SEPTIEMBRE, 2024

CONNECTASIS225

Comunidad de Profesionales de la Seguridad en Colombia

Memorias
XIV SIMPOSIO
IMPACTO DE LA IA EN LA SEGURIDAD CORPORATIVA

ASIS 225
En la Feria Internacional de Seguridad ESS+

DEL ANÁLISIS AL ANTICIPO:
Cómo la IA Está Revolucionando la Gestión de Riesgos de Seguridad

ASIS INTERNATIONAL® | Bogotá Chapter

SEPTIEMBRE, 2024

CONNECTASIS225

Comunidad de Profesionales de la Seguridad en Colombia

Memorias:
Jahat Esteban Ramirez Viatela
Yessika Barrantes Acelas
Universidad Militar Nueva Granada
Facultad de Relaciones Internacionales, Estrategia y Seguridad
Administración de la Seguridad y Salud ocupacional.

Corrección y Edición:
Jorge Romero Clavijo, CPP

Diseño y Diagramación
Yelena Castañeda - Triclick Agencia Digital

ASIS INTERNATIONAL® Bogotá Chapter

CONTENIDO

NEWSLETTER CONNECTASIS225

Palabras del presidente

Estimados miembros del ASIS Capítulo 225.

Me complace extender mi más profundo agradecimiento por su participación y apoyo en el XIV Simposio anual "Impacto de la IA en la Seguridad Corporativa", llevado a cabo durante la Feria Internacional de Seguridad de Bogotá. ESS+ en su 30º aniversario bajo el liderazgo de Patricia Acosta. Su compromiso y colaboración fueron esenciales para el éxito del evento.

Especial reconocimiento para Keren Amaya, Jorge Romero Clavijo, CPP, Julian Andres Puentes B., CPP,PSP miembros de la junta directiva, pero también a SEGURIDAD DIGITAL LTDA., Denice Garzón Malpica, Cesar Augusto Cardona Ortiz,CPP, PROSINTE SAS, @vipschoolltda., 3+ Security Colombia, Martin Tarazona, Grupo Consultor 360, John Fredy Sierra Blanco, Colpryst asesores, Maria del Pilar Jimenez, ANDRÓSS LTDA., Maria Cristina Ovalle. CPP, TriClick.co, Yelena Castañeda Useche, ISVI LTDA Vigilancia y Seguridad Privada,Jorge Eduardo La Rotta Còrdoba Organización GDC, @Romero Consultores ya la REVISTA EL MUNDO CAMBIÓ y a cada uno de los conferencistas, panelistas, invitados especiales, voluntarios y asistentes a nuestro evento.

Agradezco sinceramente su contribución y espero seguir contando con su valiosa participación en futuras ediciones.

Una vez más se demuestra que #ASISSOMOSMASFUERTES. Ademas que entre todos estamos para sumar y multiplicar. Nos vemos el próximo año, esperamos en un evento mayúsculo y lleno de sorpresas.

En esta edición compartimos las memorias de este importante evento.

¡Disfruten de la lectura!

DANIEL JIMENEZ
MBA, CPP®,PSP®, CHSS, ESRM

AGRADECIMIENTO ESPECIAL

A Nuestros Patrocinadores:

SEGURIDAD DIGITAL

ORGANIZACIÓN G.D.C
GESTIÓN, DESARROLLO Y CRECIMIENTO EMPRESARIAL

RC

SECURITY COLOMBIA

PROSINTE
Protección y Selección Integral

TRI CLICK
Marketing Digital

V.I.P SCHOOL LTDA
Forjando profesionales en seguridad

COLPRYST

ISVI

ANDRÓSS

ESS
FERIA INTERNACIONAL DE SEGURIDAD

EL MUNDO CAMBIO

ORM INTELIGENCIA ARTIFICIAL
Y LOS RIESGOS DE BCM

"Hagamos conciencia propia. ¿En dónde estamos? ¿Cómo estamos? Y que desarrollemos, que nos metamos y nos involucremos en ese mundo, porque si no, nos vamos a quedar atrás. Las tecnologías hoy en día tienen amenazas emergentes, vienen con eso. Preparémonos".

por Servio Camey

En la conferencia "ORM Inteligencia Artificial y los riesgos de BCM" el MSC Servio Camey discute la evolución en la metodología de seguridad y la adaptación a las nuevas amenazas, enfocándose en varios aspectos clave como: la evolución de la seguridad, el uso de aplicaciones, el análisis de datos, el uso de la inteligencia artificial, la capacitación y planeación organizacional y la gestión de crisis. La conferencia aboga por una integración continua de la IA en la seguridad y, una mejora constante de las habilidades y conocimientos del equipo para enfrentar las amenazas emergentes.

La seguridad moderna ha evolucionado hacía un modelo colaborativo en el que son esenciales las habilidades blandas y el brainstorming para enfrentar las amenazas actuales. La seguridad ha dejado atrás el enfoque aislado, siendo necesario formar vínculos, redes, nexos y círculos, así como el país bonding y el pair network para compensar el conocimiento insuficiente en algunas áreas y estar preparados.

El uso de aplicaciones de IA es una forma de ayudar en la detección temprana de riesgos y reducir el error humano. Se debe saber programar e indicarle a la APP qué es lo que se quiere y cómo hacerlo, por medio de las search engines. No obstante, las aplicaciones gratuitas pueden poner en riesgo los datos al no generar un bonding de privacidad que evite que la información sea filtrada, esto puede derivar en un problema legal y ético, al igual que un compliance interno.

Es por esto que, primero se debe contratar una APP de inteligencia artificial con todos los medios legales de protección de información hacia la empresa y evitar generar vulnerabilidades a futuro.

El análisis e interpretación de datos desde los enfoques reactivo, operativo y activo, viene siendo otro factor clave en materia de la cadena logística, la seguridad debe enfocarse en ayudar a los negocios a cumplir sus objetivos. La IA apoya en la recopilación y análisis de datos históricos, así como a anticipar y preparar respuestas para futuras amenazas, como se dio en el caso de los bloqueos durante las elecciones de Honduras en el que se aseguró el abastecimiento y la entrega oportuna de mercancías.

Además, se deben tener en cuenta los cinco factores de poder que desestabilizan: político, económico, social, salud y seguridad, para manejar toda esa información y empezar a tener inteligencia.

De este modo, la IA, como este cerebro electrónico que aprende y evoluciona sobre la información que va recibiendo, se utiliza para detectar riesgos y hacer análisis predictivo. Es crucial aprender a usar herramientas de IA para mejorar la seguridad, hay que tener conciencia propia de dónde estamos e involucrarnos en la IA, siempre siendo con cautela de la ética y la legalidad en la recolección de datos, teniendo en cuenta que, las tecnologías hoy en día, traen amenazas emergentes.

Se subraya también la importancia de desarrollar habilidades técnicas y blandas sobre IA, e igualmente, capacitar a los subalternos como una cuestión moral. Así como la capacitación debe ser proactiva y autodidacta, el conocimiento debe compartirse entre los miembros del equipo, especialmente cuando se confrontan los problemas actuales al poco conocimiento que se tiene sobre la IA y el ciberespacio.

