

articles in accordance with pre-established inclusion and exclusion criteria. The results demonstrate that the incorporation of AI into biometric authentication systems enhances security in terms of controlled access, protection, and data security. The analyzed studies indicate that the deployment of multimodal biometrics and advanced algorithms not only improves the reliability of the process, but also reduces false positives, which is crucial in the management of sensitive data. The combination of various biometric features, such as facial recognition and physiological signal analysis, has proven to be effective even in medical settings.

Keywords: *risk analysis, cybersecurity, intrusion detection, data privacy, health systems*

Introducción

La autenticación biométrica ha adquirido relevancia como una solución esencial para mejorar la seguridad y la exactitud en la identificación de personas en diferentes sectores industriales. Con el fin de asegurar la protección y confidencialidad de los datos sensibles, los hospitales con tecnología avanzada necesitan implementar sistemas sofisticados que verifiquen la identidad de los usuarios y identifiquen posibles irregularidades de manera inmediata. En el presente escenario, la inteligencia artificial (IA) ha evidenciado su utilidad en el mejoramiento de la autenticación biométrica y la detección de amenazas en infraestructuras críticas. La conexión de la inteligencia artificial en el proceso de autenticación biométrica no solo incrementa la exactitud en la identificación de individuos, sino que también posibilita la detección de conductas anómalas que podrían sugerir actividades fraudulentas o intentos de acceso no permitidos. En los hospitales inteligentes, es de vital importancia la identificación de irregularidades, ya que los datos médicos y personales están expuestos con frecuencia a posibles ciberataques. La mejora de la autenticación de sistemas se logra mediante el uso de inteligencia artificial, específicamente redes neuronales y algoritmos de aprendizaje profundo. Estos elementos permiten analizar las interacciones de los usuarios, lo que resulta en un aumento de la fiabilidad del proceso. La creación de perfiles seguros es un aspecto fundamental para reducir los errores en la identificación de personas. En espacios críticos, múltiples estudios han destacado la relevancia de utilizar la inteligencia artificial en el ámbito de la seguridad biométrica. Budżys et al. [1] presentaron un modelo de autenticación fundamentado en técnicas de aprendizaje profundo con el propósito de identificar posibles riesgos internos en infraestructuras críticas, específicamente en el contexto de hospitales inteligentes. En un estudio previo, Annadurai et al. [2] desarrollaron un sistema de detección de intrusiones que utiliza autenticación biométrica asistida por inteligencia artificial. Este sistema tiene como objetivo reforzar la seguridad de la información y resguardar los sistemas hospitalarios interconectados. Para lograr esto, se emplean técnicas de obtención de características y agrupación [3]. La implementación de la fusión de datos biométricos de venas y formas de dedos mediante una red neuronal convolucional (CNN) multimodal podría mejorar la seguridad de los sistemas biométricos en entornos hospitalarios inteligentes. Esta tecnología ofrece una capa suplementaria de seguridad en el acceso a los recursos médicos y a la información de los pacientes. En un estudio reciente, Aanjanadevi et al. [4] introdujeron un sistema sustentado en redes neuronales convolucionales que incrementa la seguridad de

la información mediante la combinación de biometría facial y criptografía. Este sistema proporciona un nivel adicional de protección en la especialización de la medicina. El objetivo de esta investigación es encontrar una respuesta a la pregunta de qué tecnologías ofrecen una mayor seguridad biométrica para la detección de anomalías en hospitales inteligentes basados en IA. Asimismo, se llevará a cabo un análisis cuantitativo de las publicaciones desde 2018 sobre este tema, centrando la atención en los espacios de publicación más relevantes. Se espera que esto brinde un conocimiento del estado existente de la investigación en esta área, así como de cómo la IA está redefiniendo la seguridad en los hospitales inteligentes.

Metodología

Las revisiones sistemáticas son de gran relevancia en una investigación ya que ofrecen una visión completa del conocimiento disponible en un tema particular, lo cual facilita identificar áreas que requieren un mayor estudio y formular nuevas preguntas de investigación [5]. Estas revisiones permiten descubrir problemas en investigaciones previas que necesitan ser corregidos y ayudan a desarrollar o verificar teorías sobre fenómenos relevantes. En ese sentido, al momento de realizar un análisis integral de publicaciones previas, es muy común que se presenten diversas interrogantes como saber por dónde exactamente se debe comenzar, la selección adecuada del tema o la cantidad de artículos a incluir en la revisión. Ante ello, Morales [6] nos exhorta la importancia de seleccionar una metodología apropiada que ofrezca una guía clara y estructurada, que facilite el proceso de revisión, pero a la vez asegure un enfoque coherente y sistemático. Una de las diferentes metodologías existentes es la denominada metodología PRISMA, la cual es un conjunto de directrices diseñado para fortalecer la calidad de estos documentos. Esta metodología apareció por primera vez en el área de la salud como una solución a la necesidad de estandarizar la presentación de los estudios que se realizaban, dado que la falta de consistencia en los informes dificultaba la evaluación y la interpretación de los resultados [7]. Posteriormente extendió su alcance a diversas disciplinas y hasta la actualidad es ampliamente utilizado para guiar a una realización correcta. La metodología PRISMA busca proporcionar a los autores una guía clara sobre qué información incluir en sus informes, agilizando la creación y documentación de las revisiones al mismo tiempo que aumenta la confianza en los hallazgos presentados, aspecto fundamental a la hora de tomar decisiones en diversos ámbitos de aplicación [8]. Para realizar el proceso de una manera estandarizada, La metodología PRISMA establece un riguroso sistema para llevar a cabo las revisiones [9,10], comenzando con la identificación de palabras clave para buscar literatura pertinente. Además, se definen criterios de inclusión y exclusión que aseguran que solo se consideren los estudios significativos para el desarrollo de la investigación. Incluso, se elabora un flujograma que ilustra los pasos seguidos al elegirlos, indicando cuántos fueron identificados, excluidos en cada fase y finalmente incluidos en el análisis. Teniendo en cuenta lo antes mencionado, este estudio se optó por realizarse siguiendo esta metodología PRISMA, ya que nos va a permitir analizar los estudios científicos e identificar de manera rigurosa los que son más relevantes para nuestra revisión.

