Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), septiembre-octubre 2024,
Volumen 8, Número 5.

https://doi.org/10.37811/cl_rcm.v8i5

LA INTELIGENCIA ARTIFICIAL EN LA PREVENCIÓN DEL DELITO INFORMÁTICO PARA LAS PYMES DEL SECTOR DE POMASQUI

ARTIFICIAL INTELLIGENCE IN THE PREVENTION OF COMPUTER CRIME FOR PYMES IN THE POMASQUI SECTOR

Jaime Vladimir Sancho Zurita
Instituto Tectológico Universitario Japón, Ecuador

Anthony Danilo Espinoza Altamirano
Investigador Independiente, Estados Unidos

Graciela Elizabeth Trujillo Moreno
Instituto Tectológico Universitario Japón, Ecuador

DOI: https://doi.org/10.37811/cl_rcm.v8i5.13863

La Inteligencia Artificial en la Prevención del Delito Informático para las Pymes del Sector de Pomasqui

Jaime Vladimir Sancho Zurita[1]
jsancho@itsjapon.edu.ec
https://orcid.org/0000-0002-5915-2100
Instituto Tecnológico Universitario Japón
Ecuador

Anthony Danilo Espinoza Altamirano
engtony2022@gmail.com
https://orcid.org/0009-0008-0855-010X
Investigador Independiente
Estados Unidos

Graciela Elizabeth Trujillo Moreno
gtrujillo@itsjapon.edu.ec
https://orcid.org/0009-0000-3802-9210
Instituto Tecnológico Universitario Japón
Ecuador

RESUMEN

La creciente amenaza del delito informático ha llevado a un aumento en la adopción de tecnologías de inteligencia artificial (IA) en empresas de todos los tamaños, incluidas las pequeñas y medianas empresas (PYMES). Este informe se centra en el papel de la IA en la prevención del delito informático para las PYMES del sector de Pomasqui, destacando su importancia, justificación y planteamiento del problema. La IA desempeña un papel crucial en la detección de amenazas, el análisis de seguridad, la prevención de fraudes y la autenticación avanzada, pero su implementación efectiva requiere una combinación de tecnología avanzada y una cultura de seguridad sólida dentro de la organización. El estudio se basa en una encuesta realizada a empresas de Pomasqui para evaluar el estado actual de la ciberseguridad, identificando áreas de mejora y necesidades. Se observa una falta de conciencia sobre la importancia de la ciberseguridad y la IA, así como una baja inversión en medidas de seguridad cibernética. Sin embargo, existe un optimismo generalizado sobre el futuro de la tecnología en la prevención del delito informático. Este informe destaca la necesidad de concienciar, invertir en tecnología y capacitación, y adoptar medidas de seguridad más avanzadas para proteger las PYMES contra las crecientes amenazas cibernéticas.

Palabras clave: delito informático, inteligencia artificial, prevención, tecnología

[1] Autor principal.
Correspondencia: jsancho@itsjapon.edu.ec

Artificial Intelligence in the Prevention of Computer Crime for Pymes in the Pomasqui Sector

ABSTRACT

The growing threat of cybercrime has led to an increase in the adoption of artificial intelligence (AI) technologies in businesses of all sizes, including small and medium-sized businesses (SMEs). This report focuses on the role of AI in the prevention of cybercrime for SMEs in the Pomasqui sector, highlighting its importance, justification and approach to the problem. AI plays a crucial role in threat detection, security analysis, fraud prevention and advanced authentication, but its effective implementation requires a combination of advanced technology and a strong security culture within the organization. The study is based on a survey carried out among Pomasqui companies to evaluate the current state of cybersecurity, identifying areas of improvement and needs. There is a lack of awareness about the importance of cybersecurity and AI, as well as low investment in cybersecurity measures. However, there is widespread optimism about the future of technology in cybercrime prevention. This report highlights the need to raise awareness, invest in technology and training, and adopt more advanced security measures to protect SMEs against growing cyber threats.

Keywords: computer crime, artificial intelligence, prevention, technology

Artículo recibido 08 agosto 2024
Aceptado para publicación: 10 setiembre 2024

INTRODUCCIÓN

La Inteligencia Artificial (IA) es crucial para que las PYMES prevengan el delito informático, abarcando actividades como el robo de datos y ataques cibernéticos. La IA detecta amenazas analizando grandes volúmenes de datos en tiempo real, identifica comportamientos anómalos y actividades maliciosas, y evalúa la seguridad de los sistemas, encontrando vulnerabilidades y sugiriendo mejoras. Además, ayuda a prevenir fraudes al analizar patrones de comportamiento y transacciones, detectando actividades sospechosas y accesos no autorizados. Los sistemas de autenticación avanzados, como técnicas biométricas y análisis de comportamiento, fortalecen la seguridad. Implementar IA eficazmente requiere tecnología avanzada, capacitación del personal, una cultura de seguridad y cumplimiento con regulaciones de privacidad y protección de datos.

Objetivos del estudio

Estimar la tecnología electrónica que utiliza Inteligencia Artificial, para la prevención del Delito Informático en las Pymes

Investigar y analizar el estado actual de la seguridad informática en las Pymes del sector de Pomasqui, identificando las amenazas y vulnerabilidades más comunes.

Estimar el alcance que cubren los dispositivos utilizados

La transformación digital empresarial se ha convertido en una prioridad esencial, especialmente en el contexto de la pandemia de COVID-19. Esta urgencia ha llevado a las empresas a adoptar nuevas tecnologías y a fortalecer sus medidas de seguridad en línea. La capacitación del personal y la implementación de estrategias de ciberseguridad son fundamentales para proteger los datos sensibles y mantener la confianza de los clientes. La digitalización y la seguridad cibernética son aspectos interdependientes que requieren atención constante y actualizaciones periódicas. Adaptarse efectivamente a este nuevo entorno digital es crucial para mantener la competitividad en el mercado actual. (Bueno, G. 2022).

La introducción de la inteligencia artificial (IA) en la seguridad de las ciudades ha generado debate, ya que algunos la ven como una forma efectiva de combatir el crimen mediante cámaras de vigilancia y monitoreo de personas y vehículos, mientras que otros creen que esto podría violar derechos como la privacidad y la no discriminación. Las preocupaciones sobre la privacidad se centran en la recolección

masiva de datos personales y su posible mal uso, mientras que también se plantea la preocupación por el sesgo y la discriminación al usar algoritmos de IA. Es esencial abordar estas inquietudes mediante la implementación de regulaciones sólidas, transparencia en el uso de la tecnología y debates públicos sobre sus implicaciones éticas y legales. (Guillermo, J., Quispe, J. 2022).

