Principales mecanismos de seguridad en base de datos: Una revisión sistemática

Main database security mechanisms: A systematic review

Gerson Aldair Pulache Quiroga [A], Juan Aurelio De La Cruz Gamarra [B] y Alberto Carlos Mendoza de los Santos[C]

Resumen— La seguridad de la información en las bases de datos es un elemento esencial que mantiene la confidencialidad y disponibilidad, especialmente en los últimos años, cuando las amenazas y vulnerabilidades se han incrementado debido a la constante evolución tecnológica. Esta investigación tiene como objetivos identificar y compilar los principales mecanismos de seguridad empleados en bases de datos, evaluando su efectividad y aplicabilidad en varios contextos organizacionales. Para ello, se realizó una revisión sistemática de literatura siguiendo la metodología PRISMA, lo que permitió asegurar un proceso de búsqueda, selección y análisis de información riguroso y transparente. Se establecieron criterios de inclusión y exclusión para considerar artículos publicados entre 2018 y 2025, con enfoque en contextos empresariales y académicos. Los resultados evidencian mecanismos clave como el control de acceso, cifrado de datos, auditoría, copias de seguridad y detección de intrusiones, resaltando sus fortalezas y limitaciones. Asimismo, se identificó que la combinación de medidas preventivas y reactivas es esencial para una protección integral. El principal aporte de este estudio es una nueva perspectiva que radica en ofrecer una visión actualizada y sistematizada que sirva como referencia para la implementar estrategias de seguridad más efectivas en sistemas de gestión de bases de datos

Palabras clave: bases de datos, cifrado de datos, control de acceso, seguridad de datos

C&T Riqchary

Revista de Investigación en Ciencia y Tecnología
ISSN: 2810-8124 (en línea) / ISSN: 2706-543x
Universidad Nacional Micaela Bastidas de Apurimac – Perú

Vol. 7 Núm. 1 (2025) - Publicado: 20/10/25 - Indexaciones
Número: doi.org/10.57166/riqchary/v7.n1.2025
Páginas: 82- 87 | Recibido 27/08/2025 ; Aceptado 28/09/2025

doi.org/10.57166/riqchary.v7.n2.2025.10

~~*Tenga en cuenta que en la primera entrega no debe figurar: nombres de autores, mails, filiaciones y ORCID.*~~

Autores:

A. ORCID iD https://orcid.org/0009-0008-2898-161X
Gerson Aldair Pulache Quiroga, Universidad Nacional de Trujillo, Pe. gpulacheq@unitru.edu.pe.

B. ORCID iD https://orcid.org/0009-0000-7322-2550
Juan Aurelio De La Cruz Gamarra, Universidad Nacional de Trujillo, Pe. t1053300821@unitru.edu.pe

C. ORCID iD https://orcid.org/0000-0002-0469-915X
Alberto Carlos Mendoza de los Santos, trabaja en el Departamento de Ingeniería de la Universidad Nacional de Trujillo, Pe. amendozad@unitru.edu.pe

Abstract— Information security in databases is essential for maintaining confidentiality and availability, especially in recent years, when threats and vulnerabilities have increased due to constant technological evolution. This research seeks to identify and compile the main security mechanisms used in databases, evaluating their effectiveness and applicability in various organizational contexts. To this end, a systematic literature review was conducted following the PRISMA methodology, which guaranteed a rigorous and transparent process of information search, selection, and analysis. Inclusion and exclusion criteria were determined to consider articles published between 2018 and 2025, with a focus on business and academic contexts. The results reveal key mechanisms such as access control, data encryption, auditing, backups, and intrusion detection, highlighting their strengths and limitations. Furthermore, the combination of preventive and reactive measures was identified as essential for comprehensive protection. The main contribution of this study is a new perspective that offers an updated and systematic view that serves as a reference for implementing more effective security strategies in database management systems.