Ecuaciones de búsqueda

Para iniciar con el proceso de recolección de data, en primer lugar, seleccionamos algunos repositorios o fuentes de información de los cuales obtendremos los documentos que se utilizaron en la revisión. Dichos repositorios fueron las siguientes: SCOPUS, MDPI, SCIENCE DIRECT, IEEE XPLORE y PUBMED. Luego identificamos las principales palabras clave referentes a nuestro estudio que trata sobre el uso de la IA y la biometría en la autenticación y detección de anomalías en hospitales inteligentes. Estas palabras clave nos permiten filtrar nuestros resultados para encontrar solo la información más pertinente de revisión. Las palabras claves utilizadas en cada repositorio se muestran a en la siguiente tabla:

Tabla 1. Palabras claves utilizadas en cada repositorio

REPOSITORIO	CADENA DE BÚSQUEDA
SCOPUS	biometric AND authentication AND artificial AND intelligence AND security OR hospitals
MDPI	security AND biometric AND authentication AND artificial AND intelligence AND hospitals
SCIENCE DIRECT	artificial AND intelligence AND biometric AND authentication AND security AND hospital
IEEE XPLORE	biometric AND security AND hospital
PUBMED	biometric AND Authentication AND hospital

Criterios de inclusión y exclusión

Al referirnos a estos criterios, hablamos de pautas específicas definidas al realizar una revisión y cuya función es decidir qué estudios o artículos se incluirán y cuáles se excluirán debido a su relevancia en el estudio. Todos estos criterios planteados se explicitan a continuación.

Tabla 2. Criterios de inclusión planteados para la selección de artículos

Nº	CRITERIO DE INCLUSIÓN (CI)
CI1	Artículos publicados en inglés o español
CI2	Artículos publicados desde 2018 hasta la fecha de la búsqueda
CI3	Artículos sobre IA aplicada en seguridad de datos, biometría y gestión de hospitales inteligentes

Tabla 3. Criterios de exclusión planteados para la selección de artículos

N°	CRITERIO DE EXCLUSIÓN (CE)
CE1	Artículos que no estén en el rango de años establecido (2018 – 2024)
CE2	Artículos cuyo título no esté relacionado directamente con el tema de investigación
CE3	Artículos cuyo abstract no aborde específicamente aspectos clave o relevantes del estudio

Recolección de información

La búsqueda inicial se realizó siguiendo los criterios presentados en la Tabla 2 además tomando en cuenta las palabras claves seleccionadas para cada fuente de información y las cuales están explicadas en la Tabla 1. Luego de realizar esta consulta en cada repositorio obtuvimos un total de 480 artículos, como se aprecia en la siguiente tabla:

Tabla 4. Número de artículos encontrados en cada repositorio

REPOSITORIO	NÚMERO DE ARTÍCULOS ENCONTRADOS
SCOPUS	149
MDPI	47
SCIENCEDIRECT	116
IEEEEXPLORE	109
PUBMED	59
TOTAL	480

En seguida, estos artículos encontrados fueron depurados por los revisores utilizando los criterios de exclusión presentados en la Tabla 3 a fin de poder tener una apreciación más cercana sobre el contenido desarrollado en cada uno y así poder seleccionar los artículos que ofrezcan la mayor cantidad de información pertinente y relevante para nuestro estudio. Este proceso aseguró que los documentos resultantes del filtro sean confiables y oportunos para el proceso actual de revisión. En la tabla 5 se proporciona un detalle de la cantidad de artículos obtenidos en cada repositorio luego de realizar los filtros correspondientes en cada uno:

Tabla 5. Cantidad de artículos seleccionados después de hacer el respectivo filtrado

N° ARTÍCULOS	SCO	MDPI	SD	IEEE	PUB
CANTIDAD TOTAL	149	47	116	109	59
APLICANDO CE1	105	44	114	69	31
APLICANDO CE2	15	25	14	12	11
APLICANDO CE3	10	7	6	6	5
TOTAL	34				

Asimismo, para mostrar de manera más entendible el proceso se realizó el siguiente flujograma donde se representa los pasos seguidos para el filtrado de artículos.

