UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO DE SISTEMAS

CARRERA:

INGENIERÍA DE SISTEMAS

TEMA:

"TECNOLOGÍAS DE SEGURIDAD EN BASES DE DATOS: REVISIÓN SISTEMÁTICA"

AUTOR:

MAITTÉ JAZMÍN AGUIRRE SÁNCHEZ

TUTOR:

Msg. JOE LLERENA IZQUIERDO

Abril 2021

GUAYAQUIL-ECUADOR

DECLARATORIA DE RESPONSABILIDAD

Yo MAITTÉ JAZMÍN AGUIRRE SÁNCHEZ, declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del/los/las autor/es/as.

Maitté Aguirre

Nombre: Maitté Jazmín Aguirre Sánchez

Cédula: 0919418020

Fecha: Guayaquil, 29 de enero del 2021

Firma:
(Tutor): Ing. Joe Llerena Izquierdo, MSig.
C.I.: 0914884879

Tecnologías de Seguridad en Bases de Datos: Revisión Sistemática

Maitté Aguirre Sánchez [1][0000-0002-5076-8814], Daniel Plua-Moran [1][0000-0002-5848-2888]

and Joe Llerena-Izquierdo [1][0000-0001-9907-7048]

[1] Universidad Politécnica Salesiana, Guayaquil, Ecuador
maguirres@est.ups.edu.ec, jllerena@ups.edu.ec, dplua@ups.edu.ec

Resumen. El permanente crecimiento y el auge en las redes de internet y tecnologías permiten la obtención de miles de datos día con día, los cuales se almacenan en bases de datos con grandes capacidades, esto las pone en riesgo de sufrir ataques por ciberdelincuentes. Este trabajo tiene como objetivo identificar qué mecanismos de defensa existen para mantener la seguridad de los datos almacenados, se pretende efectuar un repaso de las tecnologías de seguridad usadas para mitigar los riesgos y amenazas para obtener un registro de los trabajos y estudios orientados a mantener la seguridad. Para el desarrollo se realizó una revisión sistemática de la base de datos IEEE. Los resultados obtenidos de un total de 34 artículos muestran la forma principal para garantizar que los datos estarán protegidos, tales como; herramientas, metodologías, protocolos, la mayor parte de los artículos son recientes por lo que se puede evidenciar que las tecnologías de seguridad son y seguirán siendo un importante tema de estudio para generaciones futuras.

Abstract. The permanent growth and boom in internet networks and technologies allow the obtaining of thousands of data every day, which are stored in databases with large capacities, this puts them at risk of being attacked by cybercriminals. This work aims to identify what defense mechanisms exist to maintain the security of stored data, it is intended to carry out a review of the security technologies used to mitigate risks and threats to obtain a record of the works and studies aimed at maintaining the security. For the development, a systematic review of the IEEE database was carried out. The results obtained from a total of 34 articles show the main way to guarantee that the data will be protected, such as tools, methodologies, protocols, most of the articles are recent, so it can be seen that security technologies are and will continue to be an important subject of study for future generations.

Palabras clave: Tecnologías de Seguridad, bases de datos, análisis de tecnologías, revisión sistemática.

1 Introducción

Las bases de datos existen desde la década de los 60s, siendo en esta época el comienzo de la red como la conocemos y la incursión de bases de datos con jerarquías. La seguridad de los sistemas a lo largo de estos casi 60 años posee de mucha atención, teniendo como avances los modelos de control de acceso, y en estos últimos años implementándose sistemas como el Big Data. Desde la década de los 2000, se implementan herramientas como la minería de datos conservando la privacidad y solucionando en gran parte problemas de ciberseguridad, a través de la localización y detención de intrusos y el estudio de malware. Y con la presencia del internet se pueden obtener cantidades gigantescas de datos, por esta razón se analiza cómo mitigar los riesgos y amenazas para ofrecer soluciones a problemas de seguridad presentes día con día [1].

El uso de una técnica de seguridad en cualquier base de datos es una fase importante que seguir para garantizar la protección de los datos almacenados y mitigar el daño por ataques maliciosos evitando la corrupción de estos. Así se logran identificar amenazas como: la pérdida de la integridad, la pérdida de disponibilidad, la pérdida de seguridad y privacidad. Que emergen debido a acciones involuntarias o intencionales llevadas a cabo por los atacantes cibernéticos con el objetivo de ocasionar un daño del contenido parcial o total y permitiendo la divulgación de la información, poniendo en riesgo al organismo afectado [2].

La información como video, texto o voz queda siempre por alguna razón exhibida a riesgos en las bases de datos en donde se almacenan, debido a ciertos problemas como privilegios excesivos, auditorías o sistemas de autenticación débiles, esto puede abrir una ventana permitiendo que se accedan a los datos sin autorización. La labor de cualquier tecnología de seguridad es preservar la integridad de los datos, incluyendo la encriptación de datos, gestión de claves, y de políticas de seguridad definidas por un modelo. Esto se puede conseguir con el control y la gestión de usuarios y procesos estratégicos. Los controles se rigen por un conjunto de reglas conocidas como reglas de seguridad, las cuales resguardan los requisitos de seguridad y detallan las propiedades que se suministran al sistema, también describen los protocolos a seguir para lograr la seguridad de datos, las tecnologías de seguridad se consideran como una herramienta necesaria para calcular y analizar estas políticas, ya que permiten probar la seguridad, la integridad y la consistencia del sistema de base de datos [3].