Keywords: databases, data encryption, access control, data security

1. Introducción

Actualmente, las bases de datos son uno de los recursos más valiosos para cualquier organización, proteger los datos presentes en estas implica garantizar su disponibilidad, integridad y confidencialidad mediante la aplicación constante de diversos estándares y mecanismos de seguridad para evitar el daño por ataques maliciosos, ya que si bien el avance de la tecnología ha impulsado el desarrollo de herramientas que facilitan su gestión segura, también han aparecido métodos y programas maliciosos que buscan aprovechar vulnerabilidades para obtener acceso no autorizado, muchas empresas actualmente se enfrentan a desafíos importantes como la piratería de datos, la recopilación de datos y los ataques de denegación de servicio, debido a esto se debe analizar la forma de mitigar riesgos y amenazas para intentar solucionar los problemas de seguridad. [1]

Las organizaciones deben implementar diversos mecanismos para proteger sus datos ya que las violaciones de seguridad aparte de pérdidas económicas generan daños en la reputación y sanciones legales [2].

En la seguridad en bases de datos, intervienen tres niveles que deben integrarse: primero, los controles físicos, como el respaldo seguro e infraestructura protegida, que fortalecen la seguridad ante intrusiones físicas o desastres; segundo, los controles lógicos, que incluyen autenticación, control de acceso y cifrado para prevenir el acceso no autorizado [3]; y tercero, los controles administrativos, como lo son los procedimientos estructurados y capacitación al personal para garantizar una gestión más responsable [4]. En conjunto, estos niveles brindan una defensa integral: ningún mecanismo aislado puede garantizar la seguridad total.

Este artículo da a conocer estos mecanismos de seguridad presentes en los tres niveles mencionados anteriormente para la protección de base de datos para que las organizaciones puedan usarlos y combinar tecnologías avanzadas y políticas rigurosas, ya que ningún algoritmo de cifrado garantiza por sí solo la seguridad al 100% [5] .

El presente artículo realiza una revisión sistemática, con el objetivo principal de dar a conocer los principales mecanismos de seguridad en bases de datos, utilizando la metodología PRISMA para garantizar rigurosidad y transparencia en el proceso de revisión. Para lograr el objetivo general, se proponen los siguientes objetivos específicos:

- Sistematizar los mecanismos de seguridad presentes en la revisión de la literatura entre los años (2018 - 2025)
- Brindar recomendaciones para futuras investigaciones que aborde la seguridad en bases de datos

Finalmente, la pregunta de este artículo es:

¿Cuáles son los principales mecanismos de seguridad en bases de datos?

2. Metodología

El presente artículo de revisión optó por seguir la metodología PRISMA, la cual proporciona un marco riguroso para realizar revisiones sistemáticas y garantiza transparencia y exhaustividad en la selección y evaluación de la literatura científica.

PRISMA define un proceso claro de revisión, desde que se formula la pregunta de investigación hasta la selección final de estudios, esto es importante en este estudio ya que nos permitirá identificar correctamente los factores relacionados con los principales mecanismos de seguridad en base de datos

A través del uso del diagrama de flujo PRISMA, se muestran las etapas de identificación, elegibilidad, cribado e inclusión de estudios, para comprender el proceso que se sigue. Asimismo, la metodología PRISMA fue complementada con criterios de inclusión y exclusión, y con estrategias de búsqueda en bases de datos académicas, con el fin de obtener una muestra de estudios representativa.

2.1. Criterios de legibilidad

Una vez obtenida la recolección de artículos, se aplicaron ciertos criterios de inclusión y exclusión para asegurar que los resultados obtenidos sean acordes al objetivo de estudio. Entre los criterios de inclusión se consideraron los siguientes: artículos publicados entre 2018 y 2025, con acceso completo al texto y publicados en revistas científicas indexadas.

2.2. Fuentes de información

Para el estudio realizado se consultó en diferentes buscadores, la cantidad de investigaciones que se encontraron por buscador se resumen en la siguiente tabla.

