Inteligencia Artificial y el Aprendizaje Automático en la Ciberseguridad

Carlos Fernando Montes Vallejo
Correo: Carlos-montes1@upc.edu.co

***Resumen*— La Inteligencia artificial surgió como la nueva herramienta que permite facilitar los procesos y mejorar la efectividad de los mismos, uno de los ejemplos más relevantes es el escenario donde se utiliza junto con el Aprendizaje Automático de manera efectiva dentro de la Seguridad Informática. Sin embargo, es crítico comprender que herramientas como esta que incursionan dentro del sector tecnológico poseen diversas aproximaciones que deben ser evaluadas para determinar el grado real de éxito. En este sentido, debe evaluarse el resultado a largo plazo comprendido desde el aprendizaje, tendencias, y la capacidad de escalabilidad que el mismo escenario debería comprender en un contexto globalizado.**

Palabras clave: Ciberseguridad, Tendencias, Desafíos, Inteligencia Artificial, Aprendizaje Automático.

Abstract: Artificial Intelligence emerged as the new tool that allows facilitating processes and improving their effectiveness, one of the most relevant examples is the scenario where it is used together with Machine Learning in an effective way within Computer Security. However, it is critical to understand that tools such as this one that make incursions into the technological sector have different approaches that must be evaluated to determine the real degree of success. In this sense, the long-term results must be evaluated, including learning, trends, and the scalability capacity that the same scenario should comprise in a globalized context.

Keywords: Cybersecurity, Trends, Challenges, Artificial Intelligence, Machine Learning.

I. INTRODUCCIÓN

La Inteligencia Artificial ha logrado un nivel de penetración importante en diversos sectores del mundo actual por su grado de optimización y diferenciación en la realización de los procesos, adicional a este aspecto termina siendo necesario evaluar las implicaciones en cuanto a ética, la privacidad de la información y la manera en que se automatizan los datos de manera sistemática. Igualmente es necesario evaluar el enfoque multidisciplinar que aporta la IA dentro de elementos críticos de la sociedad actual como son el Aprendizaje Automático y las implicaciones a nivel de aplicación y el grado de responsabilidad por un lado con el tratamiento de la información y la transparencia como mecanismo de garantía de ética y legalidad. Es una época de cambio compleja que requiere parámetros lógicos de acción para garantizar una transición exitosa y que las herramientas mejoren al mejor nivel posible, siendo ese el objetivo por encima de todas las cosas.

II. DESARROLLO DEL CONTENIDO

Desde una aproximación meramente conceptual, la IA emerge como una herramienta capaz de cambiar los paradigmas tanto educativos como industriales, se ha desarrollado una poderosa tendencia de cambio que dentro de los conceptos de la misma y la posición de conocedores del tema es un escenario en extremo acelerado y que ciertamente carece de fundamentación lógica. Si bien hasta el momento todo son ventajas los limitantes a evaluar terminan siendo de enorme incertidumbre, esto se formula principalmente por que la IA es una herramienta sin registros estructurales de funcionamiento y mucho más complejo aún, se desconocen los escenarios de fallas y la repercusión de los mismos al momento de alcanzar una integración total en el desarrollo de la sociedad entera. [1].

De manera predominante la última época ha desarrollado un avance exponencial que puede solo haber sido la fase final de proyectos específicos pero que causaron un gran revuelo por la capacidad que dichos proyectos pueden tener. Sin ir muy lejos, el modelo Generative Pre-Trained Transformer o ChatGPT en su versión 3 desató la locura y un sin fin de posibilidades así como una agresiva competencia por el poder, todos los poderosos de la tecnología abrieron al público sus perspectivas de IA y la forma en que generarían resultados de manera efectiva. Es aquí, donde se debe hacer especial referencia al aprendizaje automático, siendo este la herramienta que ayudaría a lograr un enfoque multidisciplinar entre la IA y el aprendizaje automático AA. Sin embargo, aún es prematuro en algunos casos puesto que surgen dilemas éticos a tratar y la manera en que dichos sistemas se podrían integrar a sectores donde el margen de error es mínimo y básicamente no puede haber cabida para un solo detalle sin contemplar. [2].

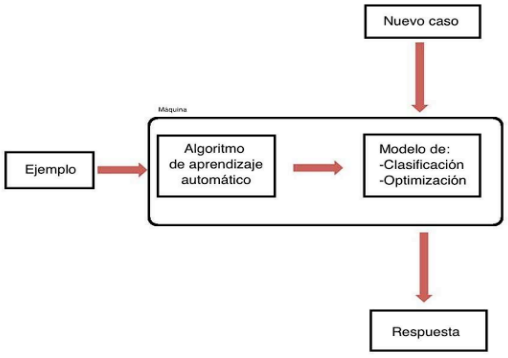

Fig. 1. Base de Aprendizaje Automático. [7].

III. MACHINE LEARNING

La Inteligencia Artificial comprende áreas que determinan la complejidad de cada uno de los sistemas que la misma aborda, se puede representar como un enfoque escalable puesto que la misma IA opera en evolución constante a fin de perfeccionarse en cada proceso que realiza. En este sentido, surge el aprendizaje automático como se venía mencionando siendo una de las disciplinas impulsadas con la IA y su similar que es el Deep Learning que será estructurado dentro de la contextualización. [3].

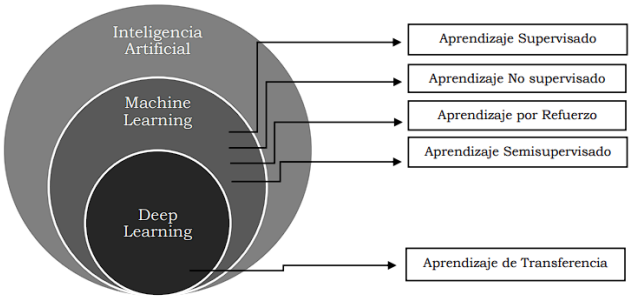

Fig. 2. Sub áreas de la Inteligencia Artificial. [3].

El Machine Learning o Aprendizaje Automático, se incorpora a una IA como un subconjunto que en términos de acción lo que hace es optimizar los procesos para que el proceso de aprender y mejorar desde una manera natural, básicamente sin requerir ordenes codificadas o programadas para tal fin. Es una disrupción dentro de los parámetros de tecnología conocidos, también dentro de su definición y la forma en que opera resulta ser factible la aproximación a diversas áreas desde la tipificación que posee y la manera como la misma permite individualizar escenarios de aplicación y complementación de procesos. [3].

Aprendizaje supervisado, básicamente es un contexto de aprendizaje con ayuda de datos ya establecidos que dan una visión sobre la respuesta correcta ejemplificado en procesos de validación. El opuesto, No Supervisado ya se define como una perspectiva de agrupación de datos desde algoritmos predefinidos, uno de sus principales usos surge en el agrupamiento de datos. Em tercer lugar, el aprendizaje de refuerzo aprende desde el entorno en el que se desarrolle, siendo la extensión de recompensas y la minimización de castigo los objetivos que se asumen en su funcionalidad. Y finalmente, el aprendizaje semi supervisado combina datos con patrones para tomar la mejor decisión posible. A largo plazo, el Machine Learning desarrolla capacidades de mejora y escalabilidad constante, sus usos son variables tales como predicción y generación de patrones de voz como mecanismo autónomo. [3].

