RITE
ISSN: 2594-1593

Seguridad en bases de datos
Una perspectiva del manejo de información en las bases de datos.

Database security
A perspective of information management in databases

Carlos Sylver Balcázar Molina
Maestrante en Ciencias de la Computación con Formación en Sistemas de Información y Bases de Datos
Universidad Mesoamericana, San Cristóbal de las Casas, Chiapas, México
carlos.bm@outook.es,
ORCID: 0000-0001-8475-4560

Mitzy Isabel Ortiz López
Maestrante en Ciencias de la Computación con Formación en Sistemas de Información y Bases de Datos
Universidad Mesoamericana, San Cristóbal de las Casas, Chiapas, México,
mitzyortiz2421@gmail.com,
ORCID: 0000-0001-5125-085X

Resumen

El administrar la información sigue teniendo la misma importancia, desde los primeros registros humanos hasta nuestros días. De la misma manera que era importante mantener la información en resguardo para que los reinos enemigos no supieran la cantidad de bajas en las batallas, lo es ahora resguardar la propiedad intelectual de la compañía y mantener la ventaja competitiva en el mercado. Esta investigación tiene como objetivo identificar los mecanismos, herramientas, políticas y buenas prácticas para administrar información en las Bases de Datos, de manera que la integridad, confidencialidad y disponibilidad de los datos nunca sean afectadas.

Palabras clave: Bases de Datos, Seguridad en Bases de Datos, Ciberseguridad, Seguridad Informática.

Abstract

Managing information continues to have the same importance, from the first human records to the present day. In the same way that it was important to keep information safe so that the enemy kingdoms did not know the number of casualties in battles, it is now important to protect the company's intellectual property and maintain a competitive advantage in the market. This research

RITE
ISSN: 2594-1593

aims to identify the standards, tools, policies and good practices to manage information in the Databases, so that the integrity, confidentiality and availability of the data are never affected.

Keywords: Databases, Database Security, Cybersecurity, Computer Security.

1. INTRODUCCIÓN

Es bien sabida la importancia de las Bases de Datos y la información que contienen para permitir que una compañía u organización logre sus metas. Los datos son ahora considerados como los activos más valiosos dentro de las organizaciones y el sostener su disponibilidad, integridad y confidencialidad intacta debe ser la tarea principal de cualquier profesional que administre datos. Es por ello que el mantener los estándares de seguridad, controles y políticas funcionando correctamente y en todo momento es fundamental.

Un estudio realizado en 2015 por el Dr. Elliot King, patrocinado por Dell Software, demostró que «si bien el mantenimiento y el rendimiento de las bases de datos son las principales responsabilidades de la mayoría de los DBA, la seguridad se está convirtiendo en un aspecto cada vez más importante en su trabajo. Sin embargo, actualmente los DBA dedican menos tiempo a problemas de seguridad que al desarrollo de bases de datos». (King Elliot, 2015) **[1]**.

Para Medina «la seguridad en bases de datos comprende :

- Liberación inapropiada de información (pérdida de secrecía o confidencialidad)
- Modificación inapropiada de datos (pérdida de integridad)
- Negación de servicio (pérdida de disponibilidad)
- Robo o fraude.» (Medina, Francisco 2022) **[2]**.

Esta investigación se centra de forma general en explicar la importancia de la correcta administración de los datos y exponer el panorama actual en cuanto a estándares, buenas prácticas y herramientas, para así lograr una verdadera seguridad en las Bases de Datos. Para su realización se usó el método de investigación bibliográfica y análisis de casos de estudio, todos relacionados con los temas de seguridad en Bases de Datos, Ciberseguridad y Normas para la Seguridad de la Información, ello mediante la recolección de información en la web.

Para el desarrollo de esta investigación se tomó como guía el estudio realizado en abril de 2021 por Maitté Jazmín Aguirre Sánchez de la Universidad Politécnica Salesiana de Ecuador. (Aguirre Maitté, 2021) **[3]**.

RITE
ISSN: 2594-1593

2. SÍNTESIS DE LA INVESTIGACIÓN

A continuación, se presenta una lista de estudios y artículos relacionados con la seguridad en Bases de Datos, la cual nos presenta un panorama general del tema en cuestión y determina cuál es el estado actual de la protección de la información en cuanto a Bases de Datos se refiere.