TABLA 1
Cantidad de Artículos Encontrados por Buscador, sin Criterios de Inclusión y Exclusión

Buscadores	Fecha de búsqueda	Cantidad
SCOPUS	07/08/2025	3
RESEARCHGATE	07/08/2025	4
SCienceDirect	07/08/2025	6
SCielo	09/08/2025	15
Google Académico	09/08/2025	26
Dialnet	09/08/2025	33
Total		87

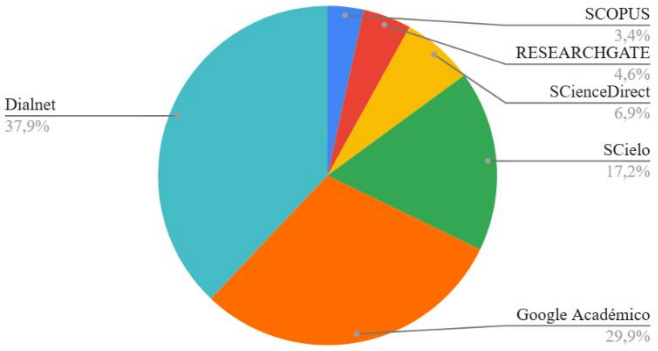

Fig. 1 Porcentaje de cantidad de artículos encontrados por buscador

2.3. Estrategia de búsqueda

Para identificar estudios relevantes relacionados con los principales mecanismos de seguridad en bases de datos, se realizó una revisión sistemática en las bases de datos académicas y bibliotecas virtuales seleccionadas (Scopus, IEEE Xplore, ACM Digital Library, ScienceDirect y Redalyc, SCielo, Google académico, Researchgate). Durante el proceso de búsqueda, se emplearon diferentes ecuaciones con términos clave en español e inglés, a fin de ampliar el alcance y asegurar la inclusión de literatura tanto nacional como internacional. Las ecuaciones de búsqueda utilizadas fueron las siguientes:

"database security" AND "mechanisms"
"seguridad en bases de datos" AND "mecanismos"
("data protection" OR "database protection") AND ("security techniques")
"mecanismos de seguridad" AND "bases de datos"
"database security" AND ("encryption" OR "access control" OR "auditing")

2.4. Proceso de selección de los estudios

Tras la recopilación de los estudios provenientes de las bases de datos académicas seleccionadas, se procedió con el proceso de selección siguiendo las directrices del protocolo PRISMA. Esta metodología fue elegida por proporcionar un marco estandarizado y transparente para la identificación, selección y evaluación de estudios en revisiones sistemáticas, lo que garantiza mayor claridad, reproducibilidad y rigor metodológico.

Durante este proceso se aplicaron los criterios de inclusión y exclusión previamente definidos, y se revisaron de manera individual los títulos y resúmenes para descartar aquellos que no resultaban pertinentes. Finalmente, se realizó un análisis completo de los textos de los artículos que cumplían con la temática central del estudio.

El siguiente diagrama refleja cada paso del proceso de selección:

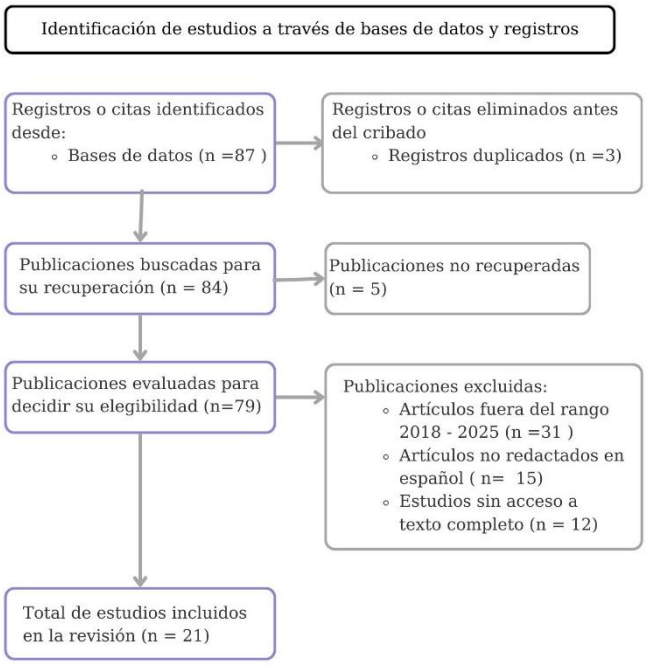

Fig. 2 Diagrama de flujo PRISMA 2020. Elaboración propia

TABLA 2
Cantidad de Artículos Encontrados por Buscador, con Criterios de Inclusión y Exclusión

