETHICAL HACKER, ARTIFICIAL INTELIGENCE, INFORMATICS SECURITY.

1. INTRODUCCIÓN

En la actualidad se tienen gran cantidad de amenazas contra los activos de información de una empresa y los ataques que se tienen contra estos activos son cada vez más sofisticados tales como malware, comandos de control de dispositivos, ataques de denegación de servicios distribuidos, suplantación entre otros.

De igual manera los sistemas de defensa se apoyan de nuevas y mejores técnicas para poder realizar la protección de su perímetro, una de estas son las basadas en inteligencia artificial que ha incursionado en este campo al igual que muchos otros con características que se basan en su capacidad de adaptarse al entorno, buscar soluciones de maneras no convencionales a los problemas planteados y apoyado por la capacidad de procesamiento de datos actual.

En este trabajo se busca dar un vistazo a los conceptos de la inteligencia artificial de esta manera generando un marco conceptual, los métodos más comunes utilizados en donde se soporta con un marco teórico, su aplicación a la ciberseguridad y el estado actual y futuro con las implicaciones éticas que el uso de esta tecnología puede presentar.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Realizar un estudio monográfico que describa el estado actual del uso de la inteligencia artificial en técnicas ofensivas y defensivas de ciberseguridad.

2.2 OBJETIVOS ESPECÍFICOS

- Recopilar información relacionada con el uso de la inteligencia artificial en técnicas defensivas y ofensivas como base referencial para el estudio monográfico.

- Analizar la información sobre las técnicas defensivas y ofensivas que utilizan la inteligencia artificial y sus aplicaciones enfocadas a la ciberseguridad.

- Realizar un análisis de las herramientas posicionadas en el mercado que utilizan inteligencia artificial para cumplir con las labores de protección del perímetro de seguridad informática.

- Examinar desde el punto de vista ético el papel del personal involucrado en las tareas de ciberseguridad y las decisiones que pueden tomar los sistemas que utilizan inteligencia artificial teniendo en cuenta su impacto tanto en la actualidad como en un futuro.

3 PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

Teniendo en cuenta que la inteligencia artificial ha hecho que las máquinas desarrollen habilidades que emulen la manera en que aprenden los seres humanos, estas técnicas han hecho que se pueda hablar de sistemas que aprenden de forma muy aproximada a un ser humano y que lleguen a tomar decisiones muy adecuadas para determinar qué medidas tomar ante eventos cambiantes en su entorno. Con respecto a lo anteriormente se plantean las siguientes incertidumbres a resolver en el curso de la investigación:

¿Cómo las técnicas defensivas y ofensivas de Ciberseguridad son influenciadas por la inteligencia artificial y la manera en que se realizan su aprendizaje?
¿Se encuentran aplicaciones de la inteligencia artificial en la Ciberseguridad que sirven para el funcionamiento de técnicas de ofensivas y defensivas?
¿Las principales herramientas que se utilizan para la protección perimetral de los sistemas de información utilizan aprendizaje basado en inteligencia artificial?
¿Es éticamente correcto involucrar herramientas que realizan aprendizaje y toman decisiones de manera autónoma sobre herramientas que protegen datos sensibles de las personas y las organizaciones?

3.2 JUSTIFICACIÓN

La importancia de la ciberseguridad y los mecanismos que se utilizan para la defensa del perímetro de seguridad de una empresa hace que las técnicas defensivas tengan que responder ante las posibles amenazas que se generan en su entorno y reaccionar ante los estímulos. Esto hace que la inteligencia artificial y su manera de aprender ante los eventos y tomar decisiones se hace cada vez más relevante.

También a su vez cuando hablamos de las técnicas que son ofensivas y que son encargadas de vulnerar un sistema de seguridad pueden llegar a utilizar esta tecnología para poder analizar las debilidades de una red entrando en un perímetro de seguridad e ir reaccionando a los posibles escenarios de defensa que se le planteen. En la actualidad las técnicas empleadas en ciberseguridad emplean conceptos de inteligencia artificial haciendo que juegue un papel importante en el futuro ya que gracias a su uso pueden se impulsar sistemas de predicción y prevención de ciber-ataques o protección de la información; por esto es que se vuelve indispensable recopilar información sobre este ámbito e investigaciones generadas a nivel mundial para tener claridad de la influencia que puede generar.

Por tanto, es de relevancia generar un documento que recopile la información que se ha generado sobre las investigaciones a nivel mundial sobre la inteligencia

artificial generando al lector un panorama de esta tecnología aplicada a la ciberseguridad, tanto en seguridad informática defensiva como ofensiva.

Finalizando con las implicaciones éticas y sobre el panorama futuro de la seguridad informática siendo influenciada por la inteligencia artificial.

4. DESARROLLO DEL PROYECTO

En el desarrollo de este documento se presenta la siguiente distribución para poder desarrollar el desglose de los puntos que conllevan a la resolución de los objetivos planteados en el proyecto:

- Se realiza una explicación de los conceptos de inteligencia artificial como contextualización del alcance de la inteligencia artificial, estos y los conceptos tanto de técnicas defensivas como de ofensivas en seguridad informática son la documentación que apoya el marco conceptual y teórico de la monografía, mostrando también las posibles aplicaciones de la inteligencia artificial en distintos campos.

- Posteriormente se realiza una recopilación de información y se presentan proyecto en los que se ha implementado la inteligencia artificial en ciberseguridad tanto para el desarrollo de técnicas ofensivas, como defensivas y los métodos utilizados por la inteligencia artificial.

- Para poder realizar el análisis de la aplicación de la inteligencia artificial a ciberseguridad se validan las limitaciones de su uso, las investigaciones desarrolladas en el sector y su panorama actual.

- Se realiza una explicación sobre el funcionamiento las herramientas posicionadas en el mercado inteligencia artificial para cumplir con las labores de protección del perímetro de seguridad informática.

- Y por último se da una visión de la ética y la inteligencia artificial dando un panorama en donde se presentan las posibles implicaciones éticas que se pueden presentar en su uso en el campo de la ciberseguridad.

5. MARCO CONCEPTUAL Y TEORICO

En este punto se realiza la explicación del cuerpo de la monografía en el cual se desarrolla el marco conceptual presentando los principales conceptos usados en la inteligencia artificial y como apoyo al marco teórico se genera un contexto global de la teoría que rodea este campo, las técnicas que se pueden utilizar y su aplicación en distintas áreas.

La monografía se apoya en distintas fuentes bibliográficas de repositorios de información públicos que han sido referenciados para brindar un soporte a los resultados y conclusiones que se presentan al finalizar el documento.

5.1 CONCEPTOS DE INTELIGENCIA ARTIFICIAL

Cuando se habla de inteligencia artificial se debe tener en cuenta que no se tiene una definición unificada por parte de los investigadores en este campo según lo dice Luis Amador: “La inteligencia en si misma suele ser un concepto mal definido y poco comprendido.”[1] Y es este hecho de que la inteligencia humana no sea haya definido el que hace que la inteligencia artificial sea un punto en el que se deben analizar varios parámetros para tener un idea clara sobre su alcance.

Se puede decir que la inteligencia artificial se relaciona con el estudio de los procesos cognitivos básicos según Carretero Díaz tales como[2]:

- Aprendizaje
- Memorización
- Solución de problemas
- Inferencia y deducción lógica
- Toma de decisiones
- Deducciones lógicas
- Comprensión del lenguaje natural

Estos procesos cognitivos básicos generan la diferencia que se tiene en un sistema de inteligencia artificial y que puede hacer que se considere que una máquina puede emular comportamientos humanos inteligentes teniendo la posibilidad de adaptarse al entorno generando lo que se considera una respuesta inteligente, teniendo la capacidad de tomar decisiones no por medio de un árbol predeterminado que es el utilizado en la programación convencional realizada por esquemas numéricos sino

[1] AMADOR, Luis. Inteligencia artificial y sistemas expertos. [En línea]. Universidad de Córdoba. 1996. Disponible en http://helvia.uco.es/bitstream/handle/10396/6938/Luis%20Amador_Inteligencia%20artificial_1996-1.pdf?sequence=1. p.16

[2] CARRETERO DIAZ, L.E. (1989), Sistemas Expertos. Aprendizaje e incertidumbre, Ed. Paraninfo, Madrid. Citado por, AMADOR, Op. Cit., p.17.

con un esquema adaptable basada en símbolos y conceptos que puede llegar a resolver problemas con alta incertidumbre y complejidad.

Por ende, se puede decir que un sistema se puede considerar inteligente según Juan Romero, Carlos Dafonte, Angel Gómez, Fernando Penousal en su libro Inteligencia Artificial y Computación Avanzada cuando: “es capaz de llevar a cabo tareas que, si fuesen realizadas por un humano, se diría de este que es inteligente. Dentro de las ciencias de la computación, la rama de la I.A. se basa en intentar dotar al funcionamiento de las aplicaciones informáticas de un comportamiento inteligente similar al humano para la toma de decisiones.”[3]

Se debe tener en cuenta que la inteligencia artificial no es una ciencia nueva y se ha hablado de este concepto desde 1950 por Alan Turing en sus libros maquinaria de computación e inteligencia y en el juego de la imitación en donde plantea la idea de máquinas inteligentes y que aprenden, incluso desarrollo un test para comprobar si un sistema puede llamarse inteligente comparándolo con un ser humano o sí es capaz de engañarlo[4]. Esto nos lleva a un punto que para el presente estudio monográfico se tiene en cuenta y es que la inteligencia artificial se enfoca en dos grandes ramas de estudio el desarrollo de la maquinas inteligentes sobre las cuales se puede realizar el test anteriormente mencionado y en métodos para resolver problemas complejos basándose en grandes cantidades de datos como se mencionó anteriormente siendo este el punto de relevancia para el caso de la ciberseguridad.

5.2 TÉCNICAS ADAPTATIVAS[5]

Estas técnicas son utilizadas para resolver problemas que tienen un entorno cambiante teniendo la capacidad de reprogramarse si es necesario. A continuación se describen las más utilizadas:

- Redes neuronales artificiales: Se basa en el funcionamiento que tiene un sistema nervioso, es basado en programas sencillos que generan múltiples conexiones entre ellas como lo hacen las neuronas en el modelo neurológico del cerebro humano. Se compone de varias capas compuestas por neuronas artificiales que obtienen un mayor peso cada vez que son utilizadas, lo que genera más peso al mejor camino entre las entradas y una salida al problema planteado. El autoaprendizaje que se obtiene por el refuerzo de las

[3] ROMERO, Juan & DAFONTE, Carlos & GOMEZ, Ángel & PENOUSAL, Fernando. Inteligencia artificial y computación avanzada. [En línea]. Fundación Alfredo Brañas Santiago de Compostela. 2007. Disponible en https://cdv.dei.uc.pt/wp-content/uploads/2014/03/ms07.pdf. p.7.
[4] ALFONSECA, Manuel. ¿BASTA LA PRUEBA DE TURING PARA DEFINIR LA “INTELIGENCIA ARTIFICIAL”?. [En línea]. Universidad de Navarra. 2014. Disponible en https://dadun.unav.edu/handle/10171/37284. p. 130
[5] ROMERO, Juan & DAFONTE, Carlos & GOMEZ, Ángel & PENOUSAL, Fernando. Inteligencia artificial y computación avanzada. [En línea]. Fundación Alfredo Brañas Santiago de Compostela. 2007. Disponible en https://cdv.dei.uc.pt/wp-content/uploads/2014/03/ms07.pdf. p.14.

conexiones y por la salida de cada neurona artificial genera una red cambiante entre las capas de la red neuronal.

- Algoritmos Genéticos: Esta basado en las teorías evolucionistas en donde se genera un algoritmo que simula la selección natural que tiene objetivo que prevalezca los individuos que se encuentren mejor adaptados al entorno, descartando a los demás. Es utilizado en problemas con gran superficie de solución y poca información en donde se generan respuestas inicialmente aleatorias que van mutando y generando cruces entre ellas para obtener individuos más fuertes (una mejor solución al problema planteado).

- Programación genética: Es una evolución de los algoritmos genéticos ya mencionados que mantiene en donde la selección natural sigue siendo la base de su funcionamiento. Pero se basa en un algoritmo construido por medio de un árbol similar a la programación convencional mientras que en el método anterior al no ser fijado el camino al problema a resolver se debía validar los resultados codificando y decodificando basados en los resultados obtenidos.

Se tienen otras técnicas adaptivas a continuación se explican algunas de estas:

- Hardware evolutivo: A partir de componentes simples una máquina o robot está en la capacidad de adaptarse al entorno en tiempo real reconfigurando su arquitectura.

- Sistema de aprendizaje con clasificadores en donde se muestran múltiples entradas y salidas correctas aprendiendo el comportamiento que se requiere.

- Simulación de una colonia de hormigas: Como lo dice su nombre se inspira en las colonias de hormigas y su funcionamiento en donde juntas tienen un comportamiento complejo, pero los agentes simples que representan a las hormigas se tienen que unir para llegar a un objetivo en común. Y como en el mundo biológico se refuerza el comportamiento a través de feromonas que hacen que prevalezca el camino más corto al objetivo planteado.

- Coevolución: Se tienen dos comunidades que interactúan y dependen entre ellas simulando presas y depredadores implicando que si uno de los dos evoluciona el otro se ve obligado a hacerlo para poder obtener los beneficios de la otra comunidad.

- Sistemas inmunes artificiales: Es un sistema diseñado para detectar comportamientos que no son normales y buscar una solución se utiliza en problemas de optimización y búsqueda.

5.3 APLICACIÓN DE LA INTELIGENCIA ARTIFICIAL

A continuación, se pueden observar algunos proyectos que se presentan en distintos campos que se han desarrollado utilizando técnicas de inteligencia artificial para su desarrollo:

- TAY[6]: Es un chatbot que al ser alimentado por las entradas de Twitter generadas por parte de personas que interactuaban tenía aprendizaje de las mismas, el resultado que se obtuvo fue el desarrollo una personalidad con comportamientos éticos no apropiados con aversión por el ser humano.

