Análisis de Seguridad de Bases de Datos: Estrategias para la Protección de Datos

Database Security Analysis: Strategies For Data Protection

Marcelo Alejandro Samamé Uceda [1]
Piero Lenin Varas Zurita[2]
Alberto Carlos Mendoza De Los Santos[3]

DOI: *https://doi.org/10.26495/kz3kyz70*

Resumen:

Una intrusión o ataque es un riesgo importante que desencadena en una violación de la confidencialidad de la informacion en una base de datos. Es por ello, que la existencia y aplicación de estrategias son esenciales para evitar estas amenazas. La presente investigación tiene como fin principal, el identificar las principales estrategias de seguridad frente a vulnerabilidades en bases de datos, que se han utilizado en la literatura existente y conocer los resultados obtenidos a partir de sus implementaciones. Esta indagación emplea enfoques exploratorios y descriptivos, que involucran un análisis exhaustivo de la literatura. Se examinaron 14 documentos, en el que se muestran como principales estrategias a: Encriptación, Sistemas de Seguridad para Base de Datos en la Nube, herramientas como Middlewares para los sitios web y también los famosos Modelos de Control de accesos. Ratificando en las conclusiones, la importancia de la aplicación de estas distintas técnicas para la preservación de los datos e información.

Palabras Clave: Seguridad en base de datos, protección de datos, prevención de intrusiones, vulnerabilidad, ciberseguridad

Abstract: An intrusion or attack is a significant risk that triggers a violation of the confidentiality of information in a database. This is why the existence and application of strategies are essential to avoid these threats. The main purpose of this research is to identify the main security strategies against vulnerabilities in databases, which have been used in the existing literature and to know the results obtained from their implementations. This inquiry employs exploratory and descriptive approaches, involving an exhaustive analysis of the literature. 14 documents were examined, in which the main strategies are shown as: Encryption, Security Systems for Databases in the Cloud, tools such as Middleware for websites and also the famous Access Control Models. Ratifying in the conclusions, the importance of the application of these different techniques for the preservation of data and information.

Keywords: Database security, data protection, intrusion prevention, vulnerability, cybersecurity

[1] *Universidad Nacional de Trujillo, t023300320@unitru.edu.pe*
[2] *Universidad Nacional de Trujillo, t023300120@unitru.edu.pe*
[3] *Universidad Nacional de Trujillo, amendozad@unitru.edu.pe*

1. Introducción

Actualmente, dentro de las organizaciones, la información es un activo sumamente valioso; ya que les permite una mejor toma de decisiones, el identificar oportunidades y amenazas para el negocio, entre otras herramientas.

La gestión y protección de la información es un proceso vital en la era digital actual. En este contexto, las bases de datos desempeñan un papel fundamental al servir como depósitos de datos críticos para organizaciones y particulares (Lapiedra et al., 2021). Sin embargo, con la creciente dependencia de las bases de datos, también ha aumentado la importancia de garantizar su seguridad.

Revisando a Avenia (2019), la definición de vulnerabilidad en un sistema informático se refiere a una debilidad o falla que puede ser explotada por un atacante para comprometer la seguridad de la información almacenada en ese sistema.

Las bases de datos son vulnerables a una serie de amenazas internas y externas, lo que puede comprometer la seguridad de la información almacenada en ellas. Estas comprenden, entre las más comunes: políticas débiles de auditoría de base de datos, privilegios excesivos, elevación de privilegios no autorizada, inyección de código malicioso y ataques de denegación de servicio.

Debido a que las bases de datos son accesibles a través de la red, cualquier amenaza a la seguridad de cualquier componente dentro o parte de la infraestructura de la red también es una amenaza para la base de datos. Además, cualquier ataque que afecte el dispositivo o la estación de trabajo de un usuario puede amenazar la base de datos. Por lo tanto, la seguridad de la base de datos debe extenderse mucho más allá de los límites de la base de datos por sí sola. (International Business Machines Corporation, 2023).

Un ataque a base de datos se refiere a cualquier intento de acceder, manipular o dañar información almacenada en una base de datos sin autorización. La gran mayoría de los datos sensibles del mundo están almacenados en sistemas gestores de bases de datos comerciales tales como Oracle, Microsoft SQL. Además, con la creciente adopción de la tecnología en la nube, es importante destacar que las bases de datos en la nube también son susceptibles a estos tipos de ataques. La información confidencial almacenada en bases de datos en la nube, como las proporcionadas por proveedores como Amazon Web Services (AWS), Microsoft Azure y Google Cloud, puede ser un objetivo para los ciberdelincuentes que buscan explotar vulnerabilidades y debilidades en la seguridad de estas plataformas.

Waqar (2020) nos manifiesta la idea de que la elección y aplicación de estrategias traen consigo ventajas como la protección de la información, mediante la implementación de medidas de seguridad como las autenticaciones. Además ayuda a mitigar riesgos y prevenir la reincidencia de este tipo de escenarios relacionados a la exposición de datos sensibles. En el ámbito legal, las organizaciones suelen estar sujetas a normativas que requieren la implementación de estas. Y como última ventaja, el ahorro referente a los costos que conllevan la recuperación de datos usurpados, perdidos y tergiversados.