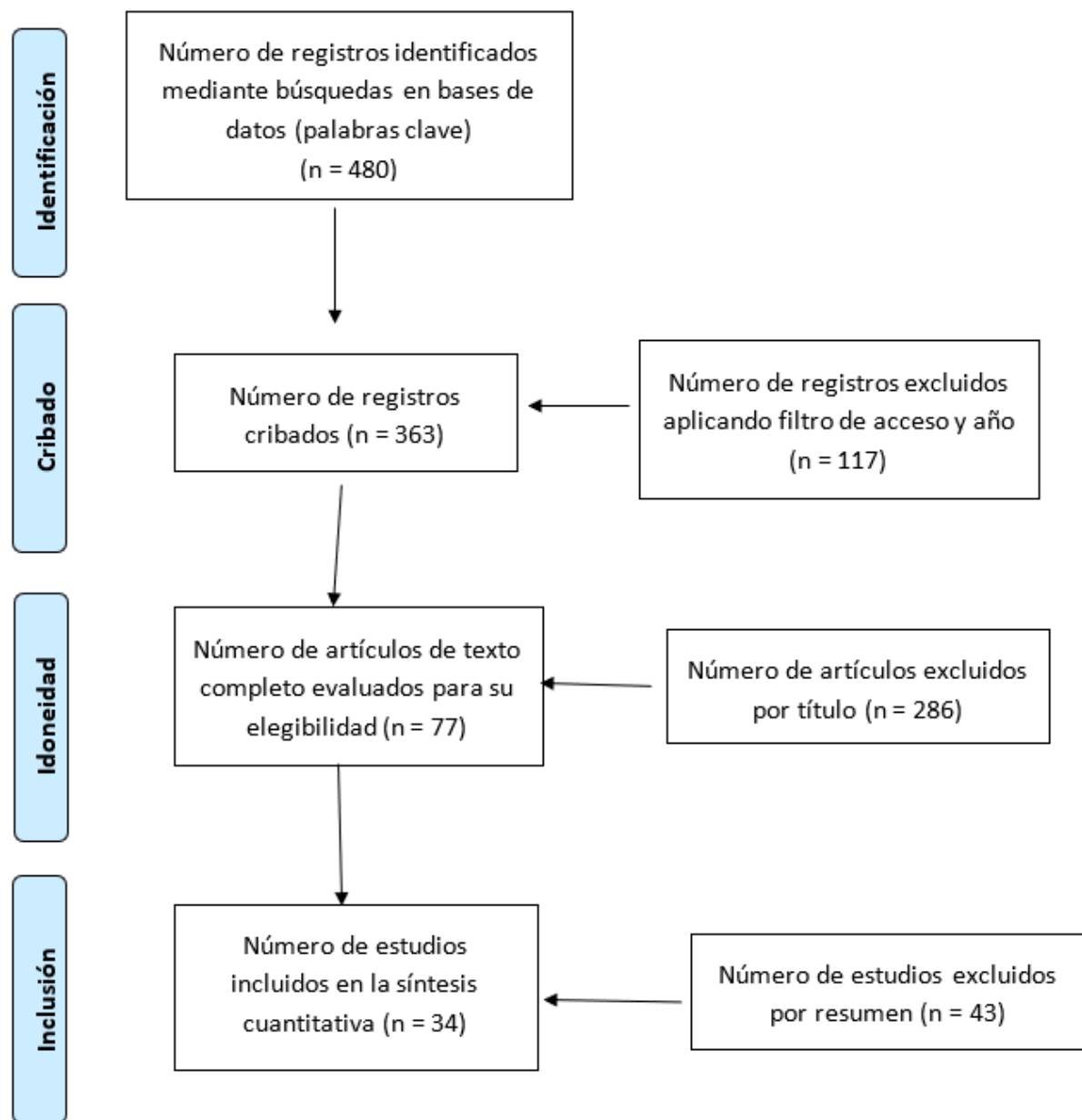


Figura 1. Flujograma PRISMA utilizado en esta revisión

Resultados

Una vez aplicado los diferentes criterios mencionados en las secciones anteriores, como resultado se obtuvo 34 artículos que cumplieran con los requisitos establecidos. La Tabla 6 presentada a continuación nos brinda un panorama detallado de cada uno de estos artículos, lo que permite observar la relevancia del tema tratado, así como sus aportes más importantes:

Tabla 6. Resultados de selección final y su respectivo enfoque de investigación

Nº	AUTORES	ATRIBUTOS	TIPO	TECNOLOGÍA
1	Budžys, Arnoldas; Kurasova, Olga; Medvedev, Viktor	ciberseguridad, biometría	Propuesta de modelo de identificación biométrica [1]	Deep Learning, biometría
2	Annadurai, C.; Nelson, I.; Devi, K.N.; Masud, M.; Jeque, A.	Seguridad de datos, resiliencia ante ataques, ciberseguridad, control de acceso, inteligencia artificial	Propuesta de sistema de detección de intrusos [2]	Inteligencia Artificial (IA), IoT, Redes Neuronales Convolucionales (VGG-16), Análisis de Componentes Principales (KPCA)
3	Wan Kim, Jong Min Song, Parque Kang Ryoung	Ciberseguridad, biometría, protección de datos, machine learning	Reconocimiento biométrico multimodal basado en CNN [3]	Redes Neuronales Convolucionales (CNN), Sensor de Infrarrojo Cercano (NIR), Biometría Multimodal, reconocimiento de venas y forma de los dedos
4	Aanjanadevi, S.; Aanjankumar, S.; Ramela, K.R.; Palanisamy, V.	Protección de datos, ciberseguridad, autenticación, privacidad de datos	Propuesta de sistema de seguridad biométrica para protección de datos [4]	Redes Neuronales Convolucionales (CNN), Biometría Facial, Criptografía, IA