La problemática es que aun con la implementación de tecnologías de seguridad, los sistemas sufren ataques informáticos ya que presentan amenazas en sus infraestructuras y en la gestión de la seguridad. Las bases de datos son el corazón de cualquier institución puesto que aquí se almacenan los registros y toda la información valiosa de las empresas. Por ello pueden convertirse en el objetivo de los delincuentes cibernéticos, así mismo los profesionales trabajan constantemente para enfrentarlos y tratan de mantenerse actualizados sobre las nuevas tecnologías de seguridad para su posterior implementación. Las instituciones presentan cierto grado de dificultad para proteger la información en sus repositorios y esto se debe a la baja eficiencia de las tecnologías tradicionales para reconocer el tráfico hacia y desde la base de datos. Los ciberdelincuentes toman esta debilidad como una gran ventaja para ellos y lograr su cometido, el de robar información crítica, que también muchas veces queda expuesta por los propios usuarios

internos que tienen poco cuidado hacia sus propios equipos y herramientas de trabajo o que tienen acceso a información sin un control riguroso. Los administradores muy pocas veces cuentan con tecnologías y soluciones eficientes que permitan implementar una estrategia para asegurar la protección de la información, y no cumplen con todos los estándares regulatorios necesarios para garantizar la seguridad de los datos.

1.1 Trabajos Previos

El siglo XXI es liderado por 3 compañías en el mundo de las bases de datos; IBM, Oracle, Microsoft. Pero con la importancia del internet la compañía que genera una gran cantidad de información y que es almacenada en sus bases de datos y en la nube es Google.

A continuación, se presenta una búsqueda de Tecnologías de Seguridad que se abordó para identificar cuál es el estado del arte en Tecnologías de Seguridad para Bases de Datos.

Una investigación presentada en 2015 propone una nueva orientación del análisis de seguridad del flujo de información, en un contexto de sistemas de información, cuando las aplicaciones de bases de datos interactúan con bases de datos back-end. Analizando los desafíos como la expresividad de los lenguajes, la concurrencia en sistemas multiproceso o distribuidos y las transacciones de bases de datos [4].

Se analiza la importancia del cifrado de bases de datos llevando a cabo una revisión en profundidad de diversas técnicas de cifrado, comparándolas en función de sus méritos, para aumentar la seguridad en los datos almacenados, comparando y estudiando los distintos cifrados de bases de datos, investigación publicada en 2015 [5].

En este trabajo de 2017, se analizan las limitaciones presentes en la auditoría de bases de datos actuales y se propone un marco de seguridad para superar las limitaciones. El marco propuesto proporciona las funciones del sistema de auditoría, administra las estrategias de auditoría, audita los registros y da un informe estadístico, dando control en tiempo real y brindando un mejor desempeño [6].

Para esta investigación presentada en 2019 se propone un nuevo tipo de mecanismo de escaneo en la base de datos, capaz de corregir automáticamente el proceso de descubrimiento y corrección de vulnerabilidades, mejorando la disponibilidad y escalabilidad del código. Un administrador puede integrar scripts de penetración para varias vulnerabilidades en el sistema, y el sistema puede escanear en busca de vulnerabilidades y otorgar medidas de protección después de obtener los resultados [7].

Esta investigación de 2019 estudia la propuesta de un marco útil para ocultar información sensible, el marco es útil para identificar información sensible y favorecer la toma de decisiones y así poder definir reglas. Este marco explora la relación entre atributos sensibles en base a la orientación del atributo que permite tomar decisiones sobre los atributos necesarios para generar información sensible [8].

Qué factores afectan el rendimiento del servidor midiendo el tiempo de ejecución de las consultas es el objetivo de esta investigación, centrándose en combinaciones de consultas en una serie para diferentes configuraciones de conexión. Obteniendo una productividad creciente de 1,93%, pero para cuatro, disminuyó significativamente en 12,77%, investigación presentada en 2018 [9].

En este trabajo de 2015 se presenta un nuevo modelo capaz de acelerar el proceso de evaluación y recuperación de daños mediante un acceso mínimo al registro de datos. Ofreciendo técnicas de evaluación y recuperación de daños al realizar una recuperación rápida y eficiente de todos los elementos de datos dañados después de un ataque a la base de datos [10].

Los autores en esta investigación de 2016 sugirieron dos métodos para formar una base de datos centralizada; uno usando dos servidores de base de datos, uno como base de datos integrada y el otro como base de datos centralizada, y otro método usando un único servidor central conteniendo los datos de la organización de los recursos. Este trabajo proporciona un modelo centrado en la organización para obtener información sobre vulnerabilidades para varios productos de software en línea. Asegurando que este método ayuda a los administradores a descubrir vulnerabilidades y administrar parches de Seguridad [11].

La computación en la nube proporciona muchos recursos configurables donde se almacenan los datos. Se propone un esquema que distribuye la base de datos entre la nube de acuerdo y en relación con el nivel de seguridad que brindan los algoritmos de cifrado, investigación presentada en 2017 [12].

En este trabajo de 2018 se presenta un algoritmo que permite ejecutar un análisis de vulnerabilidad, a treves del análisis de modelos temáticos que permiten el procesamiento del lenguaje y realizar el análisis para establecer árboles de ataque [13].

