Polo del Conocimiento

Pol. Con. (Edición núm. 55) Vol. 6, No 2
Febrero 2021, pp. 1154-1173
ISSN: 2550 - 682X
DOI: 10.23857/pc.v6i2.2430

La vinculación entre la inteligencia artificial y la seguridad cibernética en el Ecuador. Notas sobre una interconexión necesaria

The link between artificial intelligence and cybersecurity in Ecuador. Notes on a required interconnection.

O vínculo entre inteligência artificial e segurança cibernética no Equador. Notas sobre uma interconexão necessária

Sardis Otilia Mosquera-Chere [I]
sardysmosquera@gmail.com
https://orcid.org/0000-0003-3058-920X

Correspondencia: sardysmosquera@gmail.com

Ciencias técnicas y aplicadas
Artículo de revisión

***Recibido:** 20 de enero de 2021 ***Aceptado:** 26 de enero de 2021 * **Publicado:** 27 de febrero de 2021

I. Magister en Docencia y Desarrollo del Currículo, Ingeniero en Sistemas Informáticos, Tecnólogo en Informática, Docente Investigadora de la Carrera de Tecnologías de la Información en la Facultad de Ingenierías de la Universidad Técnica Luis Vargas Torres de Esmeraldas, Ecuador.

Resumen

El ser humano ha sufrido una cantidad de cambios a lo largo de los años en todos los aspectos de la vida, desde la economía hasta la forma de ver el mundo. En ese sentido, las nuevas estrategias en la informática siguen revolucionado el mundo. Desde la inclusión de la inteligencia artificial, hasta los métodos de ciberseguridad. Sin embargo, hoy en día se menciona cada vez más la vinculación entre ambas, buscando reforzar cada aspecto vulnerable de la cibernética. Por esto, y ante la necesidad de contar con sistemas de almacenamiento seguro, se busca dar a entender la importancia que tiene implementar técnicas basadas en la inteligencia artificial. Basándose en el hecho de que es un mecanismo efectivo para la prevención y la reacción ante los inminentes riesgos a los que se está expuesto, además de que permite cumplir con los lineamientos de la ciberseguridad: confidencialidad, integridad y disponibilidad. De igual manera, es necesario destacar que las técnicas desarrolladas a lo largo de los años por la inteligencia artificial han empezado a aplicarse en una gran variedad de campos que han brindado seguridad y confiabilidad a su uso constante. La interconexión entre la IA y la ciberseguridad, se alza como una de las soluciones más importantes e innovadoras para mitigar a gran escala los ataques cibernéticos que sufren los usuarios y empresas que han decidido poner su confianza en la nube y que se han visto vulnerados por estos intrusos informáticos. Los resultados obtenidos en esta investigación, han arrojado un evidente recibimiento de la interconexión como un nuevo método de reforzamiento en la seguridad cibernética.

Palabra claves: Inteligencia artificial; seguridad informática; ciberseguridad; seguridad de redes; herramientas de seguridad informática; protección de datos.

Abstract

Human beings have undergone a number of changes over the years in all aspects of life, from the economy to the way we see the world. In that sense, the new strategies in computing continue to revolutionize the world. From the inclusion of artificial intelligence, to cybersecurity methods. However, nowadays the link between the two is increasingly mentioned, seeking to reinforce every vulnerable aspect of cybernetics.For this reason, and given the need to have secure storage systems, we seek to understand the importance of implementing techniques based on artificial intelligence. Based on the fact that it is an effective mechanism for prevention and reaction to the imminent risks to which one is exposed, in addition to allowing compliance with cybersecurity guidelines:

confidentiality, integrity and availability. In the same way, it is necessary to emphasize that the techniques developed over the years by artificial intelligence have begun to be applied in a wide variety of fields that have provided security and reliability to its constant use. The interconnection between AI and cybersecurity, stands as one of the most important and innovative solutions to mitigate large-scale cyber-attacks suffered by users and companies who have decided to put their trust in the cloud and who have been compromised by these computer intruders. The results obtained in this research have shown an evident reception of interconnection as a new method of reinforcing cybersecurity.

Key Word: Artificial intelligence; Informatic security; cybersecurity; network security; computer security tools; Data Protection.

Resumo

Os seres humanos passaram por uma série de mudanças ao longo dos anos em todos os aspectos da vida, desde a economia até a forma como vemos o mundo. Nesse sentido, as novas estratégias da informática continuam revolucionando o mundo. Da inclusão da inteligência artificial aos métodos de cibersegurança. No entanto, hoje em dia a ligação entre os dois é cada vez mais mencionada, buscando reforçar todos os aspectos vulneráveis da cibernética. Por isso, e diante da necessidade de sistemas de armazenamento seguros, buscamos entender a importância da implementação de técnicas baseadas em inteligência artificial. Por se tratar de um mecanismo eficaz de prevenção e reação aos riscos iminentes a que se está exposto, além de permitir o cumprimento das diretrizes de segurança cibernética: confidencialidade, integridade e disponibilidade. Da mesma forma, é necessário ressaltar que as técnicas desenvolvidas ao longo dos anos pela inteligência artificial passaram a ser aplicadas nos mais diversos campos que têm proporcionado segurança e confiabilidade ao seu uso constante. A interconexão entre IA e cibersegurança, destaca-se como uma das soluções mais importantes e inovadoras para mitigar ciberataques em grande escala sofridos por usuários e empresas que decidiram confiar na nuvem e foram comprometidos por esses invasores de computador. Os resultados obtidos nesta pesquisa mostraram uma recepção evidente da interconexão como um novo método de reforço da segurança cibernética.

Palavras-chave: Inteligência artificial; segurança informática; cíber segurança; segurança de rede;

ferramentas de segurança informática; proteção de dados.

Introducción

Tomando en cuenta a (Rocha, 2011) "se hace énfasis en que con el inicio de la humanidad se hace presente la información y con ella distintas formas destinadas a su almacenamiento". En la actualidad, la información es aún uno de los objetos con mucho valor para la población y las diferentes organizaciones, en especial en la toma de decisiones.

La seguridad de la información comenzó en el interior de diversas organizaciones a nivel mundial, las cuales incrementaron los procesos informatizados en los cuales solo tenían acceso los administradores y los analistas técnicos, debido a que estos se encargaban de buscar las distintas fallas de seguridad que pudieran existir e intentaban solucionarlas de la mejor manera que les fuese posible.

Aunado a eso, no se contaba con un conocimiento claro y conciso acerca de la seguridad cibernética, lo que ocasionaba que durante todo este proceso se aumentara la facilidad con la que se transmitía una cantidad de información por medio de procesos automáticos que permitieron el uso de internet como plataforma de sus movimientos de información. De esta manera, se logró una mayor fluidez en las comunicaciones interpersonales, en las transacciones o en el flujo digital de todo tipo. Cabe destacar, que esto dejó muchos datos expuestos a terceros no autorizados en sus sistemas. Como bien menciona (Tori, 2008)

Gracias a la ausencia de una plataforma educativa que formalizara la seguridad informática, se apreciaría entonces un comportamiento inusual con los recursos compartidos. Los jóvenes de todo el mundo entraban a internet a divertirse con los sistemas informáticos de sus países, engañando de esta manera a las centrales telefónicas y al mismo tiempo, intercambiando información con cualquier persona en cualquier parte del mundo. Es allí, donde se originan los mejores profesionales de seguridad para ese entonces, así como los llamados intrusos cibernéticos. (Pág. 37).