Buscadores	Cantidad
SCOPUS	2
Google Académico	12
Dialnet	7
Total	21

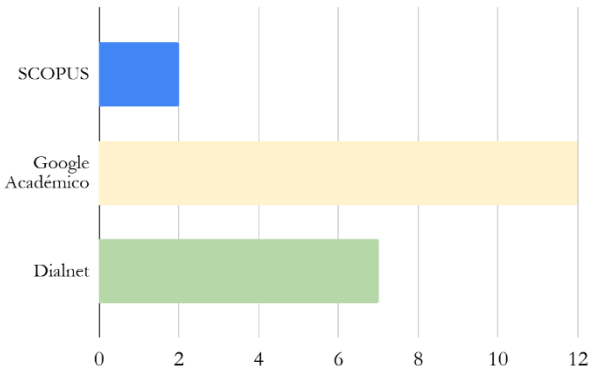

Fig. 3 Cantidad de estudios incluidos por Base de Datos para la revisión sistemática. Elaboración propia.

3. Resultados y Discusión

3.1 Resultados

TABLA 3
Recopilación y Resumen de Artículos Seleccionados

Título	Autor	Mecanismo
Mecanismos de seguridad para–Big Data basados en circuitos criptográficos [6]	I. Blokhin	Criptografía
Desarrollo de una solución informática para el análisis de datos del sistema de pagos de seguridad social para el sector financiero colombiano [7]	H. Fuquen, J. C. Salavarrieta, y F. Soto	Apache Cassandra
Propuesta de solución para la gestión de la seguridad informática de los datos personales del ciudadano [8]	A. Benitez Lavastida, H. Tamayo Ramos, y I. Barrientos Núñez	Sistema de gestión de seguridad informática basado en WSO2 Identity Server.
Biometría informática en la Ciberseguridad [9]	M. Benito Torrado	Biometría
Tecnologías y protección de datos en las administraciones públicas Seguridad y protección de datos [10]	J. Díaz	Tokenización
Análisis de los sistemas centralizados de seguridad informática a través de la herramienta Alienvault Ossim [11]	E. C. Ferruzola Gómez, O. X. Bermeo Almeida, y L. M. Arévalo Gamboa	Sistema SIEM
Mecanismos de seguridad de la información en una organización: una revisión sistemática [12]	J. Marreros, D. Acosta, y A. Mendoza	Políticas y capacitación en ciberseguridad
Análisis de Protocolos Transport Layer Security y Secure Socket Layer como mecanismos de seguridad y competitividad en las organizaciones digitales [13]	A. Flores-Vargas y M. Llerena	Autenticación multifactor (MFA)
Un modelo seguro y escalable basado en blockchain para la gestión de registros médicos electrónicos [14]	K. Pampattiwar y P. Chavan	Blockchain
Método de Compartir Seguridad de la Universidad Recursos de Educación Ideológica y Política Basados en Internet de las Cosas [15]	C. Liu y Z. Li	Doble cifrado
Tecnologías de Seguridad en Bases de Datos: Revisión Sistemática [16]	A. Sánchez, M. Jazmín	Cifrado, control de acceso, auditorías, parcheo de vulnerabilidades.
Modelo de red segura en un entorno distribuido para la transferencia de datos con mecanismos básicos de seguridad [17]	C. O. Sánchez Guzmán	Autenticación, auditoría, firewall, encriptación, respaldos de información
Control de acceso a un centro de datos usando tres mecanismos de seguridad [18]	J. I. Vega Luna , M. A. Lagos Acosta, F. J. Sánchez Rangel, J. F. Cosme Aceves, G. Salgado Guzmán.	Reconocimiento facial, huella dactilar, código o clave de acceso
Seguridad en base de datos [19]	C. S. Balcázar Molina, M. I. Ortiz López	Control de acceso, cifrado, backups, auditorías, escaneo de vulnerabilidades, controles administrativos.
Protección de datos y seguridad de la información [2]	I. González Hernández	Cifrado de datos, seudonimización, evaluaciones de impacto, notificaciones
Implementación de técnicas de encriptación en la seguridad de las bases de datos [5]	J. M. Bernal Ontivero, F. Z. Briones, M. P. Reyes, N. R. Rosales Morales,V. Farías Veloz	Cifrado de datos, control de acceso, protocolos de seguridad, criptografía asimétrica
Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe [20]	Banco Interamericano de Desarrollo (BID) y Organización de los Estados Americanos (OEA)	Cifrado y enmascaramiento, control de acceso, auditoría y trazabilidad, protección contra errores humanos.
Hyperledger Blockchain para la seguridad en bases de datos un mapeo sistemático [21]	G. Villalta, M. Gerardo	Inmutabilidad, consenso autorizado, smart contracts
Propuesta de Arquitectura de Seguridad por Diseño para Protección de Datos Personales en Entidades Públicas [22]	López Sevilla, Galo Mauricio	Cifrado, autenticación, auditoría y trazabilidad.
Análisis de Seguridad de Bases de Datos: Estrategias para la Protección de Datos [23]	M. A. Samamé Uceda, P. L. Varas Zurita, A. C. Mendoza De Los Santos	Encriptación, sistemas de seguridad de bases de datos en la nube, middleware, modelos de control