La revisión sistemática está dividida en 5 apartados. El segundo apartado determina el protocolo de investigación definido para desarrollar la revisión. En el tercero se manifiestan los resultados. En el apartado cuatro se discuten los hallazgos principales y para finalizar, en el quinto apartado se exponen las conclusiones del trabajo presentado.

2 Materiales y Métodos

2.1 Metodología

Una revisión sistemática es una evaluación crítica y una síntesis de los estudios más relevantes sobre las tecnologías de seguridad en bases de datos.

Para el desarrollo de esta revisión se emplea el método deductivo y se aplica la investigación exploratoria en un enfoque cuantitativo para el análisis de los datos y la información en los trabajos seleccionados para ser revisados. De esta forma se presenta una referencia al estado actual de las tecnologías de seguridad para bases de datos. Los materiales y métodos empleados en esta revisión se basan en la búsqueda y lectura de los trabajos y artículos detallados en la referencia para un análisis de las tecnologías para mitigar los riesgos y amenazas en una base de datos.

2.2 Definición del Protocolo

Se ha realizado una revisión sistemática porque permite obtener una perspectiva amplia del campo científico y conocer el enfoque de los investigadores. Para llevar a cabo la revisión se siguieron tres etapas: Planificación, Ejecución y Presentación.

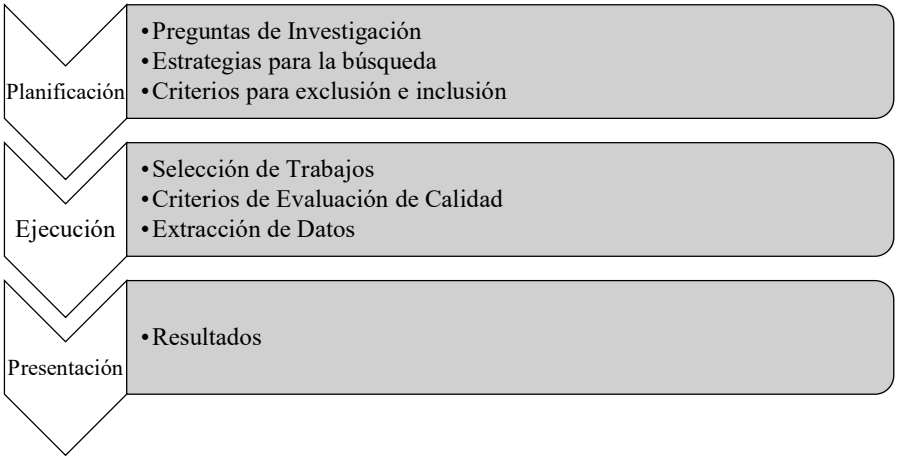

Fig. 1. Etapas de la revisión sistemática.

2.2.1 Planificación.

Para esta etapa se han definido los siguientes subapartados.

Preguntas de Investigación. El objetivo es observar el estado del arte de los estudios publicados orientados a la seguridad en las bases de datos para identificar posibles lagunas o escasez y sugerir nuevas áreas para investigación. Las preguntas se han definido en la tabla 1.

Table 1. Preguntas de Investigación.

Pregunta	Motivo
Q1. ¿Qué tipo de propuestas tecnológicas existen para mejorar la seguridad en bases de datos?	Determinar un número total de publicaciones en los últimos 5 años con relación a las tecnologías de seguridad orientadas a proteger las bases de datos
Q2. ¿Qué tipo de propuestas existen para proteger la información y mitigar los riesgos y amenazas en una base?	Identificar las tecnologías, estándares, estrategias o algoritmos que se implementan como instrumentos de seguridad para mitigar los riesgos y amenazas en bases de datos.
Q3. ¿Qué protocolos o estrategias se siguen para garantizar la seguridad en las bases de datos?	Comparar las diferentes tecnologías de seguridad en las bases de datos y concluir cuáles garantizan una mayor seguridad y protección de datos.

Estrategias para la búsqueda. Existen diversas bases de datos de publicaciones. Para este estudio nos centramos en la base de datos IEEE EXPLORE. El período de búsqueda incluye publicaciones de los últimos 5 años; 2015 hasta 2020. Para esta búsqueda se introdujo la siguiente cadena mostrada en la tabla 2.

Table 2. Cadena de búsqueda

Criterios	Términos de búsqueda	
Tecnologías de seguridad	"Security technologies"	AND
Seguridad en bases de datos	"Database Security"	
Protocolos de Seguridad	(Protocols OR methodology OR techniques OR tools)	

Para la identificación de los estudios potenciales y estudios primarios se aplicaron los siguientes filtros:

F1: Revisión de Resumen o Abstract.
F2: Revisión de Palabras claves o keywords.
F3: Lectura de publicaciones que pasaron los filtros anteriores.

Criterios de inclusión. Para la elección de estudios primarios se tendrán en cuenta los estudios publicados que cumplan con uno de los criterios de inclusión presentados a continuación:

- IC1: Publicaciones en inglés que traten temas sobre tecnologías de seguridad en ciencias de la computación y bases de datos.
- IC2: Estudios cualitativos y cuantitativos donde se propongan o evalúen metodologías, tecnologías o estrategias de seguridad.
- IC3: El estudio esta publicado en revistas o conferencias y se encuentran indexados.
- IC4: Las versiones completas de las publicaciones se pueden obtener a través de la suscripción de nuestra institución.