IV. APLICACIÓN

En términos de aplicación, son muchos los sectores donde se ha intervenido con el modelo con efectividad máxima, uno de los más esperados y que ciertamente genera más preocupación al mismo tiempo es el relacionado con Ciberseguridad, si bien hay muchos beneficios no deja de haber un grado elevado de incertidumbre a largo plazo por efectos negativos. Si bien hay proyectos en marcha con Machine Learning como identificación de usuarios, desarrollo de software potencialmente sólido, toma de decisiones y una de las más importantes que se define desde la conciencia situacional que sería de gran valor en la época actual. Sin embargo, hay cuestionamientos importantes principalmente por el poder de las herramientas y la manera en que se usan, donde si bien el Aprendizaje Automático puede funcionar para optimizar la Ciberdefensa podría ser igual de efectivo para atacarla. [4].

Uno de los ejemplos más directamente usados con éxito surge con la aplicación dentro de la Inteligencia Militar, en este caso se usa Big Data para poder procesar la información y obtener detalles específicos de manera rápida. En este caso el Aprendizaje Automático agrupa información de todo tipo para encontrar patrones y permitir una mejor toma de decisiones basado en evidencia. Militarmente, hay más sectores como el mantenimiento y la operación área que también se benefician como todo tipo de operaciones que con la aplicación a nivel lógico permite mayor seguridad al momento de cumplir objetivos. [4].

Hay más escenarios donde se usan algoritmos de Inteligencia Artificial y Machine Learning para desarrollar sistemas de Ciberseguridad robustos y proporcionar también características específicas dentro de contextos de posicionamiento y protección. El uso de Inteligencia Artificial también ha sido extrapolado a otros sectores con el uso de Machine Learning con su estructura de aprendizaje supervisado que permite predecir ataques. Dicho sistema supervisado lo que genera es cierto valor de predicción basado en los datos de entrada con un conjunto que ha sido clasificado de manera anterior con etiquetas, la salida de dicho escenario siempre va a depender del escenario donde puede ser un valor de tipo numérico o una etiqueta referente a un tipo de clase. [5].

Los sistemas de detección de intrusos han sido individualizados por su capacidad de generar valor con el uso del Machine Learning con Inteligencia Artificial, lo que se genera es una optimización de la capacidad de comprensión y anticipación de ataques en casos donde la seguridad de un sistema se vea comprometido de manera compleja. El aprendizaje automático lo que hace es optimizar la selección adecuada de atributos dando como resultado una optimización general de las intrusiones y detección de las mismas. [5].

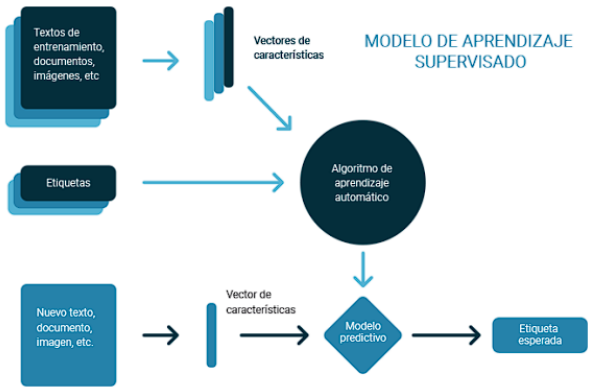

Fig. 3. Modelo de Aprendizaje Supervisado. [7].

En el 2020, uno de los aportes más efectivos fue la puesta en marcha de un sistema de detección y prevención de intrusos (IDPS) que buscaba específicamente orientarse a ataques de fuerza bruta y también dentro del aspecto de DDos en los casos encontrados de redes definidas por software. La utilización de ambos sistemas lo que permite es comparar redes neuronales, perceptrones multicapas y memoria a largo plazo. El resultado basado se estipula en un 99% de prevención de ataques y cerca del 100% en lo que se refiere a DDos. [5].

A nivel de Malware y protección el campo de uso del Machine Learning es ampliamente estructurado y ciertamente con un elevado grado de éxito, a nivel de análisis también hay una amplia utilización especialmente hablando lo referente a ATP (Amenaza avanzada persistente), siendo el factor de individualización determinante puesto que el propósito de cada situación es el que estructura mejor las técnicas a utilizar concluyendo en análisis de exploración amplios, resultando en la diferenciación de las características obtenidas y su posterior clasificación. [6].

Ejemplos relevantes resultan en el contenido en un framework propuesto que identificaba ATP´s mediante detección estructurada y que se basaba en Machine Learning. Donde su estructura se basaba en detección de amenazas, identificación y notificación de alertas, y la posterior predicción del proceso de identificación efectiva. [6].

En lo referente a IoT también hay varios modelos que se desarrollan como efectivos para la anticipación y clasificación de ataques directamente busquen denegar servicios (DoS), se enfocan entonces en la selección medida desde el objetivo mencionado. A continuación, una vista a la selección de algoritmos enfocados en ML que resultaron en beneficio para el objetivo de estudio: [8].

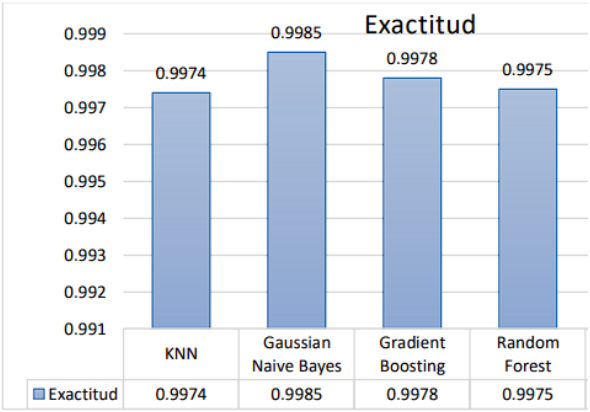

Fig. 4. Algoritmos de ML aplicados a IoT. [8].

Lo que reflejó el estudio fue un dominio importante del algoritmo de Gaussian clasifica con mejor resultado de exactitud que se refleja en un rendimiento mucho más efectivo en la clasificación de ataques de DoS. Igualmente, los algoritmos adicionales mencionados en la figura reflejan un porcentaje lo suficientemente alto como para ser efectivos dentro del mismo escenario. [8].

Desde una aproximación más enfocada en la sociedad y la cotidianidad de la misma, dejando de lado la complejidad de sistemas nacionales y globales. Es necesario también comprender que la IA y el Machine Learning desarrollan aportes dentro de la seguridad regular de las personas y la administración de los datos, probablemente el punto más directo dentro del proceso pasa por la capacidad de eliminar errores que se habían normalizado de alguna manera en el contexto industrial normal como por ejemplo pasaba con el apartado de errores humanos que terminaban esperándose pero no diseñando estrategias para evitarlos. Agregado a esto, los sistemas actuales carecen en muchos casos de escalabilidad precisamente porque su contexto no demanda mencionado proceso, sucede de otra manera cuando el objetivo es distinto pero en un sector que de alguna manera es básico la sociedad aún carece de herramientas para potenciar la detección de amenazas. Agregado a esto, es complejo asumirlo de manera total, pero la evolución de las formas de ataque e intervención de sistemas ha mejorado de manera exponencial en relación a las formas de defensa, es viable incluso asumir que en muchos casos los empresarios no se dan cuenta de que sucede y en qué momento sus sistemas se ven afectados de manera comprometida. [9].

