Revista Científica
ANFIBIOS
ISSN: 2665-1513 (Impreso) | ISSN: 2711-0532 (En línea)

Oportunidades de la Inteligencia Artificial en la seguridad organizacional

Artificial Intelligence Opportunities in Organizational Security

Marian Hoyos-Pimienta
Universidad de Córdoba - Colombia
ORCID iD: https://orcid.org/0000-0003-1960-3285
mhoyospimienta03@correo.unicordoba.edu.co

Fecha de recepción: 06/03/2025
Fecha de evaluación: 26/03/2025
Fecha de aceptación: 29/05/2025

Cómo citar: *Hoyos-Pimienta, M. (2025). Oportunidades de la Inteligencia Artificial en la seguridad organizacional. Revista Científica Anfibios, 8(1), 68-76. https://doi.org/10.37979/afb.2025v8n1.174*

Resumen

Algunas personas podrían pensar que la inteligencia artificial (IA) es algo nuevo, pero ha existido durante muchas décadas y ha evolucionado constantemente. La era de la IA comenzó en 1956 en una conferencia en Dartmouth, donde científicos introdujeron el término. Definieron la IA como la creación de máquinas inteligentes y programas de cálculo. Aunque se esperaban avances, estos comenzaron en las décadas de 1990 y 2000, cuando las empresas empezaron a invertir en sistemas inteligentes para mejorar el manejo de datos. La investigación incluía una revisión de fuentes sobre la IA y su aplicación en la seguridad organizacional, buscando información sobre cómo se usa para prevenir riesgos y ciberataques. Se destacó una evolución en las definiciones de IA, reflejando un avance en su desarrollo y reconocimiento en diferentes áreas.

Palabras clave
Inteligencia artificial; seguridad; organización; transformación tecnológica; modelo

Abstract

Some people might think that artificial intelligence (AI) is something new, but it has been around for many decades and has been constantly evolving. The era of AI began in 1956 at a conference at Dartmouth, where scientists introduced the term. They defined AI as the creation of intelligent machines and computational programs. Although advances were expected, they began in the 1990s and 2000s, when companies began investing in intelligent systems to improve data management. The research included a review of sources on AI and its application in organizational security, seeking information on how it is used to prevent risks and cyberattacks. It highlighted an evolution in the definitions of AI, reflecting an advance in its development and recognition in different areas.

Keywords
Artificial intelligence; security; organization; technological transformation; model

Introducción

Algunas personas podrían creer que la inteligencia artificial (IA) es un fenómeno reciente. Sin embargo, este concepto ha existido durante muchas décadas, evolucionando continuamente en diversos aspectos. Esta transformación tecnológica ha tenido un gran impacto en la humanidad, permitiendo un acceso más amplio a la información. Recordando los orígenes de la IA, en 1956 se marcó el comienzo de esta era durante la conferencia de Dartmouth, donde los científicos John McCarthy, Marvin Minsky y Claude Shannon introdujeron el término. Definieron la inteligencia artificial como "la ciencia e ingenio de crear máquinas inteligentes, especialmente programas de cálculo inteligentes". Aunque muchos esperaban avances significativos en la inteligencia artificial, estos no comenzaron a materializarse hasta las décadas de 1990 y 2000. En ese período, numerosas empresas comenzaron a invertir en una gran cantidad de sistemas inteligentes, con el objetivo de mejorar el procesamiento y análisis de la gran cantidad de datos generados en el mundo digital actual. (Iglesias, 2016).

En los últimos años, la inteligencia artificial ha revolucionado la forma en que las empresas operan y compiten en la economía global. De acuerdo, a un informe de Grand View Research (2023), el mercado global de inteligencia artificial alcanzó un valor de USD $196,63 en 2023 y se espera que crezca a una tasa compuesta anual del 36,6% entre 2024 y 2030. Este crecimiento se verá impulsado por la investigación y la innovación continúas lideradas por gigantes tecnológicos, que están promoviendo la adopción de tecnologías avanzadas en sectores clave como la automoción, la atención médica, el comercio minorista, las finanzas y la manufactura. Algunas de las principales empresas que lideran la investigación y la innovación en este campo son Amazon, Google, Apple, Facebook, International Business Machines Corporation y Microsoft.

