ANÁLISIS DE LAS CARACTERÍSTICAS DE SEGURIDAD DE UNA MUESTRA DE GESTORES DE BASES DE DATOS PARA DETERMINAR INDICADORES QUE PERMITA HACER UNA ELECCIÓN ADECUADA EN PYMES

JHON FERNANDO ANICHIARICO CHICA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PROYECTO DE SEGURIDAD INFORMÁTICA II
SAHAGÚN - CÓRDOBA
2020

ANÁLISIS DE LAS CARACTERÍSTICAS DE SEGURIDAD DE UNA MUESTRA DE GESTORES DE BASES DE DATOS PARA DETERMINAR INDICADORES QUE PERMITA HACER UNA ELECCIÓN ADECUADA EN PYMES

JHON FERNANDO ANICHIARICO CHICA

Monografía para optar al título de Especialista En Seguridad Informática

Director:
Msc. Katerine Márceles Villalba

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PROYECTO DE SEGURIDAD INFORMÁTICA II
SAHAGÚN - CÓRDOBA
2020

Nota de aceptación

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Sahagún, agosto de 2020

Dedicatoria

Le dedico este triunfo A Dios por Darme vida, y sabiduría a lo largo del estudio de la Especialización En Seguridad Informática

A mis padres, ya que sin ellos no hubiera alcanzado este logro, uno más en mi vida profesional.

Madre, gracias por estar a mi lado en esta etapa de mi posgrado, tu apoyo moral y ese entusiasmo brindado a diario para seguir adelante en mis propósitos.

Papá, por tu forma de ser conmigo, por compartir experiencias, conocimientos y consejos.

Jhon Fernando

Agradecimientos

Primeramente, doy gracias a Dios por permitirme tener la experiencia de realizar estudios universitarios, a la universidad por permitir convertirme en un especialista en lo que me gusta, me apasiona, gracias a cada docente que hizo parte de este proceso de formación, no ha sido nada fácil el camino para llegar a la meta, pero con mucho esfuerzo y dedicación siempre logramos los resultados que en algún momento nos propusimos.

Por último, agradezco a quien está leyendo este trabajo por permitir llegar y compartir mi investigación y conocimiento, que en algún momento de su vida será puesto en práctica estos conceptos

Jhon Fernando

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

GLOSARIO

ALGORITMOS DE ENCRIPTACIÓN: el algoritmo de encriptación es un procedimiento que transforma un mensaje, sin atender su estructura lingüística o significado, de tal forma que sea incomprensible, o por lo menos difícil de comprender para terceras personas.

AES: Estándar de Cifrado Avanzado

BD - Base de Datos: conjunto estructurado de datos que representa entidades y sus interrelaciones. La representación será única e integrada, a pesar de que debe permitir diversas utilizaciones.

DDL - Data Definition Language: lenguaje especializado en la escritura de esquemas; es decir, en la descripción de BD.

DML - Data Manipulation Language: lenguaje especializado en la utilización de BD (consultas y mantenimiento).

DES: **Data Encryption Estándar**: es un esquema de encriptación simétrico para redes de ordenadores.

DSA - **Digital Signature Algorithm:** es Algoritmo estándar estadounidense de firma digital para aplicaciones gubernamentales

IDEA - International Data Encryption Algorithm:

MIPYME: Micro, Pequeña y Mediana Empresa

RSA - Rivest, Shamir y Adleman: Es un algoritmo criptográfico de cifrado asimétrico, o de clave pública, y es uno de los algoritmos más utilizados en la actualidad.

SGBD - Sistema De Gestión De Base Datos: software que gestiona y controla BD. Sus principales funciones son facilitar la utilización de la BD a muchos usuarios simultáneos y de tipos diferentes, independizar al usuario del mundo físico y mantener la integridad de los datos. sigla: SGBD

SQL - Structured Query Language: lenguaje especializado en la descripción (DDL) y la utilización (DML) de BD relacionales. Creado por IBM al final de los años setenta y estandarizado por ANSI-ISO en 1985 (el último estándar de SQL es de 1999). En la actualidad lo utilizan prácticamente todos los SGBD del mercado.

RESUMEN

Mediante el presente estudio monográfico se desarrolló un análisis conceptual a las características de los Sistemas de Gestión de Bases de Datos [SGBD] enfatizando en la seguridad como aspecto clave para el respaldo de la información. En este sentido, el estudio se desarrolló con una metodología tipo compilación, bajo una modalidad descriptiva, mediante la cual se analizó información escrita sobre los sistemas de gestión de bases de datos y se establecieron características, factores de vulnerabilidad y demás aspectos que al final permitieron la definición de indicadores enfocados a la seguridad de los gestores, para la elección adecuada de las MiPymes.

Pudiendo establecerse con el análisis comparativo de un caso supuesto para una MiPymes, que PostgreSQL, se detalla como una opción viable por sus características de seguridad y código abierto que le permite a las medianas y pequeñas empresas respaldar su información mediante un gestor con muy buena reputación y con baja inversión monetaria.

ABSTRACT

Through the present monographic study, a conceptual analysis of the characteristics of the Database Management Systems [DBMS] will be considered, emphasizing security as a key aspect for information backup. In this sense, the study will be analyzed with a compilation-type methodology, under a descriptive methodology, through which written information on database management systems was analyzed and characteristics, protection factors and other aspects were established that ultimately allowed the definition of indicators focused on the safety of managers, for the proper choice of MSMEs.

Being able to establish itself with the comparative analysis of a supposed case for a MyPymes, which PostgreSQL, is detailed as a viable option for its security features and open source that allows medium and small companies backed up their information by a manager with a very good reputation. and with low monetary investment.

TITULO

ANÁLISIS DE LAS CARACTERÍSTICAS DE SEGURIDAD DE UNA MUESTRA DE GESTORES DE BASES DE DATOS PARA DETERMINAR INDICADORES QUE PERMITA HACER UNA ELECCIÓN ADECUADA EN PYMES

INTRODUCCIÓN

En la sociedad actual, la información se constituye en un activo de gran valor, por lo que respaldar su integridad es una necesidad absoluta de las organizaciones, en ese sentido, la seguridad de las bases de datos es un proceso fundamental que está respaldado con la elección de un buen gestor de base de datos, no obstante, esto no es una tarea fácil puesto que en el mercado hay una gran oferta con características que a primera vista pueden resultar interesantes o apropiadas.