1. IBM a través de IBM Cloud Education menciona la importancia de la seguridad de las Bases de Datos; desde los conceptos básicos de seguridad de la información, las amenazas de seguridad, hasta las buenas prácticas en el manejo de datos. La propuesta del artículo para mejorar la seguridad de las Bases de Datos es referida al uso de servidores en la nube, los que ofrecen funciones como tokenización, cifrado, supervisión, análisis de riesgos y optimización de seguridad. (IBM Cloud Education, 2019) **[4]**.
2. La empresa mexicana Telmex propone servicios de identificación y mitigación de huecos de seguridad a través de su solución Scitum, asegurando cumplimiento de normatividad, auditorías, controles administrativos y preventivos, entre otros beneficios para la administración y seguridad de Bases de Datos. (Telmex, 2022) **[5]**.
3. Amazon Redshift, un servicio de Amazon Web Services (AWS) proporciona servicios de warehouse en la nube, con cifrado de datos en estado de reposo o tránsito, administración de claves, interoperabilidad, control de acceso basado en roles y controles preventivos entre otros muchos beneficios. (Amazon Web Services, 2022) **[6]**.
4. El Instituto de Investigación en Informática de la Universidad de La Plata, en su Congreso Argentino de Ciencias de la Computación del 2019, propone una guía basada en las normas ISO/SEC 25012 para medición de calidad de los datos. Dirigido a todas aquellas organizaciones que no cuenten con los recursos ni el personal calificado para implementar dicha norma. La guía toma como referencia - entre otras características - la exactitud, consistencia, accesibilidad y confidencialidad, para medir la calidad de los datos de cualquier organización. Estás características son las mismas definidas en la norma ISO/SEC 25012. (Calabrese, et al., 2019) **[7]**.
5. En 2020, el Instituto Duranguense de Acceso a la Información Pública y de Protección de Datos Personales (idaip) en México, publicó su «Guía de Medidas de Seguridad para la Protección de Datos Personales». En ella se hace hincapié en las tareas que los responsables de manejar Bases de Datos deben realizar. El documento propone la creación de reglas propias para la protección de los datos, así como las buenas prácticas generales que se implementan al administrar Bases de Datos, como controles de acceso administrativo, seguridad física y mantenimiento eficaz de los equipos en donde se administra la información personal. (Instituto Duranguense de Acceso a la Información Pública y de Protección de Datos Personales, 2020). **[8]**.
6. El Instituto Nacional de Estadística y Geografía (INEGI) publicó el documento «Políticas de Seguridad en los Sistemas de Datos Personales del Instituto Nacional de Estadística y Geografía». En él, se menciona la forma en la que la institución protege sus Sistemas de Datos Personales, con métodos y buenas prácticas que su personal está obligado a implementar. Recurrentes análisis de brechas de seguridad, escaneo de vulnerabilidades, actualizaciones de seguridad periódicas para equipos de cómputo y software, resguardo físico de servidores y cifrado de datos, se mencionan en el documento. (Instituto Nacional de Estadística y Geografía, 2019). **[9]**.
7. En 2018 la Secretaría de Educación Pública, a través de la Dirección General De Presupuesto Y Recursos Financieros, publicó «Documento de Seguridad para la Protección de Datos Personales». Dicho documento, es un documento de conformidad de seguridad referido con

RITE
ISSN: 2594-1593

el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSO). En él, se mencionan políticas internas, metodologías para el procesamiento de los datos y puntos a cumplir por los responsables de manejar información y datos personales en la Secretaría de Educación Pública. Entre otros, se mencionan: políticas internas para la seguridad de los sistemas de información, normas ISO implementadas, cifrado de datos, acceso basado en roles de usuario, escaneo de vulnerabilidades y amenazas, copias de seguridad, entre otros. (Secretaría de Educación Pública, 2018) **[10]**.

8. Éste estudio del año 2018, orientado a la seguridad de Bases de Datos, hace hincapié en la necesidad de identificar brechas de seguridad en Bases de Datos SQL y NoSQL. Para identificarlas, la autora propone, entre muchas otras recomendaciones: copias de seguridad «… a diario, ya que las bases de datos crecen todos los días por la cantidad de registros..», control de acceso de usuarios, seguridad física de servidores y componentes, cifrado, especificación de políticas propias y normas como la ISO 27001, para resguardo y correcto manejo de la información. (Gómez Yeni, 2018). **[11]**.
9. Las copias de seguridad y el control de acceso son temas que se analizan en éste trabajo del 2021. El autor propone controles administrativos para manejar los accesos a las Bases de Datos y una sobresaliente investigación sobre tipos de copias de seguridad y herramientas para la creación de las mismas. (Vélez Luis, 2021). **[12]**.
10. ACS (Actividades de Construcción y Servicios), empresa líder en su ramo crea su «Política de Seguridad de la Información». Ésta política engloba diferentes estrategías, buenas prácticas y normas internacionales para el manejo de la información. Entre todos los puntos podemos destacar: implementación del Estándar Internacional ISO/IEC 27001, Seguridad del dispositivo de usuario final, gestión de copias de seguridad, controles estrictos de acceso, seguridad física de los sistemas de información y políticas para trabajos en cloud. **[13]**.
11. La Organización de los Estados Americanos, OAS por sus siglas en inglés, publica en 2020 el documento «Clasificación de Datos», el cual pretende instruir a los gobiernos para desarrollar un sistema de clasificación de datos, «con el fin de garantizar el acceso y la protección de la información generada y procesada por los propios gobiernos». El documento propone auditorías de datos, evaluación de vulnerabilidades y controles administrativos, entre otros puntos importantes. (Organización de los Estados Americanos, 2020). **[14]**.
12. En 2018, el Instituto Nacional Electoral (INE) en México, aprobó el «Manual en materia de Seguridad de Datos Personales» como parte de la Estrategia para el Cumplimiento de los Deberes de Seguridad y Confidencialidad de la Protección de los Datos Personales, perteneciente al Programa para la Protección de los Datos Personales 2018-2023. En él se plantea una extensa y completa guía para el correcto manejo de datos personales. Entre los puntos principales del manual se mencionan la contratación de servicios de cómputo en la nube que estrictamente implementen la familia de normas para la seguridad de la información ISO/SEC27000, controles administrativos, protección física de servidores y sistemas de información, detección de brechas de seguridad y vulnerabilidades, seguridad del dispositivo del usuario final, entre otros importantes puntos. (Instituto Nacional Electoral, 2018) **[15]**.
13. Controlar internamente los datos personales que maneja el instituto y la revisión de las medidas de seguridad para la protección de los datos, son dos de las finalidades por el cual el Instituto para la Protección al Ahorro Bancario (IPAB) emitió en 2020 el documento «Documento de Seguridad para la Protección de Datos Personales». Entre las medidas de seguridad que el documento cita se encuentran las siguientes: auditorías, controles preventivos y administrativos, reconocimiento de vulnerabilidades y mitigación de estas y la

RITE
ISSN: 2594-1593

seguridad de dispositivos de usuario final. (Instituto para la Protección al Ahorro Bancario, 2020) **[16]**.