Por lo tanto, es esencial comprender y aplicar estrategias efectivas de detección y prevención de intrusiones en el ámbito de las bases de datos para salvaguardar la información crítica en un entorno cada vez más digital y conectado. Debido a esto encontramos múltiples antecedentes de otras revisiones realizadas con el mismo objetivo en mente, identificar las estrategias de seguridad más comunes y eficientes en bases de datos.

Aguirre et al. (2021), por ejemplo, realizaron una revisión sistemática acerca de tecnologías de seguridad de base de datos, y obtuvieron como resultados 34 artículos de la base de datos IEEE. A partir de estos resultados lograron identificar protocolos y estrategias para la protección de información y concluyeron en la relevancia de estos.

Por otro lado, Machuca et al. (2022) realizaron una revisión sistemática para identificar las metodologías más usadas en seguridad de bases de datos, para lo que revisaron IEEE, ARXIV,

HINDAWI y DIALNET. Aplicando criterios de inclusión y exclusión obtuvieron 14 artículos como resultados y concluyeron que la metodología más usada es la de control de acceso con sus diferentes métodos propuestos como sistemas de autenticación y autenticaciones biométricas.

Siguiendo esta línea de investigación, esta revisión sistemática busca identificar las mejores estrategias de seguridad para la detección y prevención de intrusiones en una base de datos. Esta revisión está dividida en 4 segmentos: Metodología, Resultados, Discusión y Conclusiones, alrededor y con el propósito de responder a nuestra pregunta de investigación.

2. Metodología:

Para el trabajo investigativo, se optará por seguir el enfoque de la metodología de PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses). Esta metodología, publicada en 2009, se ha empleado en múltiples revisiones sistemáticas con el objetivo de documentar de manera transparente. Este proporciona una guía esencial mediante instrucciones y directrices ampliamente reconocidas en la comunidad académica para llevar a cabo revisiones sistemáticas de alta calidad. Al adherirnos a las pautas de PRISMA, se garantiza la exhaustividad y la calidad de la revisión lo cual facilitará la comprensión y la replicación de futuras investigaciones por parte de otros investigadores.

Esta metodología sigue un proceso claro y sistematizado, buscando reducir sesgos en la selección y síntesis de los estudios. Los pasos a seguir para la elaboración de una revisión sistemática según (Moreno et al., 2018) son: Planteamiento de la pregunta estructurada, búsqueda en base de datos, selección de artículos, extracción de datos, análisis críticos y estadísticos, y finalmente, la exposición de los resultados.

La fundamentación de esta metodología establece que una revisión sistemática es como una manera de evaluar e interpretar toda la investigación disponible en cuanto a una interrogante de investigación particular, en un área temática de interés (Kitchenham, 2004). Por lo que al desarrollar una revisión sistemática, es fundamental desarrollar una evaluación que siga cierto orden y a su vez contar con un análisis crítico de acuerdo a la evidencia obtenida.

Para este proceso, se planteó la siguiente pregunta de investigación: ¿Cuáles son las mejores estrategias y recomendaciones para la detección y prevención de intrusiones en las bases de datos? Recurrimos a la búsqueda de literatura existente, priorizando nuestra exploración en bases de datos como Scopus, Google Scholar, Dialnet y Redalyc.

2.1 Criterios de inclusión y exclusión

Los criterios de inclusión considerados fueron los siguientes: se incluyeron únicamente los escritos que fueran publicados entre 2018 y 2023. También, fueron considerados los encabezados que mencionan los siguientes términos: “Database Privacy”, “Database Security”, como se indica en la Figura 1. Asimismo, se buscaron artículos en español y en inglés para ampliar el alcance. Por otro lado, con respecto a los criterios de exclusión, se excluyeron fuentes como diapositivas o otros formatos similares, dada la poca certeza de su información.

2.2 Proceso de recolección de la información

Se puede observar en la **Tabla 01**, las combinaciones y cadenas de búsqueda, conformadas por las palabras claves que utilizamos para la recopilación de artículos en línea.

Tabla 01.

Terminología de búsqueda en las bases de datos.

Base de datos	Terminología de búsqueda
Base	database security OR database privacy year:[2018 TO 2023]
Scopus	TITLE-ABS-KEY (security AND database) AND (LIMIT-TO (SUBJAREA , "COMP") OR LIMIT-TO (SUBJAREA , "ENGI")) AND (LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (EXACTKEYWORD , "Database Systems") OR LIMIT-TO (EXACTKEYWORD , "Security Of Data"))
Google Scholar	databases, security strategies, year:[2018 TO 2023], kind of:[review articles]
Dialnet	Database security, database privacy, language:[Español y Inglés],year:[2018 A 2023],issue:[Technology and engineering]
IEEX Explore	"Security Databases" AND ("database security" OR "cybersecurity")