Ahora, con la IA, el multitasking es muy relevante; cada vez más se requieren perfiles que conozcan sobre seguridad informática y seguridad física, por ello, se debe prepararse y evolucionar.

Finalmente, la planificación y ejecución efectiva de procesos y políticas para gestionar crisis son esenciales. En este punto, la delegación de responsabilidades y el empoderamiento del equipo mejora la resiliencia organizacional, de forma que, los equipos se vuelven más dinámicos. Las herramientas para la gestión de crisis se deben mirar desde procesos, procedimientos y políticas, aquí viene siendo muy importante la planificación administrativa, operativa y estratégica, organizar por escrito, hacer una mesa redonda, hacer un plan y ejecutar el plan, para así, tener éxito.

Servio Camey

Msc, CPP Regional Security Head, PACA, Bayer

RVP para la región de Centroamérica de ASIS International, Jefe Regional de Seguridad para Centroamérica y Caribe en Bayer, licenciado en Administración de Seguridad, MSc en Criminología, postgrado en criminalística, diplomado universitario en Seguridad Privada, ha trabajado en Seguridad durante los últimos 18 años, experiencia en Gestión de Riesgos, auditorías de seguridad, prevención de pérdidas en retail (Sears Guatemala) encabezando las áreas de Seguridad y Protección como CSO.

servio-camey-msc-cpp-a3b94b80

RELACIÓN DE LA IA Y LA SEGURIDAD CORPORATIVA

por Jairo Hernán Diaz

"... En este mundo de tanta explosión de información la fuente es fundamental, osea, es la clave de todo esto... Pero ¿a dónde va todo esto? Mire, todo eso es buscar tecnología e incrementar conocimiento y en ese mismo texto, vea, ¿a mí qué me ha pasado?, ¿yo qué he buscado? gente que me hable desde la experiencia, no desde la teoría."

La relación entre la inteligencia artificial (IA) y la seguridad corporativa está en un punto crucial de desarrollo. La IA, con su capacidad para analizar grandes volúmenes de datos y detectar patrones complejos, se ha convertido en una herramienta esencial para muchas empresas que buscan proteger sus activos y mantenerse a la vanguardia en un entorno de amenazas en constante evolución. Sin embargo, es importante reconocer que la IA, a pesar de su potencial, sigue siendo una tecnología en evolución y no está completa. Esto significa que, aunque puede ofrecer soluciones avanzadas, también enfrenta limitaciones y desafíos que deben ser considerados.

Uno de los elementos clave en el uso de la IA para la seguridad corporativa es el papel de los discriminadores. Estos algoritmos tienen la capacidad de analizar y configurar datos de manera que puedan identificar amenazas potenciales o anomalías dentro de un sistema. Al procesar grandes cantidades de información, los discriminadores ayudan a las empresas a detectar patrones inusuales que podrían indicar un riesgo de seguridad. No obstante, la efectividad de estos algoritmos depende en gran medida de la calidad y la relevancia de los datos que se utilizan para su entrenamiento.

En este contexto, la calidad de las fuentes de información cobra una importancia crítica. Lo anterior señala la necesidad de utilizar publicaciones de fuentes que ofrecen datos verificados y de alta calidad.

Estas fuentes no sólo garantizan que la IA esté trabajando con información precisa, sino que también permiten a las empresas basar sus decisiones en evidencia sólida y confiable.

El acceso a internet y la fecha de entrenamiento de los modelos de IA son otros factores cruciales en su desarrollo y aplicación. La IA necesita estar conectada a una vasta red de información para mantenerse actualizada y relevante. Esto es especialmente importante en el campo de la seguridad, donde las amenazas pueden cambiar rápidamente. Si los modelos de IA no se entrenan con datos recientes, su capacidad para predecir y prevenir amenazas se ve comprometida. Además, contar con bases de datos tecnológicos especializados permite a la IA comparar datos de manera más eficiente, lo que es esencial para identificar correlaciones y tendencias que podrían no ser evidentes a simple vista.

La comparación de datos es un proceso fundamental en la aplicación de la IA en la seguridad corporativa. Al comparar datos de diferentes fuentes y en diferentes momentos temporales, la IA puede detectar incongruencias que podrían señalar un problema de seguridad. Sin embargo, este proceso no es perfecto y todavía requiere de la inteligencia humana para interpretar y aplicar los resultados de manera efectiva.

Es aquí donde la inteligencia humana (IH) entra en juego. A pesar de los avances en IA, la experiencia y el juicio humano siguen siendo elementos indispensables en la gestión de la seguridad. En resumen, la IA tiene el potencial de revolucionar la seguridad corporativa, pero su éxito depende de varios factores, incluyendo la calidad de las fuentes de información, el acceso a datos actualizados, y la colaboración con la inteligencia humana. La IA y la IH no deben verse como entidades separadas, sino como partes complementarias de un sistema de seguridad que busca proteger a las empresas en un mundo cada vez más complejo y lleno de riesgos.

Jairo Hernán Diaz Arias

Jefe CRAI (Centro de Recursos para el Aprendizaje y la Investigación)Jefe CRAI (Centro de Recursos para el Aprendizaje y la Investigación) Universidad del Quindío (Colombia).

https://www.linkedin.com/in/jairohernandiazarias/


¿Listo para llevar su carrera en seguridad AL SIGUIENTE NIVEL?
CPP (R)
Certified Protection Proffesional
Certified Protection Professional
Board Certified in Security Management
APP
Associate Protection Proffesional
APP
Associate Protection Professional
PCI (R)
Proffesional Certified Investigator
PCI
Professional Certified Investigator
Board Certified, ASIS International
PSP (R)
Physical Security Professional
PSP
Physical Security Professional
Board Certified, ASIS International
ASIS
INTERNATIONAL®
Bogotá Chapter

APLICACIONES DE LA IA EN SEGURIDAD CORPORATIVA

"Al estar involucrados con la inteligencia artificial, de una u otra forma también nos beneficia. Para nosotras las compañías de seguridad es un soporte. Pero de la misma forma tenemos que tener el cuidado, tenemos que revisar minuciosamente que esto no se nos convierta en un problema hacía nuestro aliado estratégico"

"No miren la seguridad como un gasto, mirenla como una inversión"

El panel "Aplicaciones de la IA en Seguridad Corporativa" integrado por la CEO Denice Garzón, el ingeniero Javier Villarreal y el CEO Augusto López, discute el impacto de la Inteligencia Artificial en el sector de la seguridad desde diversas perspectivas. De tal manera, se expone cómo la IA afecta el desarrollo en la gestión de seguridad, y del mismo modo, cómo la IA va a beneficiar o puede poner en riesgo a las empresas y gobiernos. Se formularon tres preguntas clave en lo que respecta: el impacto de la IA en las mejoras de las estrategias en la seguridad pública o corporativa; avances de la IA y los retos éticos y operativos que enfrenta la seguridad corporativa; y cómo prepararse y hasta dónde puede llegar la IA.

La IA se encuentra en constante cambio, y con ello ha cambiado la velocidad de transformación de las organizaciones. La IA impacta en la mejora de estrategias en la seguridad pública o corporativa partiendo del hecho de que la tecnología hace que de una forma u otra las organizaciones se vuelvan vulnerables, debido a que, en algunos contextos no hay ética ni control de la entrada y salida desde los algoritmos.