14. Éste corto y conciso artículo del año 2020, publicado por El Instituto de Ingeniería de la UNAM propone los backups, controles administrativos y preventivos y la protección física de la infraestructura de los sistemas de información como medidas preventivas al hablar de seguridad de la información. (Instituto de Ingeniería, UNAM, 2020) **[17].**
15. Oracle Database Security Assessment Tool o mejor conocida por sus siglas DBSAT, es una herramienta de control detective creada por Oracle para identificar mejoras en configuración, operación e implementación de Bases de Datos Oracle. La herramienta también evalúa el cumplimiento de políticas y normas establecidas por el cliente Oracle. (Mosquera, Carlos. 2022). **[18].**
16. Ésta investigación de 2019, propuesta por un profesional no afín a áreas computacionales, demuestra la comprensión desde otra perspectiva en cuanto a seguridad de los datos se refiere. La investigación plantea recomendaciones generales y bien establecidas para la seguridad de la información en una empresa vitivinícola, entre las que se mencionan: políticas internas basadas en normas internacionales como las ISO/27000, controles administrativos, seguridad física de los servidores y auditorías. (Sisti, María. 2019) **[19]**.
17. En 2021, la Corporación Autónoma Regional de Cundinamarca en Colombia, presentó su «Manual de Políticas de Seguridad de la Información». Éste documento tiene como objetivo sentar las pautas para generar una adecuada seguridad y protección de los datos en dicha institución. El documento comienza presentando una lista de leyes que rigen la protección de datos en Colombia y la implementación de las normas NTC ISO/27001:2013 basada en la norma internacional ISO/27001:2013. Entre las estrategías para la seguridad de los datos que propone el manual, podemos mencionar: seguridad del dispositivo del usuario final, control de acceso de usuarios y red y la seguridad física de los centros de datos. (Corporación Autónoma Regional de Cundinamarca, 2021). **[20]**.
18. Oracle presenta el artículo «¿Qué es la seguridad de datos?». En él se da una breve reseña sobre la importancia de la seguridad de la información y recomendaciones de buenas prácticas en el manejo de Bases de Datos, como son: controles preventivos, controles para el acceso de usuarios y protección de datos en la nube. (Oracle, 2022). **[21]**.
19. La empresa desarrolladora HubSpot publica el artículo «Seguridad de base de datos: qué es y tips para tu organización». En él se plantea de forma general la importancia de la seguridad de las Bases de Datos y presenta algunos métodos para su protección, entre ellos se mencionan: auditorías, enmascaramiento de datos, encriptación y supervisión de la actividad de los datos. (Terreros, Daniella. 2021). **[22]**.
20. La empresa estadounidense de tecnologías de información empresarial Hewlett Packard Enterprise Company, publica el artículo «¿Qué es la seguridad para bases de datos?». En él se menciona de forma breve la importancia de la seguridad de las Bases de Datos y propone algunas buenas prácticas para el refuerzo de la seguridad, como el cifrado de datos, fragmentación de la data y almacenamiento en la nube. Por último expone una reseña de su producto HPE GreenLake para el fortalecimiento de la seguridad de las Bases de Datos empresariales, que entre otros beneficios, implementa la supervisión de los datos en tiempo real. (Hewlett Packard Enterprise, 2021). **[23]**.
21. Las prácticas recomendadas para la seguridad del Gestor de Bases de Datos SQL Server, se mencionan en éste artículo publicado por Microsoft en septiembre de 2022. Entre ellas podemos mencionar: cifrado a nivel columna usando la herramienta Always Encrypted, Cifrado de datos transparente (TDE) para proteger los datos cuando están en nivel archivo

RITE
ISSN: 2594-1593

proporcionando cifrado en reposo, auditorías, controles administrativos y preventivos y la detección de vulnerabilidades. (Microsoft, 2022). **[24]**.

22. El Centro Criptológico Nacional de España publica en 2021 el documento « Recomendaciones de Seguridad en Bases de Datos». En él podemos encontrar recomendaciones concretas sobre seguridad en Bases de Datos, como: controles administrativos y preventivos, políticas para realizar backups, actualizaciones pertinentes de los Gestores de Bases de Datos y cifrado/enmascaramiento. (Centro Criptológico Nacional de España, 2021). **[25]**.
23. «El ABC para mejorar tu ciberseguridad y cómo proteger tu información» es el título del artículo publicado en el sitio web de noticias del Tecnológico de Monterrey. En él se explican brevemente los tipos de ciberataques más comunes, proporciona algunos consejos para crear contraseñas más seguras y da una lista de empresas gubernamentales mexicanas que fueron víctimas de ciberdelincuencia en los últimos años. Entre los puntos que se mencionan como recomendaciones para tener Bases de Datos seguras encontramos: herramientas para detección de vulnerabilidades y controles administrativos. (Treviño, Ricardo. 2021) **[26]**.
24. La Comisión Económica para América Latina y el Caribe (CEPAL) publicó el artículo «Gestión de datos de investigación», dirigido a investigadores, gestores de información y cualquier profesional interesado en implementar buenas prácticas en el manejo de datos. El artículo menciona prácticas como cifrado, almacenamiento en la nube e implementación de políticas estrictas para creación de copias de seguridad. (Comisión Económica para América Latina y el Caribe, 2020) **[27]**.
25. La revista digital de TI Computer Weekly publica el artículo «Privacidad de datos, seguridad de datos y protección de datos». En él se hace una diferenciación entre seguridad, protección y privacidad de los datos. Buena parte del artículo se centra en las copias de seguridad y restauración y el uso de normas para la protección de datos. También se mencionan otras prácticas para la seguridad de la información como: protección de la infraestructura física, controles administrativos para el acceso, cifrado y controles detectives. (Posey, Brien. 2021) **[28]**.
26. La plataforma de email marketing MDirector, publica en su sitio web el artículo «Guía efectiva para proteger la información de tu base de datos». El artículo menciona prácticas como: mantener actualizados los sistemas de información, auditorías, uso de herramientas para tener controles detectives en las Bases de Datos y algoritmos para cifrar datos. (NewsMDirector, 2022). **[29]**.
27. La empresa de ciberseguridad mexicana White Shield, en su artículo «¿Cuáles son las normas de seguridad informática?», enlista la familia de normas de seguridad informática ISO/IEC 27000. Propone usarlas como estándares de confiabilidad y estrategia para mantener la seguridad de las Bases de Datos. El artículo también hace una reseña de protocolos básicos de ciberseguridad. (White Shield, 2021). **[30]**