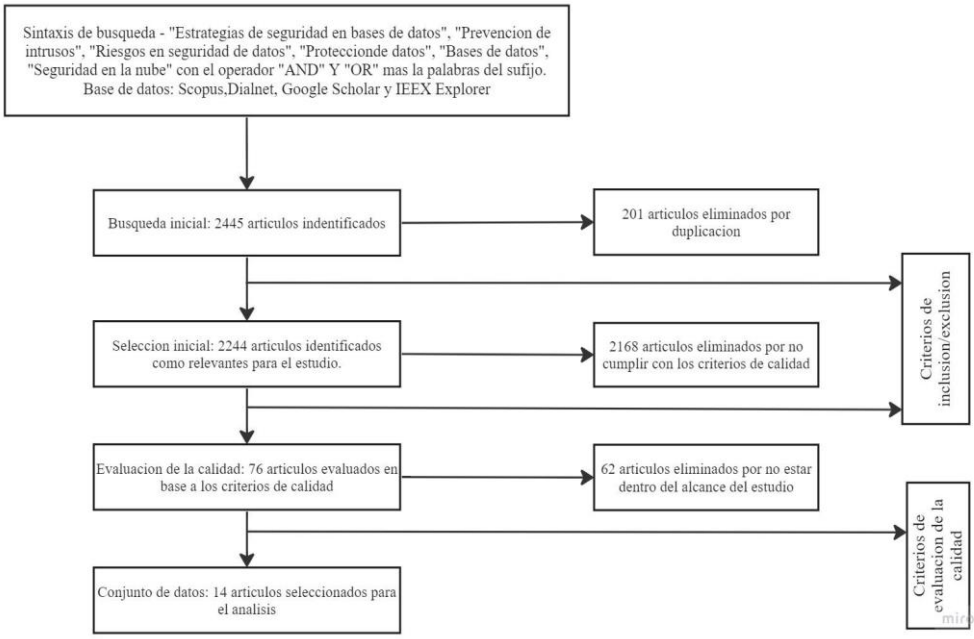
Fuente: Elaboración Propia.

3. Resultados

Para la realización del análisis acerca del tema de esta revisión, se obtuvieron 14 artículos, siguiendo las directrices de la metodología PRISMA.

Figura 1

Criterios de inclusión y exclusión.

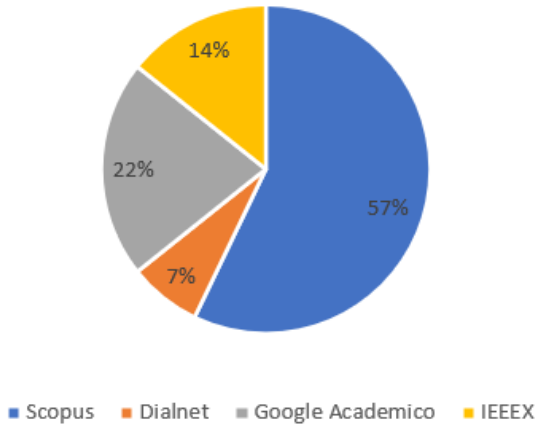


Nota. Elaboración propia.

La aplicación del filtrado mediante los distintos criterios de inclusión y exclusión, nos permitió seleccionar la literatura a analizar en esta investigación, teniendo como producto, la siguiente distribución de artículos recolectados por cada base de datos.

Figura 2

Proporción de artículos por Bases de Datos.

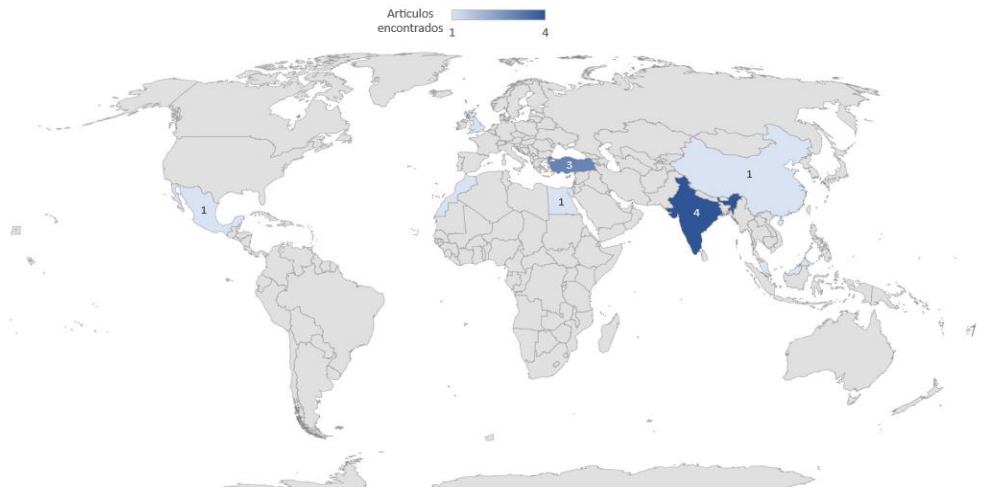


Nota. Elaboración propia

En esta sección, se mostrará un aspecto fundamental de las revisiones sistemáticas: el origen geográfico de los artículos seleccionados para nuestro estudio. A través de un gráfico, podremos obtener una visión panorámica de la contribución global a nuestra área de investigación. Siendo los países con mayor aportación: India y Turquía.

Figura 3

Distribución geográfica de los artículos encontrados



Nota. Elaboración propia.

Luego de haber realizado el análisis, en la **Tabla 02** se lista un resumen con los aportes de cada investigación.