Las pequeñas y medianas empresas (pymes) sin infraestructuras de seguridad adecuadas o con malas prácticas están expuestas a riesgos como phishing, malware y ataques de denegación de servicio. Los ciber delincuentes utilizan herramientas como kits de exploit y botnets para llevar a cabo sus ataques, lo que puede resultar en la pérdida de datos sensibles y la interrupción del negocio. Para mitigar estos riesgos, es fundamental implementar medidas de seguridad cibernética, como la capacitación de empleados, la actualización de sistemas y la realización de copias de seguridad regulares. (Carvajal O. 2022) La necesidad de digitalizar las empresas se ha vuelto crucial en el mundo actual, especialmente después del COVID-19. Según (Bueno y Haz 2022), la pandemia ha resaltado la importancia de tecnificar las operaciones empresariales para implementar estrategias sólidas de ciberseguridad. Esta evolución ha motivado a las empresas a implementar medidas más avanzadas para salvaguardar sus activos digitales y datos confidenciales.

(Smith y Johnson 2019) destacan que la relevancia de la inteligencia artificial (IA) está en constante aumento en el ámbito de la seguridad empresarial. Su investigación subraya que las utilidades de la IA en este campo abarcan desde la detección de amenazas hasta el análisis de riesgos y la autenticación avanzada. Estas innovaciones tecnológicas capacitan a las empresas para identificar y abordar de manera ágil posibles riesgos de seguridad, fortaleciendo así su capacidad defensiva frente a los ataques cibernéticos.

El uso de inteligencia artificial en el ámbito de la seguridad empresarial presenta cuestiones éticas de gran relevancia. En su estudio, (García y Rodríguez 2021) analizan las repercusiones éticas que esto conlleva, abordando aspectos como la preservación de la privacidad de los datos, la posibilidad de discriminación algorítmica y las implicaciones legales correspondientes. Es esencial que las empresas adopten prácticas éticas tanto en el desarrollo como en la implementación de sistemas de inteligencia artificial, con el objetivo de garantizar la protección de los derechos individuales y promover la equidad en su aplicación.

Las proyecciones sobre seguridad empresarial señalan un crecimiento constante en la integración de tecnologías avanzadas. Según (Chen y Wang 2023), se anticipa un incremento en la aplicación de inteligencia artificial, aprendizaje automático y análisis de datos con el fin de anticipar amenazas y reducir riesgos. No obstante, estos avances también presentan desafíos adicionales, como la demanda de formación especializada y la gestión de riesgos vinculados a la dependencia de tecnologías sofisticadas.

La adopción de tecnologías digitales por parte de las empresas ha generado nuevas formas de seguridad empresarial gracias a innovaciones tecnológicas. Un análisis reciente llevado a cabo por (Jackson y Smith, 2023) examina las tendencias más recientes en sistemas de seguridad empresarial que emplean inteligencia artificial. El estudio resalta el impacto de estas innovaciones en la protección de los activos digitales de las empresas y en su capacidad para enfrentar las constantes amenazas cibernéticas en evolución.

La implementación de estrategias avanzadas de ciberseguridad se ha convertido en un elemento indispensable para la competitividad de las empresas. De acuerdo con un estudio realizado por (Lee y Kim en 2022), aquellas empresas que dedican recursos a tecnologías de seguridad cibernética, como sistemas de detección de intrusiones basados en inteligencia artificial y análisis avanzados de comportamiento, pueden lograr una ventaja competitiva considerable al salvaguardar la integridad de su información confidencial y preservar la confianza de sus clientes.

La introducción de la inteligencia artificial en la protección empresarial también presenta significativos dilemas éticos. Un análisis realizado por (Pérez y González 2021) explora los dilemas éticos asociados con el uso de la IA en la toma de decisiones sobre seguridad informática. El documento enfatiza la importancia de establecer sólidos marcos éticos para asegurar que las decisiones automatizadas sean imparciales, transparentes y equitativas.

La correcta preparación y adiestramiento en ciberseguridad son esenciales para asegurar una aplicación eficaz de estrategias de protección en el entorno empresarial. Según un artículo de (Martínez y Pérez, 2023), se destaca la importancia de establecer programas de entrenamiento integrales que doten a los trabajadores de las competencias necesarias para detectar y contrarrestar los riesgos de seguridad en

línea. Asimismo, se examinan las tácticas más efectivas para fomentar una cultura de seguridad informática dentro del ámbito laboral.

El presente trabajo está basado en un estudio realizado en Pomasqui, en vista de la proliferación de la delincuencia a nivel de las pequeñas empresas de la localidad, además el auge de la Inteligencia artificial, los delitos Informáticos que es una amenaza global

METODOLOGÍA

Área de estudio

Pomasqui cuenta con una población de 28910 habitantes,

Ubicación

Límites

Norte: Parroquia San Antonio de Pichincha

Sur: Al Sur se encuentra las parroquias de Cotocollao y de Carcelén

Este: Parroquia de Calderón

Oeste: Al Oeste tenemos las parroquias de Cotocollao y Calacalí

Diseño de Investigación

El diseño de la investigación será mixto, combinando elementos cuantitativos y cualitativos para obtener una comprensión holística de la seguridad cibernética en las PYMES del sector de Pomasqui. Se utilizará un enfoque de encuesta para recopilar datos cuantitativos y entrevistas semiestructuradas para obtener datos cualitativos en profundidad.

Población y Muestra

La población objetivo: PYMES ubicadas en el sector de Pomasqui. Dado el alcance limitado de tiempo y recursos, se seleccionará una muestra representativa de PYMES de la población total. Se utilizará un muestreo aleatorio simple para garantizar la representatividad de la muestra.

Instrumentos de Recolección de Datos

Para la recopilación de datos cuantitativos, se utilizaron cuestionarios estructurados que incluyen preguntas cerradas sobre temas como el uso de tecnologías de seguridad cibernética, el presupuesto asignado a la ciberseguridad y la percepción de la efectividad de estas medidas.

Para la recopilación de datos cualitativos, se llevaron a cabo entrevistas semiestructuradas con propietarios de PYMES y profesionales de seguridad cibernética en la región. Las entrevistas se centrarán en explorar en profundidad las percepciones, experiencias y desafíos específicos relacionados con la seguridad cibernética en las PYMES de Pomasqui.

Análisis de Datos

Los datos cuantitativos se analizaron mediante técnicas estadísticas descriptivas, como análisis de frecuencias y análisis de tendencias. Esto permite identificar patrones y tendencias en el uso de tecnologías de seguridad cibernética en las PYMES de Pomasqui.