- Sophia[7]: Es un robot con forma humanoide que intenta mantener conversaciones inteligentes, realiza la imitación de gestos humanos e incluso ha obtenido ciudadanía Saudí. En este caso el sistema de inteligencia artificial aprende conversando todos los días con sus programadores para poder generar los esquemas necesarios durante el aprendizaje, e incluso ha visitado una universidad en Medellín Colombia[8].

- Apoyo a la diagnosis médica[9]: Se propone un modelamiento del método de diagnóstico para mejorar lo acertado del mismo, el antecedente es que dos médicos pueden llegar a dar diagnósticos distintos para un mismo caso. Se requiere de médicos con más experiencia en el campo para mejorar el tiempo en el que se acierta con la patología del paciente. Como resultado se obtuvo una herramienta base para apoyo teniendo en cuenta que se requieren datos de gran calidad para poder cargar el sistema y un seguimiento muy exhaustivo validando el comportamiento para evitar falsos diagnósticos.

- Ontología de fuentes para el mantenimiento de software[10]: Se realizó un sistema para gestión del conocimiento para apoyo al personal de mantenimiento en las búsquedas de las fuentes apropiadas reduciendo el

[6] BBC MUNDO. Tay, la robot racista y xenófoba de Microsoft. [En línea]. BBC mundo. 2016. Disponible en https://www.bbc.com/mundo/noticias/2016/03/160325_tecnologia_microsoft_tay_bot_adolescente_inteligencia_artificial_racista_xenofoba_lb

[7] BBC MUNDO. Sophia, la robot que tiene más derechos que las mujeres en Arabia Saudita. [En línea]. BBC mundo. 2016. Disponible en https://www.bbc.com/mundo/noticias-41803576

[8] EL TIEMPO. Esto dijo la robot humanoide, Sophia, tras su llegada a Medellín. [En línea]. https://www.eltiempo.com/colombia/medellin/sophia-la-robot-humanoide-llego-a-medellin-249650

[9] FERNANDEZ, Antonio & MANZANO María, GONZALEZ, Enrique & TOME, Sergio., Una Perspectiva de la Inteligencia Artificial en su 50 Aniversario Sergio, Universidad de Castilla [En línea]. Albacete. 2004. Disponible en: http://www.info-ab.uclm.es/personal/AntonioFdez/download/papers/conference/cmpi2006-volumeI.pdf . p. 79.

[10] Ibid., p. 79. p. 118.

problema de conocimiento en la organización, la información se divide en varios tipos de información: del sistema, del usuario, técnica y organizacional.

- Críticos de arte artificiales[11]: Comúnmente las piezas de arte se consideran objetos que realizados con creatividad por tanto el desarrollo de un sistema computacional que tenga la capacidad de valorar estos aspectos es un avance interesante en el campo de la inteligencia artificial. Para poder entrenar al evaluador se requieren cientos de datos de piezas de arte valoradas por expertos se basa específicamente en dos criterios el autor y el estilo. El sistema se probó con piezas musicales logrando Bach y Beethoven logrando caracterizarlos y siendo útil de cara a poder identificar los estilos de los autores siendo un punto de partida para la creación de artista artificial.
- Camiones autónomos circulan por Arizona[12]: Desde finales del 2017 los camiones de Uber circulan por Arizona realizando entregas, estos vehículos recorren largas distancias de manera autónoma pero acompañados por un operador humado en el asiento del conductor y al llegar cerca del punto de partida se transporta la mercancía un tramo por parte de un camión con un conductor. En Arizona se presta el servicio a través de Advanced Technologies Group y los partidarios consideran que los beneficios son muy altos llegando en un futuro a reducir accidentes, llegando a sitios de difícil acceso y realizar viajes largos.

- Reconocimiento y exploración de objetos basados en imágenes[13]: Se realiza por medio de deep learning que es método basado en redes neuronales para la detección de objetos por medio de un robot móvil que analiza los espacios, iluminación y alternativas de caminos que son actividades intuitivas para un ser humano.

  Se realiza un entrenamiento del robot con todos los parámetros al mismo tiempo para generar un resultado completo en el aprendizaje validándolos como un único escenario, no como dimensiones distintas. El resultado permitió que el robot navegara muy bien en la simulación, pero al pasar al robot real los resultados no fueron los esperados según se concluyó por datos errados en el aprendizaje.

[11] Ibid., p. 231
[12] EL TIEMPO. Los camiones sin conductor de Uber ya circulan en EE. UU. [En línea]. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/camiones-autonomos-de-uber-ya-circulan-en-estados-unidos-191396
[13] CONTRERAS, Javier., Aplicación de Deep Learning en róbotica móvil para exploración y reconocimiento de objetos basados en imagenes, Universidad de los Andes. [En línea]. Bogotá. 2015. Disponible en https://biblioteca.uniandes.edu.co/visor_de_tesis/web/?SessionID=L1Rlc2lzMjAxNjk5LzgxNTQucGRm

- Técnicas de planificación inteligente para cursos virtuales[14]: Teniendo en cuenta que cada estudiante aprende a su propio ritmo el propósito de este sistema es el desarrollo de un método adaptable que evalúa los logros y el perfil psicopedagógico para construir un curso personalizado. Como resultado se identifica que es necesario tanto el pedagogo, como el programador del sistema adaptativo para llegar a la construcción de un ambiente apropiado para el estudiante permitiendo gran variedad de posibilidades en el curso que se presenta y el método de aprendizaje.
  Actualmente la plataforma se encuentra en proceso de aprendizaje en la plataforma GAIA de la Universidad Nacional de Manizales con el objetivo de afinar el proceso adaptativo y la implementación de módulos de aprendizaje.

5.4 TÉCNICAS DEFENSIVAS EN SEGURIDAD INFORMÁTICA

Para entender el termino seguridad defensiva se tiene que hablar de un concepto que se llama defensa en profundidad[15] y es un concepto utilizado en la táctica militar que consiste en que el enemigo no luche con una fuerte y única defensa, se debe buscar desgastarlo al pasar por múltiples capas y que renuncie en su intención de ataque. El éxito de este tipo de defensa es diferenciar las funciones y que cada línea cumpla con una función especializada, haciendo perder el impulso inicial del ataque.

En la seguridad informática y en particular para el alcance de este numeral la seguridad defensiva se basa en el mismo principio que es generar una seria de barreras de entrada para que un atacante pueda llegar los sistemas de información a continuación se explican los niveles bajo el concepto de Andreu & Pérez[16]:

- Políticas y procedimientos: En este nivel se definen políticas a nivel de seguridad de la información que pueden llegar a mitigar grandes riesgos por intervención humana. Es de gran importancia tener un apoyo por parte de la alta gerencia de la empresa ya que sin su apoyo puede llegar a generar gran cantidad de información sin tenerla en cuenta por la organización.

- Seguridad física y del entorno: Definir controles de acceso a los dispositivos en los que reposa la información debe ser acorde a la importancia de la misma, se deben subir las restricciones de acceso a medida que crezca su valoración como activo de información. Y se deben tener en cuenta f la protección contra factores externos y ambientales.

[14] DUQUE, Néstor & OVALLE, Demetrio & JIMENEZ, Jovani, Modelo Adaptativo para Cursos Virtuales basado en Técnicas de Planificación Inteligente. Universidad Nacional de Colombia. [EN línea]. Medellín. 2007. Disponible en https://revistas.unal.edu.co/index.php/avances/article/view/9715/10245

[15] MOGOLLON, Oscar. Defensa en Profundidad - defensa elástica. Hablemos de Táctica. [En línea]. 2012. Disponible en: http://hablemosdetactica.blogspot.com/2012/08/defensa-en-profundidad-defensa-elastica.html

[16] ANDREU, M. G., & PÉREZ, G. P. P. (2004). Seguridad informática para empresas y particulares. España: McGraw-Hill España. p. 25-29.

- Defensa Perimetral: En este nivel se define un perímetro a proteger por parte del esquema de seguridad planteado con respecto a un entorno y su contacto con redes tanto privadas como públicas. La definición correcta de este perímetro que hace que sean correctamente protegidos los activos de información. El perímetro es distinto dependiendo del elemento al que se refiera, no es lo mismo proteger un servidor que proteger un pc de escritorio.

- Defensa de Equipos: En este nivel se tienen tres puntos clave en la protección de equipos que corresponde a la administración de parches y las actualizaciones, el cierre de servicios no utilizados como primer paso para cierre de vulnerabilidades y un antivirus activo y actualizado.

- Defensa de Aplicaciones: En este nivel se tienen herramientas específicas para poder proteger cada tipo de servicio que se tiene expuesto. En este punto podemos hablar de firewall especializados tales como firewall para correo, bases de datos, páginas Web por citar algunos.

- Defensa de Datos: Aquí se tiene en cuenta los parámetros de autenticación del usuario y el cifrado de los datos a nivel de usuario final.

Como se puede identificar en la explicación de los niveles cuando se habla de seguridad ofensiva se habla de la generación un entorno construido alrededor de la información a proteger formando capas de seguridad a su alrededor.

5.5 TÉCNICAS OFENSIVAS EN SEGURIDAD INFORMÁTICA

En la actualidad se tienen gran cantidad de sistemas de información alrededor del mundo, el hecho de que la información no se encuentre localizada y restringida por fronteras físicas hace que se tenga un concepto de globalización que hace la información pueda ser vulnerada y cobra más relevante el término de hacker[17] como el individuo que vulnera los sistemas informáticos sin destruir la información y con el ánimo de aprender siendo por el contrario el término cracker[18] el que se encarga de cometer los delitos informáticos con sus conocimientos.

Teniendo en cuenta estos aspectos se utiliza el termino hacker ético[19] para nombrar al hacker que utiliza las herramientas informáticas para encontrar vulnerabilidades de los sistemas y tomar las medidas necesarias para contrarrestar los posibles

[17] Bustamante R (2014) SEGURIDAD EN REDES. Universidad Autónoma de Hidalgo. [En línea]. Disponible en: de:http://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad%20en%20redes.pdf. p. 27

[18] Ibid., p. 29

[19] BETANCOURT BARRETO, Jhonny Jordan. Introducción al hacker ético. [En línea]. Universidad Piloto de Colombia. 2014. Disponible en http://repository.unipiloto.edu.co/handle/20.500.12277/2844

ataques que puedan ocurrir. Esto nos lleva a hablar de técnicas ofensivas[20] en seguridad informática, al referirse a este término se hace acotación a los procedimientos para proteger sistemas evidenciando sus vulnerabilidades, y son las técnicas ofensivas las que se basan en el poder realizar una exploración de estos con la finalidad de explotar sus falencias, evidenciarlas y corregirlas. El objetivo es llevar a la práctica los conocimientos adquiridos y que son los mismos usados por parte de los delincuentes para corromper, robar o espiar los sistemas de información para el beneficio de la organización que es propietaria de estos.

Este proceso y análisis tiene varias fases que cumple con el objetivo de entregar un informe adecuado de lo encontrado, estas son el reconocimiento, el escaneo, el ganar acceso, el mantener el acceso, y realizar borrar las huellas para no dejar evidencias[21].

Sin embargo, antes de poder iniciar con el mismo se debe tener consentimiento por parte del dueño de la información sea una persona natural o una organización quienes autorizan a estos hackers éticos para poder realizar este tipo de pruebas. Se debe tener claro este punto ya que el ignorarlo se incurre en una mala práctica que es considerada en Colombia como un delito y que es regulado y penalizado por la Ley contra delitos informáticos 1273 de 2009[22].

[20] GUTIERREZ, Fernando, Laboratorio de Seguridad Informática con Kali Linux. Universidad de Valladolid. [En línea]. http://uvadoc.uva.es/handle/10324/5141.
[21] BETANCOURT BARRETO, Jhonny Jordan. Introducción al hacker ético. [En línea]. Universidad Piloto de Colombia. 2014. Disponible en http://repository.unipiloto.edu.co/handle/20.500.12277/2844
[22] Congreso de Colombia. (2009). Ley 1273 de 2009. Recuperado a partir de: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

6. INTELIGENCIA ARTIFICIAL APLICADA A LA SEGURIDAD INFORMÁTICA.

En este capítulo se aborda información que explica como la inteligencia artificial se puede aplicar a la ciberseguridad, sus limitaciones y las investigaciones que se han realizado. Posteriormente se identifica el panorama actual de la ciberseguridad y como se puede llegar a ver afectado en un futuro el uso de la inteligencia artificial dentro de esquemas defensivos y ofensivos. Finalizando con un punto que tiene gran relevancia en sistemas autónomos que son las implicaciones éticas de su uso.

6.2 METODOS DE INTELIGENCIA ARTIFICIAL EN CIBERSEGURIDAD

La inteligencia artificial presenta varios métodos por medio de los cuales se realizan problemas de alta complejidad tales como inteligencia computacional, redes neuronales, agentes inteligentes, sistemas inmunes artificiales, aprendizaje automático, minería de datos, reconocimiento de patrones, lógica difusa y heurística. Cada uno de estos métodos permite diseñar sistemas que trabajen de manera autónoma y que puedan realimentarse generando la posibilidad de gestionar, setear sus propias configuraciones, realizar diagnósticos y generar soluciones sin intervención humana. A continuación, se da una breve explicación de algunos de los métodos que son utilizados, algunos de ellos ya fueron explicados anteriormente, pero se toma como énfasis la seguridad informática en este caso:

- Redes Neuronales Artificiales: Las redes neuronales artificiales simulan el comportamiento de un sistema nervioso de orden biológico y trabajan bajo esa estructura de correlación buscando trabajar bajo estructuras relativamente simples que facilitan predicción de ataques, clasificación en entornos cambiantes y complejos en un perímetro de seguridad.