Denis Garzón, Javier Villarral, Augusto López.

No obstante, la IA también es un soporte a las compañías de seguridad, y la seguridad tanto corporativa como pública deben ser lo suficientemente ágiles para adaptarse, prepararse para entender los cambios y aprovechar esa inteligencia artificial, pero se tiene que revisar minuciosamente para que no se convierta en un problema hacia el aliado estratégico. La IA acompaña los servicios que ofrecen las empresas de seguridad tanto en zonas urbanas y rurales, y al estar en constante cambio, se espera en algún momento poderla regular.

Desde la práctica, se puede evidenciar que, la IA viene migrando la seguridad, de una seguridad física a la seguridad electrónica.

Hoy es importante para las empresas contar con un área de tecnología e ir incursionar en IA, porque la IA aplicada a las plataformas, software y dispositivos electrónicos, permite una respuesta más ágil y eficaz a eventos de seguridad, y optimiza procesos en áreas operativas, comerciales y de marketing de las organizaciones, principalmente en el tema de automatización de tareas, análisis de datos, la predicción y la prevención.

Al considerar los avances de la IA, se plantean dos retos éticos y operativos que enfrenta la seguridad corporativa: la privacidad y la discriminación. Hay una línea muy delgada que no se debe traspasar, y hasta donde se debe llegar con el uso de la inteligencia artificial y cómo se maneja la información. Normalmente, se acoge la versión europea o norteamericana en el tema de manejo de datos.

Se va a tener que regular para que no haya discriminación y para que se guarde la privacidad de las personas, porque la IA está en todas partes, ayuda, pero también, está conociendo más sobre cada uno. En Colombia, si bien existe el Decreto 356 de 1994 que establece el estatuto de vigilancia y seguridad, en este no se incluye nada con respecto a la tecnología, por lo tanto, contar con la legislación jurídica da validez a las pruebas por medio tecnológicos en cualquier proceso judicial.

Para ello, en el caso de Colombia, el Congreso de la República debe presentar un proyecto para controlar su uso. Ya se cuenta con varios programas en universidades e instituciones del Estado que promueven el estudio de la inteligencia artificial en gerencia y recursos humanos, sin embargo, desde el Ministerio de Educación debe haber más interés en capacitar a los ciudadanos en IA y hacer más publicidad al respecto.

Por su parte, el capítulo ASIS, va a empezar a liderar la comunidad en competencia de IA, divulgación, publicidad y educación, porque es necesario.

Desde la perspectiva y el rol en las empresas, el futuro de la IA en seguridad, por una parte, plantea un miedo de reducción de empleos para diferentes profesiones, pero lo que se va a dar es una transformación para la que se debe estar preparados y generar valor a través del aprendizaje constante. Esto, teniendo en cuenta que ahora hay una convergencia en las plataformas entre ciberseguridad y seguridad física.

El mito de que la IA va a reemplazar al ser humano, no es cierto, la IA es un complemento para el ser humano en aquellas situaciones donde este no puede decidir. Por ello se debe estar a la vanguardia de la tecnología.

Existe la necesidad de mayor integración y capacitación en tecnología, tanto en el sector privado como público. Desde lo privado, la seguridad está subutilizada porque no existe un buen programa de Estado que integre a las empresas, además está la estigmatización de que se puedan confundir con grupos paramilitares y autodefensas. Pero, son las empresas quienes cuentan con la mayoría de información en temas de delincuencia.

Desde lo público, se requieren dos aspectos fundamentales: voluntad política y presupuesto. Voluntad política para trabajar en la legislación necesaria en materia de tecnología e IA; y presupuesto para invertir en herramientas y dispositivos.

La seguridad no es un gasto, es una inversión. La IA llegó para quedarse, para complementar la seguridad y la gestión de seguridad, teniendo en cuenta principios éticos.

USO DE LA IA EN LA GESTIÓN DE RIESGOS DE COMPLIANCE

EN EL CONTEXTO DE LA SEGURIDAD CORPORATIVA

Daniela Cuellar, David Ortiz, Henry Murrain, Mark Bartch.

"En este país se pierde más plata que por la corrupción, por mal conocimiento de los problemas y mala planeación, y eso si nadie lo denuncia. Nosotros no somos una sociedad de conocimiento, no nos gusta pensar problemas juiciosamente... H ay una obsesión por la acción irreflexiva... Buena parte de los errores que estamos cometiendo es porque no entendemos bien los problemas y entender bien esos problemas implica también entender de manera rigurosa, sofisticada, que está detrás del comportamiento transgresor, que llamamos corrupción, porque aquí además es un concepto súper impreciso... Hay que investigar la honestidad y transparencia debe tener también datos y ejemplos sobre honestidad, porque eso ocurre más que lo otro."

La lucha contra la corrupción y la adaptación a los cambios globales representan desafíos complejos que exigen una formación sólida y multidimensional. Las personas y las organizaciones deben estar preparadas para identificar los factores que favorecen la corrupción, así como para adoptar estrategias que promuevan la ética y la transparencia. Uno de los factores más críticos en este contexto es el socioeconómico. La pobreza y la desigualdad crean un entorno en el que las prácticas corruptas pueden institucionalizarse fácilmente. En contextos donde las oportunidades económicas son limitadas y el acceso a recursos es escaso, la corrupción se percibe como una vía necesaria para obtener empleo, protección o servicios básicos, contribuyendo así a su normalización en la sociedad.

El factor de seguridad también juega un papel crucial. En entornos marcados por la inseguridad y la falta de control estatal, la corrupción emerge como un mecanismo de acceso a recursos o protección. Los ciudadanos, enfrentando situaciones hostiles, pueden verse obligados a recurrir a actos corruptos para sobrevivir o garantizar su seguridad. En tales contextos, las fuerzas del orden y los funcionarios públicos a menudo son cómplices, lo que perpetúa un ciclo de ilegalidad. Ante este panorama, la educación se convierte en una herramienta clave para fomentar la integridad y la responsabilidad social. Sin embargo, esta educación debe ir más allá de normas técnicas y enfocarse en inculcar valores y conciencia ética, de modo que los ciudadanos comprendan el impacto nocivo de la corrupción en su entorno.

La desconexión entre lo que debería ser y lo que es, es una realidad presente en muchas sociedades. Las normas sociales suelen establecer lo que es moralmente correcto, pero la práctica muchas veces está marcada por una disonancia con estas expectativas. Este fenómeno es especialmente evidente en contextos de corrupción sistémica, donde las prácticas corruptas son aceptadas implícitamente como parte de la norma dentro de ciertas instituciones o grupos. A medida que estas prácticas se normalizan, se genera una cultura de corrupción que es muy difícil de eliminar sin un cambio estructural y cultural profundo.

En este sentido, las ciencias sociales han encontrado en las ciencias exactas una nueva perspectiva para analizar el comportamiento humano. La interdisciplinariedad ha permitido comprender mejor cómo se configuran las decisiones y acciones de las personas dentro de su entorno social. La teoría de las normas sociales, por ejemplo, explica cómo los individuos a menudo actúan más en función de las expectativas de su grupo que de sus propias convicciones morales. El concepto de ignorancia pluralista describe cómo las personas conforman su comportamiento a lo que creen que los demás esperan de ellas, aunque esto contradiga sus principios. Esta dinámica social puede perpetuar la corrupción, ya que las personas se sienten presionadas a participar en prácticas que saben son incorrectas para evitar el rechazo social o la exclusión.