Ejemplificando la importancia de la seguridad que brinda de manera directa un antivirus, ellos poseen la necesidad de implementar la IA y el Machine Learning por que los procesos básicos se mejoran y su seguridad como prestación de servicio también mejora de manera considerable. Esto se refleja en la clasificación, cursos y toma de decisiones respecto a la información disponible. También, termina siendo necesario establecer cursos de acción basados en incidencias y la síntesis de escenarios que se puedan agrupar según las probabilidades disponibles, eso logra desarrollar un pronóstico mucho más efectivo sobre cómo manejar las situaciones y brindar protección a los sistemas. [9].

Desde la demanda y la actividad de la prestación de servicios de seguridad pos antivirus y la evaluación de ellos mismos sobre factores de seguridad, la protección de datos y la administración de los mismos demandan acciones en constante mejoría para garantizar éxito. Primero, cumplimiento total de los reglamentos de datos y los perfile que termina siendo determinantes en la seguridad y el comportamiento de todos los sistemas. Segundo, una de las amenazas más grandes actualmente pasa por los bots y el poder que conllevan para afectar sistemas completos, el Machine Learning aplicado de manera global lograría detener este tipo de amenazas bloqueando directamente los sitios que desarrollan los bots y librando la amenaza de manera directa. Igualmente, notar este tipo de comportamiento le presenta al sistema una posibilidad de actúa con autonomía diseñando protocolos de prevención y anticipación basados en evidencia existente lo que mejora de manera significativa la actividad y mejora la seguridad. [9].

Adicional a las ventajas y ña cantidad de proyectos existentes hay otros enfoques donde se cuestionan ciertos aspectos que deben cumplirse para que haya éxito a largo plazo, el más importante pasa por que la IA con el Machine Learning administran datos de manera exponencial y técnicamente esto iría en contra de las leyes actuales de privacidad de datos y el tratamiento de los mismos. Bastaría con ver un caso de amenaza o infiltración por este tipo y debilitaría todo de manera inmediata, sumado a esto el otro aspecto que se desarrolla es la demanda de expertos y de personas que manipulan este tipo de herramientas. El Machine Learning demanda un nivel enorme de comprensión y mucho mas de mejoramiento, es indispensable contar con el talento necesario para poder afrontar retos y capacidad de respuesta ante las eventualidades, sucede que la cantidad de personas calificadas para esto es en extremo reducida y no parece haber una posibilidad clara de revertir la situación. [9].

Agregado a la información mencionada, existen recursos que se han potenciado dentro de las redes sociales siendo el medio masivo de comunicación a nivel global y el mismo por medio del cual las personas interactúan día a día. El caso más aplicado de primera medida fue Twitter, ya después de extrapoló a Instagram pero de primera medida de evaluará la implicación de Twitter y el funcionamiento directo. [10].

En contexto, se establece un mecanismo de análisis de publicaciones e interacción de usuarios que permiten anticipar el contenido de los mismos y la forma en que se puede evitar el acceso innecesario a información que comprometa la integridad de las personas y la seguridad de las mismas. El proceso del cual se parte es en análisis de sentimientos que a gran medida lo que hace es analizar la acción del usuario y comprender la intención del mismo desde el aprendizaje automático. Específicamente, lo que hace el algoritmo es agrupar las palabras de manera que puedan ser analizadas como parte de un todo, se observan las palabras positivas, las que tengan connotación negativa y las que son de tipo neutro. Tomando en cuenta también la apreciación referente a puntuaciones y la forma en que se expresa, esto porque también la puntuación delimita emociones al momento de escribirlas. Este proceso da como resultado intencionalidad de usuarios y la posición respecto a un tema de manera efectiva. [10].

Cabe mencionar que algunas de las técnicas lo que hacen es individualizar la intención desde el tipo de algoritmos que se aplica. Es decir, en un caso se aplica un algoritmo de árbol de decisiones y otro de clustering como K-Means, esto lo que hace es encontrar la precisión de palabras negativas y formular un camino a seguir desde la navegación de la persona y la manera en que percibe la actividad respecto a un tema. Igualmente, se aplica un grado de intencionalidad para evaluar polaridad de un comentario con aciertos muy cercanos a la perfección. [10].

Lo que permite esto es establecer análisis en tiempo real de decisiones y de contenido sobre la manera como el mismo se puede direccionar, ahora dentro de este tipo de acciones surgen una cantidad importante de problemas reflejados en la actitud ética y la forma en que se manejan los datos. Donde si bien es validado desde aproximaciones de seguridad, es muy condicional en el momento que las organizaciones lo usan para beneficio propio como el filtro de marcas y el bombardeo de spam, se entiende entonces que las personas estarían perdiendo el control de su navegación y serían mucho más manipulables de lo que se podría haber pensado jamás. [10].

V. DETECCION DE AMENAZAS

Una de las alternativas que se han potenciado de mejor manera es el uso de XDR (detección y respuesta extendida), si bien su base estructural funcionaba desde hace algunos años su nivel máximo de uso se estableció con el uso de Machine Learning y IA para enfoques de seguridad, referido especialmente a detección y amenazas. Lo que se desarrolla en este sentido es la capacidad de generar valor con acciones de primer plano en tiempo real referidas a detección y contención de todo tipo de amenazas. [11].

Conceptualmente, la XDR lo que hace es filtrar las brechas comunes dentro de sistemas de seguridad como la visibilidad y las capas de seguridad que estén presentes dentro de los sistemas, esto hace que se pueda tener una mejor percepción de amenazas y que las mismas se puedan neutralizar de manera más directa. Sumado a que con su capacidad de Machine Learning es capaz de agrupar registros, datos y todos los sucesos en cada uno de los procesos para diseñar protocolos de respuesta que ayudan a prevenir de manera más efectiva ataques e intentos de vulneración futiros. [11].

Actualmente, lo que se hace es que la XDR usa análisis avanzado y algoritmos de Machine Learning para ser capaces de identificar patrones y lograr capacidad de respuesta en tiempo real a las

situaciones que se van presentando, su acción contra amenazas como sus notificaciones de casos de interés son especialmente rápidas y fundamentadas lo que termina haciéndola una herramienta diferencial para el manejo y detección de posibles escenarios de ataque. [11].

Identificar datos se convierte en un proceso histórico tomando como referencia todos los datos existentes y clasificando la información desde este punto, se pueden determinar acciones de comportamiento y las incidencias previas a que sucedan. Su valor agregado entonces pasa por clasificación de escenarios de riesgo, apartar y filtrar equipos y direcciones afectadas de manera automática, analizar dichos equipos y escenarios de riesgo para brindar una solución. Posterior a esto se activan estrategias de mejoramiento para evitar que el mismo incidente suceda y se diseñan a su vez estrategias de impacto para relacionar el incidente con otros y tener un alcance mucho mayor en cuanto a la resolución de problemas se refiere. [11].

Sumando valor a la capacidad de XDR hay una perspectiva que permite diferenciar los caminos de acción entre una y otra apreciación, se trata del uso de SIEM (Administración de eventos de Información de Seguridad) juntos combinan una respuesta mejorada de anticipación y detección de amenazas en cualquier nivel. [12].