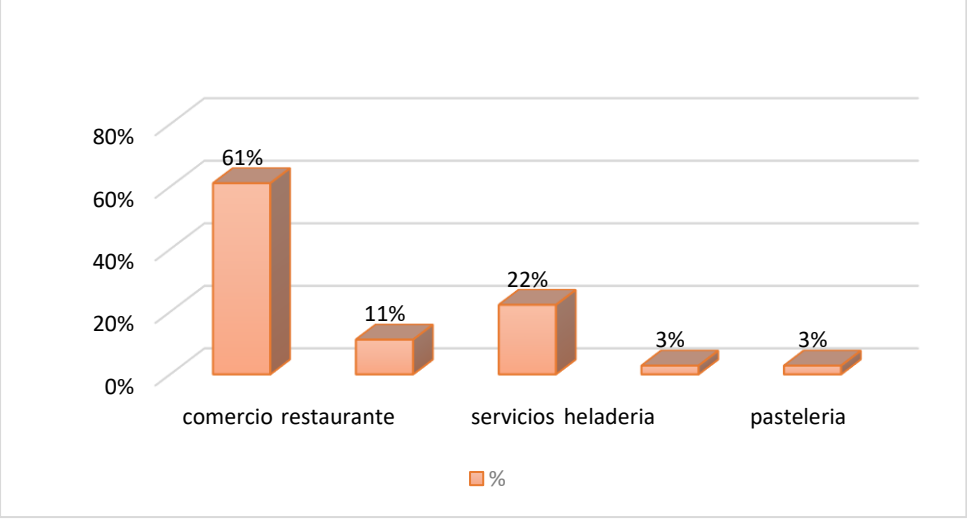
RESULTADOS Y DISCUSIÓN

Tabla1: Sector de las empresas en Pomasqui

Respuestas	Frecuencia	%
comercio	22	61%
restaurante	4	11%
servicios	8	22%
heladería	1	3%
pastelería	1	3%
TOTAL	36	100%

Fuente: Propia

Figura1: Sector de las empresas en Pomasqui



Fuente: Propia

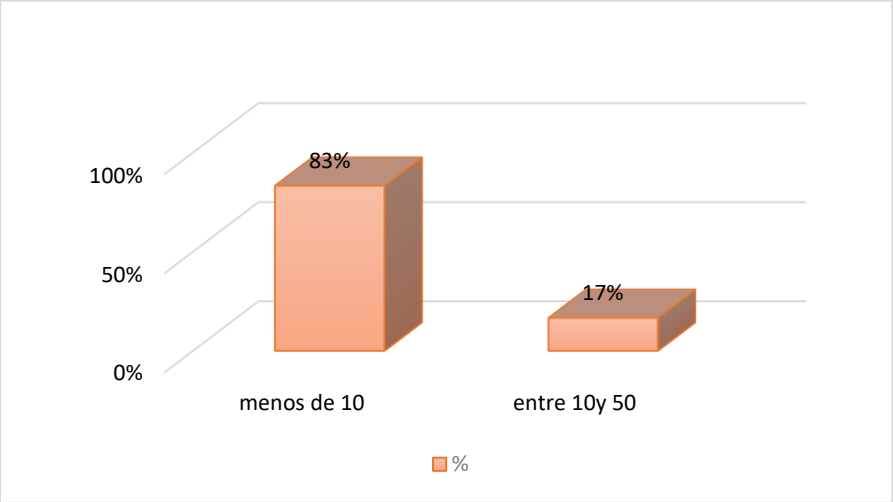
Esta pregunta muestra la distribución de las empresas encuestadas por sector. El gráfico muestra que el comercio es el sector predominante, seguido por servicios y restaurantes.

Tabla2: Número de empleados en las empresas de Pomasqui

Respuesta	Frecuencia	%
menos de 10	30	83%
entre 10y 50	6	17%
TOTAL	36	100%

Fuente: Propia

Figura2: Número de empleados en las empresas de Pomasqui



Fuente: Propia

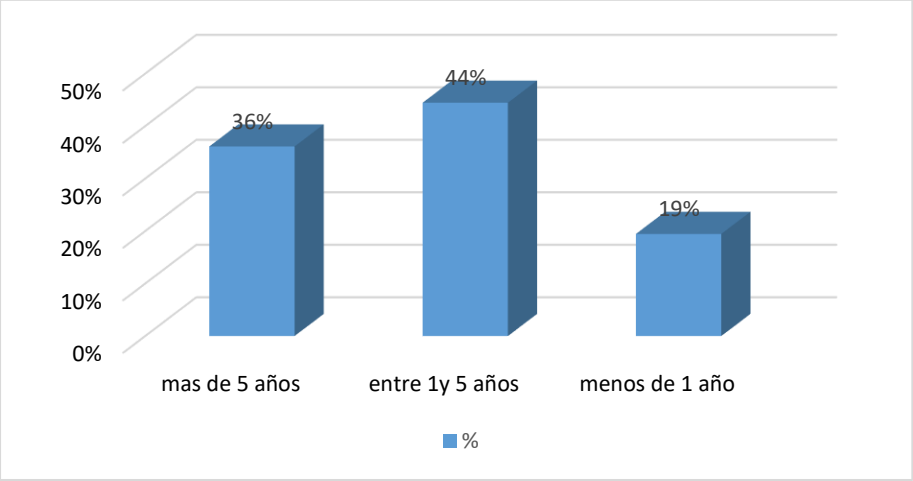
Este análisis revela el tamaño de las empresas encuestadas en términos de su fuerza laboral. La mayoría de las empresas tienen menos de 10 empleados.