En ese sentido, las pequeñas y medianas empresas, deben documentarse para realizar esta elección que en gran medida debe estar respaldad por los criterios de un profesional. En consecuencia, a esto, mediante la presente revisión monográfica se establece una propuesta de selección de un SGBD para un escenario propuesto; en base a criterios soportados por una revisión conceptual y funcional de los gestores con mayor representatividad y reputación en el mercado, bien sea por su larga trayectoria o por innovaciones particulares al contexto de los SGBD

El documento ofrece información conceptual y evolutiva sobre el contexto de las bases de datos y los sistemas de gestión, y al final una propuesta de análisis característico de varios gestores que permitió la elección de un gestor bajo un escenario propuesto. Es importante resaltar que, si bien con esta propuesta que busca brindar documentación a las MiPymes, es solo una apreciación conceptual que puede ser modificada de acuerdo a las consideraciones o necesidades de cada organización.

1. DEFINICIÓN DEL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

Actualmente se está experimentando cambios importantes en el ámbito tecnológico, los cuales afectan de manera directa las diferentes esferas de la sociedad, "la aceleración de la revolución digital está modificando los patrones de consumo y de producción en todo el mundo"[1]. En este sentido, manifiesta Gimeno[2] que el mundo de los negocios ha cambiado y que las TIC se han convertido en una herramienta trascendental que ha favorecido el éxito de las empresas, puesto a través de las diferentes herramientas que ofrecen se puede mantener un mejor control de la información y de las principales operaciones de las empresas, lo que facilita la toma de decisiones y la consecución de sus objetivos.

En el mundo globalizado de hoy, la información se conjuga en un activo vital para las empresas, en la medida que constituyen la base de todo proceso, actividad o acción que se ejecuta dentro de ellas; posibilitando la interacción de los individuos y el éxito de los procesos empresariales. La toma de decisiones acertadas en las organizaciones se fundamenta en informaciones almacenadas que cumplan las características de estar estandarizadas, actualizadas y con disponibilidad inmediata para los usuarios de la empresa[3]. De allí que el respaldo de los datos se haya convertido en un proceso fundamental.

Desde esta perspectiva, las bases de datos entendidas como "un conjunto estructurado de datos dispuestos con el objetivo de proporcionar información a los usuarios y permitir transacciones como inserción, eliminación y actualización de datos"[4], son un instrumento clave y trascendental para el almacenamiento estructurado de datos, y facilitar la ejecución de los procesos que se viven al interior de una empresa.

---

[1] DINI, Marco y STUMPO, Giovanni (coords.), "Mipymes en América Latina: un frágil desempeño y nuevos desafíos para las políticas de fomento", Documentos de Proyectos (LC/TS.2018/75), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2018.

[2] GIMENO, Vicente Alfonso. La influencia de las nuevas tecnologías de la información y las comunicaciones y su repercusión en las estrategias empresariales. La banca online y su aplicación en las cooperativas de crédito. 2015. Tesis Doctoral. Universidad de Valencia.

[3] CAPACHO PORTILLA, José Rafael, y NIETO BERNAL, Wilson. Diseño de Base de Datos. [En Línea] Barranquilla: Universidad del Norte, 2017.

[4] BENÍTEZ, Miguel y ARIAS, Ángel. Curso de introducción a la administración de bases de datos. IT Campus Academy. 2015. P, 283.

Atendiendo a este panorama que vincula la información con su almacenamiento y estructuración en un sistema denominado “Base de datos” aparece en el mundo empresarial y de la información el termino de Sistemas de Gestión de Bases de Datos - SGBD, o sencillamente software que permiten la creación, diseño y administración de las bases de datos. Estos gestores son una pieza clave en la información y seguridad de la empresa, por lo tanto, su elección debe ser un proceso responsable y estratégico.

No obstante, muchas veces las empresas toman decisiones sin establecer un mínimo de características y criterios que les permita definir que gestor de bases de datos se amolda mejor a sus necesidades como empresa. En este sentido, y comprendiendo la importancia de estos sistemas informáticos en el contexto de la sociedad de la información, se plantea la presente investigación monográfica que pretende hacer una revisión conceptual de una muestra de sistemas de gestión de bases de datos y señalar unas particularidades en el contexto de la seguridad que permitan realizar una elección adecuada basada en una decisión estratégica y acorde a los requerimientos de cada organización.

1.2. FORMULACIÓN DEL PROBLEMA

En este sentido, y con el fin de lograr este propósito se esboza la siguiente pregunta directriz: ¿Qué características de seguridad se deben tener en cuenta para definir indicadores que permita a las Pymes seleccionar un Sistemas de Gestión de Bases de Datos?

2. JUSTIFICACIÓN

En esta época en que la información se constituye en una herramienta trascendental para la toma de decisiones en el ámbito organizacional, la adecuada selección de bases de datos y sistemas de gestión de las mismas, es prioritario para el desarrollo y logro de los objetivos de la organización. Contar con sistemas informáticos sólidos, asequibles y funcionales, ya no es una opción, es una necesidad de toda organización, con el fin de estar preparados para los requerimientos que exige la toma de decisiones para la puesta en marcha de estrategias que favorecen el éxito organizacional.

"Diariamente en el mundo se generan aproximadamente 2.5 billones de datos y los formatos y plataformas en los que está disponible la información son sumamente variados, esto presenta un desafío con respecto a qué estructura de almacenamiento es más adecuada para obtener la mayor eficiencia y eficacia sobre el acceso y procesamiento de los datos, en pro de generar información de mayor utilidad y de aportar a la generación de conocimiento en un contexto determinado"[5]

En este sentido, y dada la necesidad del respaldo y seguridad de la información de las organizaciones reviste la importancia de la presente monografía que entrega pautas y criterios para la elección de un SGBD, basado en sus características, específicamente en las de seguridad. Con esto se aporta información significativa para el momento de decidir qué gestor de bases de datos es más adecuado según las particularidades de seguridad que ofrece a los usuarios.

De igual forma, el estudio monográfico ofrece al futuro Especialista en Seguridad Informática, herramientas y conocimientos, para establecer procesos documentados sobre técnicas o mecanismos al momento de tomar decisiones en su campo de acción profesional. Al igual que se establecen puntos de debate y reflexión sobre una temática tan significativa para el contexto informático y empresarial.