- Agentes inteligentes: Cada agente funciona de manera autónoma y se comunica con los demás agentes compartiendo datos, los agentes trabajan cooperando entre sí para llegar a la respuesta más adecuada para resolver la situación a resolver que para el caso de ciberseguridad es un ataque.

- Sistemas inmunes artificiales: Este sistema trabaja como un sistema inmune de un ser vivo reaccionando ante agentes patógenos externos, estos generan anticuerpos que tienen parámetros propios y que reaccionan según el tipo de ataque recibido generando la cantidad de anticuerpos para contrarrestar la infección.

6.3 LIMITACIÓN DEL USO DE INTELIGENCIA ARTIFICIAL EN CIBERSEGURIDAD[23]

La inteligencia artificial genera grandes beneficios a la ciberseguridad brindando la posibilidad de poder obtener solución a problemas donde el entorno es cambiante y se requiere adaptabilidad generando la posibilidad de detectar ataques de día cero que son los que no han sido detectados con anterioridad, se deben tener en cuenta algunas desventajas que tiene el uso de ésta. Que se citan a continuación:

- Debido a que aprenden del entorno se debe tener en cuenta que se comportan de manera diferente en un entorno que en otro, no se puede extrapolar los resultados del aprendizaje si el ambiente es muy diferente. E incluso si las condiciones cambian en su entorno pueden detectar falsos positivos y por tanto se debe realizar una actualización de la base de conocimientos del sistema.

- Se requieren datos de entrada de gran calidad en la etapa de aprendizaje del sistema corriendo con el riesgo de generar falsos positivos al igual que en el ítem anterior. Se requiere una etapa de entrenamiento exhaustivo mostrando el comportamiento normal de la red con todos los casos de uso que sean necesarios.

- Debido a que el sistema actúa de acuerdo al entorno generando un comportamiento ante una supuesta situación, puede ser que un atacante detecta cómo se comporta el sistema y este sea vulnerado.

6.4 INVESTIGACIONES REALIZADAS USANDO INTELIGENCIA ARTIFICIAL EN CIBERSEGURIDAD

En este caso en específico cuando hablamos de la utilización de inteligencia artificial en la ciberseguridad se encuentran múltiples investigaciones y aplicaciones algunas de las cuales se citan a continuación:

- Detección de aplicaciones maliciosas en sistemas Android[24]: En esta investigación se buscó realizar la clasificación de las aplicaciones con la finalidad de poder detectar malware en dispositivos Android. Se basa en la aplicación de la teoría de sistema inmune artificial y redes neuronales generando un programa que actúa como un antivirus, diferenciándose de los

[23] DILEK, Selma & CAKIR, Hüseyin & AIDIN, Mustafa., Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. [En línea]. 2015. Disponible en https://arxiv.org/ftp/arxiv/papers/1502/1502.03552.pdf

[24] BEZOBRAZOV, Sergei & SACHENKO Anatoly & KOMAR Myroslav, RUBANAU Vladimir, The methods of artificial intelligence for malicious applications detection in Android OS. [En línea]. 2017., Disponible en http://www.computingonline.net/computing/article/view/851

demás por la capacidad de autoadaptarse y la detección de amenazas sobre aplicaciones maliciosas generando el bloqueo de las mismas.

Este sistema tiene varios componentes generando un esquema que se basa en varios módulos que son los de detección y clasificación, de intrusiones, seguridad en la nube y criptografía. Este proyecto tiene relevancia debido a la proliferación de amenazas en la red para los dispositivos móviles tales como el malware de minería de datos que ha aumentado en 450% según datos de Trendmicro[25].

Su estructura se compone de detectores inmunes llamados anticuerpos que tienen un periodo de vida en el que pasa por las etapas de creación, entrenamiento, selección generando anticuerpos inmaduros que son entrenados si en la etapa de aprendizaje se detecta que uno de estos objetos detecta aplicaciones benignas como maliciosas es descartado.

- Filtrando eventos de seguridad mediante deep learning[26]: En este caso se trabajan con sistemas de correlación de eventos y su valor se encuentra en la gran cantidad de eventos que se pueden generar en una empresa siendo un parámetro que va en aumento a medida que esta crece llegando a incluso valores de millones de eventos que pueden traducirse en cientos de miles de alarmas que se requieren procesar por parte de los analistas de SOC (Security Operation Center).

  Para la prueba el sistema fue alimentado con una base pública sobre detección de anomalías y se realiza un cargue de los mismos para entrenamiento del sistema. De manera adicional se utilizan dos bases de datos mejoradas para realizar las pruebas.

  El método utilizado de inteligencia artificial es Aprendizaje profundo (Deep Learning) mediante dos etapas pre entrenamiento en donde se genera un bucle para fijar los datos base para esta etapa los datos que se utilizan son datos de comportamientos normales. Posteriormente se genera un ajuste fino que es un entrenamiento supervisado para lograr buenos datos de salida para este caso se utilizan datos normales y anómalos. Se obtuvo como resultado identificación de los datos anómalos se debe tener en cuenta que debido al alcance de la prueba no se realizó la clasificación de los tipos de ataques.

[25] TRENDMICRO, Mobile Threat LandScape. [En línea].2018. Disponible en: https://www.trendmicro.com/vinfo/hk-en/security/research-and-analysis/threat-reports/roundup/2018-mobile-threat-landscape

[26] FERRADO, Leandro & CUENCA, Matías. Filtrando eventos de seguridad en forma conservativa mediante deep learning. [En línea]. Cordoba. 2016. Disponible en http://hdl.handle.net/10915/56884

- Utilización de las técnicas Deep Learning para el desarrollo de métodos criptográficos[27]: En este caso se valida la utilización de Deep Learning para el uso de criptografía adversaria que se basa en variación del contenido incluyendo datos adicionales ocultos, se utiliza una arquitectura llamada GAN (Generative Adversarial Network) que consiste en dos redes neuronales que se encuentran compitiendo por llegar al objetivo para este caso la competencia es entre un generador de ruido en la imagen que busca engañar y un detector de las imágenes erradas finalizando la competencia al estabilizar el sistema por medio de un punto de equilibrio.

  En este caso se tiene un esquema en donde dos actores generan un esquema de cifrado seguro y se tiene un atacante que es el que ayuda a entrenar con el nuevo sistema cifrado. El atacante y los usuarios compiten llegando a obtener un esquema de cifrado que no entiende el atacante siendo exitoso el desarrollo de las pruebas.

- Proyecto de utilización de distintas de distintas técnicas que utilizan inteligencia artificial en detección de intrusos[28]: Para este caso se realiza un análisis estadístico basado en análisis de varianza para poder comparar distintos métodos de inteligencia artificial como teorías bayesianas, aprendizaje automático, algoritmos genéticos, sistemas inmunes artifíciales, redes neuronales, agentes multicapa, modelos de Markov siendo utilizadas en Sistemas de detección de intrusos (IDS).

  Para el caso de los IDS se basa en que su estrategia de análisis trabaja bajo dos métodos esencialmente, el primero es conocido como detección de uso indebido[29] que se basa en una base de firmas predeterminada y sobre la cual se realiza una exhaustiva comparación generando una alarma en caso de encontrar coincidencia. En este método se debe tener en cuenta que la tasa de detección es muy alta sobre las firmas conocidas pero no se tiene forma de detectar cosas que no se encuentren dentro de su base de firmas conocidas esto no implica que no se actualice esta base ya que si corresponde a un fabricante reconocido el sistema actualiza su base de firmas regularmente buscando que sean identificadas todas amenazas nuevas con el menor tiempo posible. Sin embargo, la desventaja sigue siendo las amenazas nuevas no categorizadas dentro de la base firmas.

[27] MUÑOZ, Alfonso & ESCRIBANO, Jose. Criptografía adversaria usando deep learning limitaciones y oportunidades. BBVA. [En línea]. Madrid. 2015. Disponible en https://www.bbvanexttechnologies.com/wp-content/uploads/2018/07/amunoz-jescribano-criptograf%C3%ADa-adversaria-recsi-2018.pdf

[28] TRIBAK, Hind. Análisis estadístico de distintas técnicas de inteligencia artificial en detección de intrusos. [En línea]. Universidad de Granada. 2012. Disponible en https://hera.ugr.es/tesisugr/20758340.pdf

[29] Ibid., p 24.

El segundo método es basado en anomalías[30] este se basa en métodos de inteligencia artificial que se basan en el comportamiento y detectar las variaciones en el basándose en patrones de comportamiento, patrones de conducto dependiendo de los datos de entrada que se alimenten en el sistema y que corresponde a comportamiento normal, de redes, usuarios, registros de auditoría de equipos, procesos, entre otros. Este método tiene como ventaja que ante variación en el comportamiento de la red es alertado pero su principal desventaja es que cualquier cambio es detectado como un falso positivo ya que un cambio no necesariamente es un acto ilícito o como falsos negativos cuando se cargan correctamente los datos y dentro de las estadísticas de comportamiento ya se tiene un incluido un comportamiento ilícito.

En este caso los resultados obtenidos evidencian que una gran base de firmas es necesaria y es el método más efectivo, las herramientas que utilizan inteligencia artificial son un apoyo para detección de amenazas día cero.

- Entornos de sistemas multiagente y ciberfísicos en la ciberdefensa[31]: Para el caso de ciberdefensa han cobrado relevancia dos tipos de sistemas, el multiagente formado por agentes inteligentes que basados en inteligencia artificial buscan una reacción automática ante las amenazas que se presenten este sistema toma las decisiones que se deben tomar son correspondientes a esta capa y se basa en tres principios capacidad de reaccionar a su entorno, capacidad de ejercer una actividad anticipándose a la situación y la capacidad de que cada agente forme parte de un equipo enfocado con un objetivo en específico.

  El otro sistema es el ciberfísico que se basa en principios en donde se recibe la información por parte de componentes que son los sensores, los actuadores y los controladores basados en interacción máquina hombre. En donde los sensores[32] toman datos medidos por medio de componentes físicos presentándose de manera que un dato se pueda utilizar como una entrada a otro componente. Y los otros componentes son los actuadores[33] que tienen la posibilidad de realizar cambios a nivel físico dependiendo de la entrada que reciban esto forman una entidad independiente, pero se coloca otro actor en estos sistemas que son los controladores que se tienen a

[30] TRIBAK, Hind. Análisis estadístico de distintas técnicas de inteligencia artificial en detección de intrusos. [En línea]. Universidad de Granada. 2012. Disponible en https://hera.ugr.es/tesisugr/20758340.pdf, p. 25.
[31] COZ FERNANDEZ, José Ramon & PASTOR PEREZ, Vicente José. Entornos de Sistemas Multiagente y Ciber-Físicos en la Ciberdefensa. [En línea]. 2014. Disponible en https://www.researchgate.net/profile/Vicente_Pastor_Perez/publication/265345858_Entornos_de_Sistemas_Multiagente_y_CiberFisicos_en_la_Ciberdefensa/links/54404fe10cf2be1758cfffe6.pdf
[32] CORONA, Leonel & ABARCA, Griselda & MARES Jesús. Sensores y actuadores, Instituto Politécnico Nacional. [En línea]. México. 2014. Disponible en https://books.google.es/books?hl=es&lr=&id=wMm3BgAAQBAJ&oi=fnd&pg=PP1&dq=actuadores+y+sensores&ots=6N6rjw95ZB&sig=dz7A0wlhea27Er81kmGKraNjUjA#v=onepage&q=actuadores%20y%20sensores&f=false p. 17.
[33] Ibid., p. 26.

distancia y reciben los datos de comportamiento para tomar acciones sobre el comportamiento del sistema.

Esta interacción entre los componentes de multiagente o ciberinteligentes y los ciberfísicos forman un esquema a tener en cuenta en el desarrollo de la ciberdefensa ya que tienen la capacidad de tomar decisiones siendo alimentados por el entorno físico y afectando este también de acuerdo a los estímulos recibidos.

- Identificación de individuos mediante señales de voz[34]: Se realiza la utilización de biometría por medio de un método basado en comportamiento para la detección de las señales de voz y comparación entre los dos patrones el almacenado y con el que se compara al realizar la entrada al sistema. Se utilizan dos sistemas uno de reconocimiento y otro de generación de voz que aprenden simultáneamente correlacionando las dos señales la original y copia desfasada.

  Con este trabajo se encontró la viabilidad de realizar la autenticación por medio de patrones de voz como elemento para autenticación biométrica, se debe tener en cuenta los parámetros de entrada en la etapa de entrenamiento y la definición de los umbrales para la correcta identificación del patrón de voz.

- Sistema en la nube de detección de incidentes[35]: Este sistema de detección de incidentes en la nube trabaja con agentes autónomos inteligentes proporcionando flexibilidad en el monitoreo de eventos ya que no se requiere la compra de ninguna infraestructura.

- Detección de Spam[36]: Se realizó un análisis por medio de técnicas de inteligencia artificial para la detección de spam obteniendo resultados con bajas tasas de falsos positivos y falsos negativos por encima de otras plataformas con esquemas tradicionales.

- Manejo de intrusiones para la tecnología basada en la Internet de las cosas[37]: Se realizaron pruebas introduciendo mecanismo de Inteligencias artificial en un entorno de Internet de las cosas (IoT), simulando esquemas de sistemas que realizaban autoadaptación y autoaprendizaje por medio de la adaptación dinámica al entorno mostrando un modelo que ofrece una efectiva forma de contrarrestar los ataques que se presentan hacía este tipo de tecnología.

[34] ROJAS, Jaime., Sistema de autenticación de individuos mediante señales de voz usando métodos de inteligencia artificial (VoID), Universidad de los Andes [En línea]. 2005. Disponible en http://hdl.handle.net/1992/22019

[35] DILEK, Selma & CAKIR, Hüseyin & AIDIN, Mustafa., Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. [En línea]. 2015. Disponible en https://arxiv.org/ftp/arxiv/papers/1502/1502.03552.pdf, p. 7.
[36] Ibid., p. 7.
[37] Ibid., p. 9.

