Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria del Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 1 de julio de 2026 | Aceptación: 20 de julio de 2026 | Publicación: 16 de agosto de 2026

Inteligencia artificial aplicada a la detección de amenazas y a la respuesta ante incidentes cibernéticos.
Inteligencia artificial aplicada a la detección de amenazas y respuesta a incidentes cibernéticos.

Gabriel Lima

Resumen

Este estudio tiene como objetivo evaluar la efectividad y viabilidad de implementar técnicas de inteligencia artificial y aprendizaje automático en la detección de amenazas y la respuesta a incidentes cibernéticos, con el fin de optimizar la seguridad operativa y proteger la infraestructura crítica contra los ciberataques. La metodología adoptada incluye el análisis de sistemas avanzados de monitoreo de red, análisis del comportamiento del tráfico y algoritmos predictivos para identificar anomalías y vulnerabilidades. Los resultados demuestran que la automatización impulsada por IA reduce significativamente el tiempo promedio de detección y respuesta a incidentes, aunque persisten desafíos como la aparición de falsos positivos, la necesidad de entrenamiento continuo del modelo y los altos costos de implementación. Se concluye que la adopción sostenible de estas tecnologías requiere inversiones en capacitación técnica, gobernanza de datos y esfuerzos continuos de investigación y desarrollo.

Palabras clave: Inteligencia artificial. Ciberseguridad. Detección de amenazas. Respuesta a incidentes. Aprendizaje automático.

Abstracto

Este estudio tiene como objetivo evaluar la eficacia y viabilidad de implementar técnicas de inteligencia artificial y aprendizaje automático para la detección de amenazas y la respuesta a incidentes cibernéticos, con el fin de optimizar la seguridad operativa y proteger las infraestructuras críticas contra los ciberataques. La metodología adoptada incluye el análisis de sistemas avanzados de monitorización de redes, análisis del comportamiento del tráfico y algoritmos predictivos para la identificación de anomalías y vulnerabilidades. Los resultados muestran que la automatización basada en IA reduce significativamente el tiempo medio de detección y respuesta a incidentes, si bien persisten desafíos como los falsos positivos, la necesidad de un entrenamiento continuo del modelo y los elevados costes de implementación. Los hallazgos sugieren que la adopción sostenible de estas tecnologías requiere inversión en formación técnica, gobernanza de datos e investigación y desarrollo continuos.

Palabras clave: Inteligencia artificial. Ciberseguridad. Detección de amenazas. Respuesta a incidentes. Aprendizaje automático.

Resumen

Este estudio tiene como objetivo evaluar la efectividad y viabilidad de implementar técnicas de inteligencia artificial y aprendizaje automático en la detección de amenazas y la respuesta a incidentes cibernéticos, con el fin de optimizar la seguridad operativa y proteger las infraestructuras críticas contra ataques virtuales. La metodología adoptada incluye el análisis de sistemas avanzados de monitoreo de red, análisis del comportamiento del tráfico y algoritmos predictivos para la identificación de anomalías y vulnerabilidades. Los resultados demuestran que la automatización impulsada por inteligencia artificial reduce significativamente el tiempo promedio de detección y respuesta a incidentes, si bien persisten desafíos como la aparición de falsos positivos, la necesidad de entrenamiento continuo de los modelos y los altos costos de implementación. Se concluye que la adopción sostenible de estas tecnologías requiere inversiones en capacidad técnica, gobernanza de datos y un esfuerzo continuo en investigación y desarrollo.

Palabras clave: Inteligencia artificial. Ciberseguridad. Detección de amenazas. Respuesta a incidentes. Aprendizaje automático.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria del Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 1 de julio de 2026 | Aceptación: 20 de julio de 2026 | Publicación: 16 de agosto de 2026

1. Introducción

Este estudio tiene como objetivo analizar la aplicación de métodos avanzados de inteligencia artificial.
(IA) y aprendizaje automático en la detección y respuesta a amenazas
incidentes cibernéticos, con el objetivo de optimizar la seguridad operativa y mitigar los riesgos de
combatir los ciberataques y promover una gestión más eficiente de la protección de datos e infraestructuras.
tecnológico.

La gestión de seguridad propuesta en este estudio se basa en la integración de algoritmos de análisis.
Sensores de monitoreo de comportamiento y de red que operan continuamente. En caso
En caso de anomalías o intentos de intrusión, estos sistemas inteligentes envían señales en tiempo real a
centro de operaciones de seguridad (SOC), que permite la identificación, contención y
mitigar las amenazas.