[5] TREVIÑO VILLALOBOS, Marlen, et al. Una comparación de rendimiento entre MongoDB, ArangoDB y CouchBase para la operación lectura sobre bases de datos geográficas. En: IEEE. 2018.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar las características de seguridad de una muestra de Gestores de Bases de Datos para determinar indicadores que permita hacer una elección adecuada en Pymes

3.2 OBJETIVOS ESPECÍFICOS

Determinar la muestra de los gestores de bases de datos especificando sus características más relevantes.

Identificar el proceso evolutivo que han tenido los gestores de bases de datos en cuanto a la característica de seguridad.

Establecer indicadores que permitan hacer una selección adecuada de un gestor de bases de datos bajo un escenario propuesto.

4. MARCO DE REFERENCIA

4.1 MARCO TEÓRICO

4.1.1 Bases de Datos – BD: La actividad empresarial de la sociedad actual demanda una gran cantidad de información que requiere ser almacenada para su constante consulta en el desarrollo de las actividades organizacionales, en este orden de ideas, tienen cabida las bases de datos, como el espacio para almacenar toda esta información, bien sea de manera física o digital. Así, una base de datos es definida como "la representación de una colección de datos estructurada que describe las actividades de una organización. Esta representación incluye entidades del mundo real y sus interrelaciones y tiene que permitir diversas utilizaciones" [6].

De igual forma, según el autor Capacho, define el concepto de bases de datos como: La representación a nivel integrado de una colección estructurada de datos que contienen físicamente el diseño lógico de un conjunto de entidades, instancias de las diferentes entidades del sistema de información que se está modelando en una organización y las interrelaciones de las entidades; representación que necesita de una gestión de datos a fin de ser utilizados de una forma compartida por todos los usuarios de una organización en la resolución de sus necesidades de información[7].

Por su parte, la Universidad Internacional de Valencia[8], asocia el termino de bases de datos, con "monumentales armarios digitales de información" que pueden contener registros de todo tipo de temas. Esta entidad expresa que las bases de datos son una herramienta fundamental que están creciendo con la tecnología y revisten de gran importancia para las empresas, debido a la variedad y amplitud de información útil que proporcionan para la toma de decisiones.

En concordancia con las definiciones anteriores, se entiende entonces, que una base de datos es una colección de datos o conjunto de información, que se organiza y asocian entre sí de forma sistemática, para que se pueda acceder, administrar y actualizar de manera fácil y práctica. Las bases de datos facilitan no solo el

---

[6] RODRÍGUEZ GONZÁLEZ, María Elena. Gestión de datos: bases de datos y sistemas gestores de bases de datos. Barcelona: Editorial UOC, 2013.
[7] CAPACHO PORTILLA, José Op Cit.,19
[8] UNIVERSIDAD INTERNACIONAL DE VALENCIA. Los principales tipos de base de datos. VIU.2018.

almacenamiento, sino también la preservación de la información, por lo que la aparición de la electrónica y la computación ha sido fundamental para el respaldo de grandes volúmenes de datos.

4.1.1.1 Estructura de una base de datos: Las bases de datos están compuestas de datos y de metadatos. Los metadatos son datos (valga la redundancia) que sirven para especificar la estructura de la base de datos; por ejemplo, qué tipo de datos se almacenan (si son texto o números o fechas ...), qué nombre se le da a cada dato (nombre, apellidos), cómo están agrupados, cómo se relacionan[9].

En este sentido, señala Sánchez, se producen dos visiones de la base de datos: una estructura lógica y una física, que el autor define de la siguiente manera.

Estructura lógica. Indica la composición y distribución teórica de la base de datos. La estructura lógica sirve para que las aplicaciones puedan utilizar los elementos de la base de datos sin saber realmente cómo se están almacenando. Es una estructura que permite idealizar a la base de datos. Sus elementos son objetos, entidades, nodos, relaciones, enlaces, que realmente no tienen presencia real en la física del sistema. Por ello para acceder a los datos tiene que haber una posibilidad de traducir la estructura lógica en la estructura física.

Estructura física. Es la estructura de los datos tan cual se almacenan en las unidades de disco. La correspondencia entre la estructura lógica y la física se almacena en la base de datos (en los metadatos)[10].

4.1.1.2 Ventajas y desventajas de las bases de datos: Como todo proceso, obtener una base de datos tiene sus ventajas y desventajas, Sánchez, las identifica de la siguiente manera:

Ventajas

- ✓ Independencia de los datos y los programas y procesos. Esto permite modificar los datos sin modificar el código de las aplicaciones.
- ✓ Menor redundancia. No hace falta tanta repetición de datos. Aunque, sólo los buenos diseños de datos tienen poca redundancia.

[9] SÁNCHEZ, Jorge. Diseño Conceptual de Bases de Datos. California: Creative Commons, 2014.
[10] Ibid., p,8.

- ✓ Integridad de los datos. Mayor dificultad de perder los datos o de realizar incoherencias con ellos.
- ✓ Mayor seguridad en los datos. Al limitar el acceso a ciertos usuarios.
- ✓ Datos más documentados. Gracias a los metadatos que permiten describir la información de la base de datos.
- ✓ Acceso a los datos más eficiente. La organización de los datos produce un resultado más óptimo en rendimiento.
- ✓ Menor espacio de almacenamiento. Gracias a una mejor estructuración de los datos.

Desventajas

- ✓ Instalación costosa. El control y administración de bases de datos requiere de un software y hardware poderoso.
- ✓ Requiere personal cualificado. Debido a la dificultad de manejo de este tipo de sistemas.
- ✓ Implantación larga y difícil. Debido a los puntos anteriores. La adaptación del personal es mucho más complicada y lleva bastante tiempo.
- ✓ Impacto en la organización por fallos: Teniendo en cuenta que los datos de la organización están centralizados en la base de datos, y todas las dependencias de la empresa se suplen de la misma estructura de los datos almacenados de la base de datos, entonces cualquier falla del SGBD impacta a la organización estructuralmente en términos de atención a las necesidades de información.
- ✓ Ausencia de estándares reales. Lo cual significa una excesiva dependencia hacia los sistemas comerciales del mercado. Aunque hay una buena parte de esta tecnología aceptada como estándar de hecho[11].

4.1.1.3 Tipos de bases de datos: La clasificación más común de las bases de datos se da de acuerdo a las características, de variabilidad y contenido. Para la primera particularidad se dividen en dinámicas y estáticas; por su contenido se clasifican en bibliográficas, de texto completo, directorios, o de tipo biblioteca.