Continúa en la siguiente página

N°	AUTORES	ATRIBUTOS	TIPO	TECNOLOGÍA
5	Khan, H.U.; Malik, M.Z.; Nazir, S.; Khan, F.	Ciberseguridad, resiliencia ante ataques, protección de datos, inteligencia artificial	Propuesta de análisis sobre la implementación de sistemas biométricos en la banca [11]	Biometría, ciberseguridad, Inteligencia Artificial (IA), IoT
6	Mainetti, L.; Panarese, P.; Vergallo, R.	Autenticación, biometría, ciberseguridad, privacidad de datos, inteligencia artificial	Propuesta de un modelo autenticación continua a través de hábitos del usuario [12]	Inteligencia Artificial (IA), Internet de las Cosas (IoT), meta-modelos, autenticación continua, datos de hábitos
7	Bordel, B.; Alcarria, R.; Robles, T.	Ciberseguridad, autenticación, biometría, protección de datos, control de acceso	Cifrado ligero para sistemas de autenticación biométrica [13]	Cifrado simétrico ligero, Pseudo Random Number Generator (PRNG), comunicaciones inalámbricas de corto alcance
8	Al Ghamdi, A.S.M.A.; Ragab, M.	Ciberseguridad, autenticación, biometría, protección de datos, inteligencia artificial	Técnica de autenticación biométrica basada en inteligencia artificial [14]	Inteligencia Artificial (IA), DenseNet-77, Redes Neuronales Profundas (DNN)
9	Maharjan, P.; Shrestha, K.; Bhatta, T.; Lee, S.; Parque, J.Y.	Ciberseguridad, autenticación, biometría, protección de datos, inteligencia artificial	Autenticación biométrica utilizando nanogeneradores híbridos [15]	Inteligencia Artificial (IA), Redes Neuronales Artificiales, Nanogeneradores Híbridos, Sensores Triboeléctricos y Electromagnéticos, Keystroke Dynamics

Continúa en la siguiente página

Nº	AUTORES	ATRIBUTOS	TIPO	TECNOLOGÍA
10	Shivanna, Preetha; Venkatesiah, Sheela Samudrala	Autenticación, biometría, seguridad de datos, machine learning	Autenticación biométrica mediante reconocimiento facial [16]	Red Neuronal Simples, IA, Reconocimiento Facial
11	Gabriela Quintanilla Mendoza	Privacidad de datos, ciberseguridad, protección de datos, biometría	Legislación, en el uso de sistemas biométricos para la identificación personal [17]	Biometría, Reglamento General de Protección de Datos (GDPR), Seguridad, Privacidad
12	Mahmoud Elkhodr, Samiya Khan, Ergun Gide	Ciberseguridad, privacidad de datos, seguridad de datos, inteligencia artificial	Middleware semántico para la gestión segura de datos en IoT utilizando blockchain y AI [18]	Internet de las Cosas (IoT), Blockchain, Inteligencia Artificial (IA), Anotación Semántica, Middleware
13	Roberto O. Andrade, Walter Fuertes, María Cazares, Iván Ortiz-Garcés, Gustavo Navas	Ciberseguridad, inteligencia artificial, protección de datos, resiliencia ante ataques, inteligencia artificial	Intersección de ciencias cognitivas y IA para la protección contra ciberataques [19]	Ciencia Cognitiva, Inteligencia Artificial (IA), minería de textos, metodología PRISMA, ciberseguridad cognitiva
14	Sandeep Kumar et al.	Biometría, ciberseguridad, protección de datos	Sistema biométrico avanzado utilizando U-Net y Alex-Net [20]	U-Net, Alex-Net, Biometría Facial, Reconocimiento Facial

Continúa en la siguiente página

Nº	AUTORES	ATRIBUTOS	TIPO	TECNOLOGÍA
15	Jan Herbst et al.	Ciberseguridad, privacidad de datos, autenticación, protección de datos, inteligencia artificial	Marco de comunicación basado en tokens para la seguridad y autenticación en redes inalámbricas de área corporal (WBAN) [21]	Redes Inalámbricas de Área Corporal (WBAN), Inteligencia Artificial (IA), Cifrado Totalmente Homomórfico
16	Vasile-Daniel Păvăloaia, George Husac	Ciberseguridad, protección de datos, control de acceso, machine learning	Reconocimiento facial utilizando aprendizaje automático y análisis de componentes principales (PCA) [22]	Aprendizaje Automático (ML), Análisis de Componentes Principales (PCA), AdaBoost, MySQL, Reconocimiento Facial
17	Farhad Ahamed et al.	Autenticación, biometría, ciberseguridad, protección de datos, inteligencia artificial	Autenticación biométrica multimodal para dispositivos y usuarios en atención sanitaria [23]	Inteligencia Artificial (IA), IoT, Biometría Multimodal
18	Kholoud Y. Najmi et al.	Control de acceso, privacidad de datos, integridad de datos	Identificación de protocolos [24]	IoT, criptografía, autenticación de dos factores, biometría
19	Ali Seyfizadeh et al.	Control de acceso, seguridad de datos	Propuesta de modelo de identificación biométrica [25]	Biometría, Deep Learning, CWT

Continúa en la siguiente página

Nº	AUTORES	ATRIBUTOS	TIPO	TECNOLOGÍA
20	Feng Wang, Yongjie Gai, Haitao Zhang	Privacidad de datos, control de acceso, resiliencia ante ataques	Propuesta de gestión de datos de identidad digital [26]	Blockchain, big data, digital twins, zero trust
21	Anastasia Levina et al.	Seguridad de datos, control de acceso, integridad de datos	Propuesta de sistema de gestión hospitalaria inteligente [27]	Wearables, IoT, cifrado E2EE, autenticación MFA, firewalls
22	Omar Alruwaili et al.	Protección de datos, control de acceso, resiliencia ante ataques, integridad de datos	Propuesta de mecanismos AKA (Authenticated Key Agreement) [28]	IoT, PUFs, cifrado simétrico, autenticación de dos vías (AKA)
23	Ghita Lazrek et al.	Resiliencia ante ataques, protección de datos, biometría, Machine Learning	Propuesta de sistema de detección de intrusiones [29]	Machine Learning, biometría, decisions trees
24	Abhishek Jain, Khushboo Tripathi	Control de acceso, seguridad de datos, integridad de datos, biometría	Propuesta de Framework de Hadoop MapReduce [30]	Redes Neuronales Recurrentes (RNN), estandarización HL7, firmas biométricas
25	Tuan-Vinh Le et al.	Control de acceso, seguridad de datos, privacidad de datos, biometría	Propuesta de sistema Centerless User-Controlled Single Sign-On (CL-UCSSO) [31]	Firma criptográfica, 6G, biometría, biohash, blockchain