Tabla3: Años de operación en Pomasqui

Respuesta	Frecuencia	%
más de 5 años	13	36%
entre 1y 5 años	16	44%
menos de 1 año	7	19%
TOTAL	36	100%

Fuente: Propia

Figura3: Años de operación en Pomasqui



Fuente: Propia

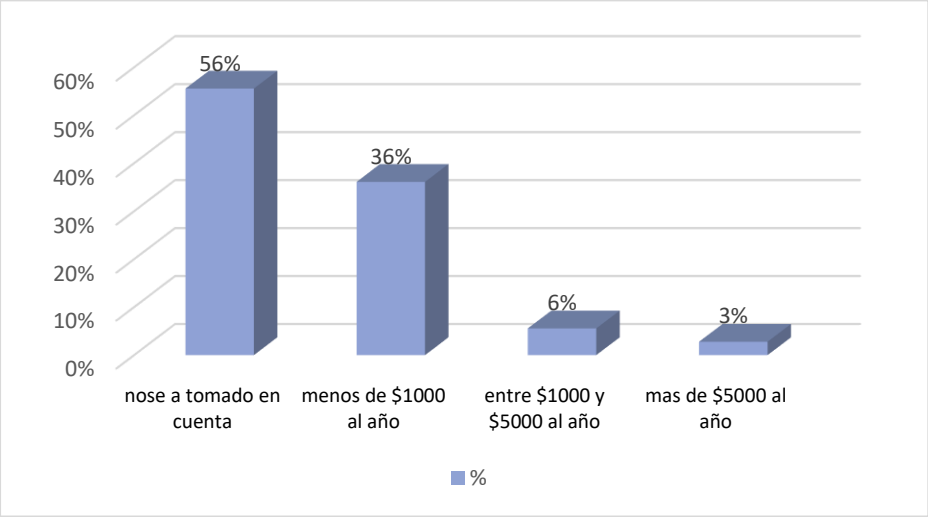
Esta pregunta muestra la antigüedad de las empresas encuestadas en Pomasqui. La mayoría de las empresas han estado operando entre 1 y 5 años en la zona.

Tabla4: Presupuesto de ciberseguridad en las empresas

Respuesta	Frecuencia	%
No se ha tomado en cuenta	20	56%
menos de $1000 al año	13	36%
entre $1000 y $5000 al año	2	6%
más de $5000 al año	1	3%
TOTAL	36	100%

Fuente: Propia

Figura4: Presupuesto de ciberseguridad en las empresas



Fuente: Propia

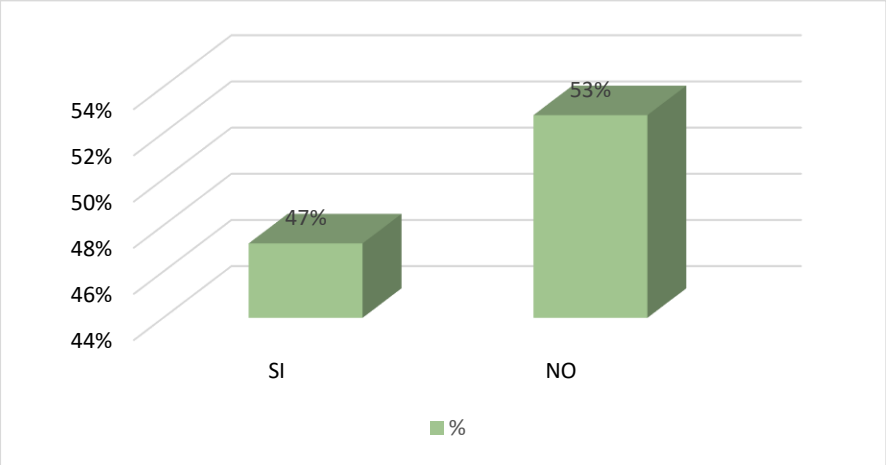
Revela la inversión de las empresas en medidas de ciberseguridad. La mayoría de las empresas encuestadas no han considerado un presupuesto específico para ciberseguridad.

Tabla5: Utilización de sistemas o herramientas de Inteligencia Artificial para prevenir el Delito Informático

Respuesta	Frecuencia	%
SI	17	47%
No	19	53%
Total	36	100%

Fuente: Propia

Figura5: Utilización de sistemas o herramientas de Inteligencia Artificial para prevenir el Delito Informático



Fuente: Propia

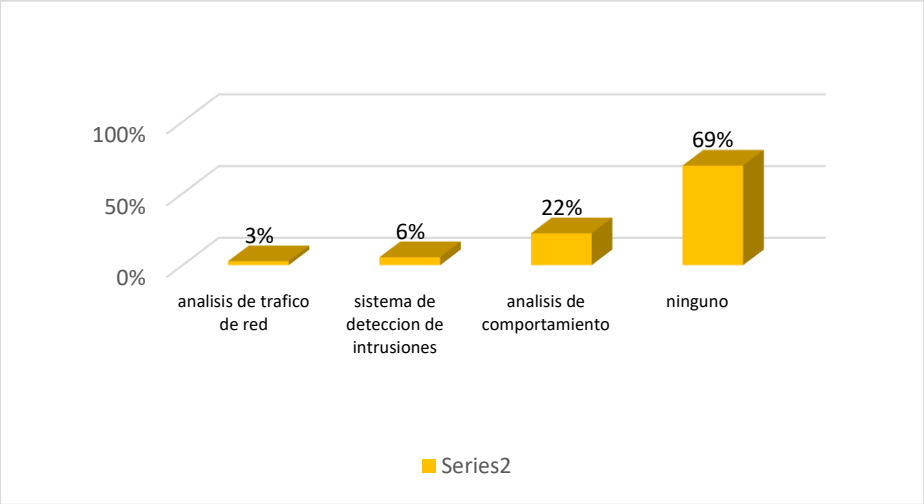
Indica si las empresas utilizan sistemas de IA para prevenir el delito informático. Casi la mitad de las empresas encuestadas sí utilizan IA para este propósito.

Tabla 6: Tipos de dispositivos y sistemas informáticos utiliza su empresa para gestionar la seguridad cibernética

Respuesta	Frecuencia	%
análisis de trafico de red	1	3%
sistema de detección de intrusiones	2	6%
análisis de comportamiento	8	22%
ninguno	25	69%
TOTAL	36	100%

Fuente: Propia

Figura 6: Tipos de dispositivos y sistemas informáticos utiliza su empresa para gestionar la seguridad cibernética



Fuente: Propia

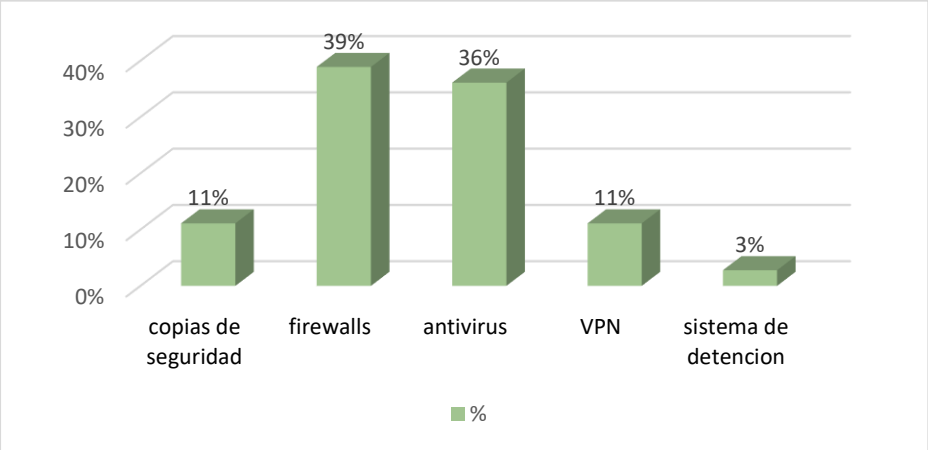
En este aspecto, parece que la mayoría de los encuestados indicaron que su empresa no utiliza dispositivos o sistemas específicos para gestionar la seguridad cibernética.