Criterios de exclusión. Para la revisión se omitirán estudios que cumplan con uno de los criterios de exclusión presentados a continuación:

- EC1: Se excluirán todos los estudios con un enfoque alejado a las tecnologías de seguridad en ciencias de la computación y bases de datos.
- EC2: Estudios que solo se puedan observar sus resumes.
- EC3: El estudio no está en inglés.
- EC4: La publicación no es la más reciente o no está en el periodo de tiempo definido anteriormente.

2.2.2. Ejecución

Para esta etapa se sigue el protocolo definido anteriormente con las siguientes etapas:

- Estudios Potenciales: Usando la base IEEE se aplican los criterios de búsqueda, teniendo un total de 92 artículos. Luego se aplicaron los filtros en los resúmenes y palabras claves.
- Estudios primarios: Aplicamos los criterios para exclusión e inclusión, quedando con 34 estudios primarios.
- Evaluación de calidad: Se ejecutará la evaluación de calidad y clasificación para cada uno de los estudios, con las posibles respuestas a las preguntas de investigación, definidas más adelante.

Selección de trabajos. Se presenta en la Tabla 3 un resumen con las revisiones elegidas que fueron 34 en total, señalando la metodología o estudio que se realizó enfocado a bases de datos, el tipo de propuestas que muestran como resultado, el número de artículos que seleccionaron los autores y su año de publicación.

Table 3. Resumen de la revisión sistemática de trabajos previos.

Ref.	Metodología o Estudio	Propuesta o Resultado	Año	Estudios Primarios
[14]	Protección Criptográfica	Evaluación de la búsqueda	2017	163
[15]	Estándares de seguridad	Evaluación de la madurez de las implementaciones de seguridad	2019	117
[16]	Blockchain	Revisión de la tecnología	2017	4
[17]	Seguridad y Calidad el Servicio	Modelo de evaluación	2016	43
[18]	Base de datos móviles	Educación practica	2017	3
[19]	Base de datos SQL	Mecanismo de control	2016	37
[20]	Mecanismo de salto	Prototipo de modelo de seguridad	2016	11
[21]	Privilegios a nivel de atributos	Jerarquía de funciones	2017	12
[22]	ISO / IEC 15408 e ISO / IEC 18045	Evaluación de seguridad	2017	12
[23]	Marca de agua reversible	Algoritmo de murciélago binario	2018	10
[24]	Bases de datos de e-commerce	Encriptación	2016	6
[25]	Cifrado	Método de cifrado AES	2018	22
[26]	Cifrado	Método de cifrado AES	2019	22
[27]	Principales bases de datos	Análisis de seguridad	2017	3
[28]	Seguridad de Big Data	Análisis en Big Data	2018	8

[29]	Base de datos de vulnerabilidades	Diseño de modelo de análisis	2015	24
[30]	Modelos de Seguridad	Identificar amenazas y desafíos	2020	13
[31]	Gestión de bases de datos	Implementación en bancos	2019	19
[32]	Caso de estudio	Blockchain	2017	14
[33]	Modelo de seguridad	Palabras claves cifradas	2017	25

Criterios de evaluación de calidad. Para asegurar la calidad de los trabajos escogidos y responder a las preguntas de investigación se definirán criterios que se evaluarán de acuerdo con un valor en una escala definida en la tabla 4. El sistema de evaluación será con valores de 1= Si cumple, 0= No cumple, -1=Deficiente.

Table 4. Criterios de Evaluación y Puntuación

Criterio	1	0	-1
¿Los objetivos del estudio relacionados con la seguridad en las bases de datos se definen claramente?	Si	No	Deficiente
¿La propuesta está puntualizada y justificada?	Si	No	Deficiente
¿La solución propuesta se ha probado en escenarios reales?	Si	No	Teórica
¿Responde adecuadamente todas las preguntas de investigación definidas?	Si	No	Deficiente
¿Está el estudio citado por más autores?	Si, por más de 5	No	Entre 1 y 5 autores
¿El estudio fue publicado en una base de datos relevante?	Muy relevante	No Relevante	Relevante

Extracción de datos. Para cada pregunta de investigación le hemos asignado una posible respuesta, como lo veremos en la tabla 5, de tal forma se podrá aplicar los criterios de extracción de datos a todos los estudios seleccionados y organizarlos en función de cada respuesta.

Table 5. Modelo de Clasificación.

Pregunta	Respuestas
Q1. ¿Qué tipo de propuestas de evaluación tecnológicas existen para mejorar la seguridad en bases de datos?	1. Modelos de seguridad 2. Escaneo de Vulnerabilidades 3. Estrategias administrativas de las bases 4. Fragmentación de la data
Q2. ¿Qué tipo de propuestas existen para proteger la información y mitigar los riesgos y amenazas en una base?	1. Control de acceso 2. Auditorias 3. Encriptación

	4.	Detección de intrusos
	5.	Framework
	6.	Detección de amenazas
Q3. ¿Qué protocolos o estrategias se siguen para garantizar la seguridad en las bases de datos?	1.	ISO/IEC
	2.	N/A
	3.	otros

2.2.3 Presentación

Resultados. A continuación, se responderán las preguntas de investigación con una representación por gráficos tomadas a partir de las respuestas dadas en la extracción de datos, y una síntesis de los datos con base a los resultados en la evaluación de calidad mostrada en la tabla 6.

Table 6. Resultados de la Evaluación.