En el ámbito empresarial, el rol del oficial de cumplimiento ha ganado una gran relevancia. Esta figura es clave para garantizar la integridad de los procesos internos y prevenir irregularidades que puedan derivar en sanciones financieras o pérdida de reputación. El oficial de cumplimiento tiene como objetivo principal fortalecer los controles internos para cumplir con las normativas legales y evitar riesgos que comprometan la estabilidad de la empresa.

Sin embargo, el éxito de esta función depende de una coordinación eficaz entre los diferentes departamentos. La falta de comunicación o la segregación entre áreas puede facilitar la implementación de prácticas corruptas o ineficiencias que afecten el buen funcionamiento de la organización.

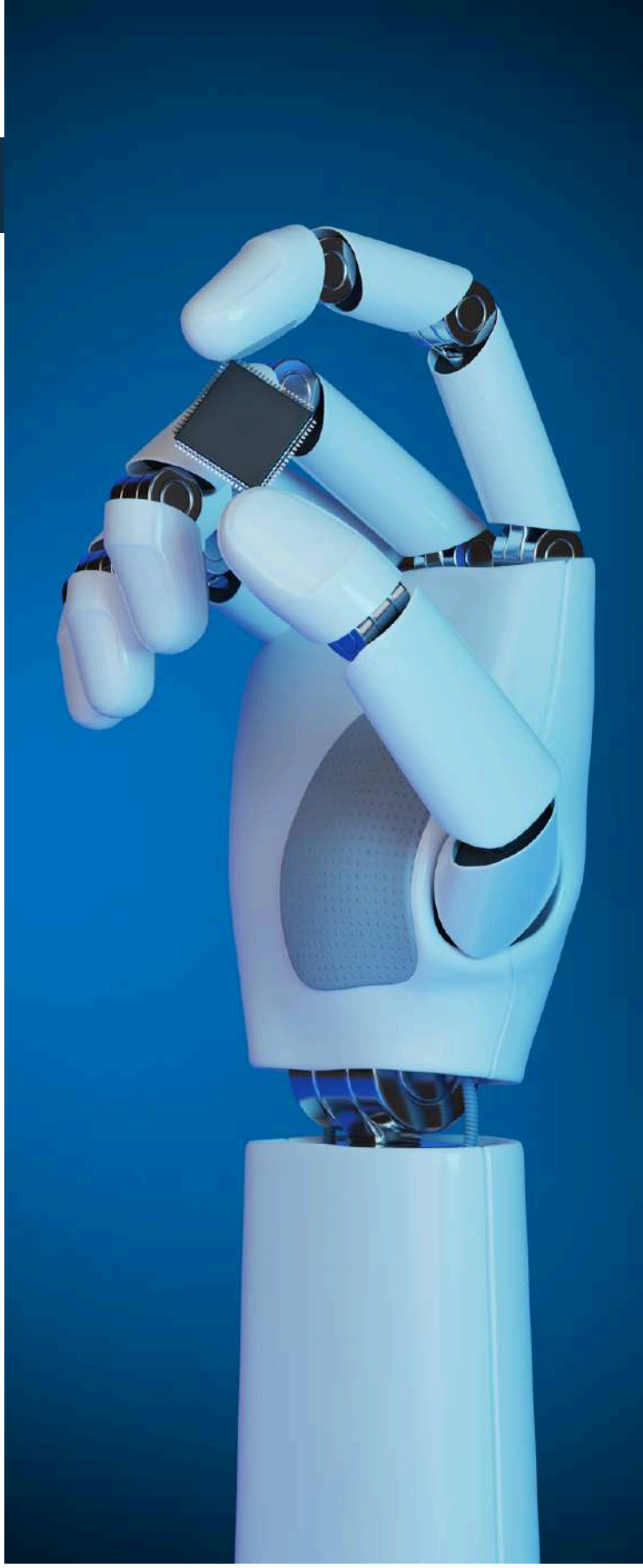
Para asegurar una mayor transparencia y evitar conflictos de interés, muchas empresas optan por contratar a terceros independientes que supervisen el cumplimiento de normativas. Este enfoque refuerza la confianza en los procesos internos, minimiza los riesgos de irregularidades y garantiza una auditoría imparcial, permitiendo a las empresas mejorar sus prácticas y detectar áreas vulnerables.

La construcción simbólica del mundo, que influye en cómo las personas interpretan su realidad, no se limita solo a cuestiones económicas, sino que afecta todas las dimensiones de la vida en comunidad. Los valores, expectativas y percepciones que una sociedad construye tienen un impacto directo en el comportamiento de los ciudadanos. A menudo, la exageración de datos sobre problemas sociales o económicos crea percepciones distorsionadas de la realidad, lo que genera decisiones impulsivas o irreflexivas que, lejos de resolver problemas, perpetúan ciclos de ineficiencia y corrupción. Este tipo de comportamiento impide la implementación de soluciones sostenibles a largo plazo.

Un claro ejemplo de esta construcción simbólica es el caso de Colombia, que durante mucho tiempo ha sido vista, tanto interna como externamente, a través de una narrativa pesimista. La violencia, el narcotráfico y la corrupción han alimentado esta percepción, afectando la autoestima colectiva y limitando la capacidad del país para proyectarse de manera positiva.

Cambiar esta narrativa es crucial para que Colombia construya una identidad nacional más sólida, basada en sus fortalezas y su capacidad de superar desafíos. Promover una visión más optimista del país, que resalta sus logros y potencial, es esencial para fomentar la cohesión social y el orgullo nacional. Este cambio no solo mejoraría la autopercepción de los colombianos, sino que también ayudaría a proyectar una imagen más favorable en el ámbito internacional, lo que podría impulsar el desarrollo y el crecimiento del país.

La inteligencia artificial (IA) puede desempeñar un papel crucial en la reducción de la corrupción al aportar herramientas que mejoran la prevención y predicción de comportamientos indebidos en las corporaciones. A través del análisis de grandes volúmenes de datos, la IA puede identificar patrones y señales que indiquen riesgos de corrupción, como transacciones sospechosas, inconsistencias en los procesos financieros o comportamientos atípicos en la gestión de recursos. Esto permite que las organizaciones actúen de manera proactiva, implementando medidas correctivas antes de que los problemas se materialicen. Además, la IA puede ser utilizada para automatizar la supervisión interna y auditar continuamente el cumplimiento de normas éticas, garantizando que se sigan las mejores prácticas de transparencia y responsabilidad. Involucrar la ética en el desarrollo y la implementación de estos sistemas es fundamental, ya que la IA no solo debe detectar posibles irregularidades, sino también fomentar una cultura corporativa basada en la integridad y el compromiso con los principios éticos. Esto fortalece la capacidad de las organizaciones para actuar de manera preventiva y reducir el margen de actuación de las prácticas corruptas.