Continúa en la siguiente página

Nº	AUTORES	ATRIBUTOS	TIPO	TECNOLOGÍA
26	Deming Mao, Huihong Liu, Wei Zhang	Seguridad de datos, control de acceso, resiliencia ante ataques, biometría	Esquema de Autenticación de Tres Factores [32]	Criptografía Rabin, verificador difuso, biometría, protocolos, sistema MMIS
27	Aravindhraj Natara- jan, N. Shanthi	Control de acceso, privacidad de datos, seguridad de datos, biometría	Propuesta de sistema biométrico multimodal [33]	Biometría, algoritmos criptográficos, fusion levels
28	Tingting Fu et al.	Control de acceso, seguridad de datos, biometría, autenticación	Propuesta de sistema de autenticación doble (EMG) [34]	Biometría, GRABM- yo, ANOVA, Senso- res EMG
29	Vincent Omollo Nyangaresi	Control de acceso, seguridad de datos, biometría, autenticación	Protocolo de autenticación de tres factores [35]	Biosensores, lógica BAN, public internet, biometría, Wireless Body Area Networks
30	Nan Wan et al.	Control de acceso, seguridad de datos, inteligencia artificial	Propuesta sistema de identificación mediante dispositivos implantables [36]	Microchips sub- cutáneos, biometría, códigos QR, imágenes por ultrasonido, Algoritmos de inteligencia artificial
31	Gabriel Guízar- Sahagún et al.	Seguridad de datos, biometría, machine learning, integridad de datos	Sistema de biometría dactilar [37]	machine learning, biometría, procesos digitales, verificación automatizada

Continúa en la siguiente página

Nº	AUTORES	ATRIBUTOS	TIPO	TECNOLOGÍA
32	Minoru Sawa et al.	Control de acceso, seguridad de datos, resiliencia ante ataques, biometría	Propuesta de sistema de autenticación biométrica [38]	Biometría, sistemas electrónicos, análisis estadístico
33	Tanushree Singh et al.	Control de acceso, seguridad de datos, biometría, integridad de datos, autenticación	Evaluación de la fiabilidad del sistema BIR para autenticación e identificación personal [39]	Reconocimiento biométrico de iris (BIR), análisis de distancia de Hamming
34	Dhananjay Nigam et al.	Control de acceso, autenticación, resiliencia ante ataques, inteligencia artificial	Sistemas de autenticación inteligentes de 2 factores [40]	Reconocimiento facial y por voz, redes neuronales, Análisis de señales ECG y EEG, base de datos, biometría, criptografía

Luego de un minucioso análisis de los 34 artículos seleccionados, se hace evidente que diferentes autores utilizan un amplio rango de atributos en sus investigaciones sobre IA, biometría y seguridad informática. Los atributos que pudimos encontrar y los cuales se encuentran documentados de manera explícita en la tabla 6 fueron (Ciberseguridad, Biometría, Resiliencia ante ataques, Protección de datos, Autenticación, Privacidad de datos, Seguridad de datos, Control de acceso, Inteligencia Artificial, Machine learning, Integridad de datos). Ahora bien, para poder atender al objetivo central de nuestra investigación, se decidió realizar una clasificación de los atributos antes mencionados y para ello a continuación se presenta de forma clara en tabla 7:

Tabla 7. Distribución de atributos obtenidos de cada artículo seleccionado

ATRIBUTO	APARICIONES EN LOS ARTÍCULOS
Ciberseguridad	15
Biometría	18
Resiliencia ante ataques	9
Protección de datos	14
Autenticación	11
Privacidad de datos	8
Seguridad de datos	15
Control de acceso	18
Inteligencia Artificial	12
Machine learning	5
Integridad de datos	6

Adicionalmente se muestra el porcentaje de atributos aplicados en los artículos seleccionados. Debemos destacar que los atributos Biometría y Control de acceso son los que más mencionan y prevalecen dentro de los artículos revisados, representando cada uno el 13.74% del total. Seguidos de igual manera por otros dos atributos, los cuales son Ciberseguridad y Seguridad de datos, cada uno representando un 11.45% del total.