Las investigaciones anteriormente mencionadas se basan en técnicas defensivas y a continuación se muestran las basadas en técnicas ofensivas:

- Mejorar el desempeño de las técnicas utilizadas en los test de penetración[38]: En un test de penetración se requiere realizar una previa planeación y utilizar en muchas ocasiones herramientas de costos elevados. En contraste a esto la propuesta es utilizar una técnica de inteligencia artificial basada en el modelo de decisiones de Markov se debe tener en cuenta que este método no es escalable y que se define para realizar a ataques a una máquina en específico debido a que la red en gran escala genera una estructura que no es estable por la cantidad de opciones a evaluar, sin embargo el beneficio que se presenta es la automatización de las pruebas haciendo que el conocimiento requerido sea menor al requerido en pruebas de penetración normales.

  La herramienta que se desarrolló con este procedimiento permite realizar pruebas reduciendo la incertidumbre realizando mezcla de escaneos de exploit tal y como lo haría un Hacker real, el setear se basa en la probabilidad de encontrar vulnerabilidades. La diferencia que esto presenta es que el algoritmo tiene la posibilidad de actualizarse según requiera para poder obtener el objetivo.

- Detección de vulnerabilidades de red[39]: Se realizó una simulación de un modelo de evaluación que valida la situación de una red a nivel de su esquema de seguridad de manera cuantitativa y en tiempo real, el estudio proporciono datos para apoyar en los ajustes de las medidas defensa.

6.5 PANORAMA DE LA CIBERSEGURIDAD EN LA ACTUALIDAD

A continuación, se muestran algunos datos con la finalidad de poder mostrar un panorama actual de la ciberseguridad y dar un contexto sobre los posibles avances que se pueden tener en este campo. Por tanto, según los datos estadísticos que se publicaron por parte de IBM el 19% de los ataques son a las entidades financieras, el 13 % a la industria transportadora, 12% a las empresas de servicios profesionales, 11% a las empresas de Retail y manufactura. También se puede observar que el 45% de las vulnerabilidades explotadas han sido ya anunciadas por

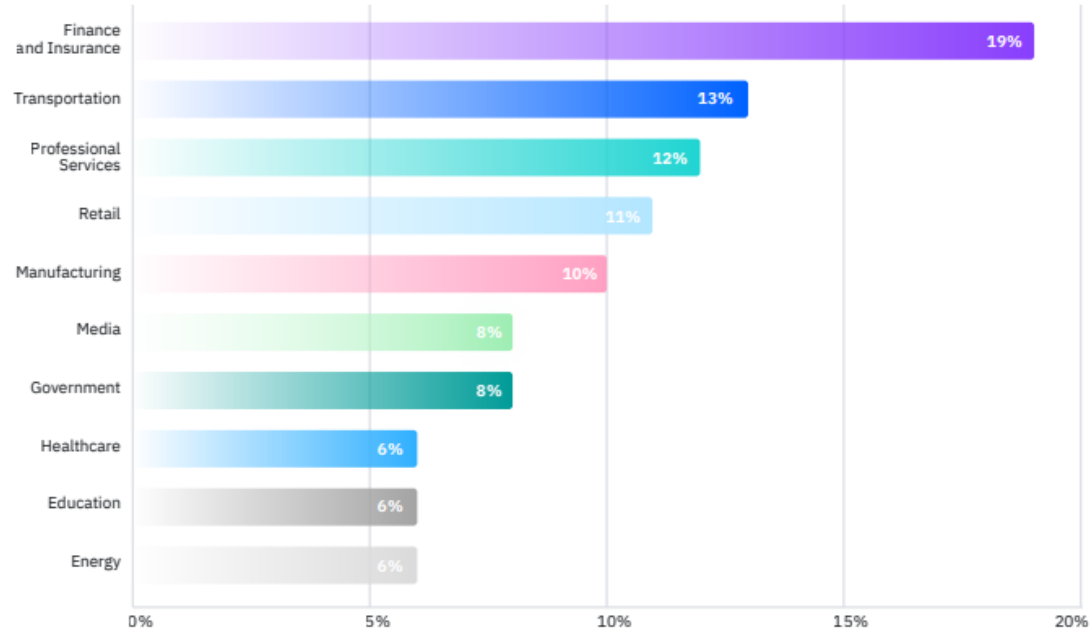
[38] SARRAUTE, Carlos & BUFFET, Olivier & HOFFMANN Jörg, POMDPs Make Better Hackers: Accounting for Uncertainty in Penetration Testing. [En línea]. AAAI Publications, Twenty-Sixth AAAI Conference on Artificial Intelligence. 2012., Disponible en https://www.aaai.org/ocs/index.php/AAAI/AAAI12/paper/viewPaper/4996

[39] DILEK, Selma & CAKIR, Hüseyin & AIDIN, Mustafa., Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. [En línea]. 2015. Disponible en https://arxiv.org/ftp/arxiv/papers/1502/1502.03552.pdf, p. 7.

el grupo de investigaciones X-Force de IBM que realiza inteligencia de amenazas[40]. Se entiende como inteligencia de amenazas "el conocimiento basado en la evidencia, incluyendo información de contexto, las implicaciones, y demás variables que giran en torno a una amenaza, peligro existente o emergente sobre los activos, y que se puede utilizar para la toma de decisiones" [41] según la definición dada por Gartner que ayuda a contextualizar sobre el tipo de labor que realizan los grupos de investigación de cada fabricante de tecnología de seguridad que constantemente están analizando el entorno de ataques a nivel mundial para mejorar el desempeño de sus productos.

A partir de este estudio también podemos evidenciar que hay muchos sectores a nivel mundial que se encuentran en este momento afectados por ataques informáticos. Estos datos se pueden observar en la siguiente gráfica tomada del reporte de IBM X-force[42]:

Figura 1 Ataques informáticos por tipo de sector económico



Fuente: IBM. X-force Threat intelligence index. 2019. [En línea].2019. Tomado de: https://xforceintelligenceindex.mybluemix.net/

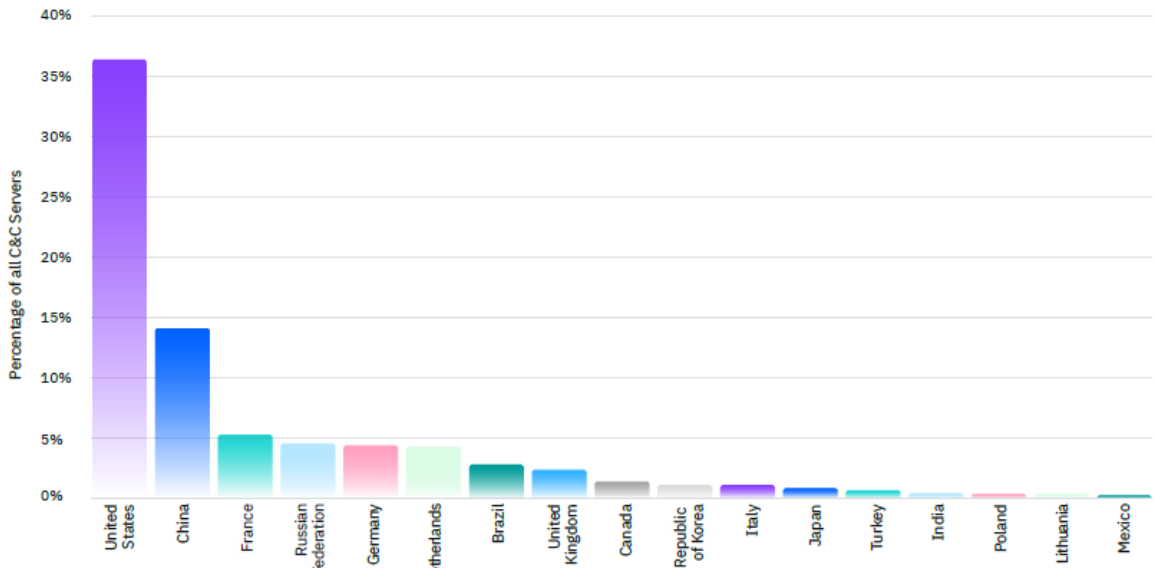
[40] IBM. X-force Threat intelligence index. 2019. [En línea].2019. Tomado de: https://xforceintelligenceindex.mybluemix.net/

[41] IEASIA. Los desafíos de la ciberseguridad en 2019. [En línea].2019. Tomado de: https://ieaisa.es/desafios-ciberseguridad-2019/

[42] IBM. X-force Threat intelligence index. 2019. [En línea].2019. Tomado de: https://xforceintelligenceindex.mybluemix.net/

Como también se puede también observar que los países que más originan ataques basados en malware y servidores de comando y control son: Estados Unidos, China, Francia y Rusia en su respectivo orden como se puede comprobar en la siguiente gráfica[43]:

Figura 2 Ataques informáticos por país



Fuente IBM. X-force Threat intelligence index. 2019. [En línea].2019. Tomado de: https://xforceintelligenceindex.mybluemix.net/

Se debe tener en cuenta también el panorama de la forma en que las tecnologías de la información vienen evolucionando, según los datos presentados por Cisco se tiene un cambio en el comportamiento de los clientes teniendo dentro de su visión el entorno de comportamiento del cliente, las expectativas de los empleados, las innovaciones tecnológicas y las amenazas de seguridad llevando a iniciativas de transformación digital para lo que el área de tecnología debe cerrar la brecha entre las expectativas en términos de: Como primer ítem su escalabilidad en donde el 90% de los datos son generados por aplicaciones, usuarios y otros dispositivos, su efectividad operativa con un 78% de recursos invertidos en mantener la

[43] IBM. X-force Threat intelligence index. 2019. [En línea].2019. Tomado de: https://xforceintelligenceindex.mybluemix.net/

infraestructura actual y a nivel seguridad en los riesgos de brechas han aumentado de 1 a 4 todos en los últimos 2 años[44].

Figura 3 Espectativas en el área de TI de una organización.

Fuente: Cisco, Cisco Intent-Based Networking At-a-Glance. 2019. [En línea]. Disponible en: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/nb-06-intent-based-networking-aag-cte-en.html?oid=aagen016865

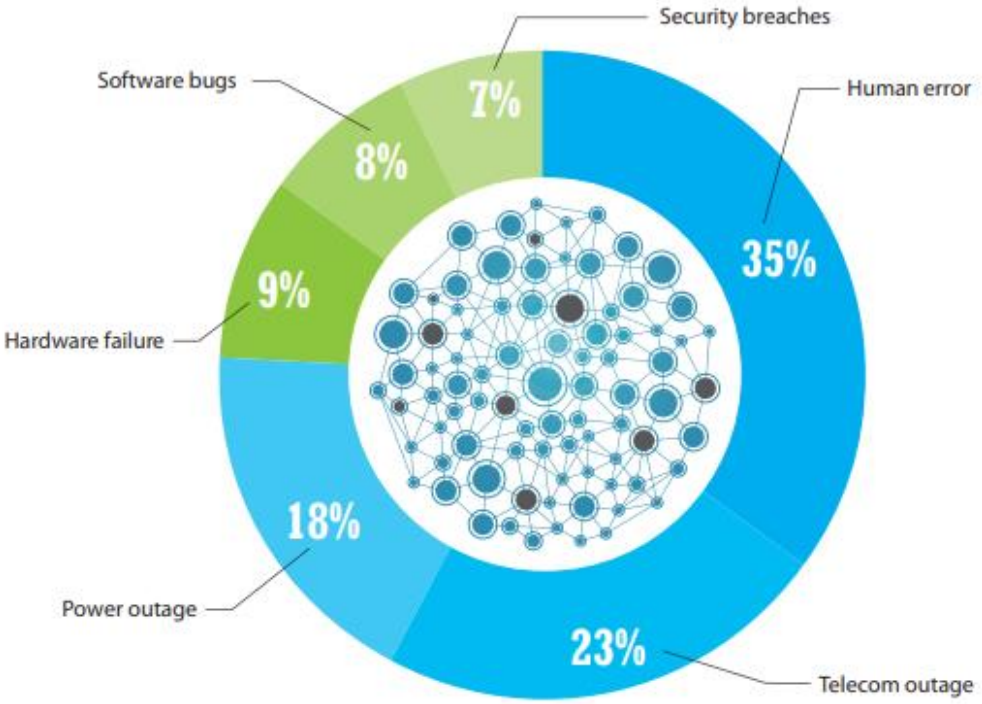
Utilizar la tecnología para adaptarse a las condiciones del mercado es trasformación digital y logra eficiencia en los procesos que redundan en posicionamiento ya que logran un mejor desempeño, por ejemplo según la investigación de ZK Research 2018 el tiempo para implementar un cambio completo en la red es de 4 meses siendo lentas y propensas a errores, siendo con el 35%[45] los errores humanos las causas de las fallas como lo muestra la figura y tiempo en investigación alcanza un 90%[46] en la búsqueda de la causa raíz.

[44] Cisco, Cisco Intent-Based Networking At-a-Glance. 2019. [En línea]. Disponible en: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/nb-06-intent-based-networking-aag-cte-en.html?oid=aagen016865

[45] KERRAVALA, Zeus. Machine Learning Powers the Next Wave of BUSINESS-CRITICAL SERVICES. 2018. [En línea] Disponible en: https://www.cisco.com/c/dam/en/us/services/collateral/se/business-critical-services-zk-machine-learning.pdf, p.4.

[46] Ibid., p. 4.