ASIS LATAM&CA 2024

Costa Rica

Congreso de Seguridad Integral

18 y 19 de noviembre

CONECTANDO LÍDERES Y EXPERTOS EN SEGURIDAD

Es el encuentro **para ejecutivos de alto nivel y autoridades** en el campo de la seguridad integral.

Regístrese hoy y asegure su lugar como **asistente, patrocinador o conferencista** en **el evento más importante de seguridad en América Latina.**

Más información en:

info@asisonline.lat
www.asisonline.lat

ASIS INTERNATIONAL | LATAM

Con el apoyo de: CRECEX

Somos esencial COSTA RICA

SECURITY MANAGEMENT AS A SERVICE

Diego Beltrán

"Muchas veces y durante muchos años, hemos visto cómo la seguridad se empieza a abarcar, no desde lo que se entiende como la organización, sino como un servicio, como un satélite que está dando vueltas, y en el fondo está apuntando hacía el core del negocio"

"Vamos a seguir utilizando la inteligencia artificial pero tenemos que mantenernos empleables. Acuérdense siempre que la inteligencia artificial jamás va a reemplazar las relaciones interpersonales, nuestra intuición y la incertidumbre. Y eso es lo que elimina el riesgo"

La conferencia "Security Management as a Service" por el CEO Diego Beltrán Alcalde, presenta el concepto de "Security Management As a Service" (SMaaS), en un contexto donde, desde hace algunos años, se comenzó a investigar cómo la inteligencia artificial (IA) cambia los enfoques tradicionales en el campo de la seguridad, pero enfatiza que, aunque la IA puede mejorar muchos aspectos, no puede reemplazar completamente la percepción humana, la intuición y las relaciones interpersonales en la seguridad.

El concepto de SMaaS aborda seis áreas clave para mejorar la seguridad y ponerla en función de la organización: gestión, riesgo, planificación, control, resiliencia e innovación. Estos conceptos buscan integrar la seguridad más profundamente en el núcleo del negocio, como un servicio, y como algo que afecta a cada área del negocio, en lugar de tratarla como una función periférica.

La gestión se refiere a la dirección centralizada de la seguridad, que permite mejorar la coordinación, supervisión y economía de escala. Mejora las negociaciones con los proveedores desde esa coordinación centralizada. La seguridad debe integrarse a las diferentes áreas del negocio, y los gerentes hablar entre sí.

Es en la medición de riesgo donde se diferencia de la IA. Muchas decisiones en Latinoamérica se toman desde la percepción, pero se debe lograr una estandarización real de las mediciones de riesgo con números discutibles para eliminar la percepción subjetiva y conocer las vulnerabilidades y amenazas de la empresa, y a partir de datos, tomar decisiones informadas.

La planificación es cómo la seguridad debe alinearse con los objetivos estratégicos de la organización, lo que es más importante para la empresa, y de este modo ser efectiva y justificar su presupuesto. Aquí surge la pregunta: ¿la seguridad es un gasto o una inversión?

Es esencial controlar el gasto y asegurar el cumplimiento y efectividad de los lineamientos estratégicos de seguridad. En este punto aplica el compliance. La seguridad no debe quedarse en lo coercitivo, se tiene que controlar la organización desde el negocio y la línea de efectividad de los recursos.

Desde el SMaaS, la resiliencia es la continuidad operativa de la organización como un proceso que depende de una buena planificación y el entendimiento de las amenazas. Conocer realmente las amenazas permite eliminar la percepción y empezar a trabajar con base a los datos duros.

La innovación se da con la integración de tecnologías avanzadas y plataformas de gestión, como los dashboards. Las herramientas tecnológicas permiten llegar en tiempo y forma a lo que pide el gerente general y los delineamientos de la empresa, y eso es clave para la efectividad del SMaaS.

El concepto SMaaS sugiere que, así como se externalizan servicios como TI, la seguridad también debe ser gestionada como un servicio que entrega valor tangible y medible. La IA puede complementar este enfoque, pero el contacto humano y la capacidad de adaptación seguirán siendo cruciales para el éxito en la gestión de seguridad.

Diego Beltrán

CEO Dynamic Trading Security \ Brain-Based Coach
Como CEO de una empresa líder en seguridad estratégica en Chile, soy responsable de dirigir el negocio, asegurando el crecimiento y la sostenibilidad a largo plazo.

diego-beltrán-alcalde-3747141b

INTELIGENCIA ARTIFICIAL
Y ESTRATEGIA ORGANIZACIONAL

por Andrés Aguilera

"Inteligencia Artificial es predicción. Para hablar de esto necesitamos entender que para que haya Inteligencia Artificial necesitamos datos. Y si ustedes se dan cuenta en los últimos ochenta años hemos acumulado datos como ustedes no se imaginan... datos es lo que nos permite hacer predicción. Data es plata"

La implementación de la inteligencia artificial (IA) dentro de la estrategia organizacional puede marcar una diferencia significativa en la capacidad de una empresa para mantenerse competitiva, eficiente e innovadora. Existen diversos tipos de IA que pueden ser utilizados para generar valor tangible, entre los cuales destacan la IA predictiva y la IA generativa. La IA predictiva, como su nombre indica, utiliza grandes volúmenes de datos para identificar patrones, realizar análisis avanzados y predecir comportamientos o tendencias futuras. Este enfoque permite a las organizaciones adelantarse a los desafíos del mercado, anticipar la demanda de productos o servicios, optimizar procesos internos y gestionar el riesgo de manera más eficaz. Por ejemplo, en el ámbito financiero, la IA predictiva puede identificar posibles fraudes antes de que se materialicen, mientras que en la industria manufacturera puede anticipar fallos en la maquinaria, reduciendo costos y mejorando la eficiencia operativa.

Por otro lado, la IA generativa es una tecnología capaz de crear nuevas soluciones, contenidos o productos a partir de los datos existentes. Esta tecnología puede generar desde textos hasta imágenes o modelos complejos, aportando innovación a sectores como el diseño, la publicidad, y hasta la medicina. Su capacidad para proponer nuevas ideas o perspectivas abre un abanico de posibilidades para la creación de productos, servicios y estrategias más avanzadas y competitivas.

A pesar de estos avances, es importante señalar que la IA no es autónoma; sigue requiriendo la supervisión y validación humana para garantizar que sus resultados sean precisos y éticos. Los sistemas de IA deben ser controlados y evaluados por profesionales que comprendan tanto sus capacidades como sus limitaciones. En este sentido, el juicio humano es fundamental para asegurar que la IA se aplique de forma responsable, especialmente en contextos donde los riesgos son elevados o las implicaciones éticas son profundas.

Sin embargo, la integración de IA en las organizaciones no está exenta de desafíos. Existen importantes barreras que deben superarse, como la desinformación, los deepfakes y la polarización política, fenómenos que pueden ser agravados por el mal uso de estas tecnologías. Los ataques cibernéticos, por ejemplo, se han vuelto más sofisticados con el uso de IA, lo que plantea riesgos significativos para la seguridad de los datos y la privacidad de los usuarios. Además, la propiedad intelectual y los efectos ambientales también son áreas de preocupación, ya que el entrenamiento de modelos de IA requiere enormes cantidades de datos y recursos computacionales, lo que genera un impacto energético considerable.