La accesibilidad está impulsando la innovación en inteligencia artificial debido a la facilidad y el bajo costo de acceso al almacenamiento y a la recuperación de información en varios conjuntos de datos, que son utilizados para entrenar modelos de IA, lo que acelera el avance en este campo. Así, las empresas están esforzándose por hacer que la IA sea más accesible para diversos casos de uso empresarial.

Por lo tanto, las empresas que están incorporando la inteligencia artificial están adoptando un enfoque holístico que abarca tres áreas simultáneamente: la transformación del negocio, el mejoramiento en la toma de decisiones y la modernización de los sistemas y procesos. Este enfoque implica la participación directa de líderes de distintas áreas dentro de la organización, lo que facilita una mayor escalabilidad y un intercambio de datos más eficiente (PwC, 2020).

En este sentido, la inteligencia artificial ha hecho posible que los dispositivos imiten e incluso superen ciertas funciones cognitivas humanas esenciales, como la percepción, el razonamiento, el aprendizaje y la resolución de problemas. Como resultado, la IA puede procesar y analizar grandes volúmenes de datos, tomar decisiones precisas basadas en patrones y automatizar procesos complejos, lo que ofrece a las empresas una ventaja competitiva en el mercado. Además, el uso de estas tecnologías como herramienta para la prevención de riesgos laborales se ha convertido en una opción viable para las empresas.

Este artículo profundizará en las diversas oportunidades que la inteligencia artificial ofrece para mejorar la seguridad organizacional, explorando cómo estas tecnologías avanzadas pueden optimizar la detección de accidentes, ciberataques y automatizar respuestas ante incidentes. Además, se analizará cómo la implementación de soluciones basadas en IA no solo mejora la eficiencia operativa, sino que también ayuda a las empresas a cumplir con los estándares de seguridad y a fortalecer la protección de los datos. También, se abordará la necesidad de una capacitación continua del personal sobre este tipo de tecnologías con el objetivo de maximizar los beneficios de la IA. De igual forma, se incluyen recomendaciones sobre cómo afrontar los desafíos y consideraciones éticas asociadas con la integración de la IA en la seguridad organizacional, incluyendo la privacidad de los datos y la dependencia de tecnologías avanzadas.

Referentes teóricos

Según, Rich & Knight (1991) la Inteligencia artificial o IA se define como la capacidad de hacer que las computadoras realicen tareas que actualmente son mejor ejecutadas por los humanos. Por su parte, Nebendah (1988) y Delgado (1998), la describen cómo la ciencia que se dedica a explicar y replicar comportamientos inteligentes a través de procesos computacionales que se basan en la experiencia y el conocimiento continuo del ambiente. Esta rama de la ciencia de la computación investiga

cómo resolver problemas no algorítmicos mediante el uso de cualquier técnica computacional disponible, sin considerar el razonamiento subyacente a los métodos utilizados para alcanzar la solución. (Fleifel, F., 2015)

La inteligencia artificial se entiende como la disciplina y la ingeniería dedicadas a crear máquinas inteligentes, particularmente programas informáticos inteligentes. Aunque este concepto está vinculado a la tarea de emplear computadoras para comprender la inteligencia humana, la IA no está limitada a los métodos observables biológicamente. En cambio, la inteligencia artificial se enfoca en desarrollar sistemas y tecnologías que simulen la inteligencia humana, permitiendo que las máquinas lleven a cabo tareas que normalmente requerirían la intervención humana (J. McCarthy, 2007).