[11] Ibid., p,9.

- ✓ Las bases de datos de tipo OLTP (On Line Transaction Processing) también son llamadas bases de datos dinámicas lo que significa que la información se modifica en tiempo real, es decir, se insertan, se eliminan, se modifican y se consultan datos en línea durante la operación del sistema. Un ejemplo es el sistema de un supermercado donde se van registrando cada uno de los artículos que el cliente está comprando y a su vez el sistema va actualizando el Inventario[12].

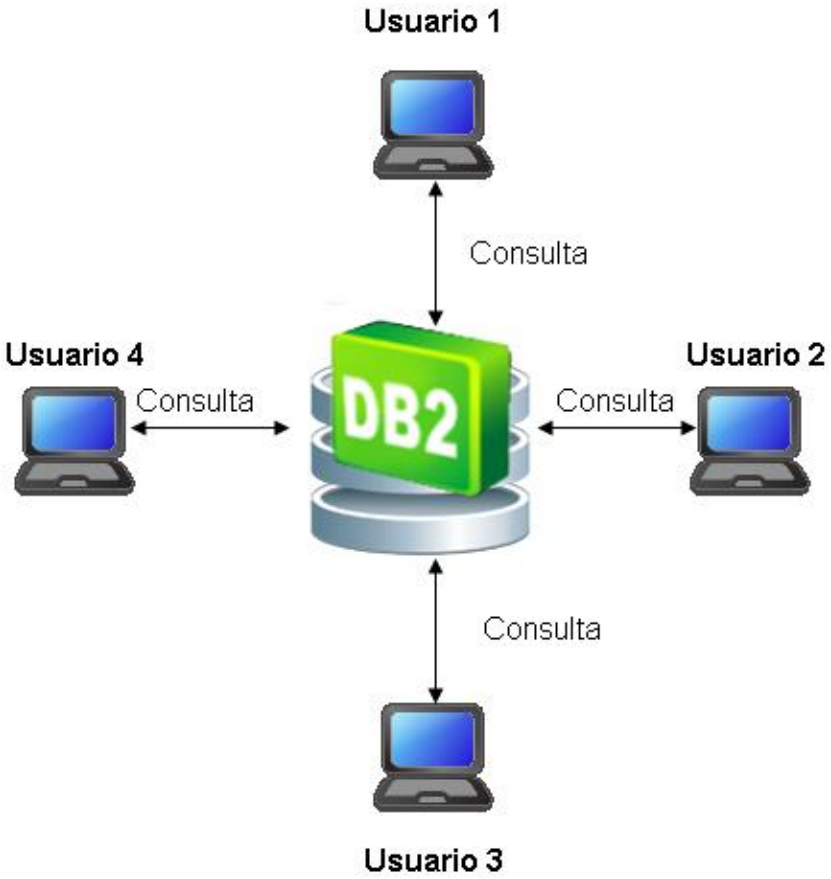
Figura 1. Esquema de funcionamiento de Bases de datos dinámicas

Fuente: Anguiano Morales, Jorge. Características y tipos de bases de datos Argentina: IBM. 2014.

[12] ANGUIANO MORALES, Jorge. Características y tipos de bases de datos. Argentina: IBM. 2014.

- ✓ Las bases de datos de tipo OLAP (On Line Analytical Processing) también son llamadas bases de datos estáticas lo que significa que la información en tiempo real no es afectada, es decir, no se insertan, no se eliminan y tampoco se modifican datos; solo se realizan consultas sobre los datos ya existentes para el análisis y toma de decisiones. Este tipo de bases de datos son implementadas en Business Intelligence para mejorar el desempeño de las consultas con grandes volúmenes de información[13].

Figura 2. Esquema de funcionamiento de Base de datos estáticas



Fuente: Anguiano Morales, Jorge. Características y tipos de bases de datos Argentina: IBM. 2014.

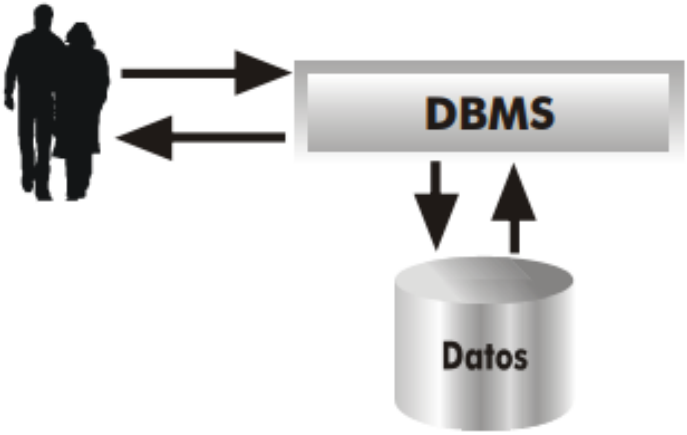
[13] Ibid.,

4.1.2 Sistemas de Gestión de Bases de Datos – SGBD: Los Sistemas de Gestión de Bases de Datos SGBD o *Database Management Systems - DBMS* se constituyen en los programas que permiten la manipulación y acceso de los datos en las BD. Un sistema de gestión de bases de datos es un software específicamente diseñado y desarrollado para asistir en la creación, manipulación y el almacenamiento de las bases de datos[14]. Por su parte, Ongo[15] lo define como una colección de programas que se ejecutan en una computadora y ayudan al usuario a recopilar, cambiar, proteger y administrar información. Generalmente los SGBD se componen de un lenguaje de definición de datos, de un lenguaje de manipulación de datos y de un lenguaje de consulta.

Según Hernández y Sánchez[16] el Lenguaje de definición de datos o DDL por sus siglas en inglés, es aquel que permite establecer la estructura o modelo de base de datos mediante una serie de definiciones que se expresan en un lenguaje especial, cuyo resultado se almacena en el diccionario de datos. Por su parte, el Lenguaje Manipulador de Datos o DML, hace referencia a una serie de expresiones que permiten manipular los datos. Y finalmente, el Lenguaje de control de datos, responde a "los elementos útiles para trabajar en un entorno multiusuario, en el que es importante la protección de los datos, la seguridad de las tablas y el establecimiento de restricciones en el acceso, así como elementos para coordinar el proceso de compartir los datos por parte de usuarios concurrentes, asegurando que no interfieren unos con otros"[17].