Debido a lo previamente mencionado, se hizo demasiado evidente la falta de un servicio profesional que fuese capaz de detectar los movimientos poco comunes que defendieran los datos, imitando al intruso y que permitiera de esa forma evaluar de manera real las condiciones de seguridad para que, en el supuesto caso de existir fallas en el sistema, fuera posible solucionarlas o manejarlas de forma preventiva, reactiva y correctiva. Dadas las crecientes amenazas para todos

los datos que se hallan en la red y su paulatina evolución de manera paralela y constante con el crecimiento de la tecnología y todo lo que concierne a la seguridad informática, se empieza a definir y reorganizar una necesaria búsqueda de soluciones con la finalidad de mitigar los riesgos y reducir la probabilidad de que estos se materialicen y afecten muy gravemente, ocupándose hasta el presente día de generar buenas prácticas destinadas a dar garantías en sistemas de información que puedan ser seguros y confiables, basándose primordialmente en la implementación del uso de la inteligencia artificial como generadora de herramientas de control tanto a nivel de hardware como de software; ya que se conoce la existencia de intrusos que pueden perjudicar el sistema operativo, las aplicaciones instaladas o, simplemente, tomar el control del equipo afectado.

Es en este punto, donde se comienza a hablar y a dar como una solución viable, la interconexión necesaria entre la IA y la ciberseguridad, debido a la gran cantidad de datos personales y con similitudes humanas que puede llegar a manejar la inteligencia artificial, buscando mejoras en la seguridad al utilizar de manera correcta y coherente los datos obtenidos. En el mismo orden de ideas, se han establecidos políticas o parámetros que garantizan el libre y abierto acceso a la información, brindando así una enorme cantidad de licencias para la recolección de datos de manera automática y autorizada por los mismos usuarios, entendiendo que `” son tecnologías seguras y utilizadas con el fin de proteger los activos de cualquier organización, lo cual la Unión Internacional de Telecomunicaciones o UIT entiende como «ciberseguridad»” (UIT, 2010).

La ciberseguridad o, dicho en otras palabras, la seguridad informática, pretende garantizar que se almacenen y se mantengan las propiedades de seguridad de los datos, permitiendo así que el constante acceso a los sistemas no sea vulnerable a ataques, intrusiones de los bien llamados y conocidos en el mundo de la tecnología como: `” hackers” presentes en el ciberentorno y que afecten la integridad y confidencialidad de los datos almacenados en la nube. La inteligencia artificial busca el camino coherente de estudiar y analizar el comportamiento humano en aspectos de comprensión, percepción, resolución de problemas y la toma de decisiones, lo cual al aplicarse en una computadora permite que se creen aplicaciones de IA que principalmente simulan actividades del hombre. Bajo estas características, los sistemas de IA tratan datos numéricos con algoritmos clásicos que permiten abordar los diferentes problemas sin solución.

El principal foco de atención para lograr darle solución a las problemáticas existentes en relación a la violación de la seguridad informática, se basa en conseguir expandir el conocimiento adecuado acerca de la importancia que posee la vinculación de la inteligencia artificial con la seguridad

cibernética, ya que el mundo de la ciberseguridad ha cambiado con el paso del tiempo. Esto se debe a que los atacantes o intrusos de la red, han aprendido a automatizar y manejar a su antojo el código malicioso a tal punto de modificarlo para su beneficio, logrando incluso inundar una empresa hasta que se produzca una brecha. Y la realidad es que muchas empresas, bien sea organizaciones pequeñas, medianas o hasta marcas mayormente conocidas, han sufrido muy probablemente ataques violentando su seguridad sin ser detectados los involucrados.

Del mismo modo, la IA afecta en distintas medidas el modo en que las personas viven su día a día, pues su implementación modifica de diferentes maneras el entorno que se conoce, ortodoxo y con parámetros establecidos. A fin de asegurar que los sistemas desarrollados se mantengan con los valores humanos, se requieren encontrar métodos que incorporen los principios éticos y las preocupaciones sociales. Actualmente, se buscan alternativas de protección y refuerzo de la seguridad cibernética, en especial mediante el uso de tecnologías avanzadas, con dominios técnicos con los que se logren solucionar problemas reduciendo el tiempo de espera y de afectación de los usuarios o de los sistemas afectados; se habla. Es por eso que se habla a menudo del uso de la inteligencia artificial o IA, concebida como un insumo crucial para el progreso y la robustez de la ciberseguridad.

Por otra parte, la seguridad informática cuenta con tres principios fundamentales: confidencialidad, integridad y disponibilidad. Estos sustentan y son la principal piedra angular de cualquier sistema que se pretenda implementar, puesto que a partir de esto la seguridad informática se vuelve indispensable, dado que frente a muchos casos no es posible estimar el valor de la información suministrada o recolectada. En tal sentido, la inteligencia artificial ha tenido un rol importante en la búsqueda de diferentes áreas de seguridad informática, como, por ejemplo, su utilización en redes mediante la detección de intrusos y bloqueos de correos no deseados o los también llamados "SPAM", antivirus, entre otros, lo cual ha generado que sistemas generalizados operen de manera automática, adaptativa y proactiva. (Cohen, 2007)

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

Marco metodológico

Según define (Hernández Sampieri, 2014) el termino diseño "se refiere al plan o estrategia concebida para obtener la información que se desea con el fin de responder al planteamiento del problema". El nivel de investigación es de tipo descriptiva y experimental, ya que se busca dar a conocer con mayor profundidad la información relacionada a la importancia y la vinculación de la ciberseguridad con la IA.

Por consiguiente, podemos acotar que el diseño de la investigación es de tipo investigativo, documental de campo, ya que se observa que las realidades sean teóricas o no, a través de varios tipos de documentos que utiliza un sistema de análisis para presentar datos e información sobre el tema a investigar, el cual ayuda con la obtención de los resultados para el desarrollo del proyecto, ya que se centra en la observación, registro, descripción, explicación y análisis; Es decir, se detecta el problema y se busca una solución viable. Por su parte, la modalidad del tipo de estudio es un proyecto factible, porque de acuerdo con (Hurtado, 2008) refiere que:

Un proyecto factible consiste en la elaboración de una propuesta, un plan, un programa o un modelo, como solución a un problema o necesidad de tipo práctico, ya sea de un grupo social, o de una institución, o de una región geográfica en un área particular del conocimiento, a partir de un diagnóstico preciso de las necesidades del momento, los procesos explicativos o generadores involucrados y de las tendencias futuras, es decir, con base en los resultados de un proceso investigativo. (pág. 45).

Es importante agregar que la población total seleccionada, eran personas pertenecientes al PYME (pequeñas y medianas empresas) que han buscado la expansión de negocio con la ayuda de la tecnología. Por último, la muestra a escoger fueron 30 personas, que manifestaron una mayor deficiencia de información sobre esta nueva alternativa de vinculación existente entre la inteligencia artificial y seguridad cibernética. Esta elección, se hizo por medio de una técnica denominada muestreo no probabilístico; el cual se refiere al estudio o el análisis de grupos pequeños de una población donde no todos los miembros tienen la posibilidad de ser seleccionados debido a ciertos factores como: conocimiento, tiempo o costo. Según (Arias, 2012) "El muestreo no probabilístico es una técnica de muestreo donde las muestras se recogen en un proceso que no brinda a todos los individuos de la población iguales oportunidades de ser seleccionados".