La IA se divide en dos áreas clave: el aprendizaje automático (machine learning) y el aprendizaje profundo (deep learning). El aprendizaje automático se enfoca en desarrollar algoritmos y técnicas que le permiten a las máquinas aprender y mejorar a partir de los datos. Su objetivo es que las máquinas sean capaces de aprender y tomar decisiones de manera similar a los humanos, con la ventaja de que pueden mejorar automáticamente a medida que reciben más información, sin necesidad de ser programadas específicamente para cada tarea (F. Bastani y A.-R. Sadeghi, 2010).

El aprendizaje automático, o machine learning, abarca varios subcampos, entre ellos las redes neuronales y el aprendizaje profundo. En este contexto, el aprendizaje profundo o Deep learning se considera un subconjunto del aprendizaje automático dentro de la inteligencia artificial, que emula el proceso de aprendizaje basado en la experiencia mediante algoritmos que imitan la estructura y el funcionamiento del cerebro humano. Hoy en día, tanto el aprendizaje automático como el aprendizaje profundo son vistos como las áreas más avanzadas de la inteligencia artificial (IBM Cloud, 2021).

Por consiguiente, de acuerdo con investigaciones llevadas a cabo por McKinsey entre 2017 y 2018, las empresas que implementaron al menos un sistema inteligente en sus procesos experimentaron un crecimiento superior al 50% (Burkhardt et al., 2019). Esto sugiere que la aplicación de la inteligencia artificial debe hacerse con precaución para evitar daños significativos a los empleados y a la organización, y en su lugar, debe facilitar la transformación de los modelos de negocio y la mejora de las actividades empresariales (Rouhiainen, 2019).

En este sentido, Rauch-Hindin (1989) señala que la inteligencia artificial tiene un impacto significativo en las organizaciones, ya que esta tecnología puede llevar a cabo tareas específicas y previamente establecidas. No obstante, advierte que no se puede reemplazar completamente a los humanos, ya que la IA nunca podrá igualar la sensibilidad humana. Por otro lado, Vela (2013) destaca que las pequeñas y medianas empresas están centrando sus esfuerzos en desarrollar y aplicar la inteligencia artificial no para sustituir el trabajo humano, sino para complementar y potenciar el desarrollo de los empleados.

Asimismo, las aplicaciones de la inteligencia artificial en el ámbito laboral incluyen una variedad de tecnologías, como robots colaborativos (cobots), dispositivos portátiles, tabletas de asistencia en líneas de producción, chatbots en fábricas, almacenes y centros de llamadas, así como equipos de protección personal inteligentes. También abarcan procesos algorítmicos en recursos humanos, como el análisis de personal (Jansen, A. et al., 2018).

En ese orden de ideas, la implementación de tecnologías de este tipo se refleja en la seguridad organizacional, la cual Perrow (1984) define como la protección contra daños a personas y bienes, especialmente aquellos que surgen de fallas tecnológicas o en la organización. Su investigación, conocida como la Teoría del Accidente Normal, sostiene que los accidentes son eventos inevitables dentro de la complejidad de los sistemas y tecnologías actuales. Dicha complejidad hace que sea imposible prever o prevenir todos los posibles accidentes. Por lo tanto, Perrow argumenta que la única manera de reducir estos riesgos es simplificando la complejidad, disminuyendo el grado de acoplamiento, o evitando el uso de tecnologías complejas.

Por su parte, James Reason (1990) señala la seguridad organizacional como la capacidad de mantener condiciones en las que personas y bienes no sufran daños o pérdidas, así como la habilidad de mantener el funcionamiento normal o de recuperarse rápidamente después de que ocurran incidentes. Desarrolló una teoría sobre el error humano y el modelo de queso suizo con un enfoque organizacional, que distingue entre errores activos, que tienen consecuencias inmediatas, y errores latentes, cuyas consecuencias pueden permanecer ocultas dentro del sistema durante mucho tiempo. Este modelo presenta una secuencia de cinco niveles: decisiones de alto nivel, gestión operativa, condiciones previas,

actividades productivas y medidas de protección. Según este modelo, los accidentes ocurren cuando todas las capas de protección son atravesadas, mientras que los incidentes se detienen si una de estas capas de defensa frena la progresión del accidente en algún punto (Dekker, 2019).