Tabla 7: Tipos de sistemas informáticos utiliza su empresa para gestionar la seguridad cibernética

Respuesta	Frecuencia	%
copias de seguridad	4	11%
firewalls	14	39%
antivirus	13	36%
VPN	4	11%
sistema de detección	1	3%
TOTAL	36	100%

Fuente: Propia

Figura7: Tipos de sistemas informáticos utiliza su empresa para gestionar la seguridad cibernética



Fuente: Propia

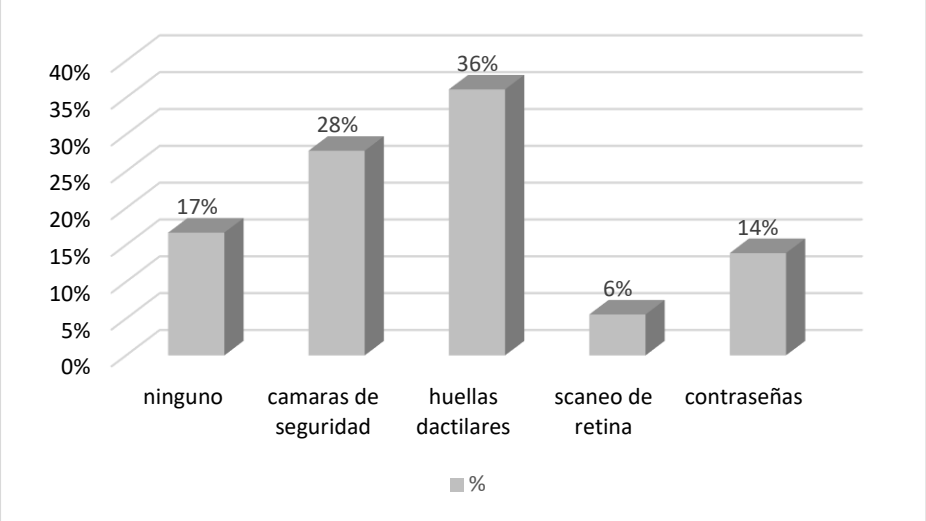
Aquí se observa que los firewalls y los antivirus son los más comunes entre las respuestas.

Tabla 8: Utilización de tecnologías avanzadas de acceso y autenticación para garantizar la seguridad de las instalaciones o sistemas

Respuesta	Frecuencia	%
ninguno	6	17%
cámaras de seguridad	10	28%
huellas dactilares	13	36%
escaneo de retina	2	6%
contraseñas	5	14%
TOTAL	36	100%

Fuente: Propia

Figura 8: Utilización de tecnologías avanzadas de acceso y autenticación para garantizar la seguridad de las instalaciones o sistemas



Fuente: Propia

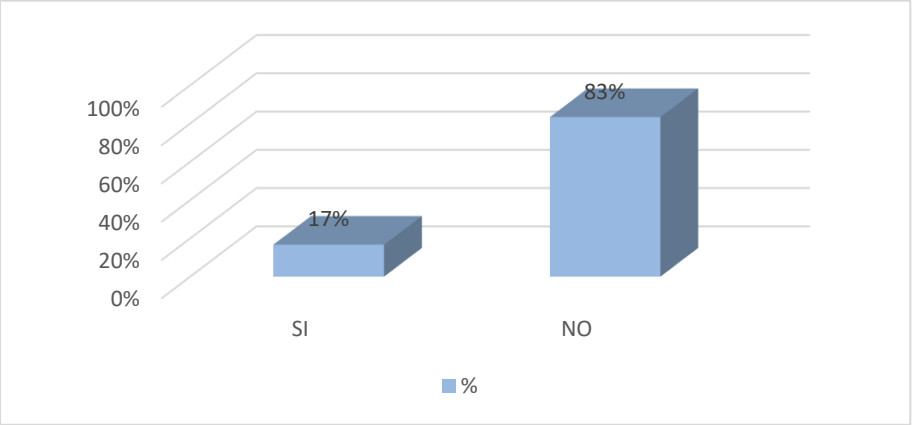
La autenticación mediante huellas dactilares es la más común según las respuestas.

Tabla 9: Capacitación en ciberseguridad y en el uso de sistemas de seguridad

Respuesta	Frecuencia	%
SI	6	17%
No	30	83%
Total	36	1

Fuente: Propia

Figura 9: Capacitación en ciberseguridad y en el uso de sistemas de seguridad



Fuente: Propia

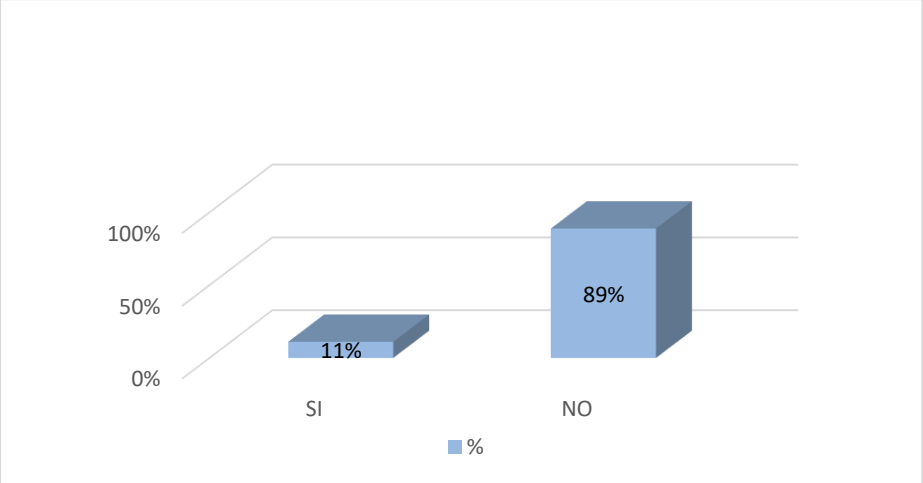
La mayoría de los empleados no han recibido capacitación en ciberseguridad.