Tabla 02

Análisis de los artículos académicos

N°	Título del Artículo	Aportes
1	"A New Scalable and Expandable Access Control Model for Distributed Database Systems in Data Security"	Propuesta de un modelo de control de acceso para bases de datos distribuidas, con aplicación en sectores educativos, públicos y de salud, logrando un 90% de aceptación.
2	"Database Security Threats and Challenges"	Identificación de amenazas externas e internas en bases de datos y medidas para combatirlas.
3	"Ensuring Data Security in Databases Using Format Preserving Encryption"	Introducción de un cifrado llamado FPE para preservar el formato de datos en bases de datos, superando deficiencias de esquemas existentes.
4	"Middleware para accesos a Bases de Datos a través de Web Services basados en el Modelo de Seguridad AXIS2"	Desarrollo de un middleware (MABDA) para accesos seguros a bases de datos remotas a través de Web Services basados en el modelo de seguridad AXIS2.
5	"SEC-NoSQL: Towards Implementing High Performance Security-as-a-Service for NoSQL Databases"	Propuesta de SEC-NoSQL, un sistema para ofrecer seguridad como servicio en bases de datos NoSQL, manteniendo alto rendimiento y escalabilidad.
6	"Using Blockchain in Cloud Computing to Enhance Relational Database Security"	Uso de tecnología Blockchain en la nube para mejorar la seguridad de bases de datos relacionales mediante autoverificación distribuida.
7	"A unique database synthesis technique for coverless data hiding"	Introducción de una técnica de ocultación de datos sin necesidad de una cubierta, mejorando la seguridad de bases de datos.
8	"Advancing database security: a comprehensive systematic mapping study of potential challenges"	Mapeo sistemático de 20 amenazas comunes a la seguridad de bases de datos, como fuga de datos y problemas de privacidad.
9	"A fully distributed secure approach using non deterministic encryption for database security in cloud"	Modelo de seguridad para bases de datos en la nube con cifrado no-determinístico y fragmentación vertical, garantizando seguridad y tiempo de consulta óptimo.
10	"Robust watermarking of databases in order-	Estrategia de protección de datos en bases de datos en

	preserving encrypted domain"	la nube mediante cifrado de preservación de orden y marcado de agua digital.
11	"Multi-Phase Algorithmic Framework to Prevent SQL Injection Attacks using Improved Machine learning and Deep learning to Enhance Database security in Real-time"	Framework multifase con machine learning y deep learning para prevenir inyecciones SQL y mejorar la seguridad de bases de datos en tiempo real.
12	"Multi-Level Security Model Developed to Provide Data Privacy in Distributed Database Systems"	Desarrollo de un modelo de control de acceso multinivel para bases de datos distribuidas, ofreciendo mayor seguridad y velocidad en la difusión de datos.
13	"Digital Watermarking Scheme for Securing Textual Database Using Histogram Shifting Model"	Técnica de histograma cambiante y marcado de agua digital para la seguridad de bases de datos textuales, resistente contra ataques de inserción.
14	"An Improved Framework for Biometric Database's Privacy"	Revisión de técnicas de biometría, propuesta de estructura para la privacidad de datos biométricos usando cifrado homomórfico completo, con implementación en Java.

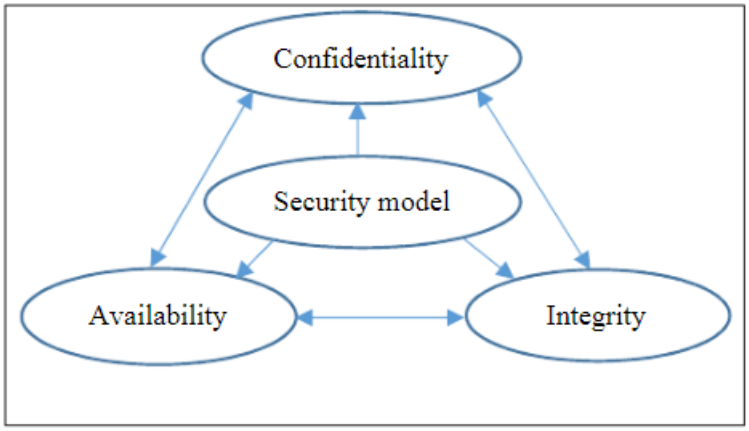
Fuente: Elaboración propia.

Ahora bien, podemos dividir la información en cuatro subtemas principales para facilitar su comprensión y análisis detallado. El primer subtema explorará las "Amenazas y Desafíos en Seguridad de Bases de Datos", examinando las distintas amenazas externas e internas que enfrentan los datos. El segundo se enfocará en los "Modelos de Control de Acceso", abarcando los enfoques innovadores propuestos para gestionar la verificación y autorización en sistemas de bases de datos distribuidos. El tercero se centrará en las "Tecnologías Emergentes y Enfoques Innovadores", destacando las estrategias novedosas, como el uso de Blockchain y técnicas de ocultación de datos, para mejorar la seguridad en bases de datos. Finalmente, el último abordará las "Estrategias Avanzadas de Protección y Prevención de Amenazas", incluyendo enfoques como el cifrado no-determinístico, la marca de agua digital y algoritmos de Machine Learning para prevenir amenazas específicas.