Dekker (2014) en su teoría Safety Differently incide que las personas deben ser vistas como la solución, y no como un problema que se deba controlar. Por lo tanto, argumenta que la seguridad es una responsabilidad ética más que legal, y que debería definirse por la presencia de capacidades positivas en lugar de simplemente la ausencia de eventos negativos.

La teoría de la Seguridad II, propuesta por Erik Hollnagel (2015), sugiere que se debe cambiar el enfoque de la seguridad, que tradicionalmente se centra en identificar fallos, por un enfoque que estudie los aspectos que están funcionando bien y que son seguros. El objetivo es comprender por qué estos elementos son seguros y funcionan adecuadamente en las organizaciones.

De esta manera, la implementación de la inteligencia artificial en las organizaciones puede ofrecer oportunidades para mejorar la vigilancia de la seguridad y la salud en el trabajo (SST), reducir la exposición a diversos factores de riesgo como el acoso y la violencia, y proporcionar alertas tempranas sobre estrés, problemas de salud y fatiga. Con esto, el control basado en inteligencia artificial puede generar información valiosa para identificar problemas de SST, incluidos riesgos psicosociales, y determinar cuándo se necesitan intervenciones en SST a nivel organizacional (European Agency for Safety and Health at Work, 2021).

El Instituto Vasco de Seguridad Laboral (2021) menciona a Ludus, la primera plataforma mundial en desarrollar formación en seguridad y salud laboral mediante realidad virtual. Esta plataforma tiene el objetivo de preparar a los empleados para prevenir y responder a riesgos laborales de manera efectiva. El entrenamiento en realidad virtual es un complemento ideal para las formaciones en prevención de riesgos, ya que permite simular situaciones de peligro sin poner en riesgo vidas o bienes materiales, y a un costo menor que en la realidad. Por lo tanto, realizan entrenamientos de realidad virtual en plantas industriales, trabajos en altura, riesgos eléctricos, y en tareas en espacios confinados y de construcción.

Además de ayudar a prevenir los riesgos laborales, la inteligencia artificial puede ser utilizada para el análisis de datos. Dado que las TIC y la IA son tecnologías disruptivas que proporcionan un flujo constante de datos, aunque esta información por sí sola no produce resultados, su procesamiento para convertirlos en respuestas o soluciones comprensibles facilita la automatización de los procesos empresariales, reformula procedimientos y condiciona las decisiones empresariales. Esto tiene como objetivo mejorar la eficiencia y la efectividad de las actividades de la empresa. De este modo, toda la información obtenida puede ser relevante para la protección del trabajador, sin importar su origen. Procesar esta información con la tecnología actual es relativamente sencillo debido a la velocidad con la que se pueden analizar grandes volúmenes de datos y a bajo costo, lo que permite aumentar las utilidades (Del Castillo, 2020).

Dado que los ataques informáticos se están volviendo cada vez más peligrosos y frecuentes, y con el crecimiento de los servicios en la nube, así como la aparición de redes de datos e interfaces de usuario cada vez más complejas, la tarea de los especialistas en seguridad informática se ha vuelto más desafiante. En respuesta a esta situación, han surgido nuevas soluciones para contrarrestar estos problemas, y una de ellas es la implementación de sistemas basados en inteligencia artificial (L. Melman, 2020).