[14] RODRÍGUEZ GONZÁLEZ, María Elena. Gestión de datos: bases de datos y sistemas gestores de bases de datos. Barcelona: Editorial UOC, 2013.
[15] ONGO, Gregorius. y KUSUMA, Gede, "Sistema de base de datos híbrida de MySQL y MongoDB en desarrollo de aplicaciones web", *Conferencia Internacional sobre Gestión de la Información y Tecnología de 2018 (ICIMTech)*, Yakarta, 2018, pp. 256-260.
[16] HERNÁNDEZ BASURTO, Tomás Uriel y SÁNCHEZ JIMÉNEZ, Diana Ivonne. Desarrollo de un sistema de administración de bases de datos terminológicas y flexibles. Tesis para optar el título de Ingeniero en computación. México: Universidad Nacional Autónoma De México. Facultad De Ingeniería. 2009.
[17] Ibid., p.9

Figura 3. Funcionamiento y utilidad de un SGBD



Fuente: Sánchez, Jorge. Diseño Conceptual de Bases de Datos. California: Creative Commons, 2014.

4.1.2.1 Funciones de los SGBD: los SGBD cumplen tres funciones básicas dentro del desarrollo y aplicación de una base de datos. Vallejos[18] las define como: función de descripción o definición, función de manipulación y función de control.

- ✓ Función de descripción o definición: Permite al diseñador de la base de datos crear las estructuras apropiadas para integrar adecuadamente los datos. Esta función es la que permite definir las tres estructuras de la base de datos (relacionadas con sus tres esquemas): Estructura interna, Estructura conceptual y Estructura externa. Esta función se realiza mediante el lenguaje de descripción de datos o DDL, el cual permite la definición de las estructuras de datos, la definición de las relaciones entre los datos y define las reglas que han de cumplir los datos.
- ✓ Función de manipulación: Permite modificar y utilizar los datos de la base de datos. Se realiza mediante el lenguaje de modificación de datos o DML. El cual posibilita añadir, eliminar, modificar y buscar datos. Actualmente se suele distinguir la función de buscar datos respecto del resto. Para lo cual se proporciona un lenguaje de consulta de datos o DQL.
- ✓ Función de control: esta última función concede a los administradores mecanismos para determinar las visiones de los datos permitidas a cada usuario, además de proporcionar elementos de creación y modificación de esos usuarios. Se suelen incluir aquí las tareas de copia de seguridad, carga de ficheros, auditoria protección ante ataques externos, configuración del sistema. El lenguaje que implementa esta función es el lenguaje de control de datos o DCL[19].

[18] VALLEJOS, SOFIA. Sistemas de BD en Dispositivos Móviles y su Integración con las BD Tradicionales. Argentina: Universidad Nacional del Nordeste. 2010
[19] Ibid., p, 20

Figura 4. Funciones de los SGBD

Función	Descripción
Definición de la base de datos	Lenguaje y herramientas gráficas para definir entidades, relaciones, restricciones de integridad y autorización de privilegios
Acceso no procedural	Lenguaje y herramientas gráficas para acceder a los datos sin necesidad de código complicado
Desarrollo de aplicaciones	Herramienta gráfica para desarrollar menús, formularios de captura de datos y reportes; los requerimientos de datos para los formularios y reportes se especifican utilizando un acceso no procedural
Interfase del lenguaje procedural	Lenguaje que combina el acceso no procedural con las capacidades totales de un lenguaje de programación
Procesamiento de transacciones	Mecanismos de control para prevenir la interferencia de usuarios simultáneos y recuperar datos perdidos en caso de una falla
Ajuste de la base de datos	Herramientas para monitorear y mejorar el desempeño de la base de datos

Fuente: Mannino, Michael. Administración de bases de datos. Diseño y desarrollo de aplicaciones. 3ra ed. México. McGraw Hill. 2007.

4.1.3 Modelos de SGBD: Existen dos modelos básicos de gestores de acuerdo a la forma como administran los datos, los sistemas de bases de datos SQL (Sistema de Consulta Estructurado) o relacionales y los NoSQL o no relacionales.

4.1.3.1 Sistema de gestión de bases de datos relacionales o SQL: Según La Universidad de Murcia, son el modelo más usado en la actualidad, y se constituye básicamente en un conjunto de tablas, similares a las tablas de una hoja de cálculo, formadas por filas (registros) y columnas (campos). Los registros representan cada uno de los objetos descritos en la tabla y los campos los atributos (variables de cualquier tipo) de los objetos. En el modelo relacional de base de datos, las tablas comparten algún campo entre ellas. Estos campos compartidos van a servir para establecer relaciones entre las tablas que permitan consultas complejas[20]

Señala Ongo[21], que el SGBD relacional es un sistema de base de datos de uso común, pero tiene un rendimiento reducido al manejar una gran cantidad de datos. Concuerdan con esto también, Chickerur, Goudar y Kinnerkar, quienes indican que todo tiene un costo y que las SGBD relacionales tienen el suyo cuando se trata de almacenar grandes volúmenes de datos.

Las bases de datos relacionales son excelentes para hacer cumplir la integridad de los datos. Son la herramienta elegida para aplicaciones de procesamiento de

[20] UNIVERSIDAD DE MURCIA. Bases de datos relacionales. UM. 2010.
[21] ONGO. Op. cit., p. 2

transacciones en línea (OLTP) como sistemas de entrada de datos o aplicaciones de pedidos en línea. RDBMS (Management system relational database) requiere que los datos se normalicen para que puedan proporcionar resultados de calidad y evitar registros huérfanos y duplicados. Utiliza claves e índices primarios y secundarios para permitir que las consultas recuperen datos rápidamente. Pero todas las buenas intenciones que tiene el RDBMS para garantizar la integridad de los datos tienen un costo. La normalización de datos requiere más tablas, lo que requiere más combinaciones de tablas, lo que requiere más claves e índices. A medida que las bases de datos comienzan a crecer en terabytes, el rendimiento comienza a disminuir significativamente. A menudo, el hardware se lanza al problema[22]

En cuanto a los atributos o ventajas de los gestores relacionales más comunes en el mercado, Ongo señala el rendimiento, el costo y la velocidad; resaltando como gestores más comunes MySQL, Oracle y PostgreSQL.