Amenazas y desafíos en Bases de Datos

Una amenaza en bases de datos se refiere a cualquier evento o acción potencial que pueda comprometer la seguridad, integridad o disponibilidad de la información almacenada en una base de datos. Estas amenazas pueden surgir tanto desde fuentes externas como internas y pueden incluir acciones maliciosas como ataques cibernéticos, intentos de robo de datos, intrusiones no autorizadas, entre otros. Es necesario su identificación para encontrar modelos de seguridad prevaleciendo el concepto de la tríada CIA en la información: Confiabilidad, Integridad y Disponibilidad. Evidenciando esa relación en la siguiente figura.

Figura 4
Concepto triada CIA



Nota. Adaptado de Mousa et. al. (2020).

La información obtenida nos brinda una visión integral de las preocupaciones de seguridad. Mousa et. al. (2020), destaca la importancia de reconocer amenazas externas, como ciberdelincuentes, y amenazas internas relacionadas con los activos humanos. Proporciona medidas para combatirlas, identificando las más comunes y delineando estrategias para su mitigación. En la misma línea, Iqbal et. al. (2023) identifica 20 desafíos distintos en la seguridad de bases de datos. Entre las amenazas recurrentes se encuentran la fuga de datos, problemas de privacidad, mal sistema de autenticación e intrusiones externas. Siendo específicos, la amenaza de inyecciones SQL, destacada por Ashlam et. al. (2022), es especialmente relevante. Las inyecciones SQL son ataques en los que los atacantes aprovechan vulnerabilidades en la entrada de datos para ejecutar comandos SQL no autorizados en una base de datos. Estos ataques pueden tener consecuencias graves, ya que los atacantes pueden manipular, borrar o agregar datos, comprometiendo la integridad de la información almacenada.

Modelos de Control de Acceso

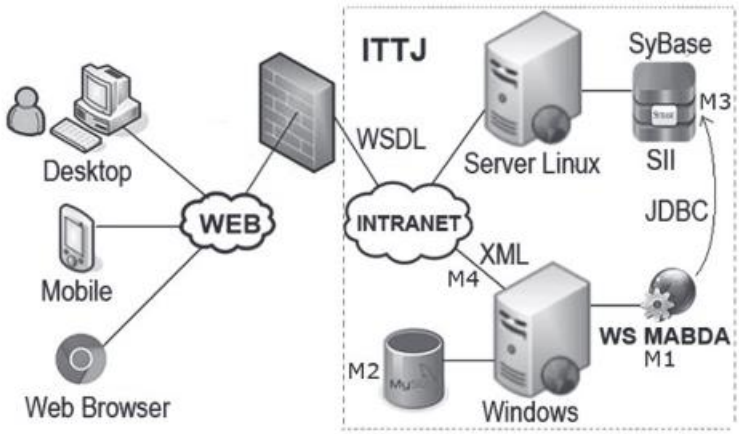
Los modelos de control de acceso son sistemas diseñados para gestionar y regular el acceso a recursos y datos en sistemas de información. Estos modelos son esenciales para garantizar la seguridad y la privacidad en entornos donde múltiples usuarios interactúan con sistemas y bases de datos.

Se observó nuevas propuestas como un modelo de control de acceso para sistemas de base de datos distribuidos. Este modelo se basa en conceptos como usuarios, objetos y dimensiones, asociando permisos de acceso a valores dimensionales y niveles de acceso. Guclu et. al. (2020), comenta que la aplicación del modelo en organizaciones educativas, públicas y de salud muestra una aceptación del 90%, superando modelos tradicionales como RBAC y MAC/DAC.

Elias et. al. (2018), propone el WS llamado MABDA con el objetivo de garantizar la seguridad de los datos. Esto se logra mediante la utilización del protocolo de seguridad Axis2, y autenticar las credenciales de los solicitantes en una base de usuarios previamente registrados. Al verificarse estas coincidencias se tiene acceso a la base almacenada en un servidor Linux, mediante una API JDBC y driver JDBC. Para tener una mejor visión de esta propuesta la figura 5 nos muestra los componentes y su interrelación.

Figura 5

Arquitectura general del Web Service MABDA.



Nota. Adaptado de Elías et. al. (2018).

Los autores estudiados destacan la importancia de evolucionar los modelos de control de acceso para hacer frente a desafíos contemporáneos. Desde la aplicación de conceptos innovadores como dimensiones y objetos hasta la implementación de servicios web seguros, se evidencia la necesidad de adaptarse a medida que las tecnologías y amenazas evolucionan.