Pol. Con. (Edición núm. 55) Vol. 6, No 2, febrero 2021, pp. 1154-1173, ISSN: 2550 - 682X

Técnicas y métodos

Según (Arias, 2012), "Un instrumento de recolección de datos es cualquier recurso, dispositivo o formato (en papel o digital), que se utiliza para obtener, registrar o almacenar información". Desde este marco referencial, las técnicas necesarias para la exitosa realización del proyecto, están principalmente basadas en la recolección y expansión de datos referente al tema en cuestión que puedan servir como guía a lo largo de la investigación.

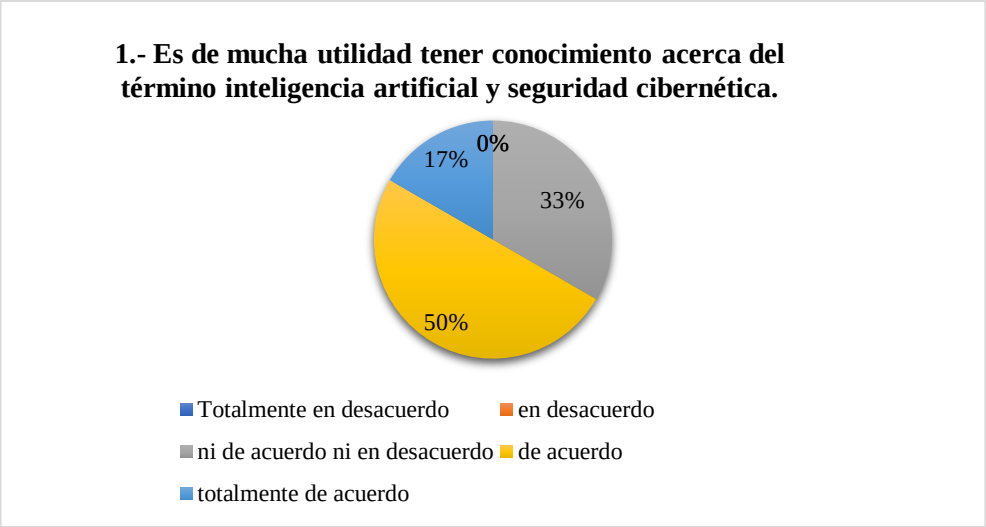
La técnica empleada para la recolección de datos, fue una encuesta de tipo opcional, la cual ayudó a obtener mucha información personalizada con el objetivo de obtener nuevas ideas y diferentes formas de pensar, así como conocer el nivel de documentación que posee cada individuo basado con la informática. Esta, estaba compuesta de quince (15) ítems que permiten llevar a cabo el estudio de forma eficaz.

De igual manera se hizo uso de la escala de Likert, la cual explica (Méndez, 2010) "Es una escala psicométrica comúnmente utilizada en cuestionarios, y es la escala de uso más amplio en encuestas para la investigación". Una vez elaborado este instrumento, se acudió a un juicio de expertos que validaron y dieron peso a la confiabilidad del mismo, dicho cuestionario, fue aplicado a la muestra en estudio, para finalmente analizar las afirmaciones obtenidas bajo técnicas estadísticas que ayudaron a formular las conclusiones del trabajo investigativo.

Análisis y discusión de los resultados

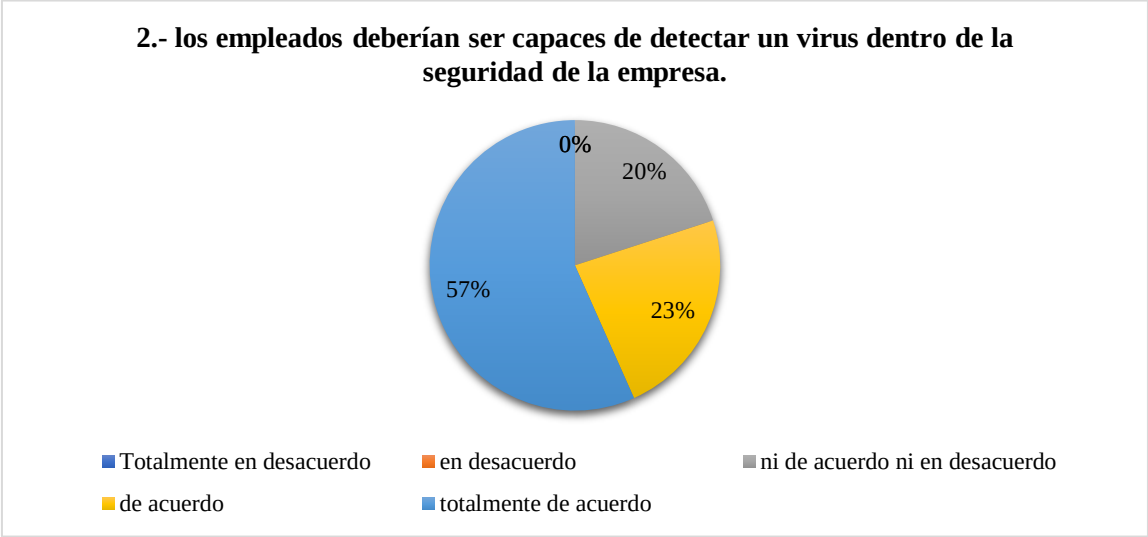
Para (Hernández Sampieri, 2010) "Recolectar los datos implica elaborar un plan detallado de procedimientos que nos conduzcan a reunir datos con un propósito específico" (p.274). De esta forma, se logró obtener la información relevante e importante para determinar qué tan exitoso puede llegar a ser la vinculación absoluta mediante la interconexión necesaria de la IA con la seguridad cibernética. Quedando comprendida de la siguiente manera:

Gráfico Nº1: Es de mucha utilidad tener conocimiento acerca del término inteligencia artificial y seguridad cibernética



Análisis: El presente gráfico resalta que el 38% de la población está totalmente de acuerdo sobre la utilidad de tener conocimientos acerca de los términos de inteligencia artificial y seguridad cibernética, y el 37% está de acuerdo con estos conocimientos, mientras que un 25% se encuentra en modo neutral ni de acuerdo ni en desacuerdo.

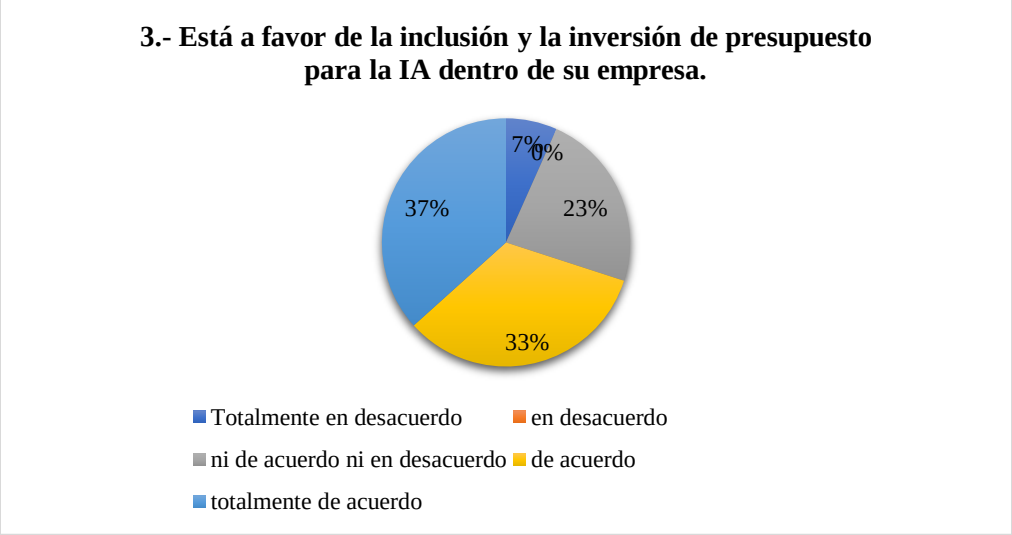
Gráfico Nº2: Los empleados deberían ser capaces de detectar un virus dentro de la seguridad de la empresa