Por lo tanto, este estudio tiene como objetivo responder a la siguiente pregunta: ¿cuál es la efectividad y la viabilidad de...?
implementación de métodos avanzados basados en inteligencia artificial para la detección de
Amenazas cibernéticas y respuesta a incidentes, con el objetivo de aumentar la resiliencia de las organizaciones.

¿Para protegerse contra los ciberataques?

El objetivo general es evaluar la eficacia y la viabilidad de implementar las técnicas.
Inteligencia artificial avanzada y aprendizaje automático en la automatización de
Monitoreo de red, detección temprana de amenazas y respuesta optimizada a
incidentes de ciberseguridad.

2. Marco teórico

2.1 Sistemas inteligentes en el contexto de la ciberseguridad

El conocimiento es fundamental para el desarrollo de la sociedad, que ha evolucionado desde

La economía agrícola está en transición hacia una economía industrial y ahora se encuentra en la era de la información, donde la información...

Se ha convertido en el activo más valioso y estratégico de las organizaciones. Este escenario influye.
un papel central en el avance de las fuerzas productivas, con éxito y resiliencia.
El éxito corporativo depende de cómo las entidades crean, gestionan y protegen sus...

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS - Revista Científica Multidisciplinaria del Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 1 de julio de 2026 | Aceptación: 20 de julio de 2026 | Publicación: 16 de agosto de 2026

conocimiento y datos frente a las crecientes amenazas digitales (Rezende, 2003).

Los cambios en la sociedad moderna son numerosos, y la mayoría están impulsados por...
El avance de las tecnologías de la información ha posibilitado el procesamiento de datos en tiempo real.
realidad, interconexión global y la eliminación de barreras geográficas. Sin embargo, esto
La hiperconectividad ha ampliado la superficie de ataque virtual, imponiendo a las organizaciones la
La necesidad de actualización y monitoreo constantes para garantizar la integridad de sus
ecosistemas digitales (Chaves Junior, 2021).

En esta transformación continua, se produce la transición del trabajo puramente físico al trabajo intelectual.
Ha establecido la información como la fuerza motriz de la economía contemporánea. En este entorno, la
Preservar la confidencialidad, la disponibilidad y la autenticidad de los datos se ha convertido en...
un requisito esencial tanto para la estabilidad económica de las empresas como para
Sostenibilidad operativa del mercado. Tecnologías de la información y la comunicación.
Al derribar las fronteras entre países, permitió nuevos modelos de negocio, pero también...
sistemas expuestos a amenazas cibernéticas transnacionales altamente sofisticadas (Rezende, 2003).

En la era del conocimiento, la adaptabilidad de una empresa y su infraestructura de ciberseguridad definen
su supervivencia en el mercado. A medida que la
La sofisticación de los ciberataques está acelerando la obsolescencia de las defensas tradicionales.
En entornos con normas rígidas, surge la necesidad de mecanismos capaces de analizar grandes volúmenes de datos.
Transmisión autónoma de datos en red. En este escenario, los avances en hardware y software
Permitieron la aplicación de Sistemas Inteligentes (SI), que utilizan técnicas
herramientas computacionales avanzadas para manipular conocimientos especializados e identificar
comportamiento malicioso.

Como lo destaca Rezende (2003), el comportamiento y los atributos de un sistema
Los sistemas inteligentes difieren sustancialmente de los sistemas informáticos convencionales.
Mientras que las herramientas tradicionales operan de manera reactiva y estática, los sistemas
Los sistemas inteligentes aplicados a la ciberseguridad son capaces de analizar patrones complejos.
para correlacionar eventos de red e inferir nuevos riesgos. Esta capacidad de manipular
Las representaciones dinámicas del mundo real permiten identificar y mitigar las anomalías.
incidentes cibernéticos con superioridad técnica y menor intervención humana (Rezende,
2003).

2.2 Inteligencia artificial y aprendizaje automático en ciberseguridad

El término "aprendizaje automático" surgió a finales del siglo XX y puede...