Según Moreno (2023), una ventaja de la inteligencia artificial sobre los sistemas de seguridad tradicionales es su capacidad para identificar posibles ataques mediante el análisis de reglas predefinidas y patrones conocidos. Sin embargo, dado que los ciberdelincuentes continuamente desarrollan nuevas técnicas y métodos para eludir estos sistemas, las medidas de protección actuales pueden no ser siempre efectivas contra amenazas más avanzadas. En contraste, la IA puede procesar grandes volúmenes de datos rápidamente, provenientes de redes y sistemas, para identificar patrones y correlacionarlos con comportamientos típicos de virus o software malicioso, basándose en amenazas anteriores. Esto permite detectar un ataque potencial en curso o incluso anticiparse a su inicio, facilitando la toma de decisiones adecuadas.

De este modo, el uso de macrodatos para mejorar la seguridad y la salud en el trabajo requiere una mayor capacidad de computación, lo que permite que el aprendizaje automático y la inteligencia artificial clasifiquen y analicen rápidamente grandes

volúmenes de datos recopilados de sistemas cada vez más complejos. Esto facilita la comprensión de los problemas, mejora la toma de decisiones en seguridad y permite predecir problemas de seguridad organizacional antes de que ocurran, así como realizar intervenciones más oportunas y eficaces (García, 2022).

Metodología

La investigación se realizó mediante una revisión exhaustiva de diferentes fuentes para entender la inteligencia artificial y su aplicación en la seguridad organizacional. Se buscaron fuentes que cumplieran con estos criterios utilizando palabras clave como "inteligencia artificial" y "seguridad en las empresas". También se recopiló información sobre las principales ramas actuales de la IA. Se identificó cómo las organizaciones están utilizando la inteligencia artificial para prevenir riesgos laborales y ciberataques que podrían amenazar su seguridad. Además, se incorporaron varias teorías y estudios relevantes para realizar un análisis que permita determinar y comprender mejor las oportunidades que la inteligencia artificial ofrece para la seguridad organizacional.

Resultados

El análisis de la información revela el creciente impacto de la inteligencia artificial (IA) en la actualidad y su crucial papel en la seguridad de las organizaciones, tanto en la protección de los empleados como en el manejo de datos e información. También se observó que las empresas, ya sean grandes o pequeñas, que implementan estas tecnologías en sus procesos, experimentan un notable crecimiento y mejoras en sus actividades.

A continuación, se presentan tablas con definiciones y teorías clave de varios autores sobre la inteligencia artificial y la seguridad organizacional, con el objetivo de facilitar la comprensión de estos conceptos y permitir un análisis efectivo que identifique las oportunidades que estos elementos ofrecen a las organizaciones.

La Tabla 1 presenta una variedad de definiciones sobre la inteligencia artificial (IA) que reflejan la evolución del concepto a lo largo del tiempo. En general, se puede observar que las definiciones se centran en la capacidad de las máquinas para realizar tareas que tradicionalmente requieren inteligencia humana, como el aprendizaje, la resolución de problemas y la toma de decisiones. Además, se destaca la importancia de la adaptación y la comunicación, sugiriendo que la IA no solo debe ejecutar tareas, sino también interactuar con su entorno de manera efectiva.

Asimismo, se puede notar una progresión en la complejidad de las definiciones, desde una visión más básica de la IA como un medio para replicar acciones humanas hasta una comprensión más amplia que incluye la toma de decisiones racionales y la maximización de objetivos. Esto indica un avance en la investigación y el desarrollo de la IA, así como un reconocimiento creciente de su potencial y sus implicaciones en diversos campos.

Tabla 1. Conceptos de la inteligencia artificial.

Autores y año de publicación	Principales aportes
John McCarthy (1956)	"La inteligencia artificial es el estudio de cómo hacer que las computadoras hagan cosas que por el momento los humanos hacen mejor". Principio del formularioFinal del formulario
Rich & Knight (1991)	"Es la ciencia y la ingeniería de hacer máquinas inteligentes, especialmente programas de computadora inteligentes".
Rauch-Hindin (1989)	"Es el estudio y diseño de agentes inteligentes".
Steels, 1993	"Es el estudio de sistemas que muestran comportamientos inteligentes similares a los humanos, como resolver problemas complejos, aprender, adaptarse y comunicarse eficazmente".
Legg & Hutter, 2007	"El estudio de agentes que toman decisiones racionales para maximizar el logro de sus objetivos, utilizando la información disponible".
Russell & Norvig, 2016	"La IA abarca cualquier tarea que una máquina pueda realizar mejor que un humano".