	Q1				Q2						Q3		
Ref.	1	2	3	4	1	2	3	4	5	6	1	2	3
[1]													
[2]	x		x				x	x					
[3]	x	x	x					x		x			
[4]		x	x			x				x			
[5]	x						x	x		x			
[6]	x		x		x				x	x			
[7]	x	x	x			x					x		
[8]			x			x							
[9]											x		
[10]	x	x	x		x	x		x	x	x	x		
[11]		x											
[12]				x					x				
[13]		x						x		x			
[14]		x				x	x						
[15]													x
[16]													x
[17]							x						
[18]			x										
[19]					x								
[20]	x												
[21]									x				
[22]											x		
[34]	x		x										
[23]							x						
[24]													x
[25]							x						
[26]							x						
[27]			x										
[28]	x												
[29]	x	x	x										

[30]			x		x
[31]				x	
[32]					x
[33]		x			x

3 Resultados

En esta etapa se responderán cada una de las preguntas definidas, los gráficos representan el numero de estudios encontrados y seleccionados luego de la evaluación de calidad.

- Q1. ¿Qué tipo de propuestas de evaluación tecnológicas existen para mejorar la seguridad en bases de datos?

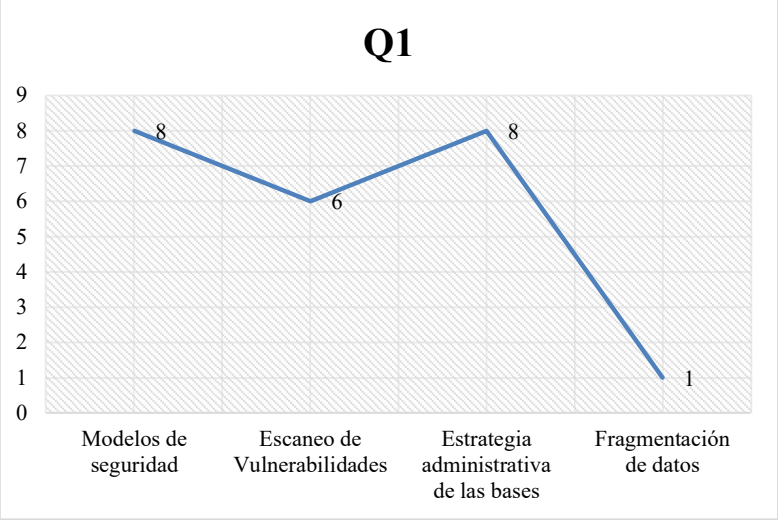

Fig. 2. Resultado de la pregunta 1 representados en gráfico de barras.

Como se muestra en la Fig. 2 del total de estudios seleccionados; 8 proponen modelos de seguridad [2, 3, 5–7, 10, 20, 28, 29, 34] y 8 presentan herramientas administrativas para las bases de datos [2, 3, 34, 4, 6–8, 10, 18, 27, 29]. Por otro lado 6 de ellos proponen un escaneo de vulnerabilidades [3, 4, 7, 10, 11, 13, 14, 29] y solo uno implementa la fragmentación de datos [12].

- Q2. ¿Qué tipo de propuestas existen para proteger la información y mitigar los riesgos y amenazas en una base?

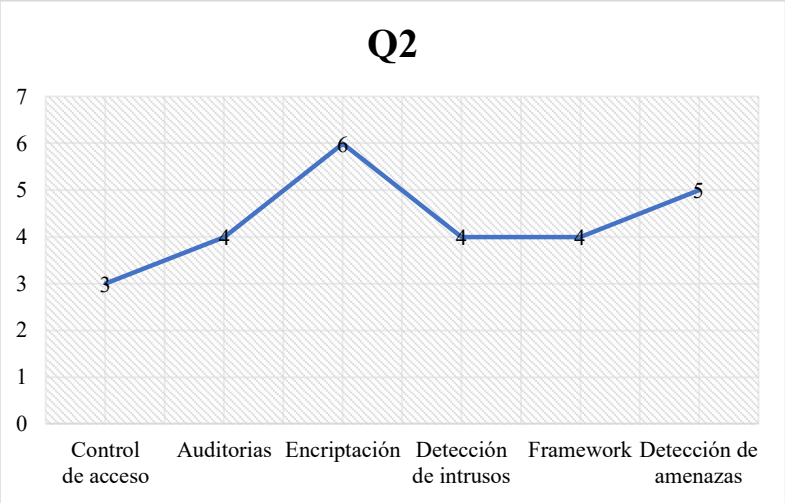

Fig. 3. Resultado de la pregunta 2 representados en gráfico de barras.

Para esta pregunta se obtuvo como resultado que del total de estudios primarios 6 proponían el uso de encriptación [2, 5, 14, 17, 23, 25, 26], 5 de ellos presentaron modelos de detección de amenazas [3–6, 10, 13, 30], con respecto a auditorias, detección de intrusos y framework se obtuvieron 4 estudios respectivamente [2, 3, 14, 21, 33, 4–8, 10, 12, 13]. Y finalmente se obtuvo 3 estudios que presentaban un modelo de control de acceso [6, 10, 19].

- Q3. ¿Qué protocolos o estrategias se siguen para garantizar la seguridad en las bases de datos?