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
IRCMOS - Revista Científica Multidisciplinaria del Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 1 de julio de 2026 | Aceptación: 20 de julio de 2026 | Publicación: 16 de agosto de 2026

ser definido como la capacidad de un sistema para mejorar su rendimiento en una tarea por
a través de la experiencia y la identificación de patrones en grandes volúmenes de datos (Magalhães,
2015). En el campo de la seguridad de la información, esta tecnología emplea herramientas como:
redes neuronales artificiales y máquinas de vectores de soporte (SVM), que han demostrado ser altamente
eficaz en el procesamiento y análisis de datos complejos y ruidosos, una característica
distintivo de los paquetes de datos y los registros de tráfico de red (Ventura, 2012).

Además, el uso del procesamiento del lenguaje natural (PLN) permite que los sistemas
Analizar textos no estructurados, como informes de inteligencia sobre amenazas, registros de
Auditar y analizar correos electrónicos sospechosos, identificar patrones de ataque y vectores de ingeniería social,
lo que contribuye a aumentar la precisión en la detección de vulnerabilidades (Syam; Sharma,
2018). De esta forma, el aprendizaje automático se establece como una herramienta
indispensable para optimizar las operaciones de seguridad en entornos digitales dinámicos y
sujeto a cambios constantes en las amenazas (Magalhães, 2015).

Ferreira (2024) explica que un modelo de aprendizaje automático adquiere y utiliza
conocimiento cuando uno es capaz de utilizar información histórica para inferir nuevos conocimientos
resultados e identificar comportamientos sin precedentes. En el contexto cibernético, esto significa
Utilice el historial de tráfico y las solicitudes anteriores para identificar nuevos vectores de ataque.
previamente impredecibles. Por lo tanto, el aprendizaje automático se refiere al campo en el que...
Se desarrollaron y analizaron algoritmos, técnicas y herramientas que permiten esta capacidad.
protección adaptativa.

Metodológicamente, el aprendizaje automático aplicado a la ciberseguridad se clasifica en
diferentes enfoques:

- Aprendizaje no supervisado: agrupa datos de red sin etiquetado previo para
identificar anomalías, comportamientos fuera de lo común y nuevas variantes de ataques (cero-
día);
- Aprendizaje supervisado: utiliza datos previamente clasificados (como
tráfico benigno versus código malicioso) como ejemplos de entrenamiento para el modelo
Puede categorizar nuevas amenazas con gran precisión;
- Aprendizaje semisupervisado: combina datos etiquetados y no etiquetados para
Optimizar el entrenamiento del sistema, reduciendo el coste operativo del etiquetado de datos.
sin comprometer la capacidad predictiva (Syam; Sharma, 2018).

En términos de mitigación de riesgos, el aprendizaje automático desempeña un papel decisivo en...
para permitir la identificación temprana de anomalías en infraestructuras informáticas complejas,
tales como redes corporativas y servidores críticos, minimizando el tiempo de exposición a

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria del Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 1 de julio de 2026 | Aceptación: 20 de julio de 2026 | Publicación: 16 de agosto de 2026

exploraciones y reducción de posibles pérdidas financieras y operativas (Arbex, 2009). Por
A su vez, la inteligencia artificial (IA) surgió en la década de 1950 con el objetivo de desarrollar
sistemas capaces de realizar tareas que requieren capacidad cognitiva humana o que no la requieren
Poseían una solución algorítmica viable a través de la programación convencional (Skalfist,
Mikelsten, Teigens, 2020). Los investigadores en el campo utilizan teorías sobre el procesamiento de
información como base para desarrollar sistemas capaces de emular el razonamiento analítico en
seguimiento de datos (Aguiar, 2025).

Estos métodos pueden codificarse en programas que permitan a las máquinas aprender.
razonamiento y toma de decisiones defensivas autónomas (Ventura, 2012). La IA ha estado evolucionando.
influyendo continuamente en áreas como la automatización de la respuesta a incidentes,
Inteligencia contra amenazas y aprendizaje automático, convirtiéndose en un pilar estratégico de
ciberseguridad moderna (Magalhães, 2015).

Aguiar (2025) destaca que la IA se puede aplicar para optimizar la vigilancia y la protección.
Supervisión continua de los ecosistemas de TI, que permite el análisis en tiempo real de los eventos de seguridad.
Con la capacidad de predecir intrusiones y ejecutar bloqueos de acceso automáticos, no puede...
Con la autorización correspondiente, la inteligencia artificial aumenta sustancialmente la resistencia de las defensas digitales.
Mediante la detección directa de fallos e intrusiones, la IA analiza las anomalías en los datos.
Los problemas operativos identifican desviaciones de comportamiento en usuarios o sistemas, reduciendo
reducir drásticamente el tiempo de inactividad causado por ataques como el ransomware o
Falta de disponibilidad de servicios en sectores críticos (Borruso, 2019).