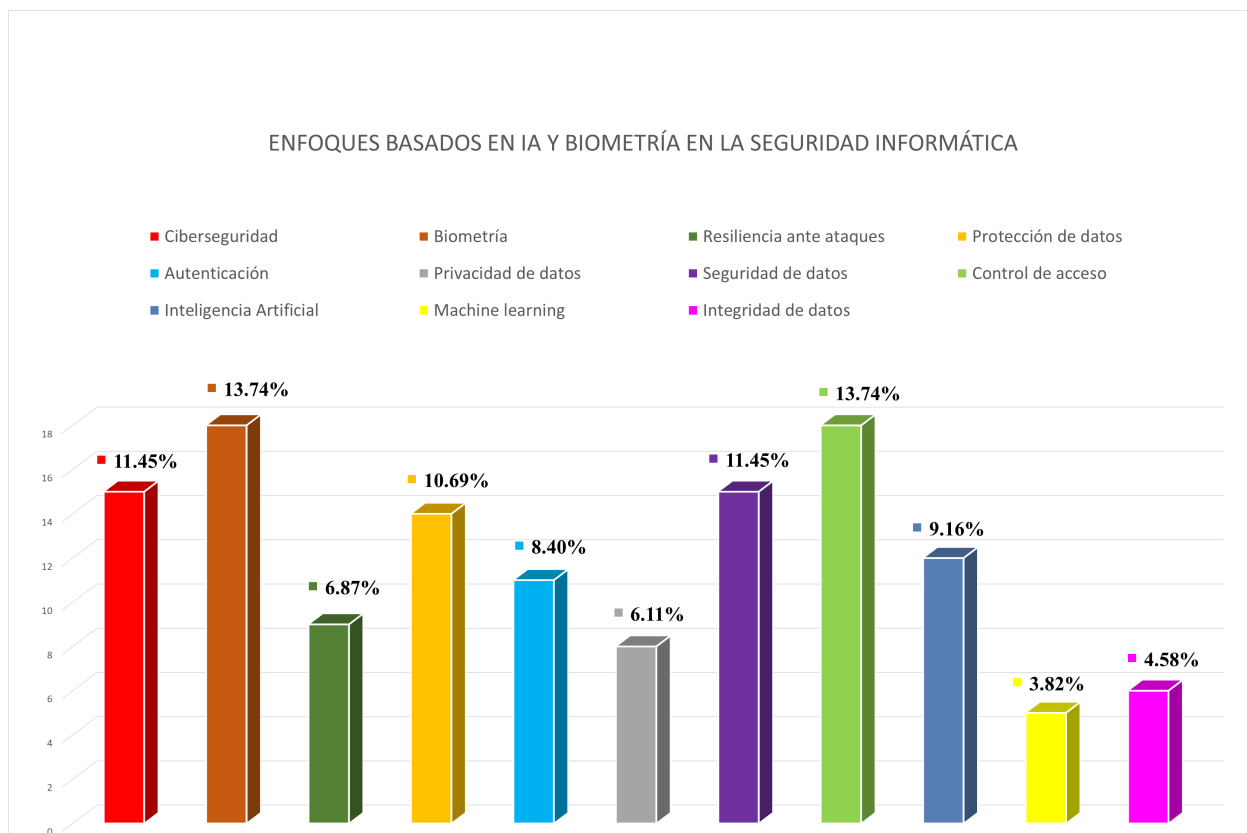


Figura 2. Distribución porcentual de los atributos encontrados

Discusión

La significancia de la inteligencia artificial en la identificación y confirmación de anomalías en hospitales inteligentes a través de la autenticación biométrica es resaltada por la revisión sistemática. En la introducción se destaca la importancia de esta tecnología en la salvaguarda de información confidencial y en la prevención de accesos no autorizados. Los progresos en Inteligencia Artificial han propiciado el desarrollo de modelos más precisos y resistentes, los cuales contribuyen a fortalecer la seguridad en las infraestructuras de los hospitales. Los resultados obtenidos en relación con los atributos fundamentales de las tecnologías basadas en inteligencia artificial para la seguridad biométrica en hospitales inteligentes se enfocan en cuatro aspectos principales: control de acceso, protección de datos, seguridad de la información y análisis predictivo. La implementación de estos atributos, según varios estudios, mejora la credibilidad de los sistemas de autenticación, disminuye los falsos positivos y garantiza la integridad de la información médica. La implementación de esta medida no solo contribuye al fortalecimiento de la confiabilidad de los usuarios y los expertos de la asistencia médica,

sino que también mejora la productividad y la seguridad en la administración de datos sensibles dentro de las infraestructuras hospitalarias, al optimizar el flujo de trabajo. Ahamed et al. [23] proponen que la autenticación biométrica multimodal, que incluye el aprendizaje profundo y diversas fuentes biométricas, es crucial para mejorar la confiabilidad del sistema y disminuir los falsos positivos. La capacidad de la inteligencia artificial para aprender e interpretar patrones de comportamiento es otro factor crítico a considerar lo que facilita la identificación temprana de amenazas. Păvăloaia y Husac [22] resaltan la utilización de algoritmos y metodologías de machine learning, como el análisis de componentes principales (PCA), para mejorar el reconocimiento facial y reducir el acceso no autorizado. Debido al flujo continuo de información médica, estas capacidades preventivas son esenciales para la protección de los datos en los hospitales. Además, las redes inalámbricas de área corporal (WBAN) son un componente crucial de los sistemas de monitoreo de pacientes. La integración de IA en estos sistemas protege los datos médicos y mejora la comunicación y el tratamiento de información sensible. Los resultados de esta investigación confirman que la aplicabilidad de la inteligencia artificial para la autenticación biométrica y la detección de amenazas en entornos hospitalarios es una solución escalable y eficaz para proteger la integridad de los datos médicos [21]. La evaluación de varias tecnologías biométricas, como el reconocimiento facial y el análisis de señales fisiológicas, refuerza la idea de que la combinación de múltiples características biométricas puede mejorar significativamente la autenticación biométrica en hospitales inteligentes. Las redes neuronales avanzadas que combinan datos biométricos (edad, género y expresión facial) proporcionan resultados extremadamente precisos en el contexto hospitalario y mejoran la seguridad de los sistemas de identificación y acceso [20].