Fuente: Elaboración propia.

La Tabla 2 aborda diversas teorías sobre la seguridad organizacional, cada una de las cuales ofrece un marco conceptual para entender cómo se gestionan y perciben los riesgos dentro de las organizaciones. De esta manera, las teorías presentadas se enfocan en describir la complejidad inherente de los sistemas organizacionales. Además, se destaca la evolución del pensamiento sobre la seguridad, desde un enfoque centrado en el error humano hacia una perspectiva más holística que considera la seguridad como una responsabilidad ética. Esto refleja un cambio en la cultura organizacional, donde la seguridad se convierte en un valor fundamental que debe ser integrado en todos los niveles de la operación.

Tabla 2. Teorías sobre la seguridad organizacional.

Autores y año de publicación	Teoría	Principales aportes
Perrow (1984)	Teoría del accidente normal	Expresa que los accidentes pasan, que son sucesos comunes dentro de la complejidad de los sistemas y de las tecnologías que se emplean en la actualidad.
James Reason (1990)	Teoría del error humano y el modelo de queso suizo	Establece la diferencia entre los errores activos que son aquellos que tienen consecuencias inmediatas y los errores latentes cuya consecuencia puede permanecer latentes dentro del sistema durante mucho tiempo.
Dekker (2014)	Safety Differently	La seguridad es una responsabilidad ética, no una responsabilidad legal y que la seguridad ha de definirse por la presencia de capacidades positivas en lugar de la ausencia de acontecimientos negativos
Erik Hollnagel (2015)	Seguridad II o Safety II	Propone modificar el enfoque tradicional de la seguridad por uno más proactivo y que permita potenciar la capacidad de los sistemas para adaptarse a situaciones cambiantes.

Fuente: Elaboración propia.

En los últimos años, la inteligencia artificial ha mostrado un crecimiento significativo y se ha comenzado a emplear para identificar riesgos laborales, prevenir accidentes en el trabajo y diagnosticar enfermedades ocupacionales de manera preventiva. Aunque la IA es una herramienta útil para la seguridad organizacional, también conlleva riesgos relacionados con brechas de seguridad, robo de datos y mal uso de información privada. Por ello, es crucial que las empresas implementen protocolos de seguridad para proteger los datos sensibles y cumplir con las regulaciones de privacidad y protección de datos. (Tenés, 2023).

En ese orden ideas, se puede identificar que uno de los principales desafíos para la adopción de la inteligencia artificial en las empresas es la falta de personal especializado en esta tecnología (Pappas, Christopher, 2023). Por lo tanto, las empresas proactivas preferirán invertir en el desarrollo de habilidades internas en lugar de recurrir a proveedores externos para la capacitación en estas tecnologías. Esto permitirá capacitar a los empleados en el desarrollo e implementación de la IA dentro de la organización.

A pesar de los desafíos que la inteligencia artificial puede presentar para las empresas, ofrece numerosas oportunidades en el ámbito de la seguridad organizacional. La IA tiene la capacidad de analizar grandes volúmenes de datos para identificar y predecir posibles incidentes de seguridad antes de que ocurran. Además, puede automatizar tareas repetitivas y propensas a errores, como la supervisión de sistemas de seguridad, aliviando la carga del personal y reduciendo posibles fallos. La IA también puede detectar comportamientos inusuales que puedan comprometer la seguridad de la organización y servir como herramienta de simulación para capacitar a los empleados en situaciones de crisis y accidentes. De este modo, la inteligencia artificial puede contribuir a una mayor resiliencia organizacional, permitiendo a las empresas recuperarse más rápidamente de eventos adversos.