Los sistemas de gestión de bases de datos relacionales (RDBMS) más utilizados son MySQL, Oracle y PostgreSQL. Cada RDBMS es bien conocido y tiene su propia superioridad. MySQL es conocido por su ejecución de consultas más rápida que las otras RDBMS. Aunque PostgreSQL tiene un rendimiento relativamente más lento que MySQL, PostgreSQL tiene más funciones que pueden ayudar al usuario a administrar los datos. Oracle generalmente se elige cuando el usuario necesita manejar datos grandes y complejos. Sin embargo, Oracle es más costoso de implementar que las otras bases de datos. Por otro lado, MySQL se registra como el almacenamiento de datos más utilizado para aplicaciones web debido a su velocidad en la lectura de datos[23].

[22] CHICKERUR, Satyadhyan; GOUDAR, Anoop y KINNERKAR, Ankita "Comparación de la base de datos relacional con la base de datos orientada a documentos (MongoDB) para aplicaciones de Big Data", *octava conferencia internacional de 2015 sobre ingeniería avanzada de software y sus aplicaciones (ASEA)*, Jeju, 2015, pp. 41-47.
[23] ONGO. Op. cit., p. 2

4.1.3.2 Sistema de gestión de bases de datos no relacional o NoSQL: El termino NoSQL, significa no solo SQL, y según Patil et a[24], ofrece más posibilidades más allá del enfoque clásico de almacenamiento y recuperación de datos, de igual forma manifiesta Ongo[25] que NoSQL es una opción de almacenamiento alternativa que es diferente de gestores de bases de datos relacionales y es conocida por su rendimiento más rápido cuando se manejan grandes cantidades de datos.

Los sistemas de bases de datos NoSQL son bases de datos no relacionales diseñadas exclusivamente para brindar alta accesibilidad, confiabilidad y escalabilidad para datos enormes. Además, la fragmentación es la principal circunstancia favorable y fundamental de la base de datos NoSQL. Varias compañías se están moviendo hacia las bases de datos NoSQL. Las bases de datos NoSQL pueden almacenar datos no estructurados como correo electrónico, multimedia, documentos y redes sociales con alto rendimiento[26].

De acuerdo con Patil et al[27], los gestores NoSQL proporciona un modelo de datos más flexible, una mayor escalabilidad y un rendimiento superior al tiempo que incorpora varias características clave de las bases de datos relacionales; tanto así, que la influencia de esta evolución ha sido muy acogida por los equipos de desarrollo de aplicaciones, dado que casi todas las aplicaciones modernas requieren que los desarrolladores creen nuevos tipos de datos que cambian rápidamente a medida que trabajan en iteraciones rápidas.

En congruencia con lo anterior, se puede afirmar que la principal característica y a la vez ventaja de los gestores NoSQL, radica en el manejo de grandes volúmenes de datos con confiabilidad. “Las bases de datos NoSQL pueden manejar enormes datos organizados y no estructurados. No hay esquema fijo; Enormes datos pueden almacenarse en forma de almacenes de datos orientados a documentos, almacenes de datos de valores clave, almacenes de datos de familias de columnas y almacenes de datos de gráficos”[28]

---

[24] PATIL, Mayur, *et al*."A qualitative analysis of the performance of MongoDB vs MySQL database based on insertion and retriewal operations using a web/android application to explore load balancing — Sharding in MongoDB and its advantages," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, 2017, pp. 325-330.

[25]ONGO. Op. cit., p. 2

[26] KUMAR, Jitender; GARG, Varsha. "Security analysis of unstructured data in NOSQL MongoDB database," *2017* International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN)*,* Gurgaon, 2017, pp. 300-305.

[27] PATIL, Op. cit., p. 5

[28] KUMAR, Op. cit., p. 1

4.1.4 Problemas de seguridad en gestores de bases de datos relacional y no relacional. Las bases de datos se constituyen en grandes y valiosos activos para las empresas, por el volumen de información que en ellas se almacena, de igual forma son de gran atractivo para personas maliciosas, por lo que cualquier foco de vulnerabilidad de los gestores puede ser usado para acceder a la información respaldada. En ese sentido, "la seguridad de la información es el conjunto de medidas técnicas, operativas, organizativas, y legales que permiten a las organizaciones resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma"[29].

Es así como, los Sistemas de Gestión de Bases de Datos deben "proveen mecanismos que garantizan la seguridad, consistencia y reglas de integridad. Estos conceptos son implementados en la práctica usando varios elementos, algoritmos genéricos y estándares y otros más particulares del motor de Bases de Datos usado"[30].

Según Tamayo, existen elementos dentro de los gestores de base de datos que pueden ayudar a garantizar la seguridad de la información y deben estar enfocados hacia la exactitud, consistencia y confiabilidad de la información para respaldar la privacidad y confidencialidad de los datos. Entre ellos, señala las Claves Primarias, Reglas de Integridad, Dominio de los atributos, Reglas de integridad del negocio, Vistas, Perfiles de usuario y acceso a objetos de la Base de Datos, Auditoría, Criptografía de Datos, Disparadores o Triggers y Procedimientos Almacenados.

4.1.4.1 Vulnerabilidades más comunes en los gestores de bases de datos: Guzmán[31] plantea los siguientes factores, los cuales señala como unas vulnerabilidades a bordo de los sistemas de gestión de bases de datos.

- ✓ Nombre de usuario/contraseña en blanco o bien hacer uso de uno débil. - Hoy en día no es raro encontrar pares de datos usuario/contraseña del tipo admin/12345 o similar. Esta es la primera línea de defensa de entrada a la información y se debe optar por el uso de algo más complejo que sea complicado de conseguir por parte de cualquier atacante.

[29] Ministerio de Tecnologías de la Información y las Comunicaciones. Guía para la Implementación de Seguridad de la Información en una MIPYME. Bogotá: MinTic. 2016.
[30] TAMAYO ÁLZATE, Alonso y DUQUE MÉNDEZ, Néstor Darío. Mecanismos de seguridad e integridad en un sistema de bases de datos. En: *Rev Departamento de Ciencias*. Universidad Nacional. 2001
[31] GUZMÁN QUESADA, Paúl Andrés. Análisis de las vulnerabilidades en Sistemas Gestores de Bases de Datos. Tesis de Grado. Pontificia Universidad Católica del Ecuador. Escuela De Sistemas y Computación. 2019

- ✓ Preferencia de privilegios de usuario por privilegios de grupo. - En ocasiones muchos usuarios reciben más privilegios sobre la base de datos de los que realmente necesitan, lo que a la larga se puede convertir en un importante problema. Es recomendable modificar los privilegios otorgados a los usuarios que estarán en contacto con la información con el fin de que no puedan realizar modificaciones más allá de las autorizadas.