Análisis: En el gráfico generado se resaltan los siguientes resultados: el 46% está totalmente de acuerdo con que sus empleados deben ser capaces de detectar cualquier virus dentro de la seguridad de la empresa. Un 29% está de acuerdo con estos conocimientos de sus empleados, sin embargo,

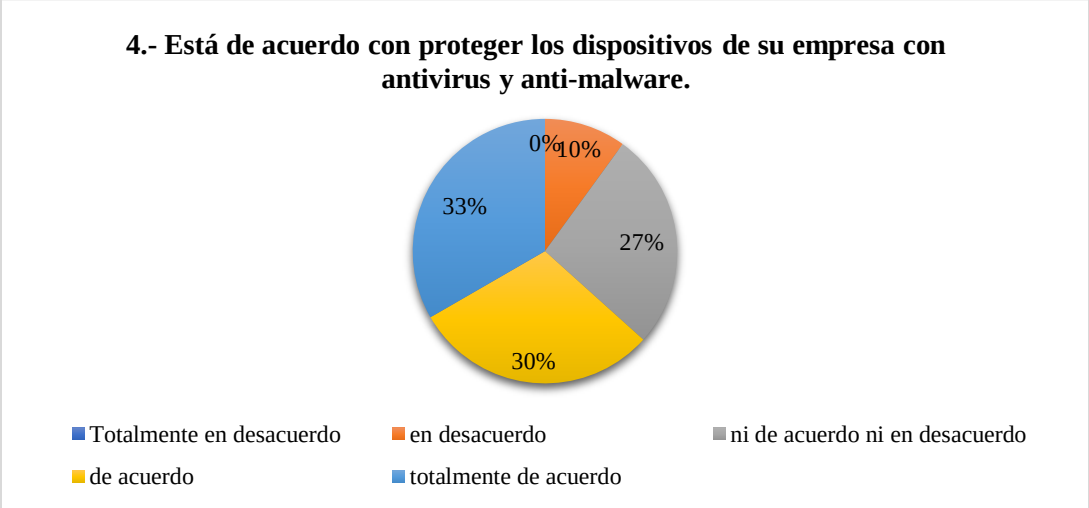
cabe destacar que un 25% no está ni de acuerdo ni en desacuerdo con la capacidad de los empleados a momento de detectar cualquier virus.

Gráfico Nº3: Está a favor de la inclusión y la inversión de presupuesto para la IA dentro de su empresa



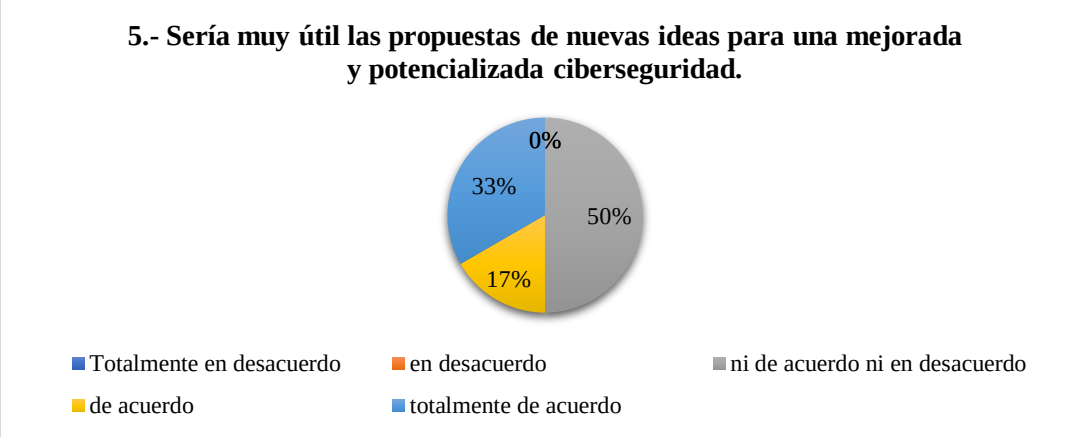
Análisis: el 35% de encuentra de acuerdo con la inclusión y la inversión de presupuesto para IA dentro de las empresas, un 34% está totalmente de acuerdo con la inversión de presupuesto para tener una mejor seguridad cibernética, mientras que un 24% se encuentra neutral, no está ni de acuerdo ni en desacuerdo, sin embargo, un 7% se encuentra en total desacuerdo con esta inclusión dentro de las diferentes empresas.

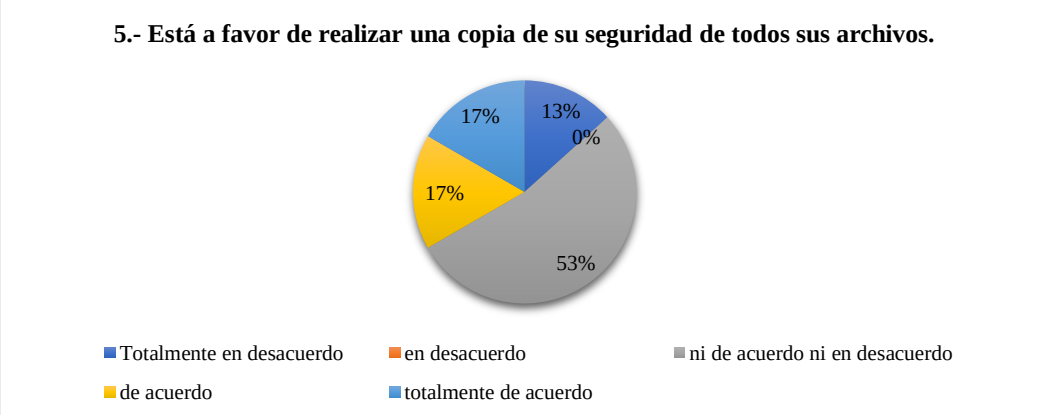
Gráfico Nº4: Está de acuerdo con proteger los dispositivos de su empresa con antivirus y anti-malware



Análisis: En el gráfico se resaltan los siguientes resultados: el 35% de la población está de acuerdo con proteger los dispositivos con antivirus y anti-malware, garantizando así una buena seguridad al momento de proporcionar cualquier información de la empresa, un 31% se encuentra escéptico ante la protección de sus dispositivos con antivirus, ya que no está ni de acuerdo ni en desacuerdo con esta protección, un 23% está totalmente de acuerdo en proteger sus dispositivos, ya que estos antivirus son garantes de proteger cualquier información importante de cualquier empresa, cabe destacar que un 11% se encuentra en desacuerdo, esto debido a la falta de información sobre las ventajas de los antivirus y anti-malware.