Conclusión

En conclusión, el artículo ha explorado las oportunidades que la inteligencia artificial ofrece para la seguridad organizacional, destacando su relevancia en la prevención de riesgos, la detección de accidentes, la protección contra ciberataques y la automatización de respuestas a incidentes. Para ello, se realizó una investigación de diversas fuentes que evidencian estos beneficios, así como las teorías que han contribuido a los avances de esta tecnología en el entorno laboral a lo largo de los años.

De esta manera, la integración de la inteligencia artificial en la seguridad organizacional puede revolucionar la manera en que las empresas gestionan y responden a los riesgos, optimizando la eficacia y eficiencia de sus operaciones de seguridad. Esto permitirá a las organizaciones abordar riesgos de manera más proactiva, mejorar la toma de decisiones, prever comportamientos humanos y reducir accidentes, así como identificar y evaluar riesgos potenciales en tiempo real. De este modo, las empresas podrán asignar sus recursos y esfuerzos de seguridad de manera más efectiva. Además, la simulación no solo ayuda a aumentar la conciencia sobre los riesgos mediante la experiencia de accidentes, sino que también permite evaluar al usuario en la prevención de estas situaciones de riesgo.

Sin embargo, teniendo en cuenta todos los beneficios que la inteligencia artificial y la automatización aportan a la seguridad organizacional, también se han provocado preocupaciones sobre el desplazamiento laboral. Se argumenta que la IA podría reemplazar algunos empleos, pero también se espera que genere nuevos puestos de trabajo. Contemplando esta situación desde un enfoque positivo, el éxito en esta era dependerá de la capacidad para adaptarse y adquirir las habilidades necesarias. Por lo tanto, es crucial que tanto las habilidades humanas como las técnicas desempeñen un papel fundamental en la configuración del futuro laboral.

Por lo tanto, incluso con los recientes avances en la tecnología de inteligencia artificial, no es práctico usarla como un reemplazo total para los seres humanos. Los sistemas de IA necesitan un nivel de supervisión y control por parte de profesionales capacitados, y las decisiones tomadas por la IA no deben reemplazar las decisiones humanas. Dado que estos sistemas requieren de un mantenimiento adecuado, las organizaciones deben garantizar que se gestionen y operen de manera correcta.

Algunas recomendaciones para maximizar los beneficios de la digitalización y reducir sus riesgos, es desarrollar e implementar estrategias adecuadas que tengan un enfoque preventivo y proactivo, que permitan anticipar y manejar los riesgos antes de que surjan. Esto incluye invertir en la formación y capacitación continua de los empleados para que estén al día con la tecnología y adquieran las habilidades necesarias. También es fundamental implementar programas que promuevan la salud mental y el bienestar en el entorno laboral. Además, deben establecerse políticas claras y estrictas sobre la privacidad y seguridad de los datos, asegurando que la recolección, almacenamiento y uso de la información personal se realice de manera ética y segura.

Finalmente, para maximizar la eficacia de la inteligencia artificial como herramienta preventiva contra riesgos laborales, ciberataques y el uso indebido de datos, es esencial implementarla adecuadamente en las organizaciones. Esto requiere adoptar un enfoque estratégico que integre las soluciones de IA con los sistemas existentes y que se ajuste a las necesidades específicas de la empresa. Al adoptar una postura proactiva y flexible hacia la IA, las organizaciones no solo protegerán sus activos y datos, sino que también mejorarán su posición competitiva al ser vistas como líderes en innovación y seguridad. La combinación de tecnología avanzada con una gestión estratégica y ética ayudará a crear un entorno empresarial más seguro, eficiente y preparado.

Referencias

Burkhardt, R., Hohn, N., & Wigley, C. (2019). Hacia una inteligencia responsable en las organizaciones.

Dekker, S. (2014). Safety differently. London: CRC Press.