3. METODOLOGÍA

3.1 metodología para la investigación

Se realizó una revisión sistemática y una síntesis de los estudios y artículos relevantes sobre seguridad en Bases de Datos y ciberseguridad.

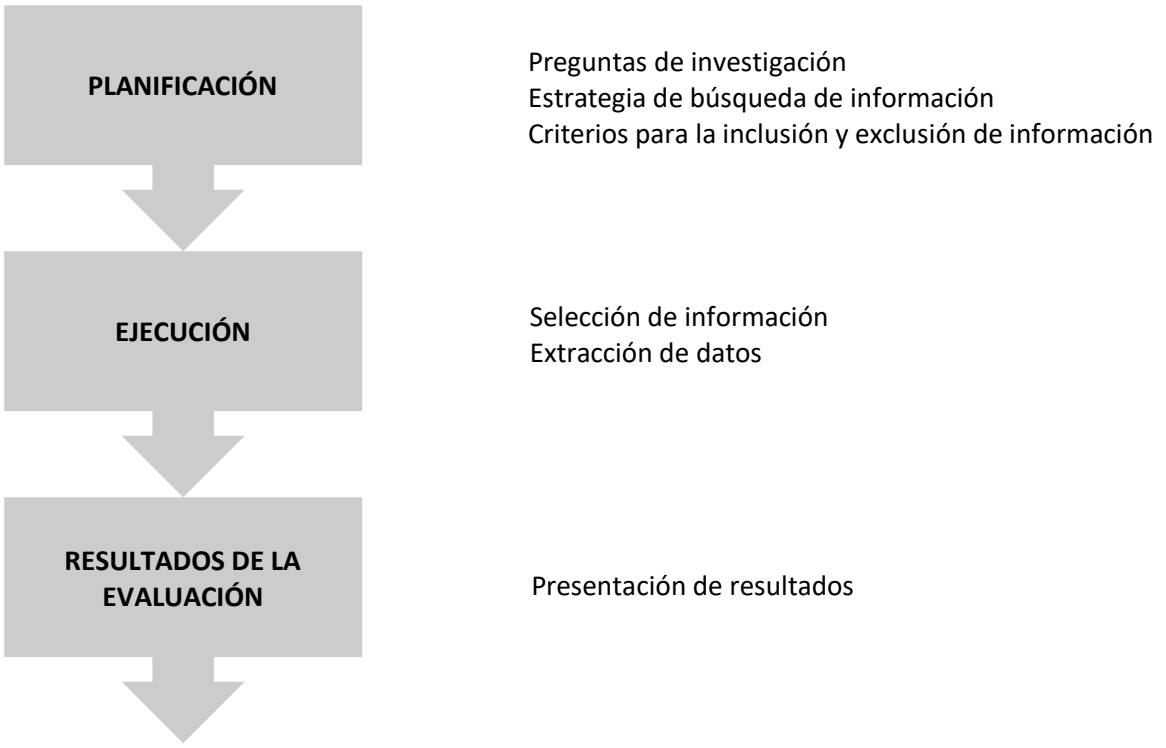
Para el desarrollo de esta investigación se emplea el método deductivo con enfoque cuantitativo y se aplica la investigación exploratoria basada en la búsqueda y lectura de estudios y artículos detallados

RITE
ISSN: 2594-1593

en la referencia, para un análisis de las herramientas, políticas, métodos y normas referentes a la seguridad de las Bases de Datos.

3.2 Definición Del Protocolo De Investigación

Se ha realizado esta investigación de manera exploratoria basada en la búsqueda de estudios y artículos porque permite obtener una perspectiva general, amplia y desde el enfoque de diferentes especialistas, empresas e investigadores. El protocolo de investigación se divide en tres etapas: Planificación, Ejecución y Presentación.



3.2.1 Planificación

Preguntas de Investigación: el objetivo de las preguntas es analizar los diferentes estudios y artículos referentes a la seguridad en Bases de Datos, de manera que se pueda identificar los avances relacionados al tema y tener un panorama actual y general en cuanto a seguridad de la información y manejo de datos se refiere. Las preguntas se definen en la tabla 1:

Pregunta	Motivo
Q1. ¿Qué propuestas existen para mejorar la seguridad en Bases de Datos?	Determinar el número total de investigaciones en los últimos 5 años referentes a las tecnologías orientadas a la seguridad de Bases de Datos.

RITE
ISSN: 2594-1593

Q2. ¿Qué tipo de propuestas existen para protección de datos, mitigación de riesgos y amenazas en Bases de Datos?	Identificar las tecnologías, herramientas, metodologías y buenas prácticas que se implementan como instrumentos de seguridad para mitigar los riesgos y amenazas en bases de datos.
Q3. ¿Qué tipo de estándares y protocolos se han creado o actualizado para garantizar la seguridad en Bases de Datos?	Identificar las políticas, protocolos y estándares que diversas organizaciones y especialistas sugieren para la protección de Datos.