Gráfico Nº5: Sería muy útil las propuestas de nuevas ideas para una mejorada y potencializada ciberseguridad



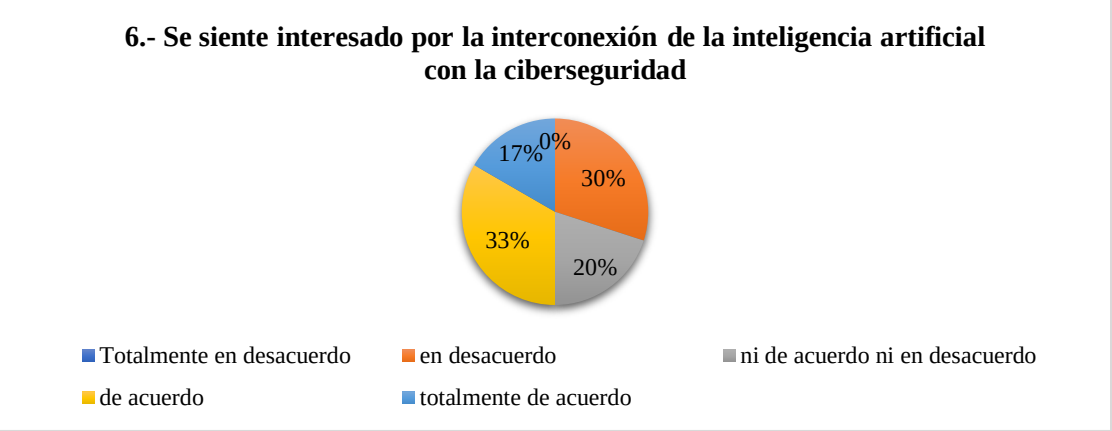


Análisis: En el gráfico se resaltan los siguientes resultados: El 53% no está ni de acuerdo ni en desacuerdo con realizar copias de seguridad a todos sus archivos, mientras que un 17% si se encuentra de acuerdo con realizar las copias de seguridad necesaria para garantizar un almacenamiento exitoso al momento de cualquier falla que pudiese existir, en ese mismo orden de

Pol. Con. (Edición núm. 55) Vol. 6, No 2, febrero 2021, pp. 1154-1173, ISSN: 2550 - 682X

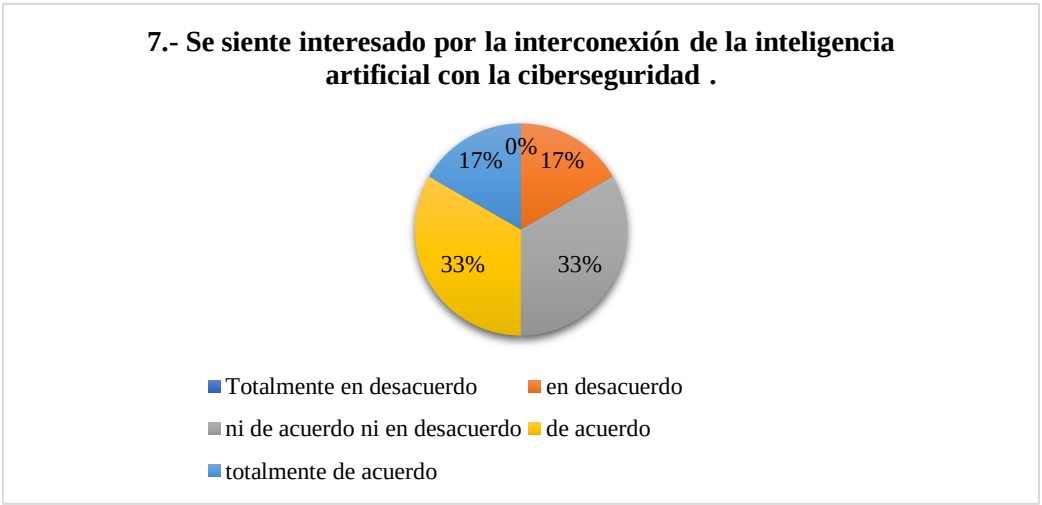
ideas un 17% se encuentra totalmente de acuerdo con estas copias, sin embargo, un 13% está totalmente en desacuerdo.

Gráfico Nº6: Se siente interesado por la interconexión de la inteligencia artificial con la ciberseguridad



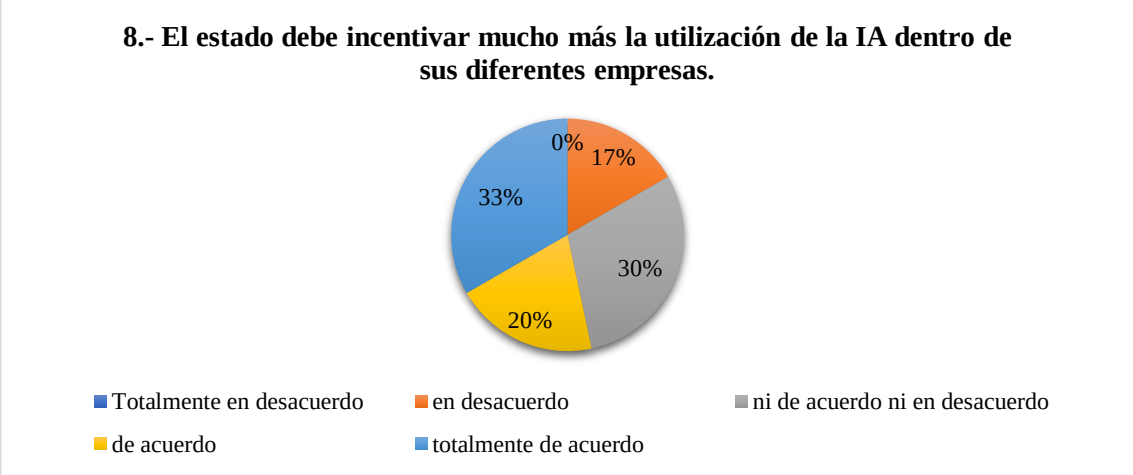
Análisis: el 27% de la población no se siente interesado por la vinculación entre la inteligencia artificial y la seguridad cibernética, mientras que un 29% está de acuerdo con esta vinculación, ya que logra garantizar una interconexión necesaria y exitosa dentro de cualquier empresa, también se cuenta con un 26% de la población que se encuentra totalmente de acuerdo con este interés hacia la inteligencia artificial con la ciberseguridad, sin embargo un 18% está en modo neutral, ni de acuerdo, ni en desacuerdo.

Gráfico Nº7: Se siente interesado por la interconexión de la inteligencia artificial con la ciberseguridad



Análisis: El presente gráfico resalta que el 35% de la población encuestada no está ni a favor ni en contra de las campañas publicitarias que promueven y apoyan la IA para garantizar una buena ciberseguridad, mientras que un 34% se encuentra de acuerdo con estas campañas publicitarias ya que impulsan y fomentan el uso de la inteligencia artificial para garantizar una seguridad cibernética exitosa, mientras que un 17% se encuentra en desacuerdo con estas campañas, sin embargo un 14% si está totalmente de acuerdo con promover la IA asegurando una buena seguridad cibernética.