Borruso (2019) destaca que la aplicación de la IA en la gestión de la ciberseguridad ofrece
beneficios significativos, como el ahorro de tiempo en la clasificación de alertas y una disminución en...
Fatiga del analista y reducción del error humano. Al automatizar procesos complejos de
En la contención de incidentes, el sistema optimiza el rendimiento de los centros de operaciones de seguridad.
(SOC). Sin embargo, es crucial reconocer que la IA también presenta desafíos, entre ellos:
el riesgo de falsos positivos, sesgos en los modelos y la aparición de tácticas adversarias
Su objetivo es engañarse a sí mismos. Estos desafíos deben gestionarse de forma continua.
para garantizar que la automatización aporte fiabilidad operativa sin introducir nuevos
vulnerabilidades (Córdova, 2025). Por lo tanto, la integración de algoritmos inteligentes en defensa
La cibernética transforma radicalmente la gobernanza de la información, siempre que vaya acompañada de
Supervisión humana especializada y mejora continua.

2 Metodología

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS - Revista Científica Multidisciplinaria del Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 1 de julio de 2026 | Aceptación: 20 de julio de 2026 | Publicación: 16 de agosto de 2026

Este estudio adoptó un enfoque metodológico cualitativo y exploratorio, basado en una revisión bibliográfica integradora para analizar la aplicación de técnicas avanzadas de Inteligencia artificial y aprendizaje automático en la detección y respuesta ante amenazas. Incidentes cibernéticos.

La búsqueda de referencias teóricas y empíricas se realizó en las bases de datos académicas de Se utilizaron bases de datos de alto impacto como IEEE Xplore, Scopus, Web of Science y Google Scholar . descriptores combinados en portugués e inglés, como por ejemplo: "inteligencia artificial en ciberseguridad" (inteligencia artificial en ciberseguridad), " detección de amenazas " detección), "respuesta a incidentes cibernéticos" , "aprendizaje" " Detección de intrusiones mediante aprendizaje automático" y "automatización en SOC" (automatización del centro de operaciones de seguridad). Además, se examinaron artículos. datos relevantes identificados a través de la técnica de muestreo de bola de nieve , mediante el análisis de las referencias de las obras seleccionadas.

Los criterios de inclusión definidos fueron los siguientes:

• Artículos científicos completos y capítulos de libros publicados en revistas indexadas;

• Estudios que abordaron directamente la efectividad, los desafíos operativos y la viabilidad de Implementación de algoritmos de inteligencia artificial y aprendizaje automático en seguridad información;

• Trabajo enfocado en detectar anomalías de red, mitigar amenazas conocidas y Amenazas desconocidas (de día cero) y automatización de la respuesta ante incidentes cibernéticos.

Se excluyeron los estudios con un enfoque puramente teórico y sin aplicabilidad práctica a la seguridad. proyectos relacionados con la automatización computacional o industrial que no tuvieran relación con la ciberseguridad.

Después de seleccionar el corpus bibliográfico, se realizó un análisis categórico para mapear el principales tecnologías, algoritmos y arquitecturas computacionales aplicadas. Para lograr el En vista de los objetivos específicos propuestos, se adoptaron los siguientes procedimientos analíticos:

• Mapeo de tecnologías de IA: Identificación y categorización de las principales tecnologías. Arquitecturas de inteligencia artificial y aprendizaje automático (supervisadas y no supervisadas) Procesamiento supervisado y del lenguaje natural aplicado a la monitorización del tráfico. Análisis de red y de registros en tiempo real;

• Evaluación de la eficacia en la detección de amenazas: Investigación del rendimiento de estos herramientas para la detección temprana de intrusiones, análisis de comportamiento de anomalías, prevención de ataques complejos (como ransomware y filtraciones de datos) y reducción de Tiempo medio de detección (MTTD);

• Análisis de respuesta e integración operativa: Evaluación de la viabilidad de la integración.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
IRCMOS – Revista Científica Multidisciplinaria del Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 1 de julio de 2026 | Aceptación: 20 de julio de 2026 | Publicación: 16 de agosto de 2026

Estas soluciones contribuyen a los ecosistemas de automatización de la seguridad, como las herramientas de seguridad . Orquestación, automatización y respuesta (SOAR) y centros de operaciones de seguridad (SOC), con el objetivo de optimizar la mitigación de incidentes y reducir el tiempo medio de respuesta. (MTTR).