Figura 4 Distribución de tiempo utilizado por parte del personal de TI

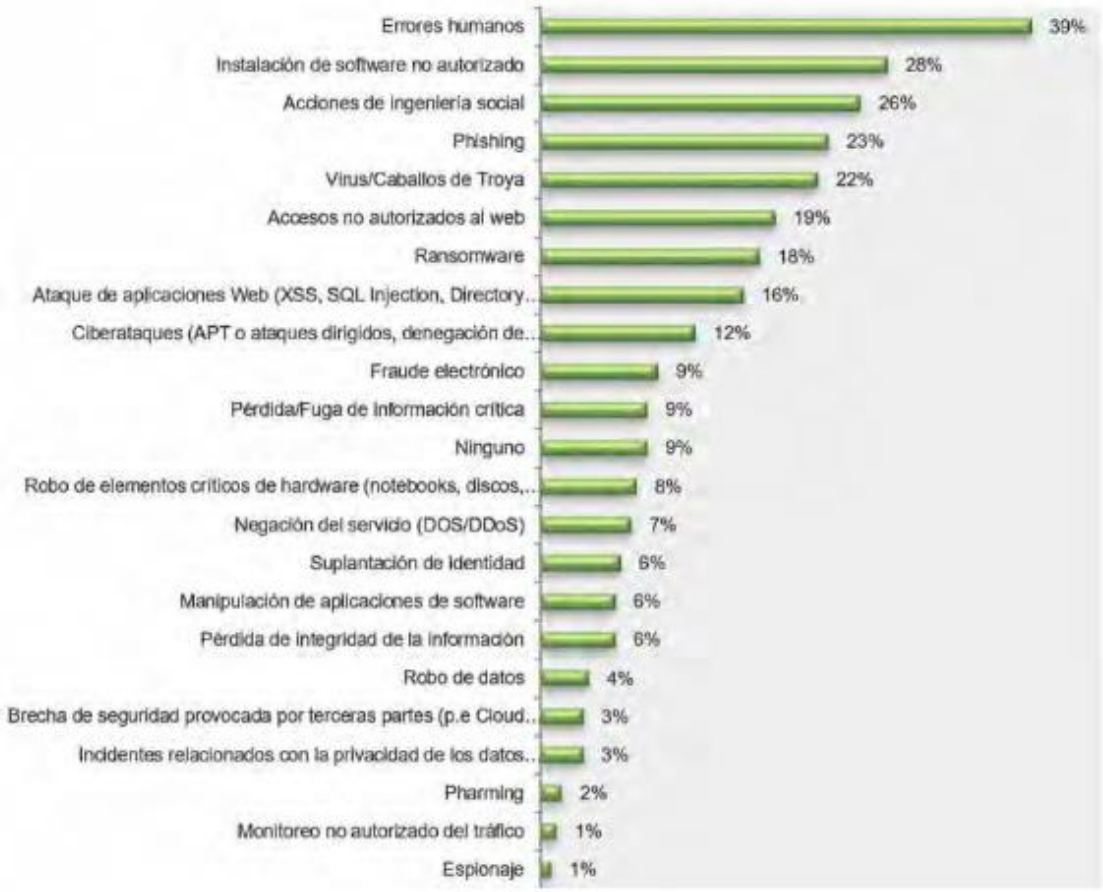


Fuente: KERRAVALA, Zeus. Machine Learning Powers the Next Wave of BUSINESS-CRITICAL SERVICES. 2018. [En línea] Disponible en: https://www.cisco.com/c/dam/en/us/services/collateral/se/business-critical-services-zk-machine-learning.pdf.

Este panorama no es muy diferente en Colombia según se puede observar en el estudio realizado por el CISO Andrés Almanza para la Asociación Colombiana de Ingenieros de Sistemas ACIS, en este se puede observar que gran cantidad de los incidentes de seguridad reportados se presentan por errores humanos llegando a un 39%[47] como se puede observar en la siguiente figura. También se pueden observar otros tipos de ataques que se presentan y que se pueden llegar a presentar en una organización siendo identificados por el personal de seguridad y de TI una empresa.

[47] ALMANZA, Andrés. XVIII Encuesta Nacional de Seguridad Informática Evolución del perfil del profesional de seguridad digital. Asociación Colombiana de Ingenieros de Sistemas. [En línea]. 2019. Disponible en: https://sistemas.acis.org.co/index.php/sistemas/article/view/42

Figura 5 Tipo de Incidentes de Seguridad según encuesta ACIS

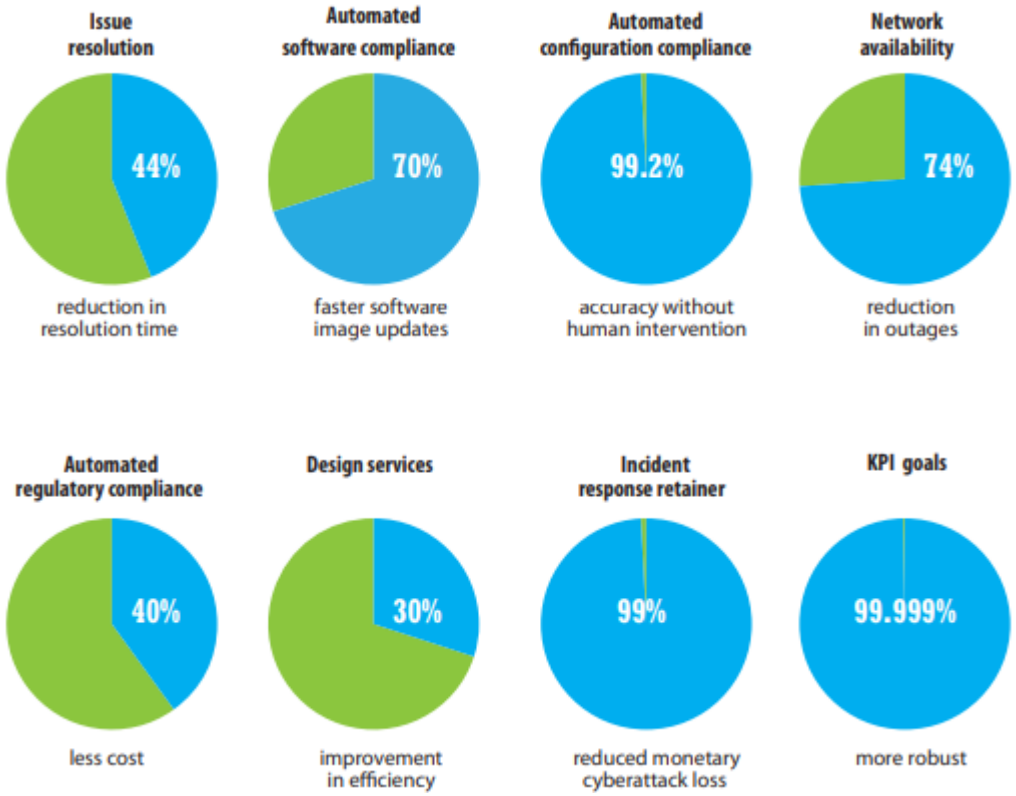


Fuente: ALMANZA, Andrés. XVIII Encuesta Nacional de Seguridad Informática Evolución del perfil del profesional de seguridad digital. Asociación Colombiana de Ingenieros de Sistemas. [En línea]. 2019. Disponible en: https://sistemas.acis.org.co/index.php/sistemas/article/view/42

Pero al involucrar técnicas de inteligencia artificial tales como el aprendizaje automático se puede optimizar ostensiblemente este tipo de resolución. Cisco le ha apostado a la visibilidad de los componentes de red buscando mejorar analítica avanzada y automatización de los servicios optimizando en muchos campos entre estos como se observa en la siguiente figura[48] reduciendo los costos por perdidas en ciberataques.

[48] KERRAVALA, Zeus. Machine Learning Powers the Next Wave of BUSINESS-CRITICAL SERVICES. 2018. [En línea] Disponible en: https://www.cisco.com/c/dam/en/us/services/collateral/se/business-critical-services-zk-machine-learning.pdf, p.10.

Figura 6 Resultados de optimización con técnicas de aprendizaje automático



Fuente: KERRAVALA, Zeus. Machine Learning Powers the Next Wave of BUSINESS-CRITICAL SERVICES. 2018. [En línea] Disponible en: https://www.cisco.com/c/dam/en/us/services/collateral/se/business-critical-services-zk-machine-learning.pdf

Por parte de Fortinet se tiene un análisis de las tendencias a nivel de seguridad de 2020 teniendo en cuenta las posibles tendencias del delito informático, investigación de amenazas y desarrollo de la tecnología buscando dar panorama de la ciberseguridad a corto y largo plazo. De este análisis podemos extraer que se tienen múltiples formas de ataques tales como técnicas de evasión avanzadas.

Adicional se hace énfasis en que se debe tener en cuenta que se considera que el atacante siempre ha tenido la ventaja teniendo en cuenta el paradigma de la seguridad informática tradicional y como se despliega en donde se cubren siempre los mismos vectores de ataque.

La implementación de 5G va a cambiar el paradigma de la seguridad, combinado con el internet de las cosas son una perfecta combinación que puede llegar a generar enjambres de ataques aprovechando la información capturada de los equipos infectados dado la naturaleza de este ataque muy pocos podrían luchar contra un ataque de ese estilo.

Este tipo de ataques cobran más relevancia si se basan en bot inteligentes que se puedan personalizar aprendiendo unos de otros en tiempo real.

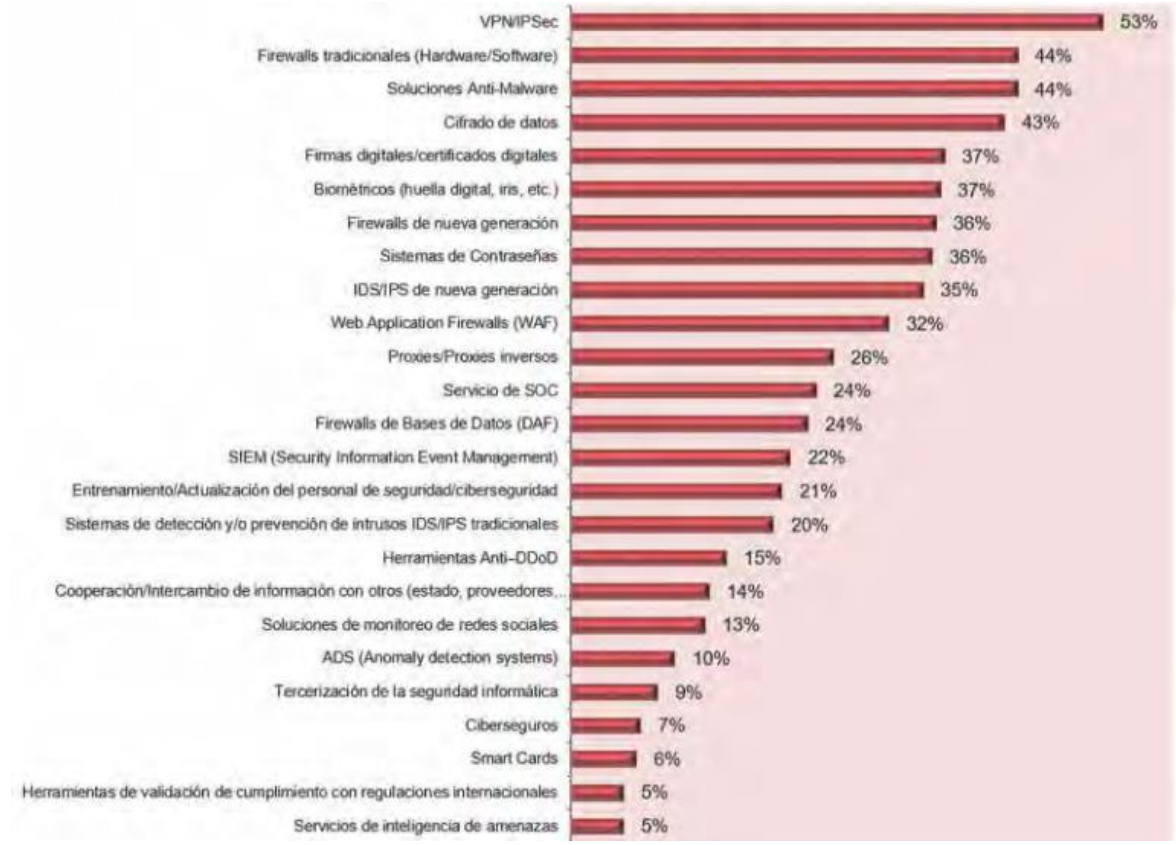
Las organizaciones pueden tomar medidas para poder contrarrestar este tipo de ataques por medio de técnicas de inteligencia artificial, utilizando un enfoque diferente y que permita un sistema inmunitario adaptivo que como en un cuerpo humano trabaje de forma autónoma para combatir la infección mientras envía la información a un sistema centralizado para que tome acciones más efectivas en la contención basado en grandes capacidades de procesamiento de datos que evalúan gran cantidad de información comportándose como una red neuronal con inteligencia distribuida.

Otro punto a tener en cuenta es el aprendizaje que se puede tener por medio de técnicas de aprendizaje automático en combinación con análisis estadístico para poder predecir ataques, descifrar patrones y predecir el comportamiento incluso para detectar la fuente del ataque para evitar próximos ataques e incluso el atacante en sí[49].

Para finalizar en el caso ciberseguridad en Colombia es importante tener en cuenta que mecanismos son utilizados para poder brindar seguridad a los activos de información de una empresa y que son tomados del estudio de ACIS que se puede observar a continuación:

[49] MARKY Derek, New Threat Predictions for 2020. [En línea]. 2019. https://www.fortinet.com/blog/industry-trends/fortinet-2020-threat-landscape-predictions.html

Figura 7 Mecanismos de Seguridad en empresas colombianas según encuesta ACIS.



Fuente: ALMANZA, Andrés. XVIII Encuesta Nacional de Seguridad Informática Evolución del perfil del profesional de seguridad digital. Asociación Colombiana de Ingenieros de Sistemas. [En línea]. 2019. Disponible en: https://sistemas.acis.org.co/index.php/sistemas/article/view/42

Es importante que se tenga en cuenta que se tiene dentro del personal que trabaja y se responsabiliza de la protección de la información conocimiento de la utilización de herramientas que pueden llegar a trabajar con algoritmos basados en inteligencia artificial tales como: soluciones antimalware, firewall de nueva generación, servicios de SOC, SIEM, servicios de inteligencia de amenazas.