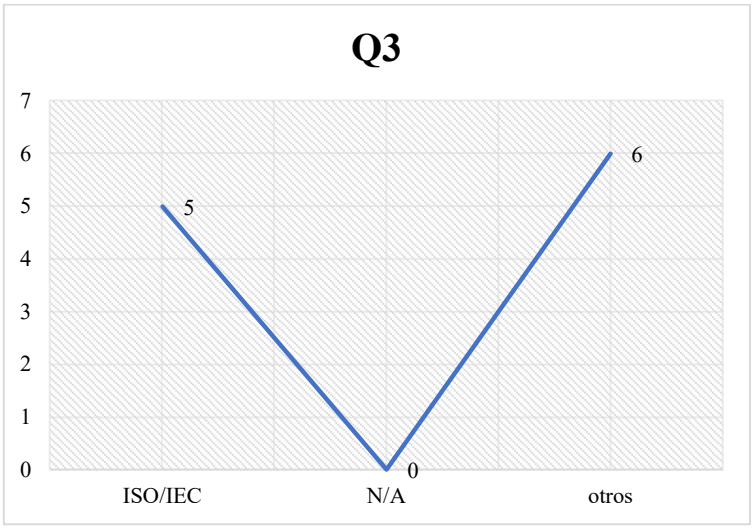

Fig. 4. Resultado de la pregunta 3 representados en gráfico de barras.

Para responder esta pregunta se seleccionaron 5 estudios que presentaban o estudiaban las bases de datos bajo los estándares ISO/IEC [7, 9, 10, 22, 31] y 6 estudios que trataban otros modelos de seguridad [15, 16, 24, 30, 32, 33].

3.1 Análisis de los datos.

Luego de analizar cada pregunta de investigación y cada estudio se puede acordar lo siguiente:

- Los resultados están directamente relacionados con otras investigaciones relacionadas con tecnologías de seguridad en bases de datos.
- La implementación de un modelo que permita mitigar los riesgos de seguridad es la forma más eficiente para que las organizaciones mantengan sus datos protegidos.
- Las propuestas para asegurar la seguridad en los datos suelen concentrarse en la encriptación y modelos para detectar amenazas.
- La encriptación, normas ISO, y el control de accesos son los modelos más utilizadas a la hora de garantizar la seguridad en las bases de datos.

3.2 Modelo de mitigación de riesgos y amenazas

Tras analizar la literatura en los estudios seleccionadas hemos podido definir un modelo para mitigar los riesgos y amenazas que se presentan en las bases de datos y que las

hacen susceptibles a posibles ataques externos poniendo en riesgo la información almacenada.

La Fig. 5 nos muestra en pasos como primero detectamos la amenazas para luego seleccionar una herramienta o tecnología de seguridad y así eliminar el riesgo.

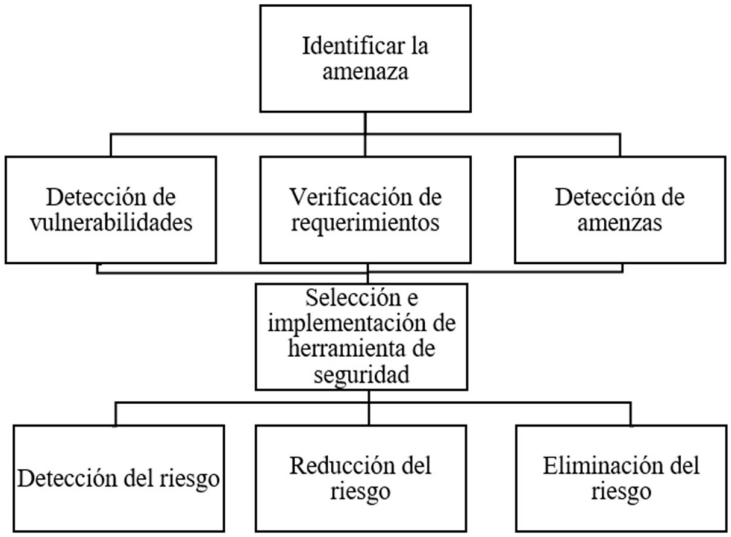

Fig. 5. Prototipo de modelo de mitigación de riesgos y amenazas

4 Discusión

El objetivo de esta revisión sistemática es efectuar un repaso de las tecnologías de seguridad identificando los protocolos y estrategias para proteger la información y mitigar los riesgos y amenazas en bases de datos.
Posterior a analizar los resultados podemos manifestar lo siguiente:

- La implementación de más de una tecnología de seguridad aumenta significativamente la protección y seguridad en una base de datos.
- Los modelos estudiados no garantizan que la seguridad de una base de datos no se vea comprometida.
- Es notoria la usencia de estudios sobre la fragmentación de datos.
- Pocos estudios con el tema tecnologías de seguridad, pero con algo de conocimiento previo y búsqueda en palabras claves se puede encontrar estudios que traten estos temas.

5 Conclusiones

Los resultados de esta revisión demuestran la importancia de las tecnologías de seguridad para bases de datos, se encontró la documentación y estudios necesarios y se pudo llevar a cabo la revisión. Es importante la constante investigación y actualización de nuevas tecnologías, estándares, protocolos o algoritmos de seguridad que permitan conservar y tener el menor riesgos con los datos que en estas se guarden. Esto va de la mano con la actualización en hardware y software y la permanente capacitación de los usuarios finales.

El desarrollo de un modelo de prevención y mitigación de amenazas en las bases de datos basado en la implementación de algoritmos de encriptación y altos estándares de seguridad, que se podrá aplicar a distintas organizaciones de manera sistemática a través de estudios y mapeos, con el objetivo de mejorar el prototipo con cada cambio y avance de las tecnologías y convertirse en un modelo válido en este ambiente de investigación.