Tabla 1. Preguntas de investigación
Table 1. Research questions

Estrategia de búsqueda de información. Para realizar esta investigación se realizó una búsqueda en la web en páginas de empresas del ramo tecnológico, instituciones educativas y bibliotecas digitales con el fin de encontrar información actualizada referente a la seguridad y protección de datos. El periodo de búsqueda incluye publicaciones de los últimos 5 años: de 2018 hasta 2022.

Para ésta búsqueda se introdujeron los términos mostrados en la tabla 2.

Criterios	**Términos de búsqueda**
Tecnologías para la seguridad de la información.	«Tecnologías para la seguridad de la información», «ciberseguridad», «Herramientas para seguridad de los datos».
Seguridad en Bases de Datos.	«Seguridad en Bases de Datos», «Seguridad de la información».
Normas, políticas y protocolos.	«Normas, políticas y protocolos para la seguridad de la información», «Normas ISO para la seguridad de la información».

Tabla 2. Términos usados para la búsqueda de información
Table 2. Terms used to search for information

Para la identificación de los artículos y estudios potenciales a ser parte de ésta investigación se aplicaron los siguientes filtros.

F1. Revisión del resumen o abstract, contrastando con el tema principal de la investigación.
F2. Revisión de palabras clave o keywords, contrastando con el tema principal de la investigación.
F3. Lectura y análisis de publicaciones que pasaron los filtros F1 Y F2.

Criterios de inclusión. Para seleccionar los estudios que formaron parte de ésta investigación, se tomaron en cuenta aquellos que cumplían con uno de los criterios de inclusión presentados a continuación:
CI1. Publicaciones que traten temas sobre tecnologías de seguridad en Bases de Datos, Seguridad de los Datos, Ciberseguridad, Normas, Protocolos y Políticas para la protección de los datos .

RITE
ISSN: 2594-1593

CI2. Estudios cualitativos y cuantitativos donde se propongan o evalúen métodos, protocolos, tecnologías o estrategias de seguridad para Bases de Datos.

CI3. Publicaciones de empresas tecnológicas (IBM, Microsoft, Oracle, etc.), universidades y organizaciones.

Criterios de exclusión. Se omitieron estudios que cumplieron cualquiera de los criterios de exclusión presentados a continuación:

CE1. Se excluye todo aquel estudio con un enfoque distinto al de seguridad en Bases de Datos.

CE2. Se excluye todo aquel estudio al que solo puede ser consultado un fragmento de éste o su resumen.

CE3. La publicación no se encuentra en el periodo de tiempo definido en la estrategía de búsqueda de información.

3.2.2 Ejecución

La ejecución del proyecto se divide en las siguientes etapas:

- **Estudios potenciales.** Haciendo una búsqueda en la web se aplicaron los criterios de búsqueda, obteniendo 58 publicaciones potenciales para ser parte de la investigación.
- **Estudios primarios.** Después de aplicar los filtros y criterios de inclusión y exclusión antes descritos, obtuvimos 27 estudios primarios.

Selección de información. Se seleccionaron 27 artículos, estudios y/o reseñas encontrados en la web, para la realización de esta investigación.

Extracción de Datos. Las Preguntas de investigación tienen asignadas un número determinado de posibles respuestas, como se muestra en la tabla 3, éstas de acuerdo al tema principal de la pregunta. De ésta forma se extrajo la información de cada estudio primario.

Preguntas	**Respuestas**
Q1. ¿Qué propuestas existen para mejorar la seguridad en Bases de Datos?	1. Bases de Datos gestionadas en la nube 2. Bases de Datos fragmentadas 3. Estrategias propias para administración de las BD 4. Escaneo de vulnerabilidades 5. Supervisión de la actividad de los datos

RITE
ISSN: 2594-1593

Q2. ¿Qué tipo de propuestas existen para protección de datos, mitigación de riesgos y amenazas en Bases de Datos?	1. Cifrado y/o enmascaramiento. 2. Seguridad física de servidores e infraestructura informática 3. Control de acceso de usuarios y de red 4. Seguridad del dispositivo de usuario final 5. Seguridad de SGBD 6. Seguridad de servidor de aplicaciones/web 7. Copias de seguridad 8. Auditorías
Q3. ¿Qué tipo de controles, políticas y/o normas existen o se han actualizado para garantizar la seguridad en Bases de Datos?	1. Controles administrativos 2. Controles preventivos 3. Controles de detectives 4. Políticas de seguridad en la nube 5. Políticas generales de ciberseguridad 6. ISO 7. ISO/IEC 8. Ninguno 9. Otras/Políticas propias

Tabla 3. Modelo de extracción de datos
Table 3. Data extraction model

3.2.3 Resultados de la evaluación

Resultados. La tabla 4 muestra los resultados de la evaluación, tomada de las respuestas obtenidas en la fase de extracción de datos.

REF.	Q1					Q2								Q3								
	1	2	3	4	5	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9
[4]	x			x	x	x	x	x	x	x	x	x	x	x	x	x	x	x				
[5]			x	x			x	x	x				x	x	x	x		x				x
[6]	x	x	x	x	x	x		x				x	x	x	x		x	x				x
[7]			x																	x		x
[8]			x	x	x		x	x		x	x			x	x	x		x				x
[9]		x	x	x		x	x	x		x		x	x	x	x	x						x
[10]			x	x	x	x	x	x	x			x	x	x	x	x		x	x			x
[11]	x		x	x		x	x	x		x	x	x	x	x	x		x	x	x			x

RITE
ISSN: 2594-1593

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

Tabla 4. Resultados de la evaluación
Table 4. Results of the evaluation

4. RESULTADOS

En esta etapa las preguntas y respuestas de la evaluación se representan en forma de gráficas y se hace una análisis individual de los resultados.