6.6 HERRAMIENTAS QUE USAN DE INTELIGENCIA ARTIFICIAL EN CIBERSEGURIDAD EN EL MERCADO ACTUAL

Teniendo en cuenta que con los avances tecnológicos presentados en la actualidad se ha incrementado la superficie de ataque, por tanto, en el mercado se tienen herramientas para protección de perímetro que son especializadas para cumplir funciones específicas protegiendo un tipo de servicio o generando una capa de protección adicional en el perímetro de seguridad; en el mercado se han identificado las siguientes:

- Firewall
- Herramientas para evitar denegación de servicio
- Red para control del contenido
- Protección contra amenazas avanzadas
- Protección contra fuga de información
- Protección de acceso a la red
- Protección de correo electrónico
- Firewall de aplicaciones Web
- Firewall de bases de datos
- Protección de usuario final

Para el caso de los componentes anteriormente mencionados de acuerdo a la investigación realizada en el mercado se identificaron las siguientes marcas que utilizan herramientas de inteligencia artificial para realizar esquemas de protección de perimetral aumentando la velocidad en la capacidad de analítica de datos sobre las posibles amenazas que puede tener un ser humano:

- Fortinet[50]: Esta compañía que provee distintas herramientas de seguridad de las mencionadas anteriormente basa su inteligencia en el desarrollo de un procedimiento que denomina “sistema de detección de evolución propia” que es propio de su departamento de investigación de seguridad llamado Fortiguard Labs el cual lleva en desarrollo durante varios años con la finalidad de aumentar la posibilidad de detección y remediación. Siendo un sistema que basado en herramientas de inteligencia artificial permite recopilar, analizar y clasificar de manera autónoma las amenazas, inclusive llegando a detectar amenazas día cero que permiten que se desarrollen firmas para que por medio de la arquitectura sea distribuida permitiendo su actualización en tiempo real.

  Este sistema se alimenta de todos los dispositivos de que se encuentran conectados a la base de datos de Fortiguard permitiendo analizar más de 100 mil millones de eventos de seguridad aprendiendo de manera automática bajo las técnicas de Deep learning, realizando un aprendizaje machine learning en dónde reacciona al aprendizaje de su entorno ante nuevas amenazas detectadas incrementando la velocidad de detección.

  Para poder realizar este tipo de actividades lo realiza basándose en tres tipos de aprendizaje:

[50] Fortinet. Using AI to Address Advanced Threats That Last-Generation Network Security Cannot. 2019. [En línea]. https://www.fortinet.com/content/dam/fortinet/assets/ebook/ebook-using-ai-to-address-advanced-threats.pdf

- Supervisado: Para este tipo de aprendizaje se entrena al sistema con datos adecuadamente identificados y resueltos.
- No Supervisado: Proporcionan datos no identificados siendo el algoritmo el que visualiza los posibles patrones, los caracteriza y aprende generando su propia identificación para estos tipos de datos.
- Refuerzo en aprendizaje: Se enfoca en mejorar el desempeño y la efectividad que se generó por medio de los dos tipos de aprendizaje anterior aprendiendo de manera independiente realimentando los datos obtenidos para mejorar las decisiones que se pueden tomar.

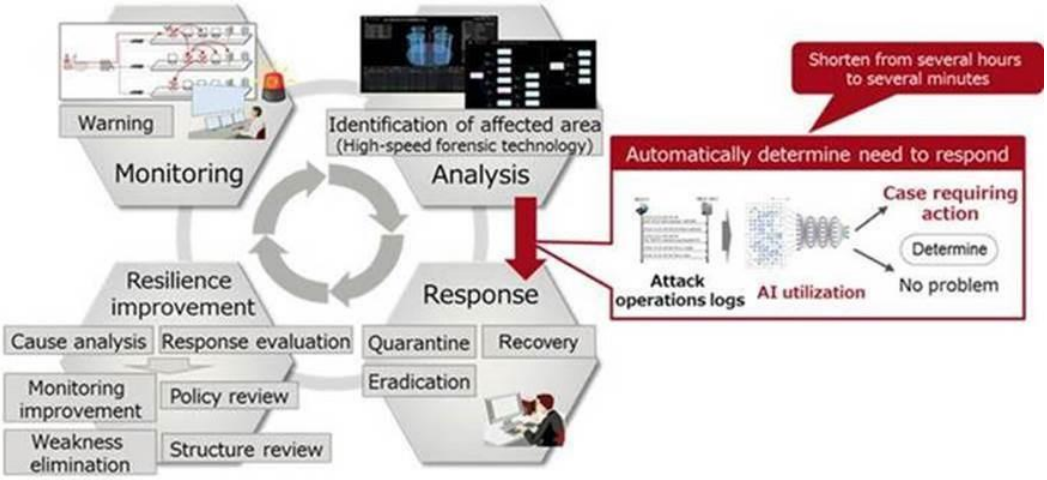
Se puede decir que por parte de Fortiguards se tienen los siguientes elementos que utilizan inteligencia artificial para la detección de amenazas:

- Aprendizaje Supervisado, no supervisado y refuerzo; analítica del entorno para usuarios y entidades; y desarrollo de paquetes personalizados.

- Fujitsu[51]: La compañía Fujitsu desarrollo este sistema llamado IA Deep Tensor para poder tomar decisiones frente ataques informáticos, validando el riesgo y las acciones a tomar, el sistema funciona siendo alimentado con gran cantidad de información sobre registros de comportamiento y muestras de ataques reales; esta información se utiliza como entrenamiento para la toma de decisiones teniendo una tasa de efectividad en las simulaciones del 95%. Se debe tener en cuenta que la gran dificultad en esta etapa es el gran volumen de registros del cual se debe identificar los que son maliciosos siendo muy importante el aporte dado por los laboratorios de Fujitsu quienes tienen gran cantidad de patrones de ataque obtenidos de la inteligencia de amenazas sobre ataques dirigidos. En la siguiente figura se puede observar el esquema por medio del cual se tiene respuesta ante un ciberataque:

[51] GALA BARXA, Iria & ALVAREZ, José. Fujitsu desarrolla una tecnología de IA para determinar la necesidad de respuesta frente a ciberataques. [En línea]. Fujitsu EMEIA. 2019. Disponible en https://www.fujitsu.com/es/about/resources/news/press-releases/2019/spain-fujitsu-desarrolla-una-tecnolog-a-de-ia-para.html

Figura 8 Esquema de funcionamiento Deep Tensor de Fujitsu



Fuente: GALA BARXA, Iria & ALVAREZ, José. Fujitsu desarrolla una tecnología de IA para determinar la necesidad de respuesta frente a ciberataques. [En línea]. Fujitsu EMEIA. 2019. Disponible en https://www.fujitsu.com/es/about/resources/news/press-releases/2019/spain-fujitsu-desarrolla-una-tecnolog-a-de-ia-para.html

- Cisco: Este empresa provee distintas herramientas tanto de seguridad perimetral como de redes de datos proponiendo un esquema que se basa en inteligencia artificial y machine learning que nos lleva a la propuesta de redes basadas en la intención o red intuitiva que realiza una optimización del aprendizaje automático y profundo llegando a dar mayores niveles de programación lo cual brinda mucha más integración a nivel de la automatización y la integración con la seguridad todo desde su sistema operático ASIC y IOS XE[52].

  Todo esto apoyándose en Talos que es el grupo de investigación de Cisco confirmado por expertos de seguridad que se encarga de realizar la inteligencia de amenazas, búsqueda de vulnerabilidades y cierre de brechas de seguridad. Cisco busca por medio de esto crear nuevas firmas, actualización de los motores que afectan directamente todos los productos de su marca ya que su filosofía es crear una infraestructura convergente formando un ecosistema con sus productos, para el caso de su herramienta de protección de correo Talos bloquea aproximadamente 200 mil millones de correos electrónicos maliciosos al día, o 2,3 millones de bloques por segundo[53].

[52] GREENE, Nolan & MERHA, Rohit. La red basada en la intención en la mira con el lanzamiento de los switches Ethernet de la serie Catalyst 9000 de Cisco. 2019. [En línea]. Disponible en: https://www.cisco.com/c/dam/global/es_mx/products/pdfs/cat9k-analyst-report-cte.pdf

[53] CISCO, Talos Group, Protecting your netrwork. [En línea]. 2015. Disponible en: https://www.cisco.com/c/dam/global/en_sg/solutions/industries/talos_white_paper.pdf

- Checkpoint[54]: Esta empresa de seguridad proporciona un esquema basado en inteligencia artificial, basada en tres herramientas que se complementan Campaing Hunting que se trabaja por medio de un ser humano quien hace la inteligencia sobre las posibles amenazas con el fin de poder rastrear los orígenes y correlacionar instancias similares. El segundo motor de búsqueda que implementa es Huntress utilizado para analizar ejecutables de código malicioso siendo analizado en un Sandbox que acelera el tiempo permitiendo el análisis con una mayor precisión y que complementa el motor anterior. Por último, se tiene un tercer motor llamado CADET que por medio de un esquema integra la totalidad de los dispositivos de red buscando total visibilidad de las amenazas, no viéndolos como dispositivos separados sino como un solo entorno.

- Palo Alto[55]: Esta compañía provee servicios de seguridad perimetral por medio de un producto llamado Cortex Data Lake integra métodos de inteligencia artificial que permite proteger información en la nube pública facilitando el manejo de la datos complejos y gran cantidad de estos manejando servicios de prevención de malware de manera global dotándolos de un contexto y permitiendo integración a indicadores de compromiso.

- Imperva[56]: Este fabricante maneja una solución de identificación de amenazas llamada Imperva Attack Analitycs que permite al firewall de aplicaciones web agrupar, consolidar y analizar alertas para identificar eventos de seguridad permitiendo rastrear amenazas globales o por sitio web que representan ataques de alto riesgo por medio de técnicas de inteligencia artificial.

- Cylance[57]: Basa su propuesta en un software para protección e Endpoint de muy poco peso a nivel almacenamiento y con un despliegue de un agente que no sube el procesamiento de la máquina a un alto porcentaje. Debido a que trabaja basada en el comportamiento y realiza su aprendizaje con técnicas de inteligencia artificial bloquea las posibles amenazas día cero sin necesidad una solución sofisticada y costosa basada en hardware.

[54] CHECK POINT SOFTWARE TECHNOLOGIES LTD. La Inteligencia Artificial al servicio de la Ciberseguridad. 2018. [En línea]. Disponible en: https://www.checkpoint.com/es/press/2018/la-inteligencia-artificial-al-servicio-de-la-ciberseguridad/

[55] PALO ALTO., CORTEX DATA LAKE. 2019. [En línea]. Disponible en: https://www.exclusive-networks.com/se/wp-content/uploads/sites/2/2019/06/cortex-data-lake-data-sheet.pdf

[56] DIGITAL SECURITY. Imperva Attack Analytics acelera la identificación de ataques críticos. 2018. [En línea]. Disponible en https://www.itdigitalsecurity.es/endpoint/2018/06/imperva-attack-analytics-acelera-la-identificacion-de-ataques-criticos

[57] CYLANCE. Continuous Threat Prevention Powered by Artificial Intelligence. 2018. [En línea]. Disponible en: https://www.arame.com.mx/wp-content/uploads/2018/05/CylancePROTECT-HOJA-DE-DATOS.pdf

- Carbon Black (VmWare)[58]: Se analiza como herramienta a parte ya que su comportamiento y funcionamiento es muy similar a la solución provista por el anterior fabricante aunque en este momento hace parte de una suite adquirida por parte de VmWare con el fin de poder incluir estas funcionalidades dentro del manejo de hipervisores y su producto para manejo de Internet de las cosas VmWare WorkSpace One.

6.7 LA INTELIGENCIA ARTIFICIAL Y SUS IMPLICACIONES ÉTICAS

Una de las principales discusiones que se tienen en el ámbito de la seguridad informática y de los expertos en seguridad es el del término HACKER, que es definida y aceptada por los profesionales del medio de la seguridad de la información como persona entusiasta por la tecnología que realiza investigación a nivel tecnología y su afán es la obtención del conocimiento sin dañar de ninguna manera en su entorno, este grupo son los que componen los oficiales de seguridad, los ethical hackers quienes apoyan con sus conocimientos el fortalecimiento de los ambientes para proteger la información de una compañía.
Pero, por el contrario un grupo de expertos en seguridad se ha desviado y con propósitos que son de beneficio personal y económico vulneran los esquemas de seguridad de las organizaciones causando daños en los sistemas de información de las organizaciones. Ellos son los que son conocidos como delincuentes informáticos y son perseguidos por la ley[59].

Este es el punto de partida para la discusión que se debe tener sobre el dilema ético del uso de la inteligencia artificial, ya en los puntos anteriores se ha tocado los posibles usos de los métodos de inteligencia artificial que se pueden usar para suplir y mejorar algunas tareas que se pueden realizar por el ser humano e incluso puede llegar a tener comportamientos que lo pueden parecer un ser humano como el robot llamado Sophia[60].

Por lo tanto se debe tener en cuenta que para poder hacer un buen uso de cualquier avance tecnológico requiere tanto de formación profesional como personal que apoye el buen uso de las mismas, debido a que el personal calificado para poder vulnerar un sistema se encuentra en dilema que es una línea delgada entre el poder obtener un beneficio y comportarse de acuerdo a los parámetros definidos por la moral, ética y las leyes[61].