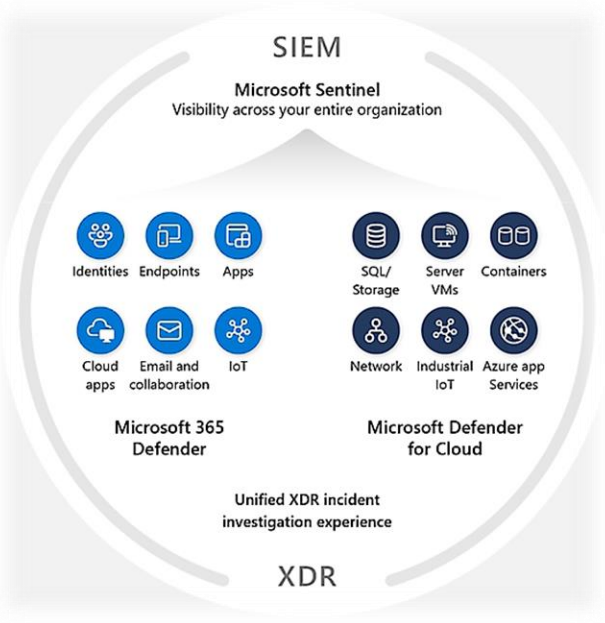

Fig. 5. SIEM y XDR. [12].

Microsoft, plantea una solución de ambos enfoques que ha sido de las más probadas y efectivas en la detección de amenazas, la herramienta en cuestión se denomina Sentinel. Lo que apunta Sentinel es una integración de manera previa en la nube con capacidades de anticipación de XDR para funcionar dentro de los entornos regulares como correos y labores de organizaciones empresariales, todo este enfoque determina una anticipación mejorada de infraestructura referente a bases de datos, contenedores, virtualización y también abarca lo referente a IoT. [12].

Igualmente, dentro de las soluciones básicas de una organización Microsoft es pionero en la articulación del SIEM con XDR al momento de encontrar una manera económica y efectiva de combatir amenazas con Inteligencia de primer nivel. Esto se refleja en la capacidad de brindar un sistema que procesa información desde el aprendizaje automático y responde de manera efectiva a los criterios que el mismo sistema demande. En este caso lo que se hace es que al obtener los datos de muestran las conexiones dentro de la infraestructura y haya una posibilidad directa de generar valor dentro de la aplicación de estándares de intervención. En este sentido utiliza bases de Sentinel y de la base de Microsoft 365 para dar un servicio diferencial que permita obtener los mejores resultados de protección con la mayor capacidad tecnológica posible. [13].

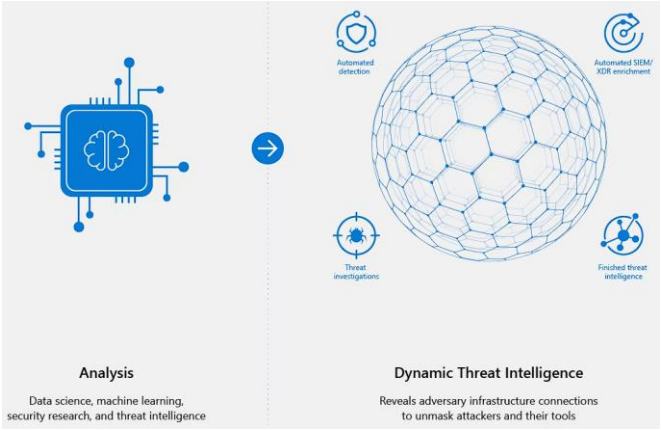

Fig. 6. Microsoft Intelligence. [13].

La tendencia muestra que las empresas van evolucionando en la prestación de un servicio diferencial teniendo en cuenta el grado de evolución de las tecnologías y la importancia de integrar las mismas. En este caso, la Administración de Eventos e Información de Seguridad y la dirección de respuesta extendida logran marcar una diferenciación en la eficacia que se requiere al proteger el patrimonio integral de una persona o directamente de las organizaciones. [13].

VI. GRAFICAS Y ESTADISTICAS

Dentro de la última época ha habido un crecimiento significativo de la IA y su uso dentro de la Ciberseguridad con todos los parámetros similares que componen su aplicación, en cuanto a proyecciones y estado actual de este sector se parte primero de la capacidad de crecimiento que tendría el sector dentro de los próximos años lo que básicamente aumentaría la demanda dando un crecimiento mucho más amplio de las herramientas ya existentes.

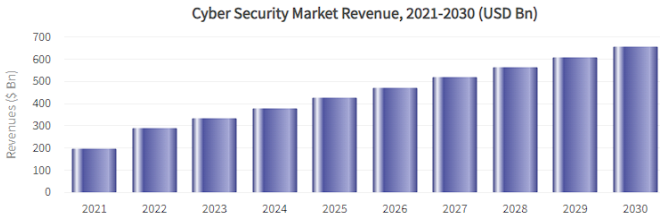

Fig. 7. Cibersecurity Market Revenue from 2021-2030. [14].

La estimación asume un crecimiento constante hasta unos 600 billones en el año 2030, la evidencia se basa en la creciente demanda de seguridad y la implementación de nuevos modelos ligados a la Inteligencia Artificial que facilitan los procesos y que a su vez brindan nuevas herramientas para obtener mejores resultados. Igualmente, se proyecta un aumento importante dentro de diversos sectores que optarían por este tipo de herramienta al contar con prestación de servicios en línea, desde el sector de salud hasta el manejo de la información de cualquier tipo. [14].

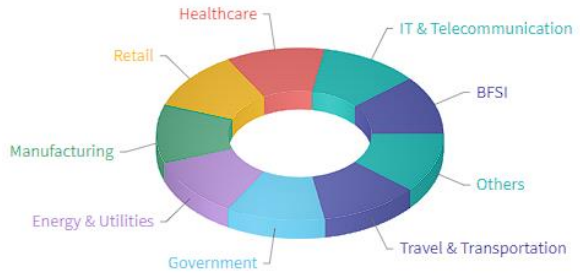

Fig. 8. Cibersecurity Market Segments. [14].

Referente a la representación de segmentos de mercado lo que se infiere es que contrario a lo que se manifiesta dentro de la última época que hay un factor predominante en el sector tecnológico en este caso no es así, hay una amplia recepción de diversos sectores que optan por incorporar la Ciberseguridad y sus derivados como mecanismo de protección de información. La sociedad afronta une época de transición donde una nueva era tecnológica será el camino y la manera como se afronte marcara la diferencia en todos los sectores existentes. [14].

Fig. 8. Cibersecurity Market Regions. [14].

La ubicación dentro de la figura lo que asume es que en la actualidad el Mercado es muy limitado más allá del crecimiento exponencial que existe, si bien hay una vasta teoría y puesta en marcha de ideas aún no se refleja de manera masiva dentro de todo el planeta. Probablemente estará limitado a sectores de gobierno o empresas cuyo dominio representan una gran mayoría como podría inferirse con Estados Unidos. Esto representa igualmente que las oportunidades de sacar provecho basado en el crecimiento descrito son muy importantes, el sector va a crecer y lejos de limitarse a la tecnología y la seguridad su campo de acción se estructura mucho más amplio que únicamente este. [14].

Dentro de las nuevas aplicaciones, también surge la mencionada Inteligencia en forma de chat como GPT que básicamente demandará a su vez iniciativas de seguridad mucho más poderosas que incorporen conceptos de IA y Machine Learning para fines de análisis en tiempo real. En este sentido, es necesario establecer escalabilidad en los sistemas y cierta capacidad de respuesta que se asemeje a las proyecciones y cifras actuales acerca de los usos de IA y el crecimiento de los mismos. [15].