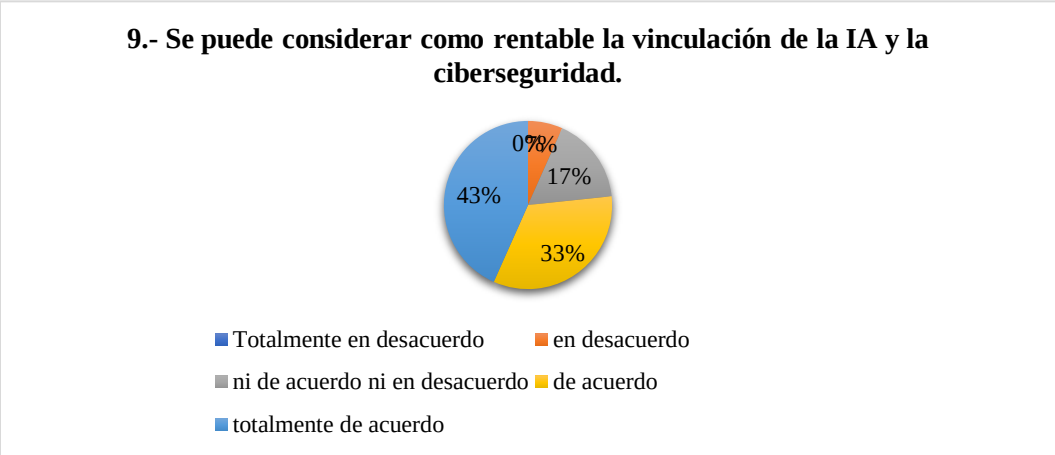
Gráfico Nº 8: El estado debe incentivar mucho más la utilización de la IA dentro de sus diferentes empresas



Análisis: En el gráfico mostrado se resaltan los siguientes resultados: el 36% no está ni de acuerdo ni en desacuerdo, está en modo neutral, respecto a que el estado debe incentivar la utilización de la IA dentro de sus empresas, mientras que un 24% si está de acuerdo con este incentivo, ya que esto puede garantizar una protección extra a sus respectivas empresas, cabe destacar que un 20% se encuentra en desacuerdo, sin embargo otro 20% de la población encuestada si está totalmente de acuerdo con la impulsión y la utilización de la IA dentro de sus empresas, por parte del estado.

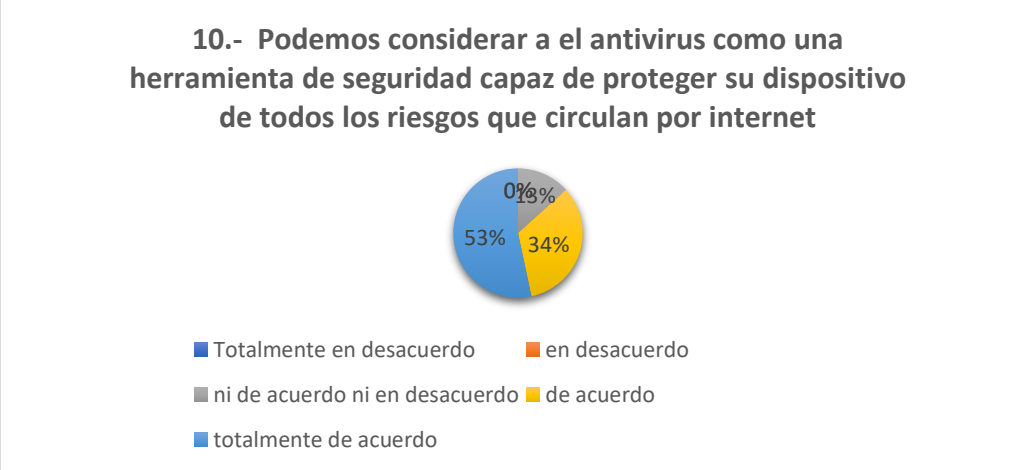
Pol. Con. (Edición núm. 55) Vol. 6, No 2, febrero 2021, pp. 1154-1173, ISSN: 2550 - 682X

Gráfico Nº9: Se puede considerar como rentable la vinculación de la IA y la ciberseguridad



Análisis: El 43% de la población considera como rentable la vinculación de la IA y la ciberseguridad, ya que esto proporciona una interconexión segura y necesaria, mientras que un 33% está de acuerdo con esta rentabilidad de la inteligencia artificial con la seguridad cibernética, sin embargo, un 17% se encuentra en modo neutral, no está ni a favor ni en contra, cabe destacar que un 7% está en desacuerdo con la consideración de la vinculación de la IA y la ciberseguridad como rentable.

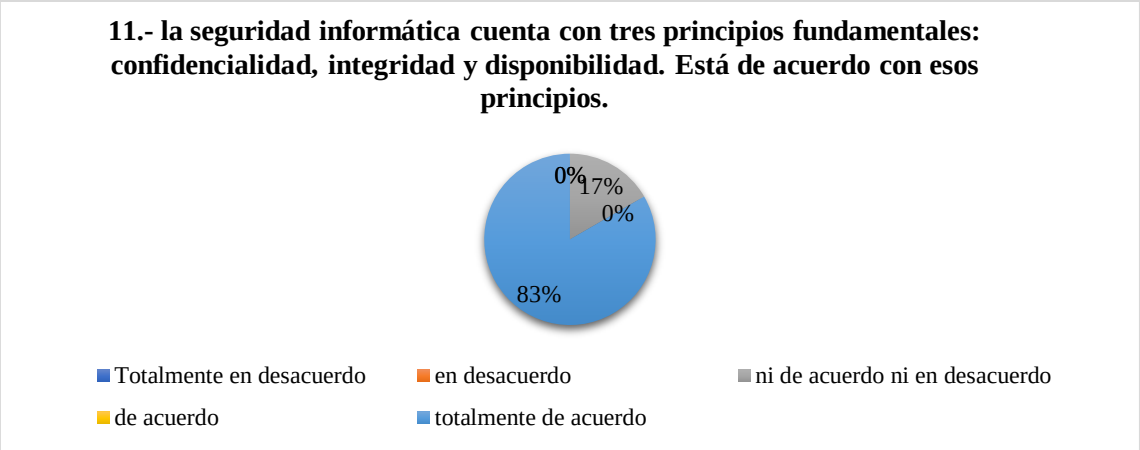
Gráfico Nº10: Podemos considerar a el antivirus como una herramienta de seguridad capaz de proteger su dispositivo de todos los riesgos que circulan por internet



Análisis: En el gráfico mostrado se puede apreciar que un 48% de la población considera al antivirus como una herramienta de seguridad con la capacidad de proteger sus dispositivos de cualquier riesgo que pudiese circular por internet, y un 37% se encuentra de acuerdo con la

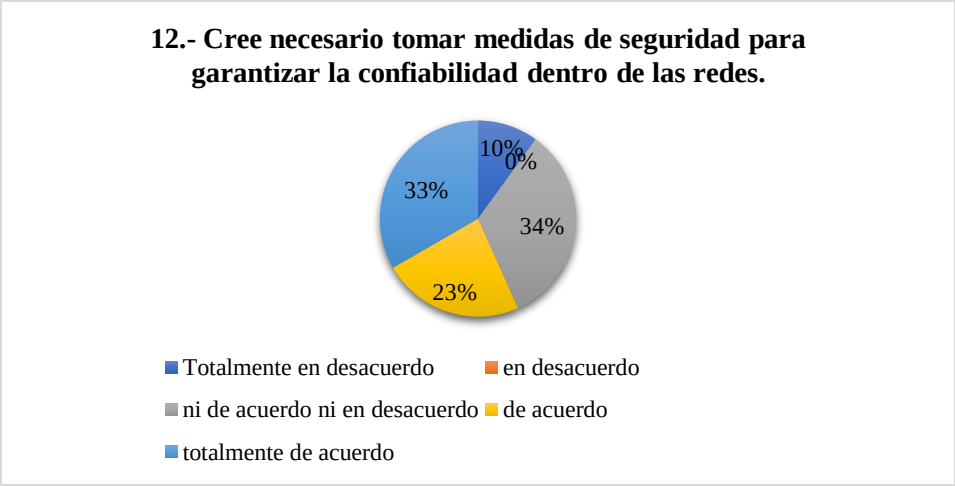
utilización del antivirus, sin embargo un 15% de la población se encuentra en modo neutral, no está ni de acuerdo ni en desacuerdo con la consideración de una antivirus como una herramienta eficaz al momento de navegar por internet.