Frente a estos retos, es fundamental que las organizaciones desarrollen una estrategia clara y bien estructurada para implementar la IA de manera efectiva. No basta con tener acceso a tecnologías avanzadas; se necesita una visión estratégica que integre la IA como un motor de transformación, apoyada por un liderazgo fuerte que guíe a la empresa en este proceso. Una buena idea, por sí sola, no es suficiente. Si bien una planificación adecuada puede asegurar su correcta ejecución, es clave tener en cuenta que sin un ejercicio práctico sólido, las tecnologías pueden no alcanzar su máximo potencial.

El éxito en la adopción de la IA también depende en gran medida de superar el desconocimiento sobre las herramientas tecnológicas disponibles. Muchas organizaciones no están al tanto de las soluciones de IA que podrían aplicar a sus modelos de negocio, lo que las deja en desventaja. La falta de conocimiento, sumada a los costos de adopción de estas tecnologías, puede ser un impedimento para su implementación. Estos costos no solo incluyen el gasto en software y hardware, sino también la inversión en la formación y capacitación del capital humano.

La formación de capital humano es esencial para superar las barreras tecnológicas. No se trata solo de adquirir la tecnología, sino de asegurar que las personas dentro de la organización cuenten con las habilidades necesarias para utilizarla de manera eficiente y estratégica. La adquisición y retención de talento especializado en IA es un desafío cada vez mayor para las empresas, que deben competir en un mercado global por los profesionales más capacitados. Sin una fuerza laboral adecuada, la adopción de IA puede quedar relegada a esfuerzos marginales o insuficientes.

En este sentido, la claridad en la estrategia organizacional es primordial. Las empresas deben definir sus objetivos a largo plazo, alinear sus recursos y establecer una hoja de ruta clara para la integración de la IA en sus operaciones. La adopción eficiente de IA requiere superar las brechas tecnológicas, pero también implica tener una visión compartida por todos los niveles de la organización, desde la alta dirección hasta los operativos.

En resumen, la IA ofrece oportunidades sin precedentes para la transformación organizacional, siempre y cuando se aborden adecuadamente sus desafíos y se adopten prácticas responsables. Con una estrategia bien articulada y el liderazgo adecuado, las empresas pueden utilizar la IA no solo para predecir el futuro, sino también para generar nuevas formas de crear valor, optimizando procesos, reduciendo riesgos y mejorando la competitividad en un mercado global en constante evolución.

Andrés Aguilera

Doctor en Estudios Globales, especializado en Economía Política Internacional, Negocios y Gobernanza de la Universidad de Urbino (Italia). Magíster en comercio internacional de la Universidad de Corea (Seúl, Corea del Sur). Licenciado en Ciencias Políticas de la Universidad Nacional de Colombia.

andrés-aguilera-castillo-phd-b3ab7811

Apreciación de Seguridad Urbana

3+ SECURITY COLOMBIA

Documentos de ALTO VALOR con análisis y prospectiva elaborados por nuestra Unidad de Análisis Político y Seguridad Corporativa UAPSC, que puede

LEER COMPLETO AQUÍ

IMPLEMENTACIÓN DE LA TECNOLOGÍA EN LA CADENA DE VALOR

"Es importante hablar de cómo generamos valor al tema del servicio y las condiciones que hoy en día nos ponen el reto de cómo no repercutir en un sobrecosto o ir excediendo el tema de costo por las regulaciones que aplican... La tecnología sin duda nos brinda la posibilidad de cómo eficientar el proceso, automatizarlo, y de ahí tener un menor impacto en el tema de medidas"

"Hablando de tecnología, muchas veces se tiene la percepción de que sí quieres lo mejor, tiene que ser lo más costoso y los más caro. Hoy día sabemos que no necesariamente es así. Y la invitación es a los usuarios finales y a sus clientes, que busquen la oportunidad de acercarse a los fabricantes, porque efectivamente, no lo más caro es lo mejor"

La conferencia "Implementación de la tecnología en la cadena de valor" por Carlos Martínez, presidente del Comité México de la Asociación Latinoamericana de Seguridad (ALAS); Martín Otauza, representante de AJAX; y José Carlos González, director del Grupo GSI, habla de cómo la convergencia entre tecnología y el factor humano es crucial en la seguridad privada, donde la tecnología apoya y fortalece las operaciones diarias de la cadena de valor.

La adaptación de los recursos humanos a los avances tecnológicos es esencial. La integración de tecnología, como GPS y sistemas de monitoreo, ayuda a mitigar riesgos y optimizar procesos, lo cual es vital para el control y la prestación de servicios de seguridad, y además, genera un valor agregado.

Aunque las situaciones varían según el país, en Latinoamérica, las empresas enfrentan desafíos similares, como costos laborales crecientes y nuevas regulaciones que complican la situación financiera.

Carlos Martínez,
José Carlos González,
Martín Otauza.

Las nuevas legislaciones en países como México, que imponen mayores costos y limitaciones laborales, agravan los problemas financieros de las empresas. En respuesta, es necesario educar y concientizar desde las empresas sobre el uso de la tecnología y cómo esta puede ser una herramienta valiosa en la cadena de valor.

Los fabricantes de tecnología, como se discute en la conversación, buscan integrar soluciones tecnológicas con las prácticas existentes para mejorar la eficiencia sin sustituir completamente al factor humano. Además, la percepción de que la mejor tecnología debe ser la más costosa no siempre es cierta.

Las soluciones tecnológicas deben ser evaluadas en términos de retorno de inversión y beneficios para el negocio. La inteligencia artificial y la automatización de procesos están redefiniendo el papel de la tecnología en la seguridad, proporcionando herramientas que permiten un monitoreo más eficaz y una mejor gestión de los recursos.

Ejemplos como el uso de monitoreo remoto durante un desastre natural, como fue el caso del huracán en el Estado de Guerrero, México, muestran cómo la tecnología puede restablecer servicios cruciales de manera rápida y efectiva.

Al final del día, la tecnología es un motor para poder solventar diferentes necesidades. Permite identificar o prevenir anomalías por medio de inteligencia artificial, notificarlas y tomar acciones al momento. Hoy en día, se cuentan con distintos sistemas de seguridad electrónica de intrusión, incendios y prevención de inundaciones, y se está trabajando para la automatización.

Finalmente, el manejo adecuado de los datos y la ciberseguridad son fundamentales para proteger la información y garantizar el buen funcionamiento de los sistemas tecnológicos en el sector de seguridad privada. El monitoreo brinda información en tiempo real, pero lo importante y el factor diferencial, es qué se hace con ella.

PROSPECTIVA Y SEGURIDAD USANDO IA

por Julián Meneses

"Cuando alguien te dice que algo no se puede hacer, lo que realmente debería decirte es, yo no sé cómo hacerlo, que es bien diferente. Y ojo, porque el futuro es la predicción en tiempo real, no son los robots y las cámaras que desde el 2011, 12, 13 ya incluyen sistemas de reconocimiento."