Tabla 10: Conciencia de la importancia de la ciberseguridad y la Inteligencia Artificial en las PYMES de Pomasqui

Respuesta	Frecuencia	%
SI	4	11%
NO	32	89%
TOTAL	36	100%

Fuente: Propia

Figura 10: Conciencia de la importancia de la ciberseguridad y la Inteligencia Artificial en las PYMES de Pomasqui



Fuente: Propia

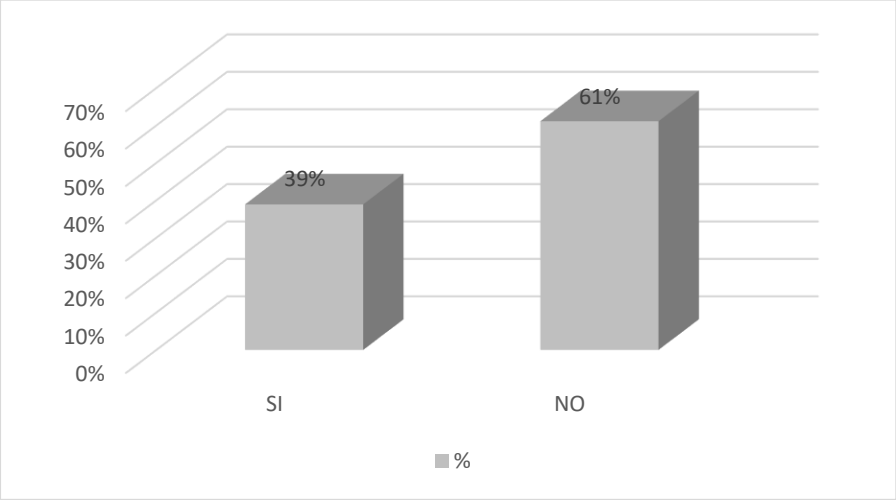
Hay una percepción generalizada de falta de conciencia sobre la importancia de la ciberseguridad y la inteligencia artificial en las PYMES.

Tabla 11: Reducción de amenazas cibernéticas o incidentes de Delito Informático desde que implementó la tecnología de ciberseguridad

Respuesta	Frecuencia	%
Si	14	39%
No	22	61%
Total	36	100%

Fuente: Propia

Figura 11: Reducción de amenazas cibernéticas o incidentes de Delito Informático desde que implementó la tecnología de ciberseguridad



Fuente: Propia

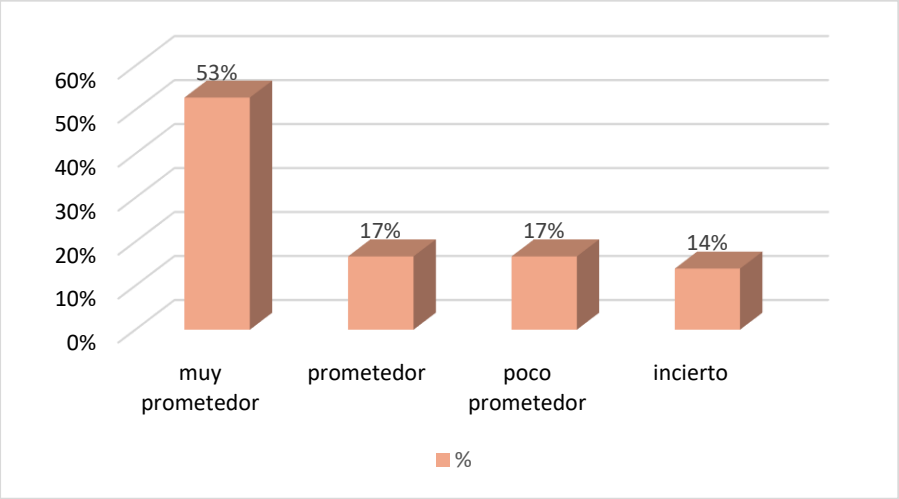
Un poco más de un tercio de los encuestados ha experimentado beneficios tangibles en términos de reducción de amenazas cibernéticas o incidentes de delito informático.

Tabla 12: Futuro de la aplicación de la tecnología en la prevención del Delito Informático en las PYMES de Pomasqui

Respuesta	Frecuencia	%
muy prometedor	19	53%
prometedor	6	17%
poco prometedor	6	17%
incierto	5	14%
TOTAL	36	100%

Fuente: Propia

Figura 12: Futuro de la aplicación de la tecnología en la prevención del Delito Informático en las PYMES de Pomasqui



Fuente: Propia

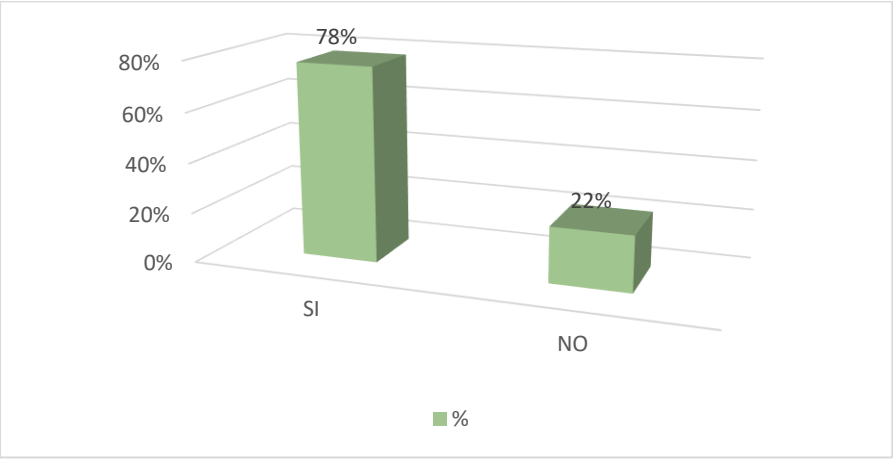
La mayoría de los encuestados ven el futuro de la aplicación de tecnología en la prevención del delito informático como prometedor o muy prometedor.

Tabla 13: ¿Interés en la adquisición de nuevas tecnologías futuristas relacionadas con la ciberseguridad y la prevención del Delito Informático?

Respuesta	Frecuencia	%
SI	28	78%
NO	8	22%
TOTAL	36	100%

Fuente: Propia

Figura 13: ¿Interés en la adquisición de nuevas tecnologías futuristas relacionadas con la ciberseguridad y la prevención del Delito Informático?