Gráfico Nº11: La seguridad informática cuenta con tres principios fundamentales: confidencialidad, integridad y disponibilidad. Está de acuerdo con esos principios



Análisis: el 58% de la población está totalmente de acuerdo con los 3 principios fundamentales de la seguridad informática, ya que se sienten seguros y tranquilos al momento de proporcionar cualquier información que sea de total confidencialidad para dichas empresas, mientras que un 42% no está ni de acuerdo ni en desacuerdo con estos principios fundamentales de la seguridad informática.

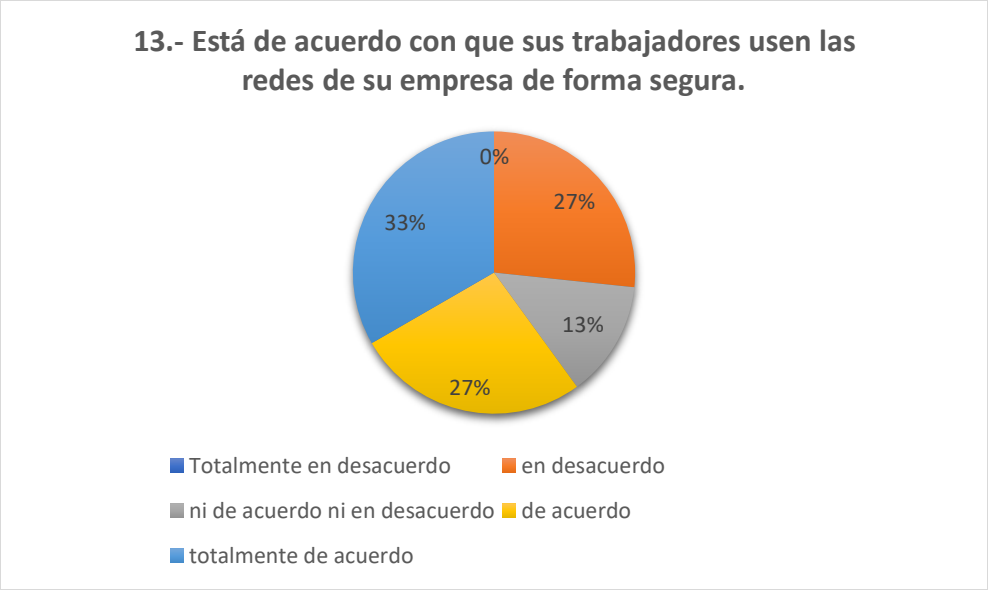
Gráfico Nº12: Cree necesario tomar medidas de seguridad para garantizar la confiabilidad dentro de las redes



Pol. Con. (Edición núm. 55) Vol. 6, No 2, febrero 2021, pp. 1154-1173, ISSN: 2550 - 682X

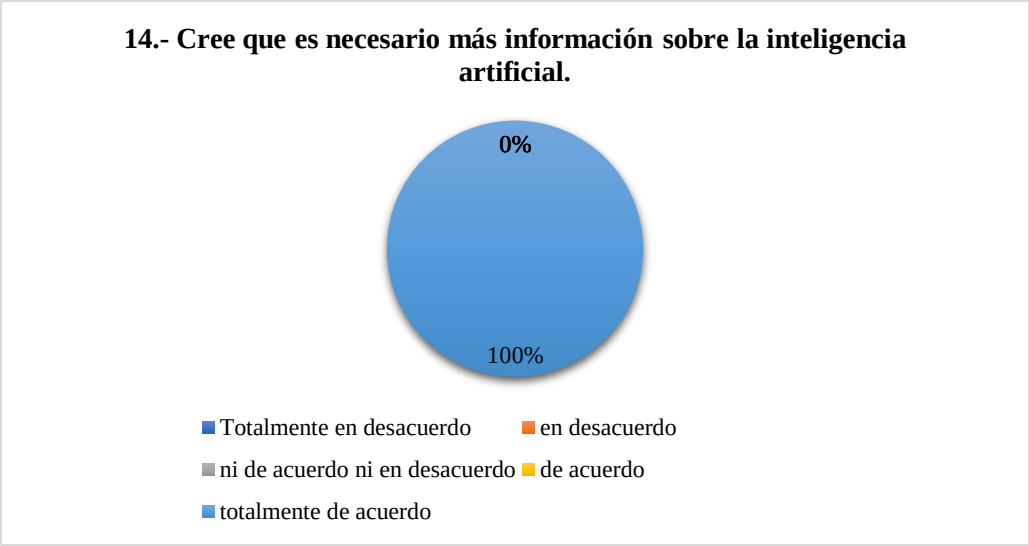
Análisis: El 37% de la población encuestada no está ni a favor ni en contra de tomar medidas de seguridad para garantizar un ambiente confiable dentro de las redes, mientras que un 26% se encuentra de acuerdo con estas medidas, ya que garantizan que cualquier virus o "hacker" puedan ser detectados a tiempo, evitando así una mayor complicación, también se cuenta con 26% de la población que está totalmente de acuerdo con estas medidas, cabe destacar que un 11% se encuentra en total negación y no cree que sea necesario tomar dichas precauciones dentro de las redes.

Gráfico Nº13: Está de acuerdo con que sus trabajadores usen las redes de su empresa de forma segura



Análisis: El 30% está de acuerdo con que sus trabajadores usen las redes de sus empresas de forma segura, un 26% está totalmente de acuerdo, ya que esto garantiza la confianza necesaria que requieren los trabajadores para una excelente función al momento de trabajar, mientras que un 29% está en desacuerdo, esto es debido a la falta de confianza tanto para seguridad cibernética de la empresa como de los trabajadores, ya que al no tener el conocimiento adecuado, no se garantiza una seguridad exitosa y confiable dentro de la empresa.

Gráfico Nº14: Cree que es necesario más información sobre la inteligencia artificial



Análisis: el 100% de la población considera necesario e importante proporcionar más información sobre la inteligencia artificial, ya que esto ayudaría a mitigar un poco los delitos cibernéticos, esto debido a que las diferentes empresas cuentan con la información necesaria para poder resolver cualquier problema que se pueda presentar, mediante los diferentes antivirus y anti-malware que puedan existir, para lograr así una interconexión necesaria.

Resultados

Teniendo en cuenta todas las experiencias de muchos países de la región y el mundo, en cuanto a la cantidad de estrategias y leyes creadas en función de defensa contra las amenazas que circundan en la red, se atiende la necesidad imperiosa del Estado ecuatoriano frente a estas nuevas amenazas, creando o formando parte de algún organismo de Ciberseguridad que garantice el principio de individualidad de los ciudadanos y de la infraestructura crítica del estado evitando la pérdida de recursos, garantizando de esa manera la seguridad de una forma preventiva y proactiva considerando la previa experiencia de países que lideran este campo y que ya tienen en funcionamiento sus políticas nacionales y estrategias de Ciberseguridad.