---

[58] SILICON,. VMware Workspace ONE integra un asistente basado en inteligencia artificial. 2019. [En línea]. Disponible en https://www.silicon.es/vmware-workspace-one-integra-un-asistente-basado-en-inteligencia-artificial-2402457

[59] GACHARNA G., F. Hacker ético vs. delincuente informático: Una mirada en el contexto colombiano. 2009. INVENTUM, 4(6), 46-49. [En línea]. Disponible en https://doi.org/10.26620/uniminuto.inventum.4.6.2009.46-49

[60] BBC MUNDO. Sophia, la robot que tiene más derechos que las mujeres en Arabia Saudita. [En línea]. BBC mundo. 2016. Disponible en https://www.bbc.com/mundo/noticias-41803576

[61] MENDOZA, Miguel Ángel., Ética, el factor humano más importante en el ámbito de la ciberseguridad. 2016. [En línea]. Disponible en https://www.welivesecurity.com/la-es/2016/09/20/etica-en-ciberseguridad-factor-humano/

Esto se une a la gran publicidad que se ha presentado en torno al concepto de la inteligencia artificial que hace que se presente un desborde de información sobre un concepto que a futuro puede llegar a hacer que la vida como se conoce actualmente cambia notablemente pero que algo que no está pronto a suceder. Los avances se han publicitado buscando seguidores pero se debe tener en cuenta que en ámbitos más complejos tiene que contarse con grandes paradigmas a nivel social llegando a tener prejuicios raciales, sexuales e incluso de género[62].

Aunque los resultados en muchos campos pueden ser sonoros como en el caso de los videojuegos en donde se ha visto como incluso en un juego en el que se requiere el manejo de estrategia como lo es Quake III el algoritmo pudo llegar a aprender y tomar las decisiones para conducirse a la victoria haciendo uso de su entorno e incluso participando en equipo para lograr su objetivo[63].

El uso de la inteligencia artificial como el de muchas otras tecnologías como las que han surgido en los últimos años, tales como: Cloud, Big Data, entre otros, son susceptibles a ser mal utilizados por parte del ser humano, esta tecnología puede reemplazar al ser humano en tareas específicas y es el uso adecuado de los recursos lo que hace que realmente se pueda llegar a pensar que es factible convivir con una u otra tecnología, esto no ha sido diferente ya que hace años se tenía miedo del impacto que podía tener el Internet en la vida diaria, siendo tan solo la confianza en el ser humano y en la sociedad lo que ha hecho que sea un recurso a favor del crecimiento y de la globalización[64].

En un estudio realizado por Instituto de Investigación Capgemini quien entrevistó a 850 expertos del medio de la seguridad de la información y analizando 20 casos de uso de la inteligencia artificial en ciberseguridad, llegaron a que en la actualidad no se puede llegar a identificar gran cantidad de las amenazas consideradas críticas sin el uso de ésta; llegando también a concluir que casi el 75% de las empresas están probando con herramientas que se basan en inteligencia artificial mejorando la precisión y la eficiencia de los análisis realizados[65].

---

[62] MOORE, Jake. La ignorancia alrededor de la Inteligencia Artificial. 2019. [En línea]. Disponible en https://www.welivesecurity.com/la-es/2019/08/16/ignorancia-alrededor-inteligencia-artificial/

[63] LOPEZ SANCHEZ, Gonzalo. La Inteligencia Artificial (IA) coopera para ganar al hombre en los videojuegos de disparos. 2019. ABC Ciencia. [En línea]. Disponible en https://www.abc.es/ciencia/abci-inteligencia-artificial-supera-hombre-videojuegos-disparos-201905302000_noticia.html

[64] MUY INTERESANTE. Chema Alonso: "En 2050 la inteligencia artificial se igualará a la humana". [En línea]. Disponible en https://www.muyinteresante.es/tecnologia/inteligencia-artificial/video/chema-alonso-en-2050-la-inteligencia-artificial-se-igualara-a-la-humana

[65] INSTITUTO DE INVESTIGACIÓN DE CAPGEMINI. Reforzando la ciberseguridad con IA. 2019. [En línea]. Disponible en https://www.capgemini.com/es-es/instituto-de-investigacion-de-capgemini/reinventando-la-ciberseguridad-con-inteligencia-artificial/

Y teniendo en cuenta, que se tienen dos tipos de investigaciones a nivel de inteligencia artificial: una global que busca realizar una imitación del comportamiento humano en toda su expresión realizando aprendizaje buscando comportamientos humanos y otra que solo busca cumplir con una tarea específica desarrollando habilidades específicas que usan técnicas tales como aprendizaje automático y aprendizaje profundo que es una división de esta última.[66] En esta última se sitúa las herramientas que buscan apoyar al personal de seguridad de una compañía en la protección de los datos generando un perímetro para poder proteger los activos de una empresa.[67] Por tanto, en este momento y con los avances presentados en el campo de la seguridad informática se presenta como una herramienta que permite utilizar las bondades que brindan los sistemas con grandes capacidades de computó en el análisis de la información que permite que se pueda identificar posibles brechas de seguridad y actuar contra posibles ataques hacia la infraestructura de TI.

Por el otro lado, se tienen también gran cantidad de herramientas para poder generar ataques masivos por medio de entes autónomos para vulnerar brechas de seguridad de un sistema informático quedando en dilema ético del adecuado uso de la tecnología en manos de los seres humanos que la utilizan.

[66] INSTITUTO DE INVESTIGACIÓN DE CAPGEMINI. Reforzando la ciberseguridad con IA. 2019. [En línea]. Disponible en https://www.capgemini.com/es-es/instituto-de-investigacion-de-capgemini/reinventando-la-ciberseguridad-con-inteligencia-artificial/

[67] MUY INTERESANTE. Chema Alonso: “En 2050 la inteligencia artificial se igualará a la humana”. [En línea]. Disponible en https://www.muyinteresante.es/tecnologia/inteligencia-artificial/video/chema-alonso-en-2050-la-inteligencia-artificial-se-igualara-a-la-humana

7. RESULTADOS Y DISCUSIÓN

Teniendo en cuenta la información que se relacionó en capítulos anteriores se tiene como resultado de la investigación realizada en fuentes documentales una contextualización sobre el funcionamiento de los métodos que utilizan inteligencia artificial tales como: “aprendizaje automático, redes neuronales, aprendizaje profundo, algoritmos genéticos, etc” por medio de los cuales se puede imitar comportamientos similares a los de un ser humano.

Pero, basado en los estudios referenciados se puede deducir que a diferencia de la búsqueda de una inteligencia global en donde se busca crear a un ser independiente, se están buscando potenciar características propias de los seres humanos relacionándose con el entorno y tomando decisiones para poder interactuar reaccionando según el entrenamiento que haya recibido el sistema.

Esto nos lleva a que en un escenario cercano no presente la posibilidad de que se reemplace al ser humano en su totalidad y que solo se potencialice las labores para las cuales los sistemas han sido entrenados, cumpliendo con tareas específicas.

Siendo un punto de discusión donde se plantea la eficacia de los métodos que utiliza inteligencia artificial para labores de ciberseguridad sobre los métodos tradicionales de ciberseguridad, esto nos permite validar que realmente en los puntos en los que se puede tener ventajas son los puntos en los que se puede entrenar un sistema para tomar acciones ante escenarios apoyándose en grandes capacidades de computó y en el aumento de estas día a día.

De hecho, este punto es el que ha hecho que una tecnología que ha sido descubierta y en donde se plantearon los algoritmos desde los años 80 cobren relevancia en este momento siendo cada vez más competitivos. Y presentándose en escenarios tanto de técnicas defensivas basadas en comportamiento UEBA o SIEM, o en técnicas ofensivas utilizadas por los atacantes tales como como ofensivas adaptativas con bots para ataques de DDoS.

Más aún cuando como se relacionó se tiene que los fabricantes tienden a realizar automatización de la gestión de la infraestructura tecnológica reduciendo errores humanos, siendo este un factor que cuesta tanto en el despliegue y adopción de nuevas tecnologías como causa de las brechas de seguridad.

En este momento fabricantes tales como CISCO, FORTINET, Amazon, VmWare quienes para defensa del perímetro de seguridad le apuestan a la inteligencia artificial como un el siguiente paso en el campo de ciberseguridad.

Para terminar, se puede decir que siempre se tiene sobre la mesa la posición ética y moral del uso de inteligencia artificial para suplir labores que realizan los seres

humanos, pero es un punto en donde la sociedad se ha visto en varias oportunidades, ha pasado con la invención de muchos artefactos tecnológicos que han reemplazado la mano de obra y en cambio de haber sido sustituidos los seres humanos se han visto beneficiados mejorando su calidad de vida. Se ha hecho que el modelo de sociedad haya cambiado reemplazando las tareas que se realizan y creando otras tareas.

8. RECOMENDACIONES

En el presente trabajo de monografía se desarrolló una investigación basándose en fuentes documentales y repositorios de información públicos en donde se presenta como una visión global del uso de la inteligencia artificial en el campo de la seguridad informática sirviendo como punto de partida para poder ahondar en varios de los temas:

- Desarrollo de una implementación de un sistema basado en inteligencia artificial aplicado a la seguridad informática ampliando las investigaciones referenciadas en el presente documento.

- Ampliación sobre el alcance del dilema ético y moral sobre la implementación de herramientas que suplan las tareas que desarrollan los analistas de seguridad informática en una organización realizando la detección de posibles amenazas de seguridad a los sistemas de información.

- Desarrollo de una investigación basada en los posibles caminos que se puedan tomar en el desarrollo de la inteligencia artificial y las posibles aplicaciones tanto en la seguridad informática como en otros ámbitos.

Se debe tener en cuenta que la inteligencia artificial en este momento, aunque haya surgido en los años ochenta hasta hace muy pocos años ha venido tomando relevancia debido a que las capacidades de procesamiento de datos han hecho posible que los sistemas autónomos sean considerados como una alternativa viable para el reemplazo en la toma de decisiones de un ser humano.

9. CONCLUSIONES

En el desarrollo del trabajo se ha presentado una temática basada en el conocimiento de la inteligencia artificial realizando una explicación de los conceptos basados en una recopilación de información basada en fuentes documentales y repositorios de información públicos por medio de los cuales se da una visión de cómo los sistemas basados en inteligencia artificial aprenden llegando a emular comportamientos que son propios de un ser humano de los cuales podemos concluir:

- Basado en los repositorios de información públicos consultados se puede generar un panorama global sobre los conceptos de inteligencia artificial que a su vez puede llegar a su vez a utilizar para implementación de técnicas ofensivas y defensivas de ciberseguridad. Estos conceptos ayudan a validar como se pueden llegar a emular los comportamientos de los seres humanos a través de los sistemas que tienen dentro de sus principales habilidades el aprendizaje y la adaptabilidad al entorno.

- Los comportamientos que son imitados por los sistemas que utilizan inteligencia artificial se basan en varios tipos de esquemas que pueden ser aprendizaje automático, redes neuronales, aprendizaje profundo, algoritmos genéticos o combinación de varios de ellos aplicados a técnicas de ciberseguridad tanto defensivas como ofensivas en donde un sistema aprende de acuerdo al aprendizaje de su entorno, a datos de entrada previamente cargados o combinación de los mismos generando un sistema que puede reaccionar ante cambios en su entorno.

- El futuro del desarrollo de las técnicas tanto defensivas como ofensivas en ciberseguridad y la utilización de inteligencia artificial para poder lograrlo es impulsado en el hecho de poder manejar grandes cantidades de datos apoyándose en la posibilidad de tener grandes capacidades de procesamiento de datos que se multiplican día tras día haciendo que la automatización de tareas sea algo necesario. Por tanto, la posibilidad que tienen los sistemas basados en inteligencia artificial de tomar decisiones autónomas ante un escenario en particular aun cuando este cambie hace que sea realmente un complemento a tecnologías de gran capacidad de procesamiento de información tales como Big Data y la computación cuántica.

- Por medio de la investigación de las herramientas que se encuentran en el mercado y validando la visión que tienen las empresas que se encargan de desarrollar estos productos para la protección de la información de una

organización, se puede visualizar el interés del desarrollo de esquemas de protección basados en inteligencia artificial.

- Se puede también observar en el documento como los fabricantes tienen un concepto del futuro de la seguridad y la inteligencia artificial en el ámbito de la seguridad defensiva protegiendo el perímetro siendo capaces de adaptarse por medio de esquemas de inteligencia de amenazas en donde se apoyan en sistemas alimentados por muchos componentes y que trabajan en la nube como un ente completo o en sistemas predictivos de análisis de comportamiento tales como UEBA (detección de amenazas basadas en comportamiento) de su sigla en inglés.

- Para el caso de la seguridad ofensiva el uso de la inteligencia artificial se puede ver su aplicación en sistemas autónomos capaces de adaptarse para realizar un ataque. Siendo esto de gran relevancia cuando se ha tenido un gran despliegue de ataques con una botnet que son cada vez más fáciles de formar debido al crecimiento del internet de las cosas. Estos dispositivos que poseen internet no tienen desarrollo de normativas fuertes en seguridad presentan una gran fuente para realizar ataques siendo en combinación con la inteligencia artificial una amenaza latente a nivel de seguridad.

- Se debe tener en cuenta que para el caso del uso de la inteligencia artificial en ciberseguridad, este uso no se desprende del dilema ético del buen uso de la tecnología para favorecer el desarrollo de la sociedad y el ser humano, para lo cual se debe apoyar de la adecuada formación del personal de seguridad tanto a nivel técnico como personal para que pueda hacer un adecuado uso de los recursos. Se debe tener en cuenta que un avance tecnológico es tan constructivo o destructivo como las personas que llegan a usarlo.

- Por último, es de concluir que para el del desarrollo de la inteligencia artificial como una tecnología emergente y especialmente en el campo de la ciberseguridad que es objeto de este trabajo se deben buscar mecanismos de control para poder vigilar el uso de esta tecnología. Se requiere que los entes reguladores a nivel mundial tanto de facto, como jure generen estándares de seguridad que sean adoptados por los fabricantes y que sean apoyados dentro de las políticas internacionales para lograr políticas globales que controlen su desarrollo para que se pueda encontrar la manera complementar las labores de los oficiales de seguridad en el trabajo diario protegiendo los activos de información de una organización.