La anticipación es un factor clave en el ámbito de la seguridad, ya que prever riesgos y actuar antes de que estos se materialicen puede ser la diferencia entre la prevención efectiva y la gestión de crisis. En un mundo que cambia constantemente y donde las amenazas evolucionan a una velocidad sin precedentes, la capacidad de anticiparse es más importante que nunca. En este contexto, la inteligencia artificial (IA) está desempeñando un papel fundamental, mucho más presente en nuestra vida diaria de lo que solemos imaginar. Aunque a menudo asociamos la IA con aplicaciones avanzadas o futuristas, lo cierto es que está integrada en una amplia gama de herramientas y sistemas que utilizamos a diario para mejorar la seguridad y reducir los riesgos.

Uno de los retos más grandes que enfrentan las organizaciones es que, a medida que las herramientas tecnológicas evolucionan, su funcionalidad tiende a tener una vida útil cada vez más corta. Esto se traduce en una necesidad constante de actualización y adaptación, lo que incrementa significativamente los costos y pone a prueba la eficiencia de los sistemas de seguridad tradicionales. En este sentido, el control de riesgos no puede enfocarse únicamente en lo que ya ha ocurrido, sino que debe tener como objetivo anticipar los posibles desafíos del futuro.

Si bien la proyección a futuro puede parecer útil en teoría, en la práctica su efectividad es limitada cuando se emplea para abordar problemas inmediatos. La IA, por otro lado, ofrece una ventaja significativa, ya que tiene el potencial de anticiparse a situaciones que aún no han sucedido, lo que proporciona una perspectiva más amplia y proactiva en la gestión de riesgos.

Uno de los ejemplos más claros de este poder de anticipación es la analítica predictiva, que utiliza modelos avanzados para analizar grandes volúmenes de datos, identificar patrones y hacer proyecciones. Sin embargo, su efectividad depende en gran medida de la calidad y cantidad de los datos disponibles. En algunos casos, la falta de datos o la inexactitud de los mismos puede limitar la capacidad de anticipación de estos sistemas.

Aun así, lo que realmente distingue a la IA es su capacidad para recalcular y adaptarse constantemente a medida que se incorporan nuevos datos, ajustando sus predicciones en tiempo real. Esto es crucial en un entorno donde los factores de riesgo pueden cambiar de un momento a otro, ya que una respuesta ágil es fundamental para garantizar la seguridad.

Además, el crecimiento continuo de nuevas herramientas tecnológicas, muchas de las cuales son accesibles de manera gratuita, ha democratizado el acceso a tecnologías avanzadas. Esto permite que tanto grandes empresas como pequeñas organizaciones puedan aprovechar el poder de la IA para mejorar sus estrategias de seguridad sin incurrir en costos desorbitados. No obstante, este rápido desarrollo de nuevas herramientas presenta un nuevo desafío: la gestión de enormes cantidades de información. Aquí es donde surge la limitación humana, ya que los individuos no están equipados para procesar y analizar tanta información a la velocidad requerida para tomar decisiones efectivas. Por ello, se requiere cada vez más el apoyo de sistemas de IA, que no solo sean generales en su aplicación, sino también específicos, capaces de adaptarse y responder a circunstancias particulares de manera eficiente y precisa.

En resumen, la inteligencia artificial no es solo una promesa de futuro, sino una realidad que está transformando la forma en que gestionamos la seguridad. Su capacidad para anticipar, analizar y ajustarse a escenarios en constante cambio la convierte en una herramienta indispensable en el mundo moderno, donde los riesgos evolucionan a un ritmo vertiginoso. La IA nos ofrece no solo la posibilidad de reaccionar rápidamente ante amenazas, sino también de adelantarnos a ellas, proporcionando un enfoque preventivo y proactivo que, en última instancia, refuerza la seguridad a nivel global.

Julián Meneses

CEO of Strategic Anticipation. Expert in Anticipatory analytics and Strategic surveillance – CEO de ANTICIPACIÓN ESTRATÉGICA. Experto en analítica anticipativa y vigilancia estratégica.

julianmeneses

5 pasos para afiliarse

1. Cree una cuenta
Para lo cual visite el siguiente enlace:
https://external.asisonline.org/eWeb//DynamicPage.aspx?WebCode=verify&Site=asis

2. Llene el formulario
Trate de ser BREVE PERO PRECISO, haga click en continuar, después del catpcha (verificar que no es un ROBOT). Complete la información a continuación para crear un perfil en línea.

3. Cree la contraseña (password)
Incluya entre 8 y 18 caracteres, y al menos un numero y continúe:

4. Hecho!!!
Se ha registrado.....

5. Cierre
Vuelva abrir su cuenta EN 8 DIAS, vaya a My Account Links/ My invoices, allí encontrará el monto a pagar . P

ASIS INTERNATIONAL® Bogotá Chapter

DEL ANÁLISIS AL ANTICIPO: CÓMO LA IA ESTÁ REVOLUCIONANDO LA GESTIÓN DE RIESGOS DE SEGURIDAD

Por: Percy Quispe MBA, ESRM

La seguridad empresarial enfrenta desafíos cada vez más complejos y dinámicos, que demandan una evolución continua en las estrategias de gestión de riesgos. Tradicionalmente, estas estrategias se han fundamentado en normas, estándares, guías y buenas prácticas adoptadas a nivel mundial. Estas herramientas aunque fundamentales, requieren de la intervención humana, donde los conocimientos y las experiencias de los especialistas en Gestión de Riesgos juegan un papel clave. Sin embargo, la irrupción IA está revolucionando este campo, ofreciendo herramientas que complementan y optimizan significativamente la identificación, evaluación y mitigación de riesgos. En el presente artículo exploraremos cómo la Inteligencia Artificial está impactando actualmente la Gestión de Riesgos de Seguridad y cómo podría transformarla en el futuro.

1. La IA en la Gestión de Riesgos de Seguridad: El Estado Actual

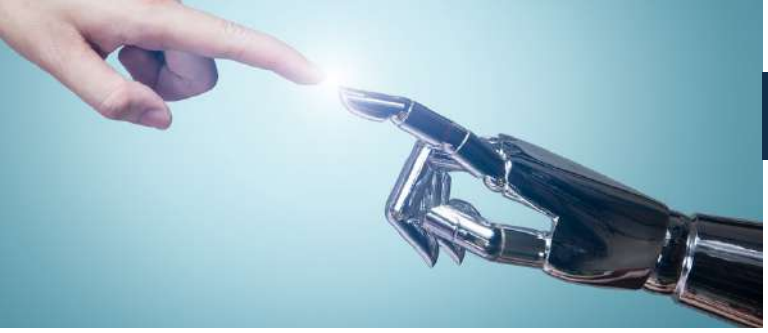
1.1. Modelos de Lenguaje de Gran Escala (LLMs)

Los Modelos de Lenguaje de Gran Tamaño (LLMs), como ChatGPT, son algoritmos de IA entrenados en grandes volúmenes de datos para poder generar textos coherentes y contextuales. Actualmente, estos modelos son utilizados para automatizar algunas tareas como la generación de informes de evaluación de riesgos, esto facilita la síntesis de grandes cantidades de información en sólo algunos reportes precisos e importantes en la toma de decisiones. Sin embargo, es fundamental que estos informes sean revisados y validados por expertos en gestión de riesgos para asegurar su precisión y relevancia.