3. Resultados y discusión

Los estudios analizados se centran en la aplicación de la inteligencia artificial (IA) y el aprendizaje automático. El aprendizaje automático en ciberseguridad muestra un progreso significativo en la identificación amenazas, en la mitigación de riesgos y en la optimización del rendimiento operativo de los centros de seguridad. Información (Centros de Operaciones de Seguridad — SOC). La literatura relacionada demuestra que la La transición de los métodos reactivos tradicionales a los ecosistemas predictivos basados en IA altera... Fundamentalmente, la dinámica de la ciberdefensa.

Los estudios centrados en la monitorización continua del tráfico de red revelan que la implementación El uso de algoritmos de aprendizaje no supervisado permite la creación de perfiles de comportamiento. Dinámico para dispositivos y usuarios. Este enfoque ha demostrado ser altamente eficaz en la detección. de anomalías sutiles e intrusiones de día cero (amenazas sin una firma conocida), Superar las limitaciones de los sistemas de detección basados estrictamente en reglas. Los resultados indican que el análisis predictivo en tiempo real reduce drásticamente el tiempo promedio de detección (Tiempo medio de detección — MTTD), identificación de fugas de datos y movimientos laterales maliciosos en las etapas iniciales del ataque.

En el contexto de la automatización de la respuesta a incidentes cibernéticos, la investigación destaca el impacto la integración entre modelos de inteligencia artificial y plataformas de orquestación y respuesta Orquestación, automatización y respuesta de seguridad (SOAR). La aplicación de Los algoritmos inteligentes en el análisis inicial de las alertas permiten la ejecución autónoma de los flujos de trabajo. medidas de contención, como el aislamiento inmediato de las máquinas comprometidas, el confinamiento Detección automática de direcciones IP sospechosas y revocación proactiva de las credenciales de acceso. Es evidente que automatizar las respuestas sencillas reduce significativamente el tiempo medio de respuesta. Tiempo medio de respuesta (MTTR), además de aliviar la presión sobre el tiempo de respuesta de los analistas. seguridad y reducción de la fatiga causada por alertas excesivas.

Además, los hallazgos de la literatura abordan la viabilidad operativa y los desafíos. Ventajas económicas inherentes a la adopción de estas tecnologías inteligentes:

• Eficacia predictiva: El uso del procesamiento del lenguaje natural (PLN) combinado con Los modelos predictivos para el análisis de inteligencia sobre amenazas permiten...

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria del Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 1 de julio de 2026 | Aceptación: 20 de julio de 2026 | Publicación: 16 de agosto de 2026

anticipación de vectores de ataque complejos, como campañas de phishing sofisticadas y
infecciones de ransomware ;

• Reducción de costos de impacto: Si bien la inversión inicial en infraestructura
Si bien los costos computacionales, las licencias de software y la capacitación especializada pueden ser altos, el análisis de
La viabilidad económica genera un retorno positivo, ya que evita la escasez de existencias.
Las soluciones sistémicas previenen pérdidas financieras astronómicas derivadas de filtraciones de datos y multas.
regulador;

• Desafíos operativos: La literatura señala limitaciones persistentes que requieren gobernanza.
riguroso, con énfasis en la tasa de falsos positivos, el riesgo de envenenamiento de datos de
entrenamiento (envenenamiento de datos) y tácticas de evasión empleadas por los ciberdelincuentes contra
modelos de inteligencia artificial propios.

La síntesis de los resultados confirma que la integración de métodos avanzados de IA y aprendizaje automático...
El uso de máquinas en la respuesta a incidentes cibernéticos no solo aumenta la resiliencia y...
fiabilidad de los ecosistemas de TI, pero también se presenta como una estrategia.
Sostenible y económicamente viable para la protección a largo plazo de activos digitales críticos.

Consideraciones finales

El objetivo general de este estudio fue evaluar la efectividad y la viabilidad de la implementación
Técnicas de inteligencia artificial (IA) y aprendizaje automático en la detección de amenazas y en
Respuesta a incidentes cibernéticos, con enfoque en la optimización de la seguridad operativa y la mitigación.
Para mitigar los riesgos de los ciberataques y promover una gestión eficaz de la protección de datos.
Con este objetivo en mente, los objetivos específicos guiaron la revisión de la literatura y sirvieron de base para...
conclusiones presentadas.