RITE
ISSN: 2594-1593

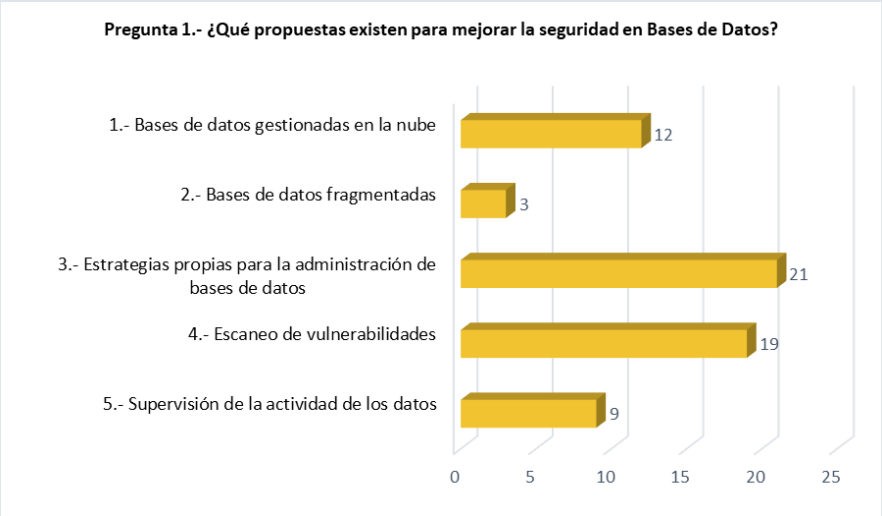


Fig.1 Resultado de la investigación en forma de gráfica. Pregunta 1 (Q1).
Fig. 1 Research Result Graph. Question 1.

Como se muestra en la figura 1, del total de estudios primarios, 21 proponen estrategías propias para la administración de Bases de Datos. Ésto por la gama diferente de organizaciones y empresas consultadas en ésta investigación y la necesidad de establecer sus propios métodos ya que, aunque las buenas prácticas generales funcionan para todas, cada una las establece en menor o mayor medida.

Podemos observar también que el escaneo de vulnerabilidades sigue siendo un punto principal a considerar al momento de proponer seguridad en Bases de datos y solo 3 estudios sugieren o implementan fragmentación de la data.

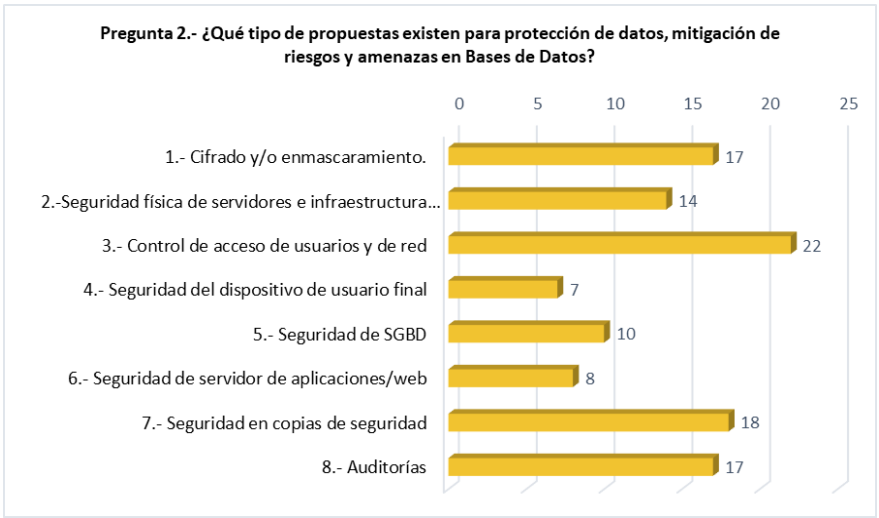


Fig.2 Resultado de la investigación en forma de gráfica. Pregunta 2 (Q2).
Fig. 2 Research Result Graph. Question 2.

RITE
ISSN: 2594-1593

Como se muestra en la figura 2, del total de estudios primarios, 22 proponen y/o implementan el control de acceso de usuario y de red como método principal para protección de los datos. Ésto por la facilidad de implementar estrategias de autenticación y en gran medida, porque muchas de las veces no se necesita configuración adicional, ya que los Gestores de Bases de Datos y Sistemas Operativos traen por defecto configuraciones para la autenticación de usuarios.

Podemos observar también que el cifrado, copias de seguridad y auditorías son técnicas implementadas o propuestas para mitigación de riesgos y amenazas en las Bases de Datos.

Lo complejo que resulta el implementar herramientas o buenas prácticas en los dispositivos de usuario final, hace que solo 7 estudios primarios propongan o implementen ésta estrategia.

Fig.3 Resultado de la investigación en forma de gráfica. Pregunta 3 (Q3).
Fig. 3 Research Result Graph. Question 3.

Como se muestra en la figura 3, del total de estudios primarios, 21 implementan controles administrativos para la gestión de las Bases de Datos, tales como administrar instalaciones de componentes o cambios de configuración. 19 estudios proponen e implementan políticas y normas propias, muchas de ellas basadas en normas internacionales de seguridad de la información. Llama la atención la creciente aceptación e implementación de controles detectives, implementados en herramientas que facilitan el monitoreo de los datos.

Aunque la gran mayoría de los estudios mencionan las normas ISO e ISO/SEC, pocas las implementan, debido a factores económicos y de personal capacitado para mantenerlas en funcionamiento.