		de acceso.
Mejores Prácticas de Auditoría de Bases de Datos [24]	J. Tapia	Triggers, Vistas de administración dinámic. auditoría C2,Change data capture.

A continuación, se muestra una matriz comparativa de efectividad en donde se muestran los principales mecanismos de seguridad en base de datos

TABLA 4
Matriz de evaluación comparativa de efectividad

Mecanismo	Nivel	Complejidad	Costo Relativo	Impacto en Rendimiento	Frecuencia de Uso (%)
Cifrado	Alto	Media	Medio	Bajo-Medio	85%
MFA	Alto	Baja	Bajo	Mínimo	71%
Control de Acceso	Medio-Alto	Media	Bajo-Medio	Mínimo	90%
Auditoría/SIEM	Medio	Alta	Alto	Medio	52%
Blockchain	Muy Alto	Muy Alta	Muy Alto	Alto	14%
Biometría	Alto	Media-Alta	Alto	Bajo	33%

Después de analizar los 21 artículos recopilados, se identificaron los principales mecanismos de seguridad utilizados para proteger las bases de datos en organizaciones, destacando su importancia para garantizar la confidencialidad, integridad y disponibilidad de la información.

La recopilación sistemática identificó 18 mecanismos diferenciados de seguridad. Los mecanismos más documentados incluyen implementaciones de circuitos criptográficos [6], sistemas Apache Casandra para la alta disponibilidad [7], y las plataformas WSO2 Identity Server para gestión unificada de identidades [8]

También se identificaron 7 variantes criptográficas distintas que van desde implementaciones comunes, hasta enfoques que van a la vanguardia como el doble cifrado para recursos educativos IoT [15] y criptografía asimétrica aplicada en protocolos de seguridad específicos [2]. Las implementaciones documentadas abarcan desde seudonimización hasta enmascaramiento de datos [20]

Se encontraron 5 modalidades de verificación como lo son los sistemas biométricos tradicionales [9], reconocimiento facial combinado con análisis de huellas dactilares [18], códigos de acceso multicapa, e implementaciones de tokens físicos y digitales [10].