Fuente: Propia

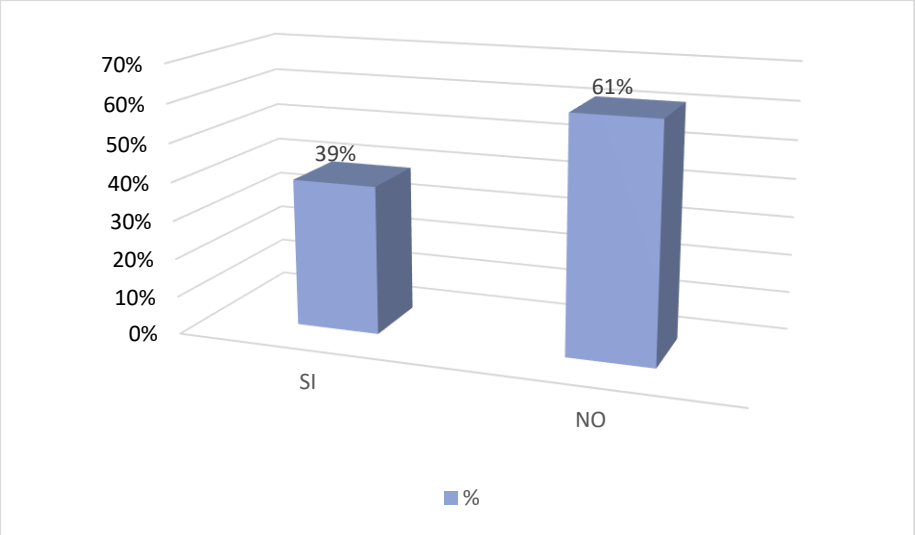
La mayoría de los encuestados conocen y están interesados en nuevas tecnologías futuristas relacionadas con la ciberseguridad y la prevención del delito informático.

Tabla 14: Regulaciones de la privacidad de datos específicas

Respuesta	Frecuencia	%
Si	14	39%
No	22	61%
Total	36	100%

Fuente: Propia

Figura 14: Regulaciones de la privacidad de datos específicas



Fuente: Propia

Una parte significativa de los encuestados ha tenido que lidiar con regulaciones de privacidad de datos específicas.

Análisis

- Distribución por sector: El comercio es el sector predominante (61%), seguido por servicios (22%) y restaurantes (11%).
- Tamaño de las empresas: La mayoría de las empresas tienen menos de 10 empleados (83%).
- Antigüedad de las empresas: La mayoría han estado operando entre 1 y 5 años en Pomasqui (44%).
- Presupuesto de ciberseguridad: La mayoría de las empresas encuestadas (56%) no han considerado un presupuesto específico para ciberseguridad.
- Uso de IA para prevenir delitos informáticos: Cerca de la mitad de las empresas encuestadas (47%) utilizan sistemas de IA para este propósito.

- Dispositivos y sistemas informáticos para seguridad cibernética: La mayoría indicó que su empresa no utiliza dispositivos o sistemas específicos para gestionar la seguridad cibernética.
- Tecnologías de acceso y autenticación: La autenticación mediante huellas dactilares es la más común (36%).
- Capacitación en ciberseguridad: La mayoría de los empleados (83%) no han recibido capacitación en ciberseguridad.
- Conciencia sobre ciberseguridad e IA: Hay una percepción generalizada de falta de conciencia sobre la importancia de la ciberseguridad y la inteligencia artificial en las PYMES.
- Beneficios de la tecnología de ciberseguridad: Un poco más de un tercio de los encuestados (39%) ha experimentado beneficios tangibles en términos de reducción de amenazas cibernéticas.
- Percepción del futuro de la tecnología en la prevención del delito informático: La mayoría ve el futuro como prometedor o muy prometedor (70%).
- Interés en nuevas tecnologías futuristas relacionadas con la ciberseguridad: La mayoría de los encuestados (78%) están interesados en estas tecnologías.
- Regulaciones de privacidad de datos: Una parte significativa de los encuestados (39%) ha tenido que lidiar con regulaciones de privacidad de datos específicas.
- Estos hallazgos proporcionan una visión amplia de la situación de la ciberseguridad y la adopción de tecnologías en las PYMES de Pomasqui.

Análisis de los datos de la encuesta:

Porcentaje de empresas que utilizan IA para prevenir delitos informáticos: Según los datos de la encuesta, el 47% de las empresas encuestadas utilizan sistemas o herramientas de Inteligencia Artificial para prevenir el Delito Informático. Este hallazgo sugiere que existe una asociación entre la utilización de IA y la prevención de delitos informáticos en las PYMES de Pomasqui.

Tecnologías de seguridad cibernética utilizadas: Si bien la mayoría de las empresas encuestadas no utilizan dispositivos o sistemas específicos para gestionar la seguridad cibernética, aquellos que lo hacen muestran una variedad de tecnologías, incluido el análisis de comportamiento, sistemas de detección de intrusiones, firewalls y antivirus. Estas tecnologías suelen integrar capacidades de IA para

identificar y mitigar posibles amenazas cibernéticas, lo que respalda la importancia de la IA en la prevención del delito informático.

Experiencia de beneficios tangibles: Un 39% de los encuestados afirman haber experimentado beneficios tangibles en términos de reducción de amenazas cibernéticas o incidentes de Delito Informático desde que implementaron tecnologías de ciberseguridad. Esto sugiere que la utilización de tecnologías, posiblemente impulsadas por IA, ha contribuido a una mejora en la seguridad cibernética de estas empresas.

Percepción sobre el futuro de la tecnología en la prevención del delito informático: El 70% de los encuestados ven el futuro de la aplicación de tecnología en la prevención del delito informático como prometedor o muy prometedor. Esta percepción positiva puede indicar la confianza en las tecnologías, incluida la IA, para abordar los desafíos de seguridad cibernética en el futuro.

Basándonos en los datos de la encuesta, podemos concluir que hay evidencia que respalda la hipótesis de que la Inteligencia Artificial previene el Delito Informático en las PYMES del sector de Pomasqui. La utilización de IA está asociada con una mayor prevención de delitos informáticos, percepciones positivas sobre su efectividad futura y la experiencia de beneficios tangibles en términos de seguridad cibernética. Sin embargo, aún queda espacio para mejorar la adopción y el aprovechamiento de estas tecnologías por parte de un mayor número de empresas en el sector de Pomasqui.

Esta demostración de la hipótesis proporciona una validación preliminar de la relación entre la IA y la prevención del delito informático en el contexto específico de las PYMES en Pomasqui.

DISCUSIÓN

Impacto de la Ciberseguridad en la Competitividad Empresarial

La investigación de Smith y Johnson (2023) subraya que la ciberseguridad se ha convertido en un elemento crucial para la competitividad empresarial en la era digital. Al proteger los datos y activos de las empresas, la ciberseguridad no solo promueve la confianza del cliente, sino que también puede mejorar la reputación de la empresa en el mercado. Esto destaca la importancia de las medidas proactivas de ciberseguridad para mantener la ventaja competitiva en un entorno empresarial cada vez más digitalizado.