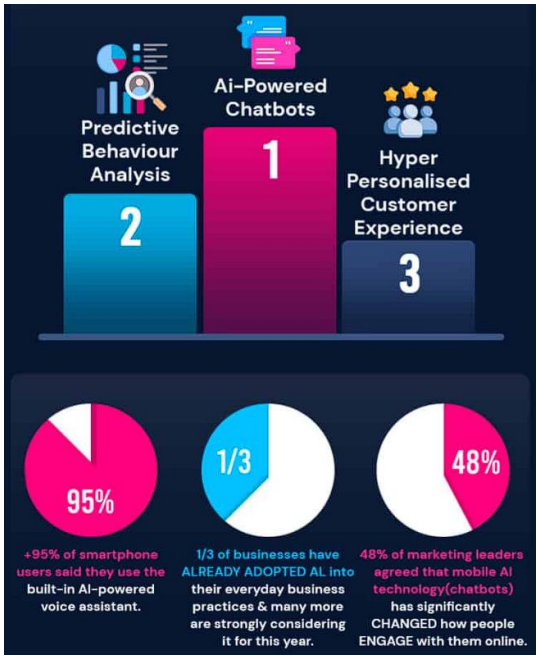

Fig. 9. Usos de IA actualmente. [15].

En contexto, las personas saben que está ocurriendo un cambio y lo reflejan en el entendimiento por ejemplo de cómo funciona el algoritmo de Instagram en cuanto a predicción de contenido se refiere y saben la cantidad de ventajas que todo esto desarrollará, la percepción sea positiva o negativa ya está y dependerá del avance el posicionamiento final. [15].

Son muchas las complicaciones que afronta el sector igualmente, se han desarrollado diversidad de ideas pero hay cierta carencia de mecanismos para llevarlas a cabo y ciertamente hay escepticismo sobre como terminaría funcionando todo dentro del futuro cercano. La Ciberseguridad estaría dentro de los sectores que más afrontaría ganancias pero serian proporcionales a los desafíos que esto asume, contrario a la IA y su expansión global la seguridad será la más afectada y con la demanda vendrá una necesidad importante de obtener resultados por encima de todas las cosas. [15].

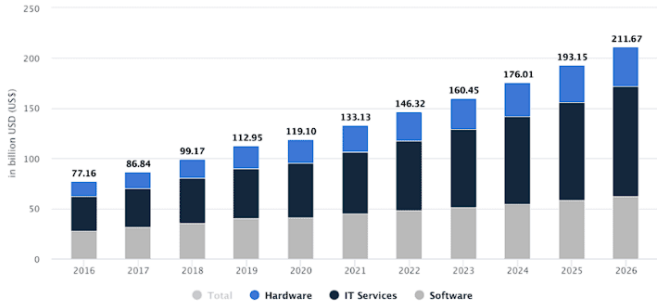

Fig. 10. Crecimiento Ciberseguridad en Billones de USD. [15].

Todos los sectores relacionados de manera directa con IT y seguridad se verán comprometidos a mejorar sus bases de operación para ser capaces de afrontar la era que se aproxima, mas allá de ser un enfoque de cambio o de eliminación como suelen llamar muchos es una oportunidad para generar valor y fortalecer de manera sistemática la capacidad de prestación de servicios. [15].

En otro apartado que se ha desarrollado como difícil de creer, un aspecto complejo de la IA pasa con la potencial reducción de fuerza laboral y la precariedad que afrontarían muchas personas, no se habla solo de Seguridad si no de la automatización de servicios que esto implica y la perdida de trabajos que asume a largo plazo. A continuación, se puede hacer una evaluación de la proyección a 2030 siendo aún un año cercano sin contemplarse como largo plazo dentro de la implementación de Inteligencia Artificial y todas sus características derivadas. [15].

Fig. 11. Proyección a 2030 de empleos relacionados con IA. [15].

La implementación de Inteligencia Artificial en ámbitos demandados por la sociedad tendrá un impacto determinante en la calidad de vida de las personas, mas allá de que haya un crecimiento en muchos sectores como la seguridad y la misma IA es complejo determinar aun el grado de daño que afrontaran diversidad de personas por la transición que se está desarrollando. [15].

En cuanto a números, la Inteligencia Artificial como todas sus derivaciones tendrán un impacto significativo en la vida de cada una de las personas que usen tecnología, ya sea para hacer procesos más sencillos o por el contrario por la complejidad que asume la misma IA. El dato con mayor relevancia viene de que China será la potencia

que va a dominar por completo el mercado de IA, con más del 25% de control global. Igualmente, es necesario recalcar que una de las razones por que la transición se demorará un tiempo es porque aún no hay gente lo suficientemente capacitada y esto demorará algo de tiempo. De ser de otra manera se hablara sin ningún problema que la IA sería el sector de más crecimiento en todo el mundo y con mayor capacidad de demanda. [15].

Como tema con menor relevancia pero que al final compromete la seguridad y el desarrollo de la inteligencia artificial viene marcado con el desarrollo de bots integrados directamente en robots, es un mercado que usualmente no se contempla pero que estará compuesto por Inteligencia Artificial, algoritmos de Machine Learning para mejoramiento continuo y de manera autónoma y sumado a eso tendrá aspectos ciertamente superiores en prestación de servicios de seguridad a todas las organizaciones o personas que los adopten. Se puede reflejar de manera directa la aproximación de crecimiento de mercado y la equivalencia durante los próximos años, se destaca que dentro de este periodo debería hacerse un nuevo estimado puesto que se materializarían muchos más escenarios de crecimiento y la sociedad tendría una mayor capacidad de absorción de información y el procesamiento de la misma con la Inteligencia Artificial. [16].

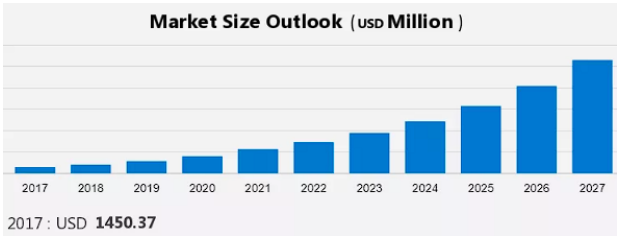

Fig. 12. Mercado de crecimiento sector de robots. [16].

Las empresas comprenderán la importancia de implementar estas herramientas de manera sistemática para reducir costos, optimizar procesos y lograr generar valor agregado por encima de todos los valores registrados de manera previa. El poder de la automatización se materializaría de manera mucho más directa con la adopción de estrategias de impacto para expandir el grado de acceso a estos elementos. [16].

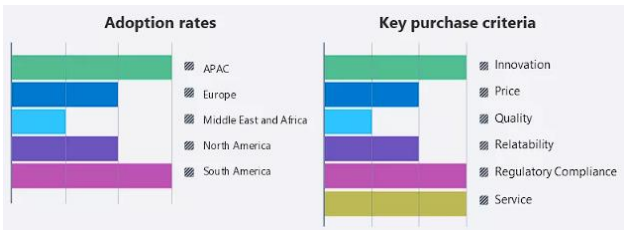

Fig. 13. Criterios y Acceso a robots. [16].

En la figura representada se observan los criterios de elección dentro de países al día de hoy, de manera preliminar ya hay un dominio por parte de china y se procura optar por la innovación como mecanismo de acceso y la forma en que los mismos terminan facilitando el cumplimiento de las tareas creando un mercado de manera efectiva. [16].

Habrá un aumento igualmente considerado de un mercado individual de IA enfocado en la prestación de servicios de este sector incluida la seguridad, la capacidad de mejoramiento y la expansión del mismo como mecanismo para proveer la demanda necesaria que sigue en crecimiento. Lo que se refleja es que los criterios harían un nuevo sector y una nueva forma de ver las cosas, los mercados regulares de IT quedarían obsoletos ante la capacidad de generar valor dentro de un sector que estructuralmente no se proyecta aun hasta donde podría crecer. [16].