1.2. Automatización en la Identificación de Riesgos

La integración de la IA con sistemas de monitoreo, como sistemas de alarma, cámaras de videovigilancia y controles de acceso, está revolucionando la identificación de amenazas en tiempo real. La tecnología permite la detección proactiva de anomalías o comportamientos sospechosos, lo que mejora significativamente la capacidad de respuesta ante incidentes y la protección de los activos críticos. Pero, aún la interpretación de estos datos y la toma de decisiones estratégicas siguen dependiendo del juicio experto de los profesionales en seguridad.

NOTA DEL EDITOR: *Se decidió incluir este artículo en esta newsletter debido a su pertinencia con el tema, a pesar de que no hizo parte de alguna ponencia del simposio.*



1.3. Evaluación Predictiva de Riesgos

Gracias a su capacidad para realizar análisis predictivos basados en datos históricos y tendencias actuales, la IA nos permite poder anticipar posibles escenarios de riesgo. Esto se traduce en una mejora en la planificación estratégica y en la toma de decisiones, ofreciendo una ventaja competitiva en un entorno de seguridad cada vez más desafiante. Sin embargo, la evaluación final y la implementación de medidas de mitigación requieren la experiencia de los especialistas, quienes deben interpretar los resultados y adaptarlos al contexto específico de su organización.

1.4. Automatización de la Respuesta a Incidentes

Las soluciones de IA están transformando la manera en que las organizaciones responden a incidentes de seguridad. Al activar automáticamente protocolos de contención o notificar a los equipos de emergencia de manera inmediata, la IA no solo minimiza el impacto de las amenazas en tiempo real, sino que también optimiza la eficiencia operativa y reduce los tiempos de respuesta. No obstante, la supervisión humana es crucial para ajustar las respuestas automatizadas y asegurar que se alineen con los objetivos y políticas de la organización.

1.5. Desafíos Actuales

A pesar de los avances, los modelos de IA no están libres de limitaciones. Pueden generar resultados inconsistentes o incorrectos, lo que representa un riesgo significativo en la gestión de seguridad. Además, debemos considerar como crucial que la implementación de IA cumpla estrictamente con las normativas de privacidad y seguridad de datos, como el Reglamento General de Protección de Datos (GDPR), esto para asegurar un manejo ético y legal de la información. La colaboración entre IA y expertos humanos es esencial para superar estas limitaciones y asegurar su efectividad.

2. El Futuro de la IA en la Gestión de Riesgos de Seguridad

2.1. Gestión de Riesgos Totalmente Automatizada

Con la continua evolución de la IA, es posible imaginar un futuro donde los sistemas de gestión de riesgos sean completamente automatizados. Estos sistemas no solo identificarían y evaluarían riesgos, sino que también implementarían y ajustarían controles en tiempo real, reduciendo significativamente la necesidad de intervención humana. Sin embargo, la supervisión y ajuste por parte de especialistas seguirá siendo vital para asegurar que las decisiones automatizadas sean precisas y adecuadas al contexto específico de cada organización.

2.2. Convergencia Tecnológica

La convergencia de la IA con tecnologías emergentes, como el Internet de las Cosas (IoT) y blockchain, ofrece la posibilidad de desarrollar soluciones de seguridad más robustas y efectivas. La combinación de estas tecnologías permitirá realizar una supervisión más precisa y una mayor integridad en los datos de seguridad, transformando radicalmente la forma en que las organizaciones gestionan sus riesgos. Aun así, el éxito de esta convergencia dependerá de la capacidad de los especialistas en gestión de riesgos para integrar y aplicar estas tecnologías de manera efectiva.

2.3. Desarrollo de Modelos con Razonamiento Mejorado

Los futuros modelos de IA incluirán capacidades de razonamiento avanzado, lo que permitirá a las organizaciones tomar decisiones más informadas y precisas en la gestión de riesgos. Esta evolución proporcionará un enfoque más sofisticado y adaptable, mejorando la eficacia en la evaluación y mitigación de los riesgos en un entorno empresarial en constante cambio. Sin embargo, es muy importante recalcar que el juicio y la experiencia humana seguirán siendo indispensables para interpretar y aplicar los resultados generados por la IA de manera efectiva.

2.4. Ética y Gobernanza

A medida que la IA se convierte en una herramienta fundamental en la gestión de riesgos de seguridad, emergen también nuevas preocupaciones éticas. Será esencial desarrollar marcos de gobernanza que regulen el uso de IA en la seguridad, asegurando que su implementación sea ética y transparente. Esto no solo protegerá a las organizaciones, sino que también garantizará la protección de los derechos y la privacidad de las personas. La intervención de expertos en ética y seguridad será crucial para establecer y mantener estos marcos de gobernanza en la organización.

3. Conclusiones

La inteligencia artificial está redefiniendo la gestión de riesgos de seguridad, proporcionando capacidades que hasta hace poco años eran inimaginables. Desde la automatización de la evaluación de riesgos hasta la predicción de amenazas, la IA está transformando la manera en que las organizaciones gestionan su seguridad. No obstante, todas estas oportunidades vienen acompañadas de grandes desafíos que deben abordarse con cuidado para asegurar un uso responsable y efectivo de estas tecnologías. El futuro de la IA en la gestión de riesgos de seguridad es prometedor, pero requiere una planificación meticulosa, una integración estratégica, y un compromiso constante con la ética, el cumpli miento normativo y la experiencia humana.

Referencias

- ISO 31000:2018 Risk management — Guidelines. International Organization for Standardization (ISO).
- Allen, B. J., & Loyear, R. (2017). Enterprise Security Risk Management: Concepts and Applications. ASIS International.
- Rossi, F., Brachman, R. J., & Reiter, R. (2020). Artificial Intelligence: A Modern Approach. Pearson.
- He, K., Zhang, X., Ren, S., & Sun, J. (2016). "Deep Residual Learning for Image Recognition." Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR).
- Brynjolfsson, E., & McAfee, A. (2014). The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. W. W. Norton & Company.
- Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.
- Shneiderman, B. (2020). Human-Centered AI. Oxford University Press.
- McKinsey & Company. (2024). "The Next Frontier: Unleashing the Economic Potential of Generative AI." McKinsey Global Institute.
- IBM Security. (2024). Cost of a Data Breach Report 2024. IBM.

Nota Final:

Este artículo tiene como objetivo ofrecer a los profesionales de seguridad una visión clara y práctica sobre cómo la inteligencia artificial (IA) está impactando y transformando la gestión de riesgos de seguridad. Las organizaciones alineándose a estándares, guías y mejores prácticas, ellas pueden estar mejor preparadas para enfrentar los desafíos del presente y del futuro, siempre con el respaldo de la tecnologá, conocimiento y la experiencia humana.

Percy Quispe

CEO and Founder - TECEM | ARVP ASIS International

percyquispe

ASIS 225 BOGOTÁ
EN LA FERIA DE SEGURIDAD ESS

SIMPOSIO XIV
INSTANTES DEL EVENTO

SIMPOSIO XIV
INSTANTES DEL EVENTO

SIMPOSIO XIV
INSTANTES DEL EVENTO

Síganos y comparta con sus contactos las publicaciones de **ASIS COLOMBIA,**

+57 310 477 0280

secretario@asiscolombia.org.co

www.asiscolombia.org.co

asis-colombia

asiscolombia

¡Unidos somos más fuertes!