5. ANÁLISIS GENERAL Y PROPUESTA

El objetivo principal de ésta investigación fue conocer las diferentes tecnologías, herramientas, políticas y metodologías con respecto a la seguridad de la información y las Bases de Datos,

RITE
ISSN: 2594-1593

propuestas y/o aplicadas en los últimos 5 años. Después de analizar los resultados de cada una de las preguntas de investigación se concluye que:

1. Los respaldos de información, detección de vulnerabilidades y control de acceso de usuario y red siguen siendo las buenas prácticas más comunes al momento de establecer normas y modelos de seguridad en Bases de Datos y mitigación de riesgos, ésto derivado de su fácil implementación.
2. Se encontraron pocas propuestas y herramientas para la fragmentación de la data.
3. El factor humano dentro de la metodología de protección de datos toma más relevancia e importancia al momento de proponer métodos y políticas para la seguridad de las Bases de Datos.
4. Las Bases de Datos en la nube se están posicionando como alternativa fiable y viable para almacenar datos. Corporativos como Oracle, Amazon e IBM ofrecen éstos servicios con gran información respecto a sus beneficios; de manera entendible, incluso para personas con poco conocimientos técnicos en Bases de Datos o ciberseguridad.
5. Existe un creciente interés por los gobiernos y organizaciones en el esfuerzo por desarrollar e implementar métodos para resguardo y seguridad de los datos que ellos administran.
6. Se encontraron pocas propuestas e investigaciones con respecto a la seguridad en los dispositivos de usuario final. Las únicas propuestas aplicables siguen siendo la ocultación de los datos por medio de autenticaciones y roles de usuario y el cifrado/enmascaramiento.

Propuesta: Cada organización es diferente y la forma en la que administra sus datos, también. Sigue siendo conveniente la creación de modelos y políticas para la seguridad de las Bases de Datos dependiendo del entorno en el que se manejan, de igual forma el guiarse de normas internacionales de protección de datos también sigue siendo la forma idónea para la seguridad de la información.

Nuestra propuesta se basa en:

- El uso de herramientas para la protección y administración de las Bases de Datos, como aquellas que nos sugieren mejoras en la configuración e implementación.
- Uso de herramientas de supervisión de la actividad de las Bases de Datos para identificar actividades sospechosas y mitigar los riesgos.
- En la medida de lo posible las empresas deberían proporcionar dispositivos informáticos a los encargados de manejar datos de la compañía, con las configuraciones de seguridad necesarias para la protección de la información. De no ser posible, otra solución viable son las políticas de seguridad de datos al usar dispositivos propios para el manejo de la información, en las que se establecen responsabilidades, autorizaciones y mutuo acuerdo para configurar los dispositivos, de manera que la información no se vea comprometida.

6. CONCLUSIONES

Al realizar esta investigación resultó notorio el interés por mejorar la seguridad de las Bases de Datos tanto por grandes compañías tecnológicas, empresas, organizaciones y profesionales, quizá más ahora que años atrás, debido a la pasada pandemia del Covid-19 que el planeta vivió dando como

RITE
ISSN: 2594-1593

resultado nuevas formas de trabajar y de conectarnos. Con ello, los datos que manejamos en esta realidad tecnológica necesitan otro nivel de seguridad. Compañías como Oracle, IBM, Microsoft o Amazon están compitiendo por llevar las Bases de Datos al siguiente nivel, la nube, y es ahí donde a pesar de los nuevos retos que habrá que enfrentar para proteger los datos, las buenas prácticas que se han implementado desde siempre aseguran la protección de las Bases de Datos; las auditorías, la correcta y oportuna detección de vulnerabilidades, las políticas para realizar copias de seguridad y el compromiso del factor humano, seguirán siendo primordiales para la Seguridad de las Bases de Datos.

La investigación no solo evidenció nuevas formas y herramientas para la protección de los datos, sino también el creciente interés de las organizaciones gubernamentales por la ciberseguridad y protección de datos. Quizá ello también sea evidencia de un nuevo salto tecnológico en el que los datos tomarán aún mayor valor para compañías y gobiernos, de ahí el interés por mantener su integridad, disponibilidad y confidencialidad.

REFERENCIAS

[1] King, Elliot. (2015). *El Mundo Real del Administrador De Bases De Datos*. Unisphere Research. https://i.dell.com/sites/csdocuments/Shared-Content_data-Sheets_Documents/es/mx/the-real-world-of-the-database-administrator-white-paper-15623_la.pdf

[2] Medina, Francisco (08 de agosto de 2022). *Seguridad en Bases de Datos. La seguridad en una base de datos*. https://www.visibilidadweb.unam.mx/capacitacion/perfilesTIC/responsableTIC/Seguridad_bases_de_datos_Diplomado_ABD.pdf

[3] Aguirre, Maitté. (Abril de 2022). *Tecnologías De Seguridad En Bases De Datos: Revisión Sistemática*. https://dspace.ups.edu.ec/bitstream/123456789/20566/1/UPS-GT003297.pdf

[4] IBM Cloud Education. (27 de agosto de 2019). *Database Security: una guía esencial*. https://www.ibm.com/mx-es/cloud/learn/database-security

[5] Telmex. (2022). *Seguridad en Bases de Datos.* https://telmex.com/web/empresas/seguridad-en-bases-de-datos

[6] Amazon Web Services. (2022). *Amazon Redshift: Guía para desarrolladores de bases de datos*. https://docs.aws.amazon.com/es_es/redshift/latest/dg/redshift-dg.pdf#r_Database_objects

[7] Calabrese, Julieta., Esponda, Silvia., Pasini, Ariel., Boracchia, Marcos., Pesado, Patricia. (2019). *Guía para evaluar calidad de datos basada en ISO/IEC 25012*. https://core.ac.uk/download/pdf/301104068.pdf