- ✓ Características de bases de datos innecesariamente habilitadas. - Cada instalación de base de datos viene con una serie de paquetes o módulos adicionales de distintas formas y tamaños que en muy pocas ocasiones todos ellos son utilizadas por las compañías, lo que las convierten en una posible puerta de entrada para sufrir algún tipo de ataque si en esos paquetes se descubre cualquier problema de seguridad.

- ✓ Desbordamiento de búfer. - Se trata de otro de los medios favoritos utilizados por los piratas y que se dan por el exceso de información que se puede llegar a enviar por medio del ingreso de información mediante el uso de formularios, es decir, se recibe mucha más información de lo que la aplicación espera.

- ✓ Bases de datos sin actualizar. - Como ocurre con cualquier tipo de aplicación que se tiene instalada en un computador, es necesario ir actualizando la versión de la base de datos con las últimas versiones lanzadas al mercado, ya que en ellas se solucionan aquellos problemas de seguridad detectados.

- ✓ Datos sensibles sin cifrar. – La encriptación de datos importante en la base de datos ayuda a dificultar la tarea en caso de que una persona ajena acceda a ella sin permiso y desee visualizar la información. Debido a que no se encuentra legible y le imposibilita la lectura de la información

4.1.4.2 Amenazas a las que están expuestos los Gestores de Bases de Datos: Las amenazas se constituyen en unos factores de peligro, externos o incluso internos, que pueden influir sobre los sistemas de gestión de bases de datos y por ende quebrantar la seguridad de la información respaldada.

- ✓ Ataques externos

• Inyección SQL: Consiste en la inserción de código SQL por medio de los datos de entrada desde la parte del cliente hacia la aplicación. Es decir, por medio de la inserción de este código el atacante puede modificar las consultas originales que debe realizar la aplicación y ejecutar otras totalmente distintas con la intención de acceder a la herramienta, obtener información de alguna de las tablas o borrar los datos almacenados, entre otras muchas cosas[32].

[32] Ibid., p, 21

Por su parte, Su, Wang y Li[33] explican que este tipo de ataques se ha vuelto muy común en las bases de datos, dado que se puede obtener información privada o en su defecto controlar el servidor. Sostienen, además, que una forma para poder detectar este tipo de ataques es la prueba de penetración.

- Fuerza Bruta: esta amenaza responde a la "forma de recuperar una contraseña probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso. Una de las desventajas de este ataque es que puede tener un costo elevado, ya que utilizan un método de prueba y error el cual puede llevar días semanas incluso meses en poder descifrar una clave para tomar el control y son muy costosos en tiempo computacional"[34]

- Ataque de Diccionario: Este ataque se caracteriza por el uso de palabras escritas en el diccionario como fuente para descifrar la contraseña. Este tipo de ataque es más optimo que el de fuerza bruta, ya que un gran porcentaje de personas utilizan palabras de su lengua, siendo una forma más fácil de recordar la clave. Los ataques de diccionario tienen pocas probabilidades de éxito con sistemas que emplean contraseñas fuertes con letras en mayúsculas y minúsculas mezcladas con números (alfanuméricos) y con cualquier otro tipo de símbolos[35].

Por su parte los ataques internos, provienen como su nombre lo dice, de la organización misma, y se consolidan cuando se realizan modificaciones a los datos almacenados por medio de personas que trabajan dentro de la empresa. En este caso pueden ser realizados por:

Usuario administrador que modifica datos, es decir, un usuario con privilegios de administrador tiene la capacidad de modificar absolutamente toda la información almacenada en la base de datos; o un usuario de la empresa que modifica datos, o sea, un usuario trabajador de la empresa tendrá acceso a la información almacenada, dependiendo de los privilegios que tenga y haya sido dados por el administrador, estará en la capacidad de modificar los registros almacenada en ella[36].

[33] SU, Guanyu, WANG Fang. y LI Qi., "Research on SQL *Injection Vulnerability Attack model",* 5ta Conferencia Internacional IEEE de 2018 sobre Sistemas de Computación e Inteligencia en la Nube (CCIS)*,* Nanjing, China, 2018, pp. 217-221.
[34] GUZMÁN, Op. cit., p. 1
[35] Ibid., p,2
[36] Ibid., p,2

4.1.4.3 Riesgos e impactos que puede generar un incidente de seguridad sobre un gestor de base de datos en una empresa. En el contexto de la seguridad de los gestores de bases de datos, existen vulnerabilidades, como las mencionadas en el ítem anterior, que dejan la puerta abierta para ataque que afectan los protocolos de seguridad de la información consignada en la base de datos. Estos ataques pueden provocar daños fatales, que van desde errores y daños en la infraestructura del sistema, perdida de información, secuestro o robo de información para fines malintencionados. "A nivel global, los ciberataques más comunes son daños en infraestructura, con el 22,3% del total. Mientras que, en Latinoamérica, el principal delito es el robo de información estratégica, con el 39% de los casos. La extorsión, en tanto, se transformó en los últimos años en un fenómeno en todo el mundo, con un impacto del 17,1% a nivel global, pero de 28,1% en Latinoamérica"[37].

En este sentido, los impactos que genera en las organizaciones este fenómeno del hackeo o ciberataque van desde pérdidas de información y económicas hasta detrimentos en la reputación de la empresa. "Bien sea por extorsión o por los costes de reparación y limpieza de las infraestructuras afectadas, un ciberataque siempre conlleva un desembolso económico para la empresa. Y la merma es más acusada cuando se trata de empresas pequeñas**,** porque no sólo tienen que hacer frente al coste de recuperar los datos robados, sino también a la posible pérdida de clientes"[38]

Según Portafolio, la reputación, que es una de las claves del éxito de las empresas, sufre una fuerte afectación en un caso de 'hackeo', dado que la confianza de los clientes se puede ver minimizada, cuando se conoce que una compañía ha sido víctima de robo de información.