3.2. Discución

Según nuestros resultados, una de los mecanismos más importantes para mantener seguras las bases de datos es, sin duda, el cifrado de la información. El Instituto Nacional de Estándares y Tecnología (NIST) señala que emplear normas como AES-256 y TLS resulta crucial para asegurar la privacidad de los datos y evitar que personas no autorizadas puedan acceder a ellos. [25]

Otros de los mecanismos son el control de acceso que junto con la autenticación multifactor (MFA) son muy efectivas. Un estudio de Microsoft Research mostró que más del 99,99 % de las cuentas con MFA se mantienen seguras y que gracias a ese mecanismo se reduce el riesgo de compromiso en un 99,22 %, este estudio respalda la inclusión de la MFA como una parte fundamental en la seguridad. [26]

Microsoft también señala que la autenticación multifactor puede detener más del 99,2 % de los intentos de acceso no autorizado a cuentas, lo que la hace clave para la protección de los datos en las empresas. No obstante, también se menciona que tácticas como la fatiga de MFA son cada vez más comunes, ya que algunos usuarios dan el visto bueno a solicitudes de acceso sin comprobar si son legítimas o no. [27]

La auditoría y trazabilidad también son mecanismos importantes para detectar incidentes y proteger los datos, este artículo menciona herramientas como SIEM la cual ayuda a las organizaciones a detectar y responder a amenazas en tiempo real, sin embargo, para que sea totalmente efectiva depende de ciertas configuraciones y de la capacitación del personal para que entiendan los registros y sepan distinguir entre alertas legítimas y falsos positivos. [28]

La concentración geográfica en países latinoamericanos (Colombia, Perú, México y Ecuador) refleja el creciente interés regional por fortalecer la seguridad en bases de datos, evidenciando un contexto particular de adopción tecnológica que puede servir como modelo para otras regiones en desarrollo con características similares

Este artículo muestra que no existe solo un mecanismo que sea capaz de garantizar la seguridad total, lo ideal es combinar los diferentes mecanismos ya mencionados para reducir el riesgo y aumentar la seguridad en base de datos.

4. Conclusiones

Los mecanismos de seguridad en bases de datos representan una necesidad fundamental y demostrada para las organizaciones contemporáneas, al permitirles proteger su información crítica, cumplir con regulaciones y mantener su competitividad en entornos digitales. Esta revisión sistemática permitió identificar los principales mecanismos de seguridad empleados, así como sus fortalezas y limitaciones en diferentes contextos organizacionales.

La recopilación confirma la obsolescencia de enfoques basados en mecanismos únicos, estableciendo como estándar la implementación de arquitecturas defensivas multicapa que integran controles técnicos, administrativos y físicos.

Las organizaciones exitosas comparten características específicas: liderazgo técnico especializado, presupuestos dedicados y programas de capacitación integral que abarcan desde usuarios finales hasta nivel ejecutivo. Estas organiza-

ciones demuestran capacidad de adaptación tecnológica y resiliencia ante amenazas emergentes, fortaleciendo la confianza de clientes y socios comerciales.

Finalmente, esta revisión sistemática crea una base para futuras investigaciones que estén en busca de evaluar la efectividad de estos mecanismos. Asimismo, se sugiere la revisión de metodologías de evaluación de riesgos y estrategias graduales para la adopción de las medidas de seguridad más eficaces, de tal manera que el proceso transversal de implementación de medidas de seguridad más efectivas sea evidente en el contexto de la empresa u organización.

Referencias

[1] S. U. Khan, M. Niazi y M. Humayun, «Advancing database security: a comprehensive systematic mapping study of potential challenges,» Wireless Networks, 2023.

[2] I. González Hernández, Protección de datos y seguridad de la información, 2023.

[3] A. K. Youssef Sayed Mohamed, D. Auer, D. Hofer y J. Küng, «A systematic literature review of authorization and access control requirements and current state of the art for different database models,» International Journal of Web Information Systems, 2024.

[4] D. Sargiotis, «Data Governance Policies and Standards: Development and Implementation,» de Data Governance, Springer, Cham, 2024. https://doi.org/10.1007/978-3-031-67268-2

[5] J. M. Bernal Ontivero, F. Zorrilla Briones, M. Palacios Reyes, N. R. Rosales Morales y V. Farías Veloz, Implementación de técnicas de encriptación en la seguridad de las bases de datos, 2023. https://doi.org/10.61117/ipsumtec.v6i7.247

[6] I. Blokhin, «Mecanismos de seguridad para Big Data basados en circuitos criptográficos,» 2020.