RITE
ISSN: 2594-1593

[8] Instituto Duranguense de Acceso a la Información Pública y de Protección de Datos Personales. (12 de septiembre de 2020). *Guia Medidas De Seguridad Para La Protección De Datos Personales*. https://www.idaip.org.mx/archivos/formatos/Promocion_Vinculacion/Gu%C3%ADa%20medidas%20de%20seguridad.pdf

[9] Instituto Nacional de Estadística y Geografía. (25 de septiembre de 2019). *Políticas De Seguridad En Los Sistemas De Datos Personales Del Instituto Nacional De Estadística Y Geografía*. Recuperado: 24 de Octubre de 2022. https://sc.inegi.org.mx/repositorioNormateca/P_25Sep19.pdf

[10] Secretaría de Educación Pública. (25 de julio de 2018). *Documento De Seguridad Para La Protección De Datos Personales*. https://sep.gob.mx/work/models/sep1/Resource/16974/1/images/documentode_seguridad.pdf

[11] Gómez, Yeni. (2018). *Estudio de Seguridad en Bases de Datos SQL y NoSQL*. https://repository.unad.edu.co/bitstream/handle/10596/21429/52488191.pdf?sequence=4&isAllowed=y

[12] Vélez, Luis. (2021). *Gestión de Bases de Datos Versión 1.0*. https://readthedocs.org/projects/gestionbasesdatos/downloads/pdf/latest/

[13] Actividades de Construcción y Servicios. (27 de julio de 2022). *Política de Seguridad de la Información*. https://www.grupoacs.com/ficheros_editor/File/05_Compliance/Pol%C3%ADticas/31_Pol%C3%ADtica%20de%20Seguridad%20de%20la%20Informaci%C3%B3n.pdf

[14] Organización de los Estados Americanos. (24 de febrero de 2020). *Clasificación de Datos*. https://www.oas.org/es/sms/cicte/docs/ESP-Clasificacion-de-Datos.pdf

[15] Instituto Nacional Electoral. (2018). *Manual en materia de Seguridad de Datos Personales*. https://ine.mx/wp-content/uploads/2021/05/SSPPDP-Manual-SegDP.pdf

[16] Instituto para la Protección al Ahorro Bancario. (2020). *Documento de Seguridad para la Protección de Datos Personales*. https://www.gob.mx/cms/uploads/attachment/file/556985/Documento-de-Seguridad-para-la-Proteccion-de-Datos-Personales.pdf

[17] Instituto de Ingeniería, UNAM. (2020). *Seguridad Informática*. http://www.ii.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/seguridadinformatica.aspx

[18] Mosquera, Carlos. (Enero 11 de 2022). *Seguridad a nivel de bases de datos: ¿realmente estás protegido?*. https://blogs.oracle.com/oracle-latinoamerica/post/seguridad-bases-datos-proteccion

[19] Sisti, María. (2019). Seguridad Informática: La Protección de la Información en una Empresa Vitivinícola de Mendoza, 2019. https://bdigital.uncu.edu.ar/objetos_digitales/15749/sistimariaagustina.pdf

[20] Corporación Autónoma Regional de Cundinamarca. (28 de octubre de 2021). *Manual de Políticas de Seguridad de la Información*. https://www.car.gov.co/uploads/files/61840aaf4c32e.pdf

[21] Oracle. (2022). *¿Qué es la seguridad de datos?*. https://www.oracle.com/mx/security/database-security/what-is-data-security/#:~:text=La%20seguridad%20de%20los%20datos%20se%20refiere%20a%20las%20medidas,de%20la%20base%20de%20datos.

[22] Terreros, Daniella. (2021). *Seguridad de base de datos: qué es y tips para tu organización*. https://blog.hubspot.es/marketing/que-es-seguridad-base-de-datos

[23] Hewlett Packard Enterprise. (2021). *¿Qué es la seguridad para bases de datos?*. https://www.hpe.com/es/es/what-is/database-security.html

[24] Microsoft. (26 de septiembre de 2022). Prácticas recomendadas de seguridad para SQL Server. https://learn.microsoft.com/es-es/sql/relational-databases/security/sql-server-security-best-practices?source=recommendations&view=sql-server-ver16

[25] Centro Criptológico Nacional de España. (Diciembre 2021). *Recomendaciones de Seguridad en Bases de Datos*. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6356-ccn-cert-bp-24-recomendaciones-de-seguridad-en-bases-de-datos-1/file.html

[26] Treviño, Ricardo. (20 de agosto de 2021). *El ABC para mejorar tu ciberseguridad y cómo proteger tu información*. https://conecta.tec.mx/es/noticias/nacional/educacion/el-abc-para-mejorar-tu-ciberseguridad-y-como-proteger-tu-informacion

[27] Comisión Económica para América Latina y el Caribe. (18 de diciembre de 2020). *Gestión de datos de investigación*. Recuperado: 26 de octubre de 2022. https://biblioguias.cepal.org/c.php?g=495473&p=3390849

[28] Posey, Brien. (julio de 2021). *Privacidad de datos, seguridad de datos y protección de datos*. Recuperado: 27 de octubre de 2022. https://www.computerweekly.com/es/definicion/Privacidad-de-datos-seguridad-de-datos-y-proteccion-de-datos

[29] NewsMDirector. (09 de septiembre de 2022). *Guía efectiva para proteger la información de tu base de datos*. https://www.mdirector.com/blog/proteger-la-informacion-de-tu-base-de-datos/

[30] White Shield. (08 de octubre de 2021). ¿Cuáles son las normas de seguridad informática?. https://whiteshield.io/blog/normas-de-seguridad-informatica/