Referencias

1. Thuraisingham, B.: Database Security: Past, Present, and Future. In: Proceedings - 2015 IEEE International Congress on Big Data, BigData Congress 2015. pp. 772–774. Institute of Electrical and Electronics Engineers Inc. (2015). https://doi.org/10.1109/BigDataCongress.2015.128.
2. Pratap Singh, S., Nath Tripathi, U.: IJESRT INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY PRESERVING DATABASE CONFIDENTIALITY USING MODIFIED USER SUPPLIED KEY BASED ENCRYPTION. Int. J. Eng. Sci. Res. Technol. https://doi.org/10.5281/zenodo.192615.
3. Shastri, A.A., Chatur, P.N.: Efficient and effective security model for database specially designed to avoid internal threats. In: 2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials, ICSTM 2015 - Proceedings. pp. 165–167. Institute of Electrical and Electronics Engineers Inc. (2015). https://doi.org/10.1109/ICSTM.2015.7225407.
4. Haider, R.: Language-based security analysis of database applications. In: Proceedings of the 2015 3rd International Conference on Computer, Communication, Control and Information Technology, C3IT 2015. Institute of Electrical and Electronics Engineers Inc. (2015). https://doi.org/10.1109/C3IT.2015.7060109.
5. Singh, P., Kaur, K.: Database security using encryption. In: 2015 1st International Conference on Futuristic Trends in Computational Analysis and Knowledge Management, ABLAZE 2015. pp. 353–358. Institute of Electrical and Electronics Engineers Inc. (2015). https://doi.org/10.1109/ABLAZE.2015.7155019.

6. Huijie, W.: A Security Framework for Database Auditing System. In: Proceedings - 2017 10th International Symposium on Computational Intelligence and Design, ISCID 2017. pp. 350–353. Institute of Electrical and Electronics Engineers Inc. (2017). https://doi.org/10.1109/ISCID.2017.64.
7. Pan, J.W., Min, Z., Ping, C., Xu, W.G.: A Lightweight Vulnerability Scanning and Security Enhanced System for Oracle Database. In: Proceedings of 2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference, IAEAC 2019. pp. 1699–1702. Institute of Electrical and Electronics Engineers Inc. (2019). https://doi.org/10.1109/IAEAC47372.2019.8997534.
8. Albalawi, U.: Countermeasure of Statistical Inference in Database Security. In: Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018. pp. 2044–2047. Institute of Electrical and Electronics Engineers Inc. (2019). https://doi.org/10.1109/BigData.2018.8622241.
9. Skulimowski, S., Sugier, A.: Impact of Database Connection Security on Response Time: Case Study. In: Proceedings of the 2018 Conference on Electrotechnology: Processes, Models, Control and Computer Science, EPMCCS 2018. Institute of Electrical and Electronics Engineers Inc. (2018). https://doi.org/10.1109/EPMCCS.2018.8596439.
10. Kurra, K., Panda, B., Li, W.N., Hu, Y.: An agent based approach to perform damage assessment and recovery efficiently after a cyber attack to ensure E-government database security. In: Proceedings of the Annual Hawaii International Conference on System Sciences. pp. 2272–2279. IEEE Computer Society (2015). https://doi.org/10.1109/HICSS.2015.272.
11. Ur Rahman, M., Deep, V., Multhalli, S.: Centralized vulnerability database for organization specific automated vulnerabilities discovery and supervision. In: International Conference on Research Advances in Integrated Navigation Systems, RAINS 2016. Institute of Electrical and Electronics Engineers Inc. (2016). https://doi.org/10.1109/RAINS.2016.7764378.
12. Alsirhani, A., Bodorik, P., Sampalli, S.: Improving Database Security in Cloud Computing by Fragmentation of Data. In: 2017 International Conference on Computer and Applications, ICCA 2017. pp. 43–49. Institute of Electrical and Electronics Engineers Inc. (2017). https://doi.org/10.1109/COMAPP.2017.8079737.
13. Umezawa, K., Mishina, Y., Wohlgemuth, S.: Threat Analysis using Vulnerability Databases-Matching Attack Cases to Vulnerability Database by Topic Model Analysis-"e-learning for Next Generation" Special Research Program View project Mobile Security View project. (2018).
14. Fuller, B., Varia, M., Yerukhimovich, A., Shen, E., Hamlin, A., Gadepally, V., Shay, R., Mitchell, J.D., Cunningham, R.K.: SoK: Cryptographically Protected Database Search. In: Proceedings - IEEE Symposium on Security and Privacy. pp. 172–191. Institute of Electrical and Electronics Engineers Inc. (2017). https://doi.org/10.1109/SP.2017.10.
15. Samaraweera, G.D., Chang, M.J.: Security and Privacy Implications on Database Systems in Big Data Era: A Survey. IEEE Trans. Knowl. Data Eng. 1–1