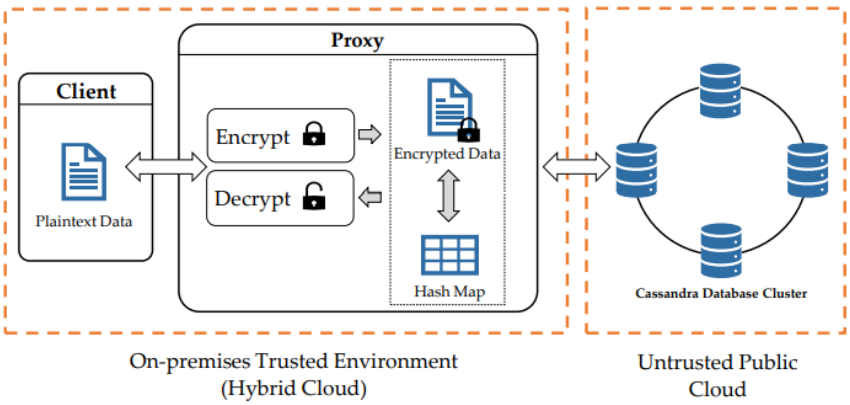
Tecnologías Emergentes y Enfoques Innovadores

En la constante evolución del panorama tecnológico, la seguridad de las bases de datos se ha vuelto una prioridad fundamental y los estudios revelan cómo las tecnologías emergentes y enfoques creativos están transformando la manera en que abordamos y aseguramos nuestras bases de datos en un mundo digital en constante cambio.

Samaraweera (2021), presenta el concepto de SEC-NoSQL, un sistema diseñado para ofrecer seguridad como servicio en bases de datos NoSQL. Este enfoque innovador permite la consulta de datos cifrados sin comprometer el rendimiento del sistema, demostrando su eficacia mediante la evaluación de su desempeño con una alta carga de clientes concurrentes. A continuación la figura 6, muestra la arquitectura básica y los elementos de su propuesta.

Figura 6

Arquitectura básica de SEC-NoSQL



Nota. Adaptado de Samaraweera (2021).

Blockchain es una tecnología de registro descentralizado y distribuido que utiliza criptografía para garantizar la seguridad e inmutabilidad de la información. Basándose en esto, Awadallah y Samsudin (2021) proponen un sistema de autoverificación que dispersa la base de datos entre diversos proveedores de servicios en la nube, aprovechando la inalterabilidad y transparencia inherentes a Blockchain para asegurar la integridad de los datos almacenados.

En una línea similar, Xiang et. al. (2022) presenta una estrategia para la protección de la privacidad y los derechos de autor en bases de datos en la nube. Su enfoque combina el cifrado de preservación de orden (OPES) con la tecnología de marcado de agua digital. Utiliza un histograma circular para agrupar y modificar datos de manera segura, proporcionando una capa adicional de seguridad que es resistente ante ataques comunes a las bases de datos.

Protección Avanzada y Prevención de Amenazas

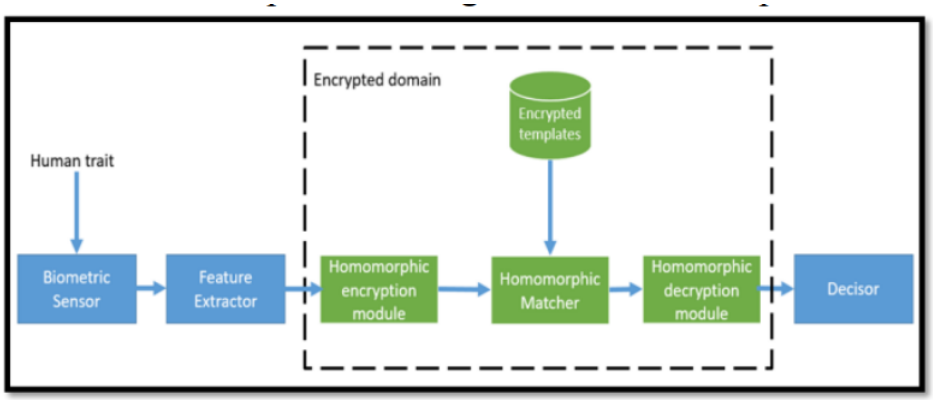
En el dinámico escenario de la gestión de datos, la protección avanzada y la prevención de amenazas en bases de datos emergen como elementos cruciales para salvaguardar la integridad y la privacidad de la información sensible. Este conjunto de artículos arroja luz sobre estrategias innovadoras diseñadas para elevar el nivel de seguridad en entornos de bases de datos.

Banothu et. al. (2022), propone un modelo innovador para la seguridad de bases de datos en la nube, haciendo uso de cifrado no-determinístico y homomórfico. Este modelo emplea el algoritmo AES-256-CBC para el cifrado de datos y la técnica de fragmentación vertical para su distribución, demostrando ser más seguro y eficiente en el tiempo de respuesta de las consultas.

Por otro lado, El-Yahyaoui y Omary (2021) realizaron una revisión extensiva de técnicas de biometría junto con una nueva estructura de privacidad basada en cifrado homomórfico completo. La implementación inicial de este modelo en Java demuestra su aplicación práctica y sus beneficios en la protección de datos biométricos.

Figura 7

Esquema descriptivo del uso de biometría en el cifrado



Nota. Adaptado de El-Yahyaoui y Omari (2021).

4. Discusión

Luego de analizar la literatura, notamos que frente a las distintas vulnerabilidades que existen tanto en bases de datos distribuidas como la de las plataformas en la nube, los autores proponen estrategias de prevención para promover la protección y confidencialidad. Tal como redactó Mousa et. al. (2020), lo primero es reconocer los tipos de amenazas que existen: las externas que suelen comprender los ataques de los ciberdelincuentes a los sistemas informáticos en las organizaciones. Y también las amenazas internas que principalmente están relacionadas con el manejo de la información a cargo del activo humano.