BIBLIOGRAFÍA

- ALFONSECA, Manuel. ¿Basta la prueba de turing para definir la “inteligencia artificial”?. [En línea]. Universidad de Navarra. 2014. Disponible en https://dadun.unav.edu/handle/10171/37284

- ALMANZA, Andrés. XVIII Encuesta Nacional de Seguridad Informática Evolución del perfil del profesional de seguridad digital. Asociación Colombiana de Ingenieros de Sistemas. [En línea]. 2019. Disponible en: https://sistemas.acis.org.co/index.php/sistemas/article/view/42

- AMADOR, Luis. Inteligencia artificial y sistemas expertos. [En línea]. Universidad de Córdoba. 1996. Disponible en http://helvia.uco.es/bitstream/handle/10396/6938/Luis%20Amador_Inteligencia%20artificial_1996-1.pdf?sequence=1

- Andreu, M. G., & Pérez, G. P. P. (2004). Seguridad informática para empresas y particulares. España: McGraw-Hill España. Pag 25-29

- BBC MUNDO. Sophia, la robot que tiene más derechos que las mujeres en Arabia Saudita. [En línea]. BBC mundo. 2016. Disponible en https://www.bbc.com/mundo/noticias-41803576

- BBC MUNDO. Tay, la robot racista y xenófoba de Microsoft. [En línea]. BBC mundo. 2016. Disponible en https://www.bbc.com/mundo/noticias/2016/03/160325_tecnologia_microsoft_tay_bot_adolescente_inteligencia_artificial_racista_xenofoba_lb

- BETANCOURT BARRETO, Jhonny Jordan. Introducción al hacker ético. [En línea]. Universidad Piloto de Colombia. 2014. Disponible en http://repository.unipiloto.edu.co/handle/20.500.12277/2844

- BEZOBRAZOV, Sergei & SACHENKO Anatoly & KOMAR Myroslav, RUBANAU Vladimir, The methods of artificial intelligence for malicious applications detection in Android OS. [En línea]. 2017., Disponible en http://www.computingonline.net/computing/article/view/851

- CHECK POINT SOFTWARE TECHNOLOGIES LTD. La Inteligencia Artificial al servicio de la Ciberseguridad. 2018. [En línea]. Disponible en : https://www.checkpoint.com/es/press/2018/la-inteligencia-artificial-al-servicio-de-la-ciberseguridad/

- CISCO, Cisco Intent-Based Networking At-a-Glance. 2019. [En línea]. Disponible en: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/nb-06-intent-based-networking-aag-cte-en.html?oid=aagen016865

- CISCO, Talos Group, Protecting your netrwork. [En línea]. 2015. Disponible en: https://www.cisco.com/c/dam/global/en_sg/solutions/industries/talos_white_paper.pdf

- CONTRERAS, Javier., Aplicación de Deep Learning en róbotica móvil para exploración y reconocimiento de objetos basados en imagenes, Universidad de los Andes. [En línea]. Bogotá. 2015. Disponible en https://biblioteca.uniandes.edu.co/visor_de_tesis/web/?SessionID=L1Rlc2lzMjAxNjk5LzgxNTQucGRm

- CORONA, Leonel & ABARCA, Griselda & MARES Jesús. Sensores y actuadores, Instituto Politécnico Nacional. [En línea]. México. 2014. Disponible en https://books.google.es/books?hl=es&lr=&id=wMm3BgAAQBAJ&oi=fnd&pg=PP1&dq=actuadores+y+sensores&ots=6N6rjw95ZB&sig=dz7A0wlhea27Er81kmGKraNjUjA#v=onepage&q=actuadores%20y%20sensores&f=false

- COTTON, Thalia & BHATNAGAR, Sankalp. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. [En línea]. 2018. Disponible en https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf

- COZ FERNANDEZ, José Ramon & PASTOR PEREZ, Vicente José. Entornos de Sistemas Multiagente y Ciber-Físicos en la Ciberdefensa. [En línea]. 2014. Disponible en https://www.researchgate.net/profile/Vicente_Pastor_Perez/publication/265345858_Entornos_de_Sistemas_Multiagente_y_CiberFisicos_en_la_Ciberdefensa/links/54404fe10cf2be1758cfffe6.pdf

- CYLANCE. Continuous Threat Prevention Powered by Artificial Intelligence. 2018. [En línea]. Disponible en: https://www.arame.com.mx/wp-content/uploads/2018/05/CylancePROTECT-HOJA-DE-DATOS.pdf

- DIGITAL SECURITY. Imperva Attack Analytics acelera la identificación de ataques críticos. 2018. [En línea]. Disponible en https://www.itdigitalsecurity.es/endpoint/2018/06/imperva-attack-analytics-acelera-la-identificacion-de-ataques-criticos

- DILEK, Selma & CAKIR, Hüseyin & AIDIN, Mustafa., Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. [En línea]. 2015. Disponible en https://arxiv.org/ftp/arxiv/papers/1502/1502.03552.pdf

- DUQUE, Néstor & OVALLE, Demetrio & JIMENEZ, Jovani, Modelo Adaptativo para Cursos Virtuales basado en Técnicas de Planificación Inteligente. Universidad Nacional de Colombia. [EN línea]. Medellín. 2007. Disponible en https://revistas.unal.edu.co/index.php/avances/article/view/9715/10245

- ELEVEN PATHS. ElevenPaths Radio – 1×10 Entrevista a Ramón López de Mántaras. 2019. Disponible en https://empresas.blogthinkbig.com/elevenpaths-radio-entrevista-a-ramon-lopez-de-mandaras/

- EL TIEMPO. Esto dijo la robot humanoide, Sophia, tras su llegada a Medellín. [En línea]. https://www.eltiempo.com/colombia/medellin/sophia-la-robot-humanoide-llego-a-medellin-249650

- EL TIEMPO. Los camiones sin conductor de Uber ya circulan en EE. UU. [En línea]. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/camiones-autonomos-de-uber-ya-circulan-en-estados-unidos-191396

- ESCRIBANO, José. Seguridad Ofensiva y defensiva con machine learning. INCIBE. 2018. [En línea]. Disponible en https://cybercamp.es/videos/t01-seguridad-ofensiva-y-defensiva-con-machine-learning

- ESPITIA GARZON, Angelica María. Ingeniería social amenaza latente para la seguridad informática. [En línea]. Universidad Piloto de Colombia. 2016. Disponible en http://repository.unipiloto.edu.co/handle/20.500.12277/2878

- FERNANDEZ, Antonio & MANZANO María, GONZALEZ, Enrique & TOME, Sergio., Una Perspectiva de la Inteligencia Artificial en su 50 Aniversario Sergio, Universidad de Castilla [En línea]. Albacete. 2004. Disponible en: http://www.info-ab.uclm.es/personal/AntonioFdez/download/papers/conference/cmpi2006-volumeI.pdf

- FERRADO, Leandro & CUENCA, Matías. Filtrando eventos de seguridad en forma conservativa mediante deep learning. [En línea]. Córdoba. 2016. Disponible en http://hdl.handle.net/10915/56884

- FELIX BREZO, Fernández. Detección de tráfico de control de botnets modelizando el flujo de los paquetes de red. [En línea]. Universidad de Deusto (España). 2014. Disponible en https://dialnet.unirioja.es/servlet/tesis?codigo=118090

- Fortinet. Using AI to Address Advanced Threats That Last-Generation Network Security Cannot. 2019. [En línea]. https://www.fortinet.com/content/dam/fortinet/assets/ebook/ebook-using-ai-to-address-advanced-threats.pdf

- GACHARNA G., F. Hacker ético vs. delincuente informático: Una mirada en el contexto colombiano. 2009. INVENTUM, 4(6), 46-49. [En línea]. Disponible en https://doi.org/10.26620/uniminuto.inventum.4.6.2009.46-49

- GALA BARXA, Iria & ALVAREZ, José. Fujitsu desarrolla una tecnología de IA para determinar la necesidad de respuesta frente a ciberataques. [En línea]. Fujitsu EMEIA. 2019. Disponible en https://www.fujitsu.com/es/about/resources/news/press-releases/2019/spain-fujitsu-desarrolla-una-tecnolog-a-de-ia-para.html

- GREENE, Nolan & MERHA, Rohit. La red basada en la intención en la mira con el lanzamiento de los switches Ethernet de la serie Catalyst 9000 de Cisco. 2019. [En línea]. Disponible en: https://www.cisco.com/c/dam/global/es_mx/products/pdfs/cat9k-analyst-report-cte.pdf

- GUTIERREZ, Fernando, Laboratorio de Seguridad Informática con Kali Linux. Universidad de Valladolid. [En línea]. http://uvadoc.uva.es/handle/10324/5141.

- IBM. X-force Threat intelligence index. 2019. [En línea].2019. Tomado de: https://xforceintelligenceindex.mybluemix.net/

- IEASIA. Los desafíos de la ciberseguridad en 2019. [En línea].2019. Tomado de: https://ieaisa.es/desafios-ciberseguridad-2019/

- INSTITUTO DE INVESTIGACIÓN DE CAPGEMINI. Reforzando la ciberseguridad con IA. 2019. [En línea]. Disponible en https://www.capgemini.com/es-es/instituto-de-investigacion-de-capgemini/reinventando-la-ciberseguridad-con-inteligencia-artificial/

- KERRAVALA, Zeus. Machine Learning Powers the Next Wave of BUSINESS-CRITICAL SERVICES. 2018. [En línea] Disponible en: https://www.cisco.com/c/dam/en/us/services/collateral/se/business-critical-services-zk-machine-learning.pdf

- LOPEZ SANCHEZ, Gonzalo. La Inteligencia Artificial (IA) coopera para ganar al hombre en los videojuegos de disparos. 2019. ABC Ciencia. [En línea]. Disponible en https://www.abc.es/ciencia/abci-inteligencia-artificial-supera-hombre-videojuegos-disparos-201905302000_noticia.html

- LUCANGELI, Jorge & SARRAUTE, Carlos & RICHARTE, Gerardo., Attack Planning in the Real World, Instituto Tecnológico [En línea]. Buenos Aires. 2013. Disponible en https://arxiv.org/pdf/1306.4044.pdfMILLER, Sean & BUSBY, Curtis., The role of machine learning in botnet detection. [En línea]. Barcelona. 2016. Disponible en https://ieeexplore.ieee.org/abstract/document/7856730

- MARKY Derek, New Threat Predictions for 2020. [En línea]. 2019. Disponible en: https://www.fortinet.com/blog/industry-trends/fortinet-2020-threat-landscape-predictions.html

- MENDOZA, Miguel Ángel., Ética, el factor humano más importante en el ámbito de la ciberseguridad. 2016. [En línea]. Disponible en https://www.welivesecurity.com/la-es/2016/09/20/etica-en-ciberseguridad-factor-humano/

- MOGOLLON, Oscar. Defensa en Profundidad - defensa elástica. Hablemos de Táctica. [En línea]. 2012. Disponible en: http://hablemosdetactica.blogspot.com/2012/08/defensa-en-profundidad-defensa-elastica.html

- MORA VILLAZAN, Elena. Análisis Probabilista de Seguridad de Redes de Tráfico Basado en Redes Bayesianas [En línea]. Universidad de Cantabria. 2017. Disponible en http://hdl.handle.net/10902/13112

- MOORE, Jake. La ignorancia alrededor de la Inteligencia Artificial. 2019. [En línea]. Disponible en https://www.welivesecurity.com/la-es/2019/08/16/ignorancia-alrededor-inteligencia-artificial/

- MUÑOZ, Alfonso & ESCRIBANO, Jose. Criptografía adversaria usando deep learning limitaciones y oportunidades. BBVA. [En línea]. Madrid. 2015. Disponible en https://www.bbvanexttechnologies.com/wp-content/uploads/2018/07/amunoz-jescribano-criptograf%C3%ADa-adversaria-recsi-2018.pdf

- MUY INTERESANTE. Chema Alonso: “En 2050 la inteligencia artificial se igualará a la humana”. [En línea]. Disponible en https://www.muyinteresante.es/tecnologia/inteligencia-artificial/video/chema-alonso-en-2050-la-inteligencia-artificial-se-igualara-a-la-humana

- PALO ALTO., CORTEX DATA LAKE. 2019. [En línea]. Disponible en: https://www.exclusive-networks.com/se/wp-content/uploads/sites/2/2019/06/cortex-data-lake-data-sheet.pdf

- ROJAS, Jaime., Sistema de autenticación de individuos mediante señales de voz usando métodos de inteligencia artificial (VoID), Universidad de los Andes [En línea]. 2005. Disponible en http://hdl.handle.net/1992/22019

- ROMERO, Juan & DAFONTE, Carlos & GOMEZ, Ángel & PENOUSAL, Fernando. Inteligencia artificial y computación avanzada. [En línea]. Fundación Alfredo Brañas Santiago de Compostela. 2007. Disponible en https://cdv.dei.uc.pt/wp-content/uploads/2014/03/ms07.pdf

- SARRAUTE, Carlos & BUFFET, Olivier & HOFFMANN Jörg, POMDPs Make Better Hackers: Accounting for Uncertainty in Penetration Testing. [En línea]. AAAI Publications, Twenty-Sixth AAAI Conference on Artificial Intelligence. 2012., Disponible en https://www.aaai.org/ocs/index.php/AAAI/AAAI12/paper/viewPaper/4996

- SILICON.ES. VMware Workspace ONE integra un asistente basado en inteligencia artificial. 2019. [En línea]. Disponible en https://www.silicon.es/vmware-workspace-one-integra-un-asistente-basado-en-inteligencia-artificial-2402457

- TRIBAK, Hind. Análisis estadístico de distintas técnicas de inteligencia artificial en detección de intrusos. [En línea]. Universidad de Granada. 2012. Disponible en https://hera.ugr.es/tesisugr/20758340.pdf

- ZÁRATE LUNA, Paola Andrea. Guerra por el ciberespacio. [En línea]. Universidad Piloto de Colombia. 2014. Disponible en http://repository.unipiloto.edu.co/handle/20.500.12277/2891