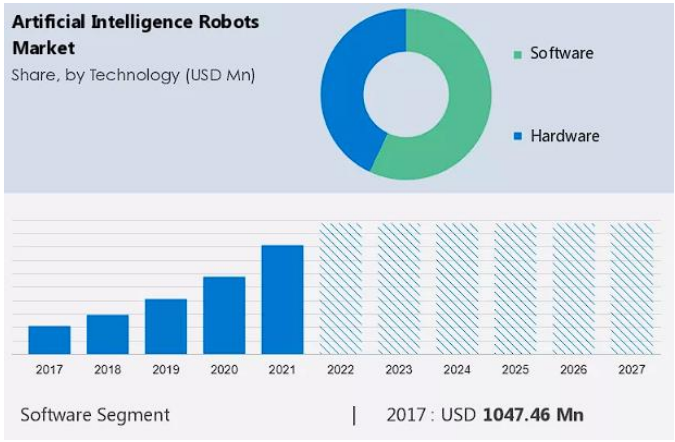

Fig. 14. Mercado especifico de Robots con IA. [16].

El mercado de APAC comandado por China será el que domine de manera completa este mercado de robots por 2027, habrá un cambio para la próxima era tecnológica y la forma en que los poderes se van a manejar. [16].

VII. TENDENCIAS

Dentro de la época actual hay dos aspectos que han desarrollado una necesidad de uso de la Ciberseguridad en su máxima expresión y los derivados de la misma como la inclusión de IA y la manera en que la misma genera beneficios de manera individual, desde la creciente amenaza de ataques por las vulnerabilidades de los sistemas hasta la pérdida de confianza de las personas que consideran los mismos sistemas no son seguros ya y no observan una capacidad de anticipación a todos estos problemas. Principalmente, se contempla el grado insuficiente de prestación de servicios en el aspecto de seguridad y la disponibilidad directa de la información más allá de contar con un sistema precisamente diseñado para brindar protección. [17].

La época de pandemia dejó un profundo grado de afectación en lo que refiere a seguridad, las personas se vuelven increíblemente confiadas y el trabajo termina siendo complejo de cualquier manera pues básicamente todas las personas se encuentran expuestas y demandan claves directas para afrontar los desafíos con miras al medio y largo plazo. [17].

El primer aspecto que se toma en cuenta es el referido al IoT, este enfoque lo que hace es conectar muchos más dispositivos de manera compartida. La Ciberseguridad es el sector que se determina como responsable dentro de este aspecto por que básicamente a mayor cantidad de dispositivos conectados mayor posibilidad de vulnerar un sistema habría, los encargados de Ciberseguridad deben brindar un esfuerzo agregado pero también desde un aspecto de gobierno debe existir un espacio donde se verifique y se diseñe un enfoque normativo que aplique a los problemas actuales y que como se hace con todo el aspecto de IA sea escalable a las necesidades y escenarios que se van presentando. [17].

Las conexiones en casa es otro elemento que debe revisarse y estructurarse como parte directa de una empresa, el trabajo remoto o el hibrido en dado caso son enfoques donde hay una conexión desde un sito ajeno a la empresa que no se puede proteger de manera inmediata, los desafíos demandan ser capaces de brindar acople a las necesidades de todos los sectores con el fin de proteger a máxima capacidad lo que pueda suceder. [17].

Las redes sociales no solo son filtros de información falsa en la actualidad, se han convertido en el vehículo para realizar ataques a personas que cuentan con un elevado grado de ingenuidad y que terminan exponiendo todos los recursos de los cuales son responsables. No es descabellado pensar que una persona se enfrente a procesos penales por violación de información sin saber que la misma sucedió. La parte digital debe evaluarse con o mas importancia que lo que se antoja actualmente como organización, es una época

compleja de transición que demanda esfuerzos en conjunto para afrontar los cambios. [17].

Ya se ha hablado de manera sistemática pero el papel de la IA seguirá evolucionando y no es descabellado asumir que el proceso seguirá creciendo demandando distintos objetivos a cumplir en cada caso empresarial, el reconocimiento de patrones por ejemplo puede adaptarse a diversos sectores aunque no se han evaluado y seguramente demandara acción de todas las partes. [17].

Cultura, es necesario que dentro de la época actual se genere un elevado grado de cultura y que las personas comprendan el grado de importancia de la información y la forma en que generarían valor desde la misma. Como en su momento sucedió con los celulares y la necesidad de proteger la información desde allí con seguridad y contraseñas, así como guardar la información de manera individual. Debe suceder lo mismo con el aspecto de seguridad enfocado a las organizaciones y lo que termine abarcando la IA como en el desarrollo y protección de datos. [17].

A nivel de Colombia, lo que se ha determinado es impulsar una revolución digital construida como 4.0 que busca estar a la vanguardia de los procesos que se viven en países de primer mundo y la necesidad de dar garantía a una gestión completa aprovechando los beneficios en automatización de procesos y la sistematización de las cosas. [18].

Colombia diseña sus bases de apertura a nuevas tecnologías desde tres aspectos críticos dentro de su conformación, el primero es la apertura de datos como parte de la transparencia de gobierno, seguido por la implementación de Inteligencia Artificial como mecanismo de generación de valor y optimización de la Ciberseguridad para generar fortalecimiento y progreso a un nivel mucho más alto. Y finalmente, Colombia dentro de su idea de proyectarse a largo plazo también toma en cuenta el marco ético que debe tenerse en cuenta en estos casos y que eventualmente va a tener una necesidad de profunda evaluación y generación de cambios. [18].

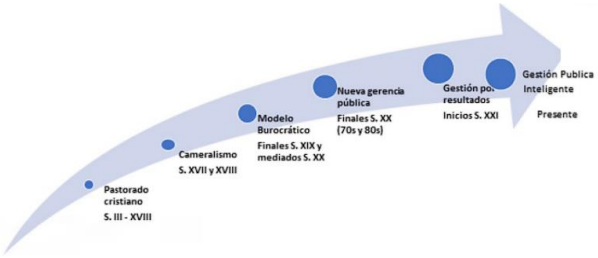

Fig. 15. Evolución de la Gestión en Colombia. [18].

La gestión dentro de estos aspectos lo que determina es la necesidad de brindar diferenciación y establecer un nuevo capítulo basado en los modelos gerenciales existentes y la forma en que los mismos manejen el país. [18].

En lo referido a Gobierno Digital, ya hay pioneros a nivel departamental:

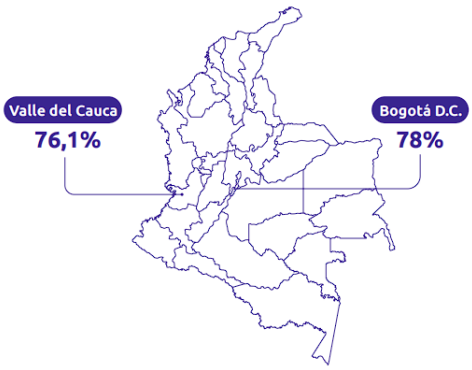

Fig. 16. Manejo y evolución de datos. [18].

Bogotá y el Valle del Cauca se convirtieron en pioneros de la transición de administraciones electrónicas a gobiernos digitales completos, esto lo que permite es posicionar precedentes de acción para las demás entidades que demanden acciones de cambio. Siendo la meta lograr una transición completa para todo el país en periodos de tiempo muy cortos y terminando con el resultado de ser la nación más innovadora y disruptiva en Latinoamérica. [18].