Es en este contexto que se consideró la investigación de Iqbal et. al. (2023), donde se analizan 100 artículos distintos con el objetivo de identificar las principales amenazas a la seguridad de bases de datos. Según dicho estudio, entre las más comunes amenazas se encuentran: "Problemas de privacidad", "Mala autenticación", "Intrusiones externas" y "Uso malicioso autorizado". Para cada una de estas amenazas se han encontrado distintas estrategias para disminuir su impacto en las bases de datos.

Algunas investigaciones proponen a la encriptación o cifrado como una herramienta vital para la seguridad y protección de datos. Como propone Gupta et. al. (2018), y la robusta propuesta de un nuevo tipo de cifrado para mantener la estructura de los datos, en busca de la integridad; que supera las limitaciones de esquemas ya existentes, en los cuales fue basado el mismo. Así también, se observa el caso de la investigación de Banothu et. al. (2022), la cual propone un algoritmo que emplea múltiples tipos de cifrado ya existentes para optimizar tanto tiempo de respuesta como la seguridad de los datos

De la misma forma, también encontramos aplicaciones de encriptación en otros contextos, Xiang et. al. (2022) propone un modelo que aplica Watermarking, o marcado de agua, para la protección de derechos de autor en una base de datos encriptada con un cifrado de preservación de orden (OPES), y El-Yahyaoui y Omary (2021) emplea el cifrado homomórfico en una base de datos biométricos. Debido a la frecuencia con la que observamos el uso de distintos cifrados para proveer seguridad a bases de datos de múltiples formas, es fácil concluir que este método, en todas sus versiones, es uno de los más populares en cuanto a protección de datos.

Existen también diseños de nuevos sistemas de seguridad. Samaraweera (2021), trabajando en la nube, creó un sistema donde se concentró en demostrar la eficiencia que este tiene para mantener un alto rendimiento y escalabilidad bajo las grandes cargas recurrentes que suceden en las transacciones en la red. En línea con esta investigación, Awadallah y Samsudin (2021) nos manifiesta al concepto de blockchain como una herramienta para la busca de transparencia en las transacciones de datos. Todo esto mediante un sistema de autoverificación, donde también trabaja con proveedores de servicios en la nube.

Otro tipo de seguridad menos tradicional pero de considerable popularidad para las bases de datos en la nube es el watermarking, el cual no busca hacer los datos inutilizables, sino que los marca para que cuando sean utilizados, siempre se pueda identificar al dueño de estos, protegiendo así los derechos de autor, un concepto que está cada vez más presente. Ejemplos de esto lo vemos en la investigación de Xiang et. al. (2022), el cual implementa la técnica de watermarking a modelos de seguridad ya existentes, generando una doble capa de seguridad.

Por otro lado, Elias et. al. (2018), mediante su trabajo, nos señala la importancia del concepto Middleware en los web services, donde prevalecen las técnicas de autenticación y autorización. Además de optimizar las consultas y transacciones, y administrar las conexiones con el fin de mejorar las aplicaciones en general.

Así también, observamos que los modelos de control de acceso son una frecuente estrategia de seguridad, la cual, a diferencia de otras ya mencionadas como el cifrado de datos, no consiste en disfrazar o esconder la información, sino más bien en tener un control más efectivo sobre quienes tienen acceso a ella, contribuyendo a su disponibilidad y confidencialidad, es por ello Guclu (2022), basó su modelo en la gestión de permisos donde estos están asociados a una puntuación brindada a las dimensiones, que es definir el alcance a ciertas funciones específicas, para poder calcular el nivel de acceso a cada usuario. Por otro lado, Guclu et. al. (2020) propone un modelo de control de acceso multinivel el cual demostró que, siguiendo el mismo principio de limitar accesos, provee un tiempo de respuesta más ágil e incluso más seguro que otros modelos tradicionales.

Finalmente, entre otros métodos de seguridad que aparecen menos frecuentemente encontramos estrategias como el uso de Machine Learning y Deep Learning por Ashlam et. al. (2022) para permitir a una base de datos detectar, clasificar y adaptarse a ataques de inyección sql en tiempo real, una implementación bastante creativa y que abre la puerta hacia todo un nuevo paradigma de protección. Así como también el trabajo de Majumder et. al. (2023), en el cual se observa la estrategia del Data Hiding y se busca contrarrestar una de sus principales desventajas.

5. Conclusiones

En conclusión, nuestra revisión sistemática destaca la importancia crítica de salvaguardar la integridad, confidencialidad y disponibilidad de los datos en un entorno cada vez más vulnerable a amenazas cibernéticas. Para lograr una protección efectiva, es esencial identificar y comprender las diversas amenazas, tanto internas como externas, que pueden comprometer la seguridad de la base de datos.

La encriptación y el cifrado se presentan como herramientas vitales para garantizar la confidencialidad de los datos almacenados, mientras que el control de acceso, ya sea a través de modelos multinivel o de sistemas de autenticación y autorización, contribuye a limitar quién puede acceder a la información y cómo se puede utilizar.