Dekker, S. (2019). Foundations of safety science: A century of understanding accidents and disasters. Routledge.

Del Castillo, M. C.: "El uso de la inteligencia artificial en la prevención de riesgos laborales", Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo, vol. 8, núm. 1, 2020.

Delgado Alberto. Inteligencia Artificial y Mini Robots. VII Congreso Nacional de Estudiantes de Ingeniería Industrial, Administrativa y de Producción. Universidad Nacional Sede Manizales. Memorias Congreso. Octubre 4 – 10 de 1998.

El impacto de la inteligencia artificial en la seguridad y la salud en el trabajo. (2021). European Agency For Safety And Health At Work.

F. Bastani and A.-R. Sadeghi, "Rethinking the role of machine learning in mobile systems," IEEE Transactions on Mobile Computing, vol. 9, no. 11, pp. 1572–1585, 2010.

Fleifel, F. (2015) Inteligencia Artificial. Red científica ciencia tecnología y pensamiento.

García, M.C. La inteligencia artificial para el entorno laboral. Un enfoque en la predicción de accidentes. (2021). e-Revista Internacional de la Protección Social, Vol. VII(N° 1).

Grand View Research. (2023). Artificial Intelligence Market Size, share & Trends Analysis Report by solution, by technology (Deep Learning, Machine Learning, NLP, Machine Vision, Generative AI), by function, by end-use, by region, and segment Forecasts, 2024 - 2030. (s. f.).

Hollnagel, E.,Wears, R. L., & Braithwaite, J. (2015). From Safety-I to Safety-II: A White Paper.

IBM Cloud. (2021) Ai vs machine learning vs deep learning vs neural networks.

Iglesias, A. (2016). La historia de la inteligencia artificial: Desde los orígenes hasta hoy. Ticbeat.

Instituto Vasco de Seguridad y Salud Laborales (2021). Realidad virtual aplicada a la formación en seguridad y salud en el trabajo.

J. McCarthy, "What is artificial intelligence?" Stanford University, Tech. Rep., 2007.

Jansen, A. et al., 2018, Emerging risks to workplace safety; working in the same space as a cobot (Nuevos riesgos para la seguridad en el lugar de trabajo: trabajar en el mismo espacio que un cobot), informe R10742 de TNO.

Legg, S. y Hutter, M. (2007). Una colección de definiciones de inteligencia. Frontiers in Artificial Intelligence and applications , 157 , 17.

Melman, L. (2020). "La Inteligencia Artificial Implementada en la Seguridad Informática".

Moreno, C.R. (abr de 2023). "La Inteligencia Artificial en la Seguridad Informática".

Nebendah Dieter. Sistemas Expertos. Ingeniería y Comunicación. Editores Marcombo. Barcelona 1988.

Pappas, how Christopher, to overcome "Ai implementation them. (2023).

Perrow, C (1984). Normal Accidents. Living with High-Risk Technologies.

PwC. (2020) Ai business survey. PricewaterhouseCoopers LLP.

Rauch-Hindin, W. B. (1989). Aplicaciones de la inteligencia artificial en la actividad empresarial, la ciencia y la industria. Ediciones Díaz de Santos.

Reason, J. (1990). Human error. Cambridge university press.

Rich, E.; Knight, K. (1994). Inteligencia artificial. Segunda edición. Madrid: McGrraw-Hill.

Rouhiainen, L. (2019). Inteligencia artificial para empresas.

Russell, SJ, y Norvig, P. (2016). Inteligencia artificial: un enfoque moderno. Malasia; Pearson Education Limited.

Steels, L. (1993). Las raíces de la vida artificial y la inteligencia artificial. Vida artificial, 1 (1_2), 75-110.

Tenés, T. (2023). Impacto de la Inteligencia Artificial en las Empresas.

Vela, A. (2013). La inteligencia artificial: ¿oportunidad de progreso o amenaza? ticbeta.