Conclusiones

Podemos notar que la IA se presenta como un recurso de gran importancia para la autenticación biométrica y la detección de anomalías en hospitales inteligentes, cumpliendo con el objetivo de identificar las tecnologías más efectivas para la protección de datos médicos en infraestructuras críticas. Los resultados de esta revisión refuerzan la importancia de tecnologías como el aprendizaje profundo y la biometría multimodal, que mejoran la fiabilidad de los controles de acceso al igual que mantienen los datos seguros y en privado para intrusos, tal como se identificó en la introducción de este estudio. El presente estudio aporta de manera relevante al ámbito al resaltar la capacidad de la Inteligencia Artificial para identificar riesgos a través del análisis de patrones de comportamiento, lo cual resulta en una mejora de la seguridad en las infraestructuras de hospitales. Se proporciona una evaluación detallada de los enfoques más prometedores, lo cual constituye una base sólida para investigadores y desarrolladores interesados en el campo de la seguridad biométrica. En futuras investigaciones, se podría enfocar en la aplicación de dichas tecnologías en entornos menos desarrollados, como en naciones latinoamericanas, donde persiste un considerable potencial sin investigar. Sería de gran utilidad investigar nuevas estrategias para personalizar y hacer escalables estas soluciones, centrándose en la integración

efectiva de tecnologías de Inteligencia Artificial en sistemas hospitalarios a nivel mundial. Esta revisión no solo contribuye al avance del conocimiento actual sobre autenticación biométrica, sino que también propone nuevas orientaciones para el desarrollo tecnológico, lo cual facilita el progreso hacia un entorno hospitalario más seguro y eficiente.

Contribución de Autoría

Cesar Alexander Acuña Cisneros: [Conceptualización](#), [Investigación](#), [Metodología](#), [Análisis formal](#), [Validación](#), [Redacción - borrador original](#), [Curación de datos](#), [Escritura](#), [revisión y edición](#), [Visualización](#). Carlos Daniel Gutiérrez Sandoval: [Conceptualización](#), [Investigación](#), [Metodología](#), [Análisis formal](#), [Validación](#), [Visualización](#), [Redacción - borrador original](#), [Curación de datos](#), [Escritura](#), [revisión y edición](#). Alberto Carlos Mendoza de los Santos: [Redacción - borrador original](#), [Curación de datos](#), [Validación](#), [Visualización](#).

Referencias

- [1] A. Budžys, O. Kurasova, and V. Medvedev, “Deep learning-based authentication for insider threat detection in critical infrastructure,” *Artif. Intell. Rev.*, vol. 57, no. 10, August 2024.
- [2] C. Annadurai *et al.*, “Biometric authentication-based intrusion detection using artificial intelligence internet of things in smart city,” *Energies*, vol. 15, no. 19, p. 7430, October 2022.
- [3] W. Kim, J. M. Song, and K. R. Park, “Multimodal biometric recognition based on convolutional neural network by the fusion of finger-vein and finger shape using near-infrared (nir) camera sensor,” *Sensors*, vol. 18, no. 7, p. 2296, July 2018.
- [4] S. Aanjanadevi, S. Aanjankumar, K. R. Ramela, and V. Palanisamy, “Face attribute convolutional neural network system for data security with improved crypto biometrics,” *Comput. Syst. Sci. Eng.*, pp. 1–12, 2023.
- [5] M. J. Page *et al.*, “Declaración prisma 2020: una guía actualizada para la publicación de revisiones sistemáticas,” *Rev. Esp. Cardiol.*, vol. 74, no. 9, pp. 790–799, 2021.
- [6] W. G. B. Morales, “Análisis de prisma como metodología para revisión sistemática: Una aproximación general,” *Saúde em Redes*, vol. 8, no. sup1, pp. 339–360, 2022.
- [7] S. Sánchez-Serrano, I. Pedraza-Navarro, and M. Donoso-González, “¿cómo hacer una revisión sistemática siguiendo el protocolo prisma?: Usos y estrategias fundamentales para su aplicación en el ámbito educativo a través de un caso práctico,” *Bordón Rev. Pedagog.*, vol. 74, no. 3, pp. 51–66, 2022.

- [8] M. J. Page *et al.*, “Prisma 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews,” *BMJ*, vol. 372, p. n160, 2021.
- [9] C. Y. nez Baeza, R. A. Aguilera-Eguía, H. Fuentes-Barría, and A. Roco-Videla, “Importance of the prisma guideline,” *Nutr. Hosp.*, vol. 40, no. 3, pp. 670–675, 2023.
- [10] M. L. Rethlefsen *et al.*, “Prisma-s: An extension to the prisma statement for reporting literature searches in systematic reviews,” *Syst. Rev.*, vol. 10, no. 1, p. 39, 2021.
- [11] H. U. Khan, M. Z. Malik, S. Nazir, and F. Khan, “Utilizing bio metric system for enhancing cyber security in banking sector: A systematic analysis,” *IEEE Access*, p. 1, 2023.
- [12] L. Mainetti, P. Panarese, and R. Vergallo, “Wox+: A meta-model-driven approach to mine user habits and provide continuous authentication in the smart city,” *Sensors*, vol. 22, no. 18, p. 6980, September 2022.
- [13] B. Bordel, R. Alcarria, and T. Robles, “Lightweight encryption for short-range wireless biometric authentication systems in industry 4.0,” *Integr. Computer-Aided Eng.*, vol. 29, no. 2, pp. 153–173, March 2022.
- [14] A. S. A.-M. AL-Ghamdi and M. Ragab, “Artificial intelligence techniques based learner authentication in cybersecurity higher education institutions,” *Comput., Mater. Continua*, vol. 72, no. 2, pp. 3131–3144, 2022.
- [15] P. Maharjan *et al.*, “Keystroke dynamics based hybrid nanogenerators for biometric authentication and identification using artificial intelligence,” *Adv. Sci.*, vol. 8, no. 15, p. 2100711, June 2021.
- [16] P. Shivanna and S. S. Venkatesiah, “Biometric identification for a secured environment using ai-based facial recognition,” *Int. J. Saf. Secur. Eng.*, vol. 14, no. 1, pp. 185–190, February 2024.
- [17] G. Q. Mendoza, “Legislación, riesgos y retos de los sistemas biométricos,” *Rev. Chil. Derecho Tecnol.*, vol. 9, no. 1, p. 63, June 2020.
- [18] M. Elkhodr, S. Khan, and E. Gide, “A novel semantic iot middleware for secure data management: Blockchain and ai-driven context awareness,” *Future Internet*, vol. 16, no. 1, p. 22, January 2024.
- [19] R. O. Andrade *et al.*, “An exploratory study of cognitive sciences applied to cybersecurity,” *Electronics*, vol. 11, no. 11, p. 1692, May 2022.
- [20] S. Kumar *et al.*, “Face spoofing, age, gender and facial expression recognition using advance neural network architecture-based biometric system,” *Sensors*, vol. 22, no. 14, p. 5160, July 2022.