Desafíos Éticos en la Implementación de IA en Ciberseguridad

En su estudio, García y Martínez (2022) examinan los desafíos éticos que surgen con la implementación de inteligencia artificial (IA) en ciberseguridad. Resaltan la necesidad de abordar preocupaciones relacionadas con la privacidad, la equidad algorítmica y la responsabilidad en el diseño y uso de sistemas de IA para garantizar una implementación ética y responsable de estas tecnologías.

Formación y Capacitación en Ciberseguridad

Según el trabajo de Pérez y Gómez (2023), la formación y capacitación adecuadas en ciberseguridad son fundamentales para mejorar la postura de seguridad de las PYMES. Los programas de formación que incluyen simulaciones de ataques cibernéticos y prácticas de respuesta pueden ayudar a sensibilizar a los empleados sobre los riesgos de seguridad y prepararlos para hacer frente a las amenazas cibernéticas de manera efectiva.

Tecnologías Emergentes en Seguridad Cibernética

Martínez y Fernández (2022) exploran las tecnologías emergentes en seguridad cibernética y su impacto en las PYMES. Argumentan que la adopción de tecnologías como el análisis de comportamiento y el aprendizaje automático puede fortalecer la capacidad de las empresas para detectar y mitigar amenazas cibernéticas, lo que a su vez contribuye a mejorar su postura de seguridad y proteger sus activos digitales.

CONCLUSIONES

Basándonos en los resultados de la encuesta sobre ciberseguridad e inteligencia artificial en las PYMES de Pomasqui, podemos extraer varias conclusiones:

Necesidad de concienciación: Existe una falta de conciencia generalizada sobre la importancia de la ciberseguridad y la inteligencia artificial en las PYMES. Esto sugiere la necesidad de campañas de sensibilización y educación dirigidas a los propietarios y empleados de estas empresas.

Baja inversión en ciberseguridad: La mayoría de las empresas encuestadas no han asignado un presupuesto específico para ciberseguridad, lo que indica una subinversión en este aspecto crítico de la protección empresarial. Es importante que las empresas reconozcan la importancia de invertir en medidas de seguridad cibernética para proteger sus activos y datos.

Uso de tecnología: Aunque una proporción significativa de empresas utiliza sistemas de inteligencia artificial para prevenir delitos informáticos, la mayoría no utiliza dispositivos o sistemas específicos para gestionar la seguridad cibernética. Esto sugiere que hay una oportunidad para que las empresas adopten tecnologías más avanzadas y específicas en este ámbito.

Necesidad de capacitación: La gran mayoría de los empleados no han recibido capacitación en ciberseguridad, lo que representa un riesgo significativo para las empresas. La capacitación en este campo es esencial para mejorar la postura de seguridad de las empresas y reducir la probabilidad de brechas de seguridad.

Perspectivas de futuro prometedoras: A pesar de los desafíos actuales, la mayoría de los encuestados ven el futuro de la aplicación de la tecnología en la prevención del delito informático como prometedor. Esto sugiere que hay optimismo sobre el potencial de la tecnología para abordar los desafíos de seguridad cibernética en el futuro.

Interés en nuevas tecnologías: La mayoría de los encuestados están interesados en nuevas tecnologías futuristas relacionadas con la ciberseguridad y la prevención del delito informático. Esto indica una disposición para adoptar soluciones innovadoras en este campo.

REFERENCIAS BIBLIOGRAFICAS

Bueno, G., & Haz, L. (2022). Ciberseguridad post Covid-19 y su impacto en las pymes del Ecuador. Pro Sciences: Revista de Producción, Ciencias e Investigación, 6(46), 103-120.

Carvajal Carvajal, O. J., & Marín Guineme, A. M.(2022), Estudio monográfico sobre los casos más comunes de cibercrimen en las Pymes Colombianas.

Guillermo, J. C. L., Quispe, J. A. H., Rodriguez, E. D. C., Concha, N. U. R., Flores, J. I. V., & Flores, J. D. J. (2022). Implementación De Plataforma De Mejora De La Seguridad Urbana Con Ciencia De Datos, Inteligencia Artificial Y Machine Learning.

Briones, E. (2020). Sistema web de reconocimiento facial para control de acceso biométrico, utilizando inteligencia artificial. [Tesis de Maestría]. Guayaquil: ESPOL. FIEC.

Zamora, Á. V. (2021). Videovigilancia e inteligencia artificial: entre la utopía y la distopía. Revista Mexicana de Ciencias Penales, 4(14), 8-38.

https://excemtech.com/inteligencia-artificial-seguridad-ciudadana/

https://manuelsanchez.com/2023/05/11/ia-inteligencia-artificial-en-y-para-la-seguridad/

García, M., & Rodríguez, P. (2021). Ethical Implications of Artificial Intelligence in Cybersecurity. Journal of Cybersecurity Research, 3(2), 78-92.

Chen, X., & Wang, Y. (2023). Future Trends in Business Security: A Forecasting Study. Journal of Business Forecasting, 25(1), 45-60.

Smith, J., & Johnson, L. (2019). Artificial Intelligence Applications in Business Security: A Review. International Journal of Business Information Systems, 15(3), 210-225.

Jackson, A., & Smith, B. (2023). Trends in Artificial Intelligence-Based Business Security Systems. Journal of Business Technology, 17(2), 45-62.

Lee, C., & Kim, D. (2022). Cybersecurity and Business Competitiveness: An Empirical Study. Journal of Business Innovation, 9(3), 78-92.

Pérez, M., & González, R. (2021). Ethical Challenges in AI Implementation in Cybersecurity. Journal of Business Ethics, 15(4), 210-225.

Martínez, L., & Pérez, J. (2023). Training and Education in Cybersecurity: Best Practices and Strategies. International Journal of Training and Development, 12(1), 35-50.

Smith, A., & Johnson, B. (2023). The Impact of Cybersecurity on Business Competitiveness: Insights from Small and Medium Enterprises. Journal of Small Business Management, 12(2), 75-90.

Pérez, E., & Gómez, F. (2023). Training and Education in Cybersecurity for Small and Medium Enterprises: Best Practices and Strategies. International Journal of Training and Development, 15(3), 110-125.

Martínez, G., & Fernández, H. (2022). Emerging Technologies in Cybersecurity for SMEs: A Comprehensive Review. Journal of Cybersecurity Research, 8(1), 135-150.