[7] H. Fuquen, J. C. Salavarrieta y F. Soto, «Desarrollo de una solución informática para el análisis de datos del sistema de pagos de seguridad social para el sector financiero colombiano,» 2020.

[8] A. Benitez Lavastida, H. Tamayo Ramos y I. Barrientos Núñez, «Propuesta de solución para la gestión de la seguridad informática de los datos personales del ciudadano,» 2021.

[9] M. Benito Torrado, «Biometría informática en la Ciberseguridad,» 2023.

[10] J. Diaz, «Tecnologías y protección de datos en las administraciones públicas Seguridad y protección de datos,» 2021.

[11] E. C. Ferruzola Gómez, O. X. Bermeo Almeida y L. M. Arévalo Gamboa, «Análisis de los sistemas centralizados de seguridad informática a través de la herramienta Alienvault Ossim,» 2022. https://doi.org/10.46480/esj.6.1.181

[12] J. Marreros, D. Acosta y A. Mendoza, «Mecanismos de seguridad de la información en una organización: una revisión sistemática,» 2024. https://doi.org/10.54943/ricci.v4i1.384

[13] A. Flores y M. Llerena, «Análisis de Protocolos Transport Layer Security y Secure Socket Layer como mecanismos de seguridad y competitividad en las organizaciones digitales,» 2024.

[14] K. Pampattiwar y P. Chavan, «Un modelo seguro y escalable basado en blockchain para la gestión de historiales médicos electrónicos,» 2025.

[15] C. Liu y Z. Li, «Método de Compartir Seguridad de la Universidad Recursos de Educación Ideológica y Política Basados en Internet de las Cosas,» 2025.

[16] M. J. Aguirre Sánchez, Tecnologías de Seguridad en Bases de Datos: Revisión Sistemática, 2021.

[17] C. O. Sánchez Guzmán, Modelo de red segura en un entorno distribuido para la transferencia de datos con mecanismos básicos de seguridad, 2021.

[18] J. I. Vega Luna, M. A. Lagos Acosta, F. J. Sánchez Rangel, J. F. Cosme Aceves y G. Salgado Guzmán, Control de acceso a un centro de datos usando tres mecanismos de seguridad, 2018.

[19] C. S. Balcázar Molina y M. I. Ortiz López, Seguridad en bases de datos.

[20] Banco Interamericano de Desarrollo (BID) y Organización de los Estados Americanos (OEA), Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe, Banco Interamericano de Desarrollo, 2020.

[21] M. G. Guaman Villalta, Hyperledger Blockchain para la seguridad en bases de datos un mapeo sistemático, 2021.

[22] G. M. López-Sevilla, Propuesta de Arquitectura de Seguridad por Diseño para Protección de Datos Personales en Entidades Públicas, 2024.

[23] M. A. Samamé Uceda, P. L. Varas Zurita y A. C. Mendoza De Los Santos, Análisis de Seguridad de Bases de Datos: Estrategias para la Protección de Datos, 2024. https://doi.org/10.26495/kz3kyz70

[24] J. Tapia, Mejores Prácticas de Auditoría de Bases de Datos, 2022.

[25] E. B. Barker, «Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms,» NIST, 2020. https://doi.org/10.6028/NIST.SP.800-175Br1

[26] L. A. Meyer, S. Romero, G. Bertoli, T. Burt, A. Weinert y J. Lavista Ferres, «How effective is multifactor authentication at deterring cyberattacks?,» 2023.

[27] Microsoft, «Mandatory Multi-Factor Authentication,» 08 05 2025. [En línea]. Available: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mandatory-multifactor-authentication. [Último acceso: 11 08 2025].

[28] Splunk, «SIEM: Security Information & Event Management Explained,» 2025. [En línea]. Available: https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html. [Último acceso: 11 08 2025].