Además, las investigaciones están explorando nuevas vías de seguridad, como el uso de tecnologías emergentes como blockchain, machine learning y deep learning, que pueden detectar y mitigar amenazas en tiempo real. Asimismo, estrategias como el watermarking se aplican para proteger los derechos de autor en bases de datos encriptadas.

En resumen, la prevención de intrusiones en bases de datos es un campo en constante evolución que requiere una combinación de medidas técnicas y estratégicas para proteger eficazmente los datos críticos.

6. Referencias

Ashlam, A., Badii, A., & Stahl, F. (2022). Multi-phase algorithmic framework to prevent SQL injection attacks using improved machine learning and deep learning to enhance database security in real-time. Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/SIN56466.2022.9970504

Avenia, C. (2017). Fundamentos de la seguridad informática. Bogotá D.C., Fundación Universitaria del Área Andina.

Awadallah, R., & Samsudin, A. (2021). Using blockchain in cloud computing to enhance relational database security. Institute of Electrical and Electronics Engineers, 9, 137353-137366. https://doi.org/10.1109/ACCESS.2021.3117733

Banothu, S., Govardhan, A., & Madhavi, K. (2022). A fully distributed secure approach using non deterministic encryption for database security in cloud. Journal of Theoretical and Applied Information Technology, 100(7).

Elías, M., Gama, L., Torres, J. & Murguía, C. (2018). Middleware para acceso a bases de datos a través de web services basados en el modelo de seguridad AXIS2. Revista Gerencia Tecnológica Informática, 16(44), 17-24. https://revistas.uis.edu.co/index.php/revistagti/article/view/8073

El-Yahyaoui, A., & Omary, F. (2021). An improved framework for biometric Database's privacy. International Journal of Communication Networks and Information Security, 13(3), 499-510. https://doi.org/10.17762/ijcnis.v13i3.5143

Franco, J. & Coatrieux, G. (2017). Database Traceability by Means of Watermarking with Optimized Detection, 343-357. Lecture Notes in Computer Science. http://dx.doi.org/10.1007/978-3-319-53465-7_25

Guclu, M., Bakir, C., & Hakkoymaz, V. (2020). A new scalable and expandable access control model for distributed database systems in data security. Scientific Programming, 1-10.

Guclu, M. (2022). Multi-level security model developed to provide data privacy in distributed database systems. Hrčak - Portal de revistas científicas de la República de Croacia, 29(2), 369-378. https://doi.org/10.17559/TV-20200516084319

Gupta, S., Jain, S., & Agarwal, M. (2018). Ensuring data security in databases using format preserving encryption. Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/CONFLUENCE.2018.8442626

International Business Machines Corporation. (2023). Database Security. https://www.ibm.com/mx-es/topics/database-security

Iqbal, A., Khan, S., Niazi, M., Humayun, M., Sama, N., Khan, A., & Ahmad, A. (2023). Advancing database security: a comprehensive systematic mapping study of potential challenges. Wireless Networks, 1-28. https://doi.org/10.1007/s11276-023-03436-z

Lapiedra, R., Forés, B., Puig-Denia, A., & Martínez-Cháfer, L. (2021). Introducción a la gestión de sistemas de información en las empresas. Repositorio Universitat Jaume I. http://dx.doi.org/10.6035/Sapientia178

Majumder, A., Kundu, S., & Changder, S. (2023). A unique database synthesis technique for coverless data hiding. Journal of Visual Communication and Image Representation, 96, 103911. https://doi.org/10.1016/j.jvcir.2023.103911

Mousa, A., Karabatak, M., & Mustafa, T. (2020). Database security threats and challenges. Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/ISDFS49300.2020.9116436

Samaraweera, G., & Chang, J. (2021). SEC-NoSQL: Towards Implementing High Performance Security-as-a-Service for NoSQL Databases. Cornell University. https://doi.org/10.48550/arXiv.2107.01640

Waqar, A., Raza, A., Abbas, H., & Khan, M. K. (2020). A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata. Journal of Network and Computer Applications. https://doi.org/10.1016/j.jnca.2012.09.001

Xiang, S., Ruan, G., Li, H., & He, J. (2022). Robust watermarking of databases in order-preserving encrypted domain. Frontiers of Computer Science, 16, 1-9. https://doi.org/10.1007/s11704-020-0112-z

Moreno, B., Muñoz, M., Cuellar, J., Domancic, S., & Villanueva, J. (2018). Revisiones Sistemáticas: definición y nociones básicas. http://dx.doi.org/10.4067/S0719-01072018000300184

Aguirre, M., Plua-Moran, D., & Llerena-Izquierdo J (2021). Tecnologías de Seguridad en Bases de Datos: Revisión Sistemática. https://dspace.ups.edu.ec/handle/123456789/20566

Machuca, L., & Braul, R., (2022). Metodologías más usadas en la seguridad de bases de datos: una revisión de la literatura científica, 2016-2021. https://www.aulavirtualusmp.pe/ojs/index.php/rc/article/view/2218

Kitchenham, B. (2004). Procedures for performing systematic reviews. Keele, UK, Keele University, 33(2004), 1-26. https://www.researchgate.net/publication/228756057_Procedures_for_Performing_Systematic_Reviews