La meta de Colombia es lograr dicho objetivo de manera sistemática donde haya un crecimiento elevado o en el peor de los casos constante de las cifras necesarias para hablar de transición. [18].

Política	2018	2019	2020	2021
Gobierno digital	79,6	81,3	81,3	85,5
Seguridad digital	74,3	78,5	82,1	86,3

Tabla. 1. Crecimiento digital en Colombia. [18].

Se hace énfasis en que si bien las cifras van hasta 20221, es porque aún no se toma referentes completos por incorporación de Inteligencia Artificial de manera más amplia y con un alcance dentro de organizaciones regulares, esto habla de una época de transición acelerada y la importancia de mantener las ideas de crecimiento a toda costa en los gobiernos actuales y los próximos. [18].

Colombia está adelante en el dinamismo necesario para fomentar la IA y todas sus variantes, siendo el 2023 un año trascendental para materializar dicha ventaja y ser capaces de otorgar valor a la tecnología y desarrollar el impacto necesario. Colombia se caracteriza por ofrecer experiencias de consumo individuales que determina un gran avance en recopilación de datos y patrones para poder encontrar una expansión a nivel de mercadeo mucho más amplia de lo que se pudiera imaginar. En Colombia se impulsa una mejor toma de decisiones, mejores técnicas de consumo y optimización de procesos a nivel de organización. [19].

Uno de los desafíos más grandes para Colombia siendo potencia del comercio pasa por la necesidad de usar al máximo la IA para propagar sus ideas dentro del contexto y usar la Ciberseguridad para protegerse como país y para proteger a todas las personas que prestan el servicio. En cifras, el 44% de las empresas procura en al menos uno de los procesos usar Inteligencia Artificial, en un ámbito más avanzado el Aprendizaje Automático mejora las experiencias a nivel de cliente y brinda respuestas sobre la seguridad también. [19].

Lastimosamente, el problema es que a largo plazo Colombia carece de la infraestructura necesaria y la cantidad de profesionales adecuados para modelos de enseñanza, una inversión mucho más completa permitiría desarrollar mejores caminos de acción y evitar retroceder respecto al liderazgo existente en la región. Colombia cuenta con la capacidad de ser pionero en la región e impulsar de manera significativa su crecimiento y la productividad de todos sus sectores económicos. [19].

VIII. PLANTEAMIENTO DE PROBLEMA

Posterior al análisis realizado en toda la investigación se pueden concluir diversos escenarios de análisis que deben ser evaluados para poder contemplar un éxito generalizado de la IA junto la Ciberseguridad y el impacto que la misma desarrolle dentro de toda la sociedad. Si bien se establecen dentro de aspectos independientes debe comprenderse también que el éxito de la IA dependerá del cumplimiento de cada uno de ellos como un todo.

Primero, la normativa ética se desconoce a fin de que básicamente no existe. Técnicamente hablando se puede ejemplificar el ChatGPT donde ciertamente desarrolla una manera más simple de hacer las cosas pero al mismo tiempo condiciona gravemente la estabilidad de los modelos de aprendizaje y la forma en que los mismos ayudan a las personas. Sumado al grado de inseguridad que el mismo brinda por ser capaz de dar respuesta básicamente a lo que sea si se pregunta de manera adecuada, cuesta entonces comprender de qué manera se modificaría este tipo de acciones y como se frenaría el mismo impacto

que podrían tener dentro de toda la sociedad en un futuro cercano o incluso inmediato. Todos los cambios deben evaluarse desde aportes positivos y negativos.

Segundo, debe existir una normativa ética y regulatoria de la manera en que se administraran los datos y la forma en que se evitara asumir violaciones directas de privacidad de la información. La sociedad no está preparada básicamente porque no hay ningún contexto sobre el cual se pueda generar un análisis y desde el cual se pueda corregir y tratar potenciales errores. En este sentido, es viable que suceda un escenario a gran escala para el cual no haya ninguna justificación viable de acción y mucho menos de respuesta efectiva ante escenarios negativos, la reformulación de normativas y nuevas regulaciones seria de manera globalizada en este caso para contemplar un mejor resultado.

Tercero, es importante examinar potenciales efectos a largo plazo de las iniciativas de acción puesto que son escenarios con elevada incertidumbre que necesitan ayuda, entendido desde el sentido que debe haber formas efectivas de afrontar avances más profundos como sería el equivalente de amenazas más complejas. Contemplando que una avería dentro del tratamiento de datos podría tener consecuencias catastróficas para los involucrados e incluso contemplar un daño global a una economía de manera irreversible en cuanto a recursos es perfectamente contemplable.

En contexto, el planteamiento del problema pasa por que se han evaluado hasta ahora todos los beneficios y las mejoras que otorgan estas herramientas pero aún no se evalúa el grado de afectación que todo pueda tener a largo plazo. Ciertamente en su momento era una fase preliminar pero en este caso es necesario dimensionar ya escenario complejos de funcionamiento por que la sociedad demanda acciones en base a los beneficios que está absorbiendo y sus eventualidades.

Finalmente, es necesario direccionar que las necesidades de la IA deben contemplarse a nivel de sociedad contempla y la forma en que la misma asumirá un cambio de tal magnitud. La escalabilidad de cualquier sistema que se diseñe será crucial dentro de los procesos de mejora y modificación misma en busca de resultados positivos, igualmente surgirán muchos más detalles a tener en cuenta que deben evaluarse y que se irán presentando dentro del proceso. El tiempo es una variable a contemplar y que también marcara una diferencia en cualquier escenario que se evalúe.

IX. RESULTADOS

La Inteligencia Artificial ha desarrollado una nueva época de desarrollo tecnológico y una nueva forma de ver las cosas, los datos pasan a tener una importancia remarcable actualmente y la manera en que se desarrolle su uso determinara el éxito de las tecnologías. Igualmente, recién en la época actual se pueden evaluar realmente la cantidad de beneficios que esto aporta a una sociedad saturada por información y sin capacidad de manejarla, la inclusión de Machine Learning y la capacidad del mismo para brindar autonomía se asume aun como una fase preliminar dentro de los procesos de cambios que afronta la sociedad y la forma en que se genera valor en cada acción.

Si bien la información recolectada mayoritariamente asume beneficios es complejo asumir igualmente que no habría ningún escenario negativo dentro del proceso, la sola parte ética asume un grado elevado de preocupación y la forma en que la misma termine afectando la estabilidad de las sociedades a largo plazo. Contrario a lo que se considera como un único beneficio, deben evaluarse las implicaciones en materia de seguridad como la situación tratada dentro de la Ciberseguridad y la forma en que la misma pueda prepararse y capacitarse realmente para tener una base de respuesta sobre los escenarios que se puedan presentar para tratarlos de manera efectiva.

En síntesis, la IA y sus derivados no son una opción y se estarán propagando de manera más rápida cada vez, el punto de inflexión va a terminar siendo la manera en que los mismos se manejen y la forma en que se asuman beneficios como inconvenientes por el grado de impacto que la herramienta tiene contemplándola a nivel global. Igualmente, debe existir un espacio para evaluar la manera en que se desarrollen estrategias de respuesta ante eventualidades de carácter global, la Ciberseguridad es una herramienta efectiva pero no entrenada al día de hoy para un elevado grado de daños, este escenario se contempla al momento de evaluar el desempeño y funcionamiento de una implementación de IA de manera global. Debe contemplarse un marco ético sobre el cual operen las herramientas y que a su vez permita tener una respuesta antes las eventualidades que se van desarrollando, siendo el problema que dicho escenario al día de hoy no existe de manera correcta y complica asumir escenarios futuros sin ninguna base procedimental. Es cuestión de tiempo para que la sociedad se va inmersa en una encrucijada similar a la situación que se vive con las redes sociales y el control que se puede implementar sin demasiado esfuerzo, se requiere acción y de manera efectiva para mejorar las condiciones actuales y evitar daños que incluso ameriten evaluar la implementación de las herramientas.