- [21] J. Herbst *et al.*, “Medical data in wireless body area networks: Device authentication techniques and threat mitigation strategies based on a token-based communication approach,” *Network*, vol. 4, no. 2, pp. 133–149, April 2024.
- [22] V.-D. Păvăloaia and G. Husac, “Tracking unauthorized access using machine learning and pca for face recognition developments,” *Information*, vol. 14, no. 1, p. 25, December 2022.
- [23] F. Ahamed *et al.*, “An intelligent multimodal biometric authentication model for personalised healthcare services,” *Future Internet*, vol. 14, no. 8, p. 222, July 2022.
- [24] K. Y. Najmi *et al.*, “A survey on security threats and countermeasures in iot to achieve users confidentiality and reliability,” *Mater. Today*, vol. 81, pp. 377–382, 2023.
- [25] A. Seyfizadeh *et al.*, “Enhancing security in brain-computer interface applications with deep learning: Electroencephalogram-based user identification,” *Expert Syst. Appl.*, vol. 253, p. 124218, 2024.
- [26] F. Wang, Y. Gai, and H. Zhang, “Blockchain user digital identity big data and information security process protection based on network trust,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 36, no. 4, p. 102031, 2024.
- [27] A. Levina *et al.*, “Towards a smart hospital: Smart infrastructure integration,” *J. Open Innov.*, vol. 10, no. 3, p. 100339, 2024.
- [28] O. Alruwaili *et al.*, “Securing the iot-enabled smart healthcare system: A puf-based resource-efficient authentication mechanism,” *Heliyon*, vol. 10, no. 18, p. e37577, 2024.
- [29] G. Lazrek *et al.*, “An rfe/ridge-ml/dl based anomaly intrusion detection approach for securing iomt system,” *Results Eng.*, vol. 23, p. 102659, 2024.
- [30] A. Jain and K. Tripathi, “Biometric signature authentication scheme with rnn (biosig_rnn) machine learning approach,” in *2018 3rd International Conference on Contemporary Computing and Informatics (IC3I)*, 2018, pp. 298–305.
- [31] T.-V. Le *et al.*, “A novel three-factor authentication protocol for multiple service providers in 6g-aided intelligent healthcare systems,” *IEEE Access*, vol. 10, pp. 28 975–28 990, 2022.
- [32] D. Mao, H. Liu, and W. Zhang, “An enhanced three-factor authentication scheme with dynamic verification for medical multimedia information systems,” *IEEE Access*, vol. 7, pp. 167 683–167 695, 2019.
- [33] A. Natarajan and N. Shanthi, “A survey on multimodal biometrics authentication and template protection,” in *2018 International Conference on Intelligent Computing and Communication for Smart World (I2C2SW)*, 2018, pp. 64–71.

- [34] T. Fu *et al.*, “Comparison of wrist and forearm emg for multi-day biometric authentication,” *Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, vol. 2023, pp. 1–4, 2023.
- [35] V. O. Nyangaresi, “Privacy preserving three-factor authentication protocol for secure message forwarding in wireless body area networks,” *Ad Hoc Netw.*, p. 103117, 2023.
- [36] N. Wan *et al.*, “Implantable qr code subcutaneous microchip using photoacoustic and ultrasound microscopy for secure and convenient individual identification and authentication,” *Photoacoustics*, vol. 31, p. 100504, 2023.
- [37] G. Guízar-Sahagún, I. Grijalva-Otero, and I. Madrazo-Navarro, “Fingerprints: origin, uses and challenges in the face of its verification failure,” *Rev. Med. Inst. Mex. Seguro Soc.*, vol. 59, no. 6, pp. 568–573, 2021.
- [38] M. Sawa, T. Inoue, and S. Manabe, “Biometric palm vein authentication of psychiatric patients for reducing in-hospital medication errors: a pre-post observational study,” *BMJ Open*, vol. 12, no. 4, p. e055107, 2022.
- [39] T. Singh, S. Zaka-Ur-Rab, and S. Arrin, “Effect of pupil dilation on biometric iris recognition systems for personal authentication,” *Indian J. Ophthalmol.*, vol. 71, no. 1, pp. 57–61, 2023.
- [40] D. Nigam *et al.*, “Biometric authentication for intelligent and privacy-preserving healthcare systems,” *J. Healthc. Eng.*, vol. 2023, p. 9821301, 2023.