Abordando la cantidad de problemas que se han evidenciado en la red, y la apremiante busca de soluciones que puedan garantizar la privacidad, protección y confiablidad absoluta de la nube, y teniendo en cuenta la principal idea basada en vinculación de la inteligencia artificial con la seguridad cibernética para hacerle frente a los ataques informáticos, surge una interrogante:

Pol. Con. (Edición núm. 55) Vol. 6, No 2, febrero 2021, pp. 1154-1173, ISSN: 2550 - 682X

¿Está lejos el día que las aplicaciones tengan la potestad para tomar decisiones?

Al momento de presentar una idea siempre existen cuestionamientos, y mucho más en este ámbito, donde se maneja una gran cantidad de información y datos muy relevantes para el Estado, es cierto que uno de los principales cuestionamientos que se crean frente a la inminente adaptación y vinculación de estas nuevas herramientas basadas en inteligencia artificial, es precisamente el hecho de dejar de lado la mano del ser humano, donde sea solo la IA que se haga cargo de todo, incluyendo la toma de decisiones. Pero, no es el principio de funcionamiento de la inteligencia artificial, el ser humano seguirá siendo indispensable en todos los aspectos y la toma de decisiones no correspondería solamente a un sistema, se busca contar con herramientas cibernéticas que trabajen con las personas para brindar una mayor seguridad y funcionamiento óptimo de la red, teniendo en cuenta que son más las ventajas que se verían reflejadas en el buen uso y la seguridad que implicaría el manejo de todo tipo de datos e información y por supuesto a los riesgos existente de un descontrol en la administración de los sistemas informáticos para cualquier aplicación. Es por ello que se hace evidente la necesidad de abordar con mayor énfasis la investigación y el estudio de la inteligencia artificial y su vinculación en la seguridad informática, con el propósito de mejorar los procesos informáticos.

Conclusiones

Debido a la cantidad de información digital que actualmente se genera, es de vital importancia contar con sistemas de almacenamiento seguros que garanticen la integridad, la calidad y la trasmisión de los datos, de lo contrario se expone con mayor facilidad a los ataques o intrusiones que están presentes y que cada día se vuelven más frecuentes en el entorno cibernético, lo cual ocasiona una pérdida de datos y de privacidad que afecta al usurario. En razón de lo anterior, surge la necesidad de implementar y vincular distintas técnicas basadas en la inteligencia artificial con la finalidad de mejorar de forma continua el tema de la seguridad en la información, puesto que es un mecanismo efectivo en la prevención y la reacción ante los inminentes riesgos, y que permite cumplir con los lineamientos de la ciberseguridad: confidencialidad, integridad y disponibilidad.

Es cierto que día a día aparecen nuevos y complejos tipos de incidentes, que solo buscan dañar de una forma u otra al sistema, bien sea por el robo de información o sencillamente ataques directos al usuario. Es claro que aún se registran fallas de seguridad de fácil resolución técnica, las cuales ocurren en muchos casos por falta de conocimientos. Pero, por otro lado, los incidentes de

seguridad informática impactan en forma cada vez más directa. En consecuencia, se requieren efectivas acciones de concientización, capacitación y difusión de mejores prácticas.

Los ataques cibernéticos están teniendo el mayor éxito en el eslabón más débil y difícil de proteger. Es evidente que los intrusos o piratas informáticos, conocen a profundidad lo que están haciendo, se han preparado por años en dicha tarea, por ende, les resulta fácil identificar el punto de débil de su objetivo, teniendo en cuenta que algunos ni siquiera cuenta con sistemas de seguridad que puedan garantizar su protección. Por ende, no importando los procesos y la tecnología, finalmente el evitar los ataques queda en manos de los usuarios.

Referencias

1. APD. (2020). Los cuatro tipos de inteligencia artificial que debes conocer. Redacción APD. Obtenido de https://www.apd.es/tipos-de-inteligencia-artificial/
2. Arias, F. G. (2012). El proyecto de investigación, introducción a la metodología científica (6ª edición ed.). Episteme.
3. B-secure. (2019). Centro de operaciones de ciberseguridad. Obtenido de CSOC: https://bit.ly/34roQli
4. Cohen, E. (2007). Information and beyond: Part I. Informing Science press.
5. Dignum, V. (2017). Responsible artificial intelligence: designing AI gor human values. ITU. ICT Discoveries., 1-8. Obtenido de https://bit.ly/31qpnSo
6. Europeo., P. (2020). ¿Qué es la inteligencia artificial y como se usa? Parlamento Europeo. Obtenido de https://www.europarl.europa.eu/news/es/headlines/society/20200827STO85804/que-es-la-inteligencia-artificial-y-como-se-usa
7. Gestión. (2018). ¿Qué es la inteligencia artificial y para qué sirve? Obtenido de Gestión, Tecnología: https://gestion.pe/tecnologia/inteligencia-artificial-historia-origen-funciona-aplicaciones-categorias-tipos-riesgos-nnda-nnlt-249002-noticia/
8. Hernández Sampieri, R. (2014). Metodología de la investigación (6º edición ed.). McGrawhill.
9. Hernández Sampieri, R. F. (2010). Metodología de la Investigación. Mexico: Mc Graw Hill.
10. Hurtado, J. (2008). Metodología de la Investigación (Vol. 4º).

11. Kaspersky. (1997). La IA y el aprendizaje automático en la ciberseguridad: como determinaran el futuro. Obtenido de Latam: https://latam.kaspersky.com/resource-center/definitions/ai-cybersecurity
12. Kotler, P. y. (2008). Fundamentos del marketing. México: Pearson.
13. Lab., K. (1997). ¿Qué es la ciberseguridad? Obtenido de Karspersky: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security
14. Lipton, D. (2018). Las amenazas a la seguridad cibernética exigen una respuesta mundial. Fondo monetario internacional. Obtenido de https://blog-dialogoafondo.imf.org/?p=12698
15. Méndez, C. (2010). Metodología. Diseño y Desarrollo del Proceso de Investigación. Bogotá. Colombia.: Editorial Mc Graw Hill.
16. Pascual Estape, J. (2019). Inteligencia artificial: que es, como funciona y para que se está utilizando. Computer Hoy. Obtenido de https://computerhoy.com/reportajes/tecnologia/inteligencia-artificial-469917
17. Pastor, J. (20 de Noviembre de 2018). Xataka. ¿Obtenido de Que es la inteligencia artificial?: https://www.xataka.com/robotica-e-ia/que-inteligencia-artificial
18. Rocha, C. (2011). La seguridad informática. Ciencia EMI, 4, 26-33. Obtenido de https://doi.org/10.29076/issn.2528-7737vol4iss5.2011pp26-33p
19. Salesforce. (22 de Junio de 2017). Salesforce Latinoamérica. Obtenido de inteligencia artificial: ¿Qué es?: https://www.salesforce.com/mx/blog/2017/6/Que-es-la-inteligencia-artificial.html
20. Schnarch K. (2008). Marketing del siglo XXI: Innovación, creatividad y tecnología. IV Congreso Internacional y XII Nacional de Marketing.
21. Shead, S. (14 de Enero de 2020). Que es el "invierno de la inteligencia artificial" y por qué hay expertos que creen que estamos acercándonos a uno. BBC News. Obtenido de https://www.bbc.com/mundo/noticias-51097189
22. Tori, C. (2008). Hacking ético. rosario: autoedición. Obtenido de https://bit.ly/3glzY5n.
23. UIT. (2010). Unión internacional de Telecomunicaciones. Obtenido de Ciberseguridad.