X. CONCLUSIONES

La Inteligencia Artificial dentro de su capacidad de prestación de servicios lo que ofrece es un factor diferencial entre las formas como operan los servicios y una nueva visión del mismo proceso, en términos de avance y generación de cambio el proceso termina siendo más una transición que una opción por la cantidad de beneficios y los potenciales resultados a largo plazo de la misma idea. Se trata de competitividad al máximo estado posible.

La Ciberseguridad afrontará una época compleja en cuanto a desafíos pero también en lo referente a crecimiento y a la capacidad de generar valor dentro de un servicio, deberá potenciarse a gran escala con el fin de ser capaz de asumir el grado de demanda que habrá y la forma en que la misma terminaría generando valor en todo el desarrollo y puesta en marcha de sistemas de IA y todos los elementos que eso conlleva.

Un dato muy importante es que por parte del gobierno debe existir una iniciativa a regular de manera temprana los mecanismos sobre los cuales opera la IA y el tratamiento de la información, resulta ser prudente hacerlo pronto previo a una implementación completa de los servicios. Esto evitaría contemplar conflictos de intereses y la complejidad de manejar escenarios de infracciones relacionadas con datos y el tratamiento de los mismos a gran escala, también violaciones de normativas y tratados de información.

Deben direccionarse marcos éticos para el uso y promoción de los servicios de IA así como evaluar el impacto en juventudes y los modelos de aprendizaje actuales, herramientas como ChatGPT complican a gran escala la forma en que los jóvenes consumen información y afecta a largo plazo la productividad y el desarrollo de cualquier sociedad.

La sociedad afronta una transición relacionada con la tecnología y la capacidad de generar valor y enfocar un espacio completamente distinto a la forma en que se manejan los datos actualmente, se abren posibilidades ilimitadas en la forma en que se puede conectar una economía y el crecimiento de todas las ciudades vendría siendo exponencial a largo plazo.

El Machine Learning surge como un acompañante directo de la IA como prestadores de un servicio diferencial en lo referente a generación de valor y autonomía de procesos, resulta necesario entonces brindar información y un profundo contexto sobre como estructurar más canales de información y uso especialmente para que los procesos de cambio no terminen siendo más demorados de lo necesario.

Las transformaciones obedecen también a una necesidad profunda de cambio por vulnerabilidades y falta de acción en sistemas obsoletos que necesitan mejoras para seguir prestando un servicio efectivo, la automatización de un proceso se asume como el beneficio principal

dentro del sector y la forma en que se generaría valor de manera sistemática.

A nivel de Colombia, los procesos de transformación obedecen a una profunda necesidad de necesidades sociales como el acceso a redes de internet y la banda ancha como mecanismo de avance en forma de sociedad, se proyecta que el país podría solucionar diversos problemas dentro de su condición general al momento de lograr generar conciencia y operatividad sobre sus ciudadanos dando acceso a las redes y la información como medio de educación para poder generar beneficios.

Finalmente, la sociedad ha afrontado muchas épocas complejas de cambio y esta no será una excepción falta ver como se haría dicho proceso y de qué manera se afrontarán potenciales consecuencias. El cambio es comparable a la aparición del internet y las comunicaciones de manera global, dependerá de todos como colectividad para poder generar el mejor resultado posible. Lo que se ve hasta este momento es apenas una perspectiva que sigue en evolución y que dicha evolución debe contar con criterios serios para poder garantizar el debido proceso y una respuesta clara a las necesidades que se demanden en el mundo constantemente.

XI. REFERENCIAS

[1] Álvarez, J. Inteligencia artificial: ¿Oportunidad o amenaza? Revista de Investigación y Evaluación Educativa, 10(1), 2023, 4-5.

[2] Diaz, J. J. S., Rincón, A. R., & Jiménez-Canizales, C. E. Inteligencia artificial y aprendizaje automatizado, ¿oportunidad o amenaza? Revista Colombiana de Endocrinología, Diabetes & Metabolismo, 2023, 10(2).

[3] Pedraza Caro, J. D. La inteligencia artificial en la sociedad: explorando su impacto actual y los desafíos futuros, 2023.

[4] Alcántara Suárez, E. J. Análisis de la aplicación de Machine Learning en sistemas de defensa, 2023.

[5] Montes-Gil, J. A., Isaza-Cadavid, G., & Duque-Méndez, N. D. Efecto de la selección de atributos en el desempeño de un IDS basado en machine learning para detección de intrusos en ataques DDoS. South Florida Journal of Development, 4(2), 2023, 918-928.

[6] Liras, L. F. M. Identificación de" malware" perteneciente a ataques APT mediante la selección de características altamente discriminatorias usando técnicas de" Machine Learning" (Doctoral dissertation, Universidad de León), (2023).

[7] Fernández Khatiboun, A. Machine learning en Ciberseguridad, 2019.

[8] Vargas Salamanca, O. E. (2023). Detección de amenazas en redes IoT empleando modelos híbridos de machine learning y redes neuronales.

[9] Kaspersky (2023). La IA y el Machine Learning en la Ciberseguridad: cómo determinarán el futuro. [Online]. Available: https://www.kaspersky.es/resource-center/definitions/ai-cybersecurity

[10] Arnedo Nieto, D. Detección de amenazas cercanas en la ciudad mediante el uso de redes sociales, 2023.

[11] IBM. (2023) ¿Qué es XDR? [Online]. Available: https://www.ibm.com/mx-es/topics/xdr

[12] Microsoft. (2023) ¿Por qué se recomienda combinar SIEM y XDR? [Online]. Available: https://www.microsoft.com/es-co/security/business/solutions/siem-xdr-threat-protection

[13] Microsoft. (2023). Inteligencia contra amenazas de Microsoft Defender. [Online]. Available: https://www.microsoft.com/es-co/security/business/siem-and-xdr/microsoft-defender-threat-intelligence

[14] Nextmsc (2022). Cyber Security Market. [Online]. Available: https://www.nextmsc.com/report/cyber-security-market

[15] Search Logistics (2023). Artificial Intelligence for 2023. [Online]. Available: https://www.searchlogistics.com/learn/statistics/artificial-intelligence-statistics/

[16] AI robots market based on Technology, type and location. 2023-2027. [Online]. Available: https://www.technavio.com/report/artificial-intelligence-robots-market-industry-analysis

[17] Marr, B. (2022). Las cinco principales tendencias de Ciberseguridad para 2023. [Online]. Available: https://forbes.es/empresas/194234/las-cinco-principales-tendencias-de-ciberseguridad-para-2023/

[18] Diaz, M. R. O., & Ospina, K. J. Z. Gobierno digital e inteligencia artificial, una mirada al caso colombiano. Administración & Desarrollo, 53(1), 2023, 1-34.

[19] Diaz, L. Colombia entre los líderes en inversión y crecimiento de analítica e IA. [Online]. Available: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/colombia-entre-los-lideres-de-inversion-y-crecimiento-de-ia-747148