La investigación sobre las tecnologías disponibles para la monitorización en tiempo real ha demostrado
La aplicación de la IA y el aprendizaje automático es ampliamente reconocida por su impacto.
positivo en la detección temprana de intrusiones y la automatización de la defensa de la red. Sin embargo, el
El estudio también indicó que la eficacia de estas herramientas depende directamente de su calidad.
de los datos de entrenamiento y la gobernanza sobre los modelos computacionales, lo cual es crucial
La gestión precisa de registros y eventos es esencial para optimizar el aprendizaje de los algoritmos y prevenir errores.
sesgos operacionales.

Al evaluar la detección temprana de amenazas y la prevención de incidentes complejos (como
(En relación con el ransomware y las filtraciones de datos), se ha hecho evidente que el análisis predictivo del comportamiento es fundamental.
Supera las limitaciones de los enfoques tradicionales basados únicamente en firmas estáticas.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 1 de julio de 2026 | Aceptación: 20 de julio de 2026 | Publicación: 16 de agosto de 2026

Sin embargo, se observó que la aparición de falsos positivos y la sofisticación de las técnicas de
Las tácticas evasivas empleadas por los ciberdelincuentes siguen presentando desafíos técnicos que requieren...
mantener la supervisión humana especializada en los centros de operaciones de seguridad.
(SOC).

En cuanto a la viabilidad económica y operativa, el estudio evaluó el equilibrio entre
Inversiones y beneficios de la automatización en ciberseguridad. Aunque adquisición e integración
y el mantenimiento de herramientas inteligentes presentan altos costos iniciales, el análisis
Esto demuestra que esta inversión se ve compensada en gran medida por la reducción del tiempo promedio.
tiempo de respuesta al tratamiento (MTTR) y la prevención de pérdidas financieras devastadoras resultantes de
Fugas de datos, fallos del sistema y sanciones regulatorias.

Por lo tanto, este estudio reafirma la importancia crucial de la inteligencia artificial para fortalecer
de la ciberseguridad moderna. Sin embargo, destaca la necesidad de superar desafíos como
Reducir los falsos positivos, mitigar los riesgos de envenenamiento de datos y la necesidad
formación técnica continua. Para maximizar los beneficios observados, es esencial mantener
Esfuerzos constantes en investigación y desarrollo, asegurando que las soluciones de
La inteligencia artificial evoluciona al mismo ritmo que las ciberamenazas.

Referencias

AGUIAR, David. Uso de inteligencia artificial para la detección proactiva de amenazas cibernéticas en entornos corporativos. Aurum, págs. 57-67, 2025.

CHAVES JUNIOR, Wankes Solony de Carvalho. Ingeniería de materiales dentro del ámbito de Industria
4.0. RCMOS-Revista Científica Multidisciplinaria El Conocimiento, vol. 1, n.º 6, págs. 1-9, 2021.

CÓRDOVA, Paulo Roberto. Inteligencia artificial: entre la fascinación y el miedo. Contexto, 2025.

FERREIRA, Pauliana N. Aprendizaje automático. Senac São Paulo, 2024.

MAGALHÃES, Renato Vasconcelos. Inteligencia artificial y derecho: una breve introducción. Histórico. Revista de Derecho y Libertad, ESMARN, Mossoró, vol. 1, n.º 1, págs. 355–370, jul./dic. 2015. ISSN impreso 1809-3280 | ISSN electrónico 2177-1758.

REZENDE et al. Sistemas inteligentes: fundamentos y aplicaciones. Barueri, SP: Manole. 2003.

SYAM, Niladri; SHARMA, Arun. A la espera de un renacimiento de las ventas en el cuarto sector industrial. Revolución: El aprendizaje automático y la inteligencia artificial en la investigación y la práctica de ventas. Gestión de Marketing Industrial, vol. 69, págs. 135-146, 2018.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS - Revista Científica Multidisciplinaria del Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 1 de julio de 2026 | Aceptación: 20 de julio de 2026 | Publicación: 16 de agosto de 2026

SKALFIST, P., MIKELSTEN, D., TEIGENS, V. Inteligencia artificial: La cuarta revolución industrial. Cambridge Stanford Books. 2020.

VENTURA, RV et al. Uso de redes neuronales artificiales en la predicción de valores genéticos para Peso a los 205 días en ganado de raza Tabapuã. Arq. Bras. Med. Vet. Zootec., v.64, n.2, p.411–418, 2012.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.