(2019). https://doi.org/10.1109/tkde.2019.2929794.
16. Halpin, H., Piekarska, M.: Introduction to security and privacy on the blockchain. In: Proceedings - 2nd IEEE European Symposium on Security and Privacy Workshops, EuroS and PW 2017. pp. 1–3. Institute of Electrical and Electronics Engineers Inc. (2017). https://doi.org/10.1109/EuroSPW.2017.43.
17. Zhao, X., Lin, Q., Chen, J., Wang, X., Yu, J., Ming, Z.: Optimizing security and quality of service in a Real-time database system using Multi-objective genetic algorithm. Expert Syst. Appl. 64, 11–23 (2016). https://doi.org/10.1016/j.eswa.2016.07.023.
18. Qian, K., Lo, D., Shahriar, H., Li, L., Wu, F., Bhattacharya, P.: Learning database security with hands-on mobile labs. In: Proceedings - Frontiers in Education Conference, FIE. pp. 1–6. Institute of Electrical and Electronics Engineers Inc. (2017). https://doi.org/10.1109/FIE.2017.8190716.
19. Guarnieri, M., Marinovic, S., Basin, D.: Strong and provably secure database access control. In: Proceedings - 2016 IEEE European Symposium on Security and Privacy, EURO S and P 2016. pp. 163–178. Institute of Electrical and Electronics Engineers Inc. (2016). https://doi.org/10.1109/EuroSP.2016.23.
20. Cui, Z., Zeng, J., Wu, C., Zhang, S.: Design and implementation of a new database security model based on hopping mechanism. In: Proceedings of the International Conference on Anti-Counterfeiting, Security and Identification, ASID. pp. 1–5. IEEE Computer Society (2016). https://doi.org/10.1109/ICASID.2015.7405649.
21. Nandasana, D., Barot, V.: A framework for database intrusion detection system. In: Proceedings - International Conference on Global Trends in Signal Processing, Information Computing and Communication, ICGTSPICC 2016. pp. 74–78. Institute of Electrical and Electronics Engineers Inc. (2017). https://doi.org/10.1109/ICGTSPICC.2016.7955272.
22. Chen, H., Bao, D., Gao, H., Cheng, J.: A Security Evaluation and Certification Management Database Based on ISO/IEC Standards. Presented at the January 20 (2017). https://doi.org/10.1109/cis.2016.0064.
23. Hina Tufail, K.Z.R.B.: Digital Watermarking for Relational Database Security Using mRMR Based Binary Bat Algorithm - IEEE Conference Publication, https://ieeexplore.ieee.org/document/8456164, last accessed 2020/08/05.
24. Yang, L.: Study on the Database Security Technology in E-commerce Environment. Presented at the June 1 (2016). https://doi.org/10.2991/mmebc-16.2016.52.
25. Gupta, S., Jain, S., Agarwal, M.: Ensuring Data Security in Databases Using Format Preserving Encryption. In: Proceedings of the 8th International Conference Confluence 2018 on Cloud Computing, Data Science and Engineering, Confluence 2018. pp. 214–218. Institute of Electrical and Electronics Engineers Inc. (2018). https://doi.org/10.1109/CONFLUENCE.2018.8442626.
26. Zaw, T.M., Thant, M., Bezzateev, S. V.: Database Security with AES Encryption, Elliptic Curve Encryption and Signature. In: 2019 Wave Electronics and its Application in Information and Telecommunication Systems, WECONF 2019. Institute of Electrical and Electronics Engineers Inc. (2019).

https://doi.org/10.1109/WECONF.2019.8840125.
27. Wang, Y.-B.: Study on Security Management Strategy of Internet Network Database. Presented at the February 1 (2017). https://doi.org/10.2991/meita-16.2017.95.
28. Lighari, S.N., Hussain, D.M.A.: Hybrid model of rule based and clustering analysis for big data security. In: 2017 1st International Conference on Latest Trends in Electrical Engineering and Computing Technologies, INTELLECT 2017. pp. 1–5. Institute of Electrical and Electronics Engineers Inc. (2018). https://doi.org/10.1109/INTELLECT.2017.8277627.
29. Fedorchenko, A., Kotenko, I., Chechulin, A.: Design of integrated vulnerabilities database for computer networks security analysis. In: Proceedings - 23rd Euromicro International Conference on Parallel, Distributed, and Network-Based Processing, PDP 2015. pp. 559–566. Institute of Electrical and Electronics Engineers Inc. (2015). https://doi.org/10.1109/PDP.2015.38.
30. Mousa, A., Karabatak, M., Mustafa, T.: Database Security Threats and Challenges. In: 8th International Symposium on Digital Forensics and Security, ISDFS 2020. Institute of Electrical and Electronics Engineers Inc. (2020). https://doi.org/10.1109/ISDFS49300.2020.9116436.
31. Al-Maawali, Z.A., Noronha, H., Prakash Kumar, U.: Big data acquisition, preprocessing and analysis to Develop and Implement Effective Database System with High Security Standards. In: 2019 4th MEC International Conference on Big Data and Smart City, ICBDSC 2019. Institute of Electrical and Electronics Engineers Inc. (2019). https://doi.org/10.1109/ICBDSC.2019.8645583.
32. Gaetani, E., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., Sassone, V.: Blockchain-based database to ensure data integrity in cloud computing environments. (2017).
33. Jiang, P., Mu, Y., Guo, F., Wen, Q.Y.: Private Keyword-Search for Database Systems Against Insider Attacks. J. Comput. Sci. Technol. 32, 599–617 (2017). https://doi.org/10.1007/s11390-017-1745-8.
34. Patil, P., Shettar, P., Akki, M., Sunag, B., Meena, S.M.: Web technologies integrated with advance database management system: A laboratory experience. In: Proceedings of the 2015 IEEE 3rd International Conference on MOOCs, Innovation and Technology in Education, MITE 2015. pp. 301–305. Institute of Electrical and Electronics Engineers Inc. (2016). https://doi.org/10.1109/MITE.2015.7375334.