Así mismo, afirma ReasonWhy39, que el impacto de un ciberataque, en términos generales, siempre lleva implícita una pérdida de reputación, que conlleva a que se cuestionen la capacidad de la empresa para protegerse de este tipo de ataques y se pone en tela de juicio sus procesos internos."Uno de los casos más relevantes a nivel mundial tiene que ver con Facebook, que tras la revelación de la firma de marketing político Cambridge Analytica sobre el acceso a la información de más de 50 millones de usuarios de la red social para usarla en campañas de propaganda

[37] EL CRONISTA. Seguridad informática en riesgo: cada vez más empresas sufren ciberataques, Argentina. 2017.
[38] REASONWHY. Qué consecuencias puede tener un ciberataque para tu empresa. Madrid: REASONWHY. 2017.
[39] Ibid.

política, la compañía llegó a perder en un solo día 119.000 millones de dólares de valor de mercado"[40].

4.2 MARCO CONCEPTUAL

Para el desarrollo de este trabajo es importante tener claridad en los siguientes conceptos:

4.2.1 Vulnerabilidad: El termino de vulnerabilidad se define como "el riesgo que una persona, sistema u objeto puede sufrir frente a peligros inminentes. La palabra vulnerabilidad deriva del latín *vulnerabilis*. Está compuesto por *vulnus*, que significa 'herida', y el sufijo -*abilis*, que indica posibilidad; por lo tanto, etimológicamente, vulnerabilidad indica una mayor probabilidad de ser herido. Las vulnerabilidades adoptan diferentes formas, dependiendo de la naturaleza del objeto de estudio, sus causas y consecuencias"[41].

En el contexto de la informática el termino de vulnerabilidad responde a "una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos"[42].

4.2.2 Amenaza: El termino amenaza encierra "el peligro inminente, que surge, de un hecho o acontecimiento que aún no ha sucedido**,** pero que de concretarse aquello que se dijo que iba a ocurrir, dicha circunstancia o hecho perjudicará a una o varias personas en particular"[43].

---

[40] PORTAFOLIO. El secuestro de información desangra a las empresas del país. Bogotá: Portafolio.2019.

[41] SIGNIFICADOS. Significado de Vulnerabilidad. [citado 25-03-2020] Disponible en: https://www.significados.com/vulnerabilidad/

[42] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? CIBER. 2017.

[43] SIGNIFICADOS. Significado de Amenaza.

Aterrizando este término a la informática, “una amenaza es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio”[44]
“una amenaza es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de un sistema. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas”[45]. En otras palabras, una amenaza es una situación desfavorable que puede ocurrir sobre los activos informáticos de una empresa, generando resultados negativos.

4.2.3 Riesgo: El riesgo se define como la “posibilidad de que algo desagradable acontezca**.** Se asocia generalmente a una decisión que conlleva a una exposición o a un tipo de peligro**”**[46]. Para el caso de la informática, el riesgo se concibe cuando hay una “probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños. Se mide asumiendo que existe una cierta vulnerabilidad frente a una determinada amenaza, como puede ser un hacker, un ataque de denegación de servicios, un virus, entre otro. El riesgo depende entonces de los siguientes factores: la probabilidad de que la amenaza se materialice aprovechando una vulnerabilidad y produciendo un daño o impacto. El producto de estos factores representa el riesgo”[47], a continuación, en la figura 5 se visualiza como se representa el riesgo.

[44] Ministerio de Tecnologías de la Información y las Comunicaciones, Op, cit. p,4
[45] INSTITUTO NACIONAL DE CIBERSEGURIDAD, Op, cit.
[46]SIGNIFICADOS. Significado de Amenaza.
[47] INSTITUTO NACIONAL DE CIBERSEGURIDAD, Op, cit.

Figura 5. Representación del riesgo

Fuente: Instituto Nacional De Ciberseguridad. Gestión de riesgos. Una guía de aproximación para el empresario. España: INCIBE.

4.2.4 Impacto: El Instituto Nacional de Ciberseguridad define el impacto como una "consecuencia de la materialización de una amenaza sobre un activo aprovechando una vulnerabilidad. El impacto se suele estimar en porcentaje de degradación que afecta al valor del activo, el 100% sería la pérdida total del activo"[48].

[48] INCIBE. Gestión de riesgos. Una guía de aproximación para el empresario. España: INCIBE

Figura 6. Relación de los términos amenaza, vulnerabilidad e impacto

Fuente: INCIBE. Gestión de riesgos. Una guía de aproximación para el empresario. España: INCIBE.

4.2.5 Seguridad en Gestores de Bases de Datos: El proceso de seguridad de un sistema de gestión de bases de datos, es un elemento fundamental para la organización, dado que depende de esto el respaldo de la información almacenada en la base de datos. En el campo de los SGBD, el término seguridad se suele utilizar para hacer referencia a los temas relativos a la confidencialidad, las autorizaciones, los derechos de acceso, etc[49].

"La seguridad de las bases de datos es un área amplia que abarca múltiples temas, entre ellos: cuestiones éticas y legales relativas al derecho de tener acceso a cierta información; cuestiones de política a nivel gubernamental, institucional o corporativo, relacionadas con el tipo de información que no debe estar disponible

[49] CAMPS PARÉ, Rafael *et al.* Bases de datos. 1ra ed. Barcelona: Universitat Oberta de Catalunya. 2005

para el público; y, cuestiones relacionadas con el sistema, como los niveles del sistema en que deben manejarse diversas funciones de seguridad"[50].

Domínguez[51] señala dos mecanismos de seguridad: el primero orientado a definir, políticas de control de acceso basadas en la identidad del usuario. Generalmente se usan para otorgar privilegios a los usuarios, incluida la capacidad de tener acceso a archivos, registros o campos de datos específicos en un determinado modo. Y el segundo, enfocado a restringir el acceso a información sistematizada como confidencial al personal autorizado. Estos mecanismos que se denominan obligatorios, sirven para imponer igualdad de múltiples niveles clasificando los datos y los usuarios en varias clases (o niveles) de seguridad e implementando después la política de seguridad apropiada de la organización.

4.2.6 MIPYME: El termino MIPYMES significa micro, pequeña y mediana empresa, que según lo conferido en la Ley 590 de 2000**,** "se entiende por micro, pequeña y mediana empresa, toda unidad de explotación económica, realizada por persona natural o jurídica, en actividades empresariales, agropecuarias, industriales, comerciales o de servicios, rural o urbana"[52] para la clasificación de estas empresas, en el caso colombiano, la Ley 590, estableció unos parámetros de planta de personal y activos totales, quedando catalogadas de la siguiente manera:

Mediana Empresa: corresponde a las empresas que tengan una planta de personal entre cincuenta y uno (51) y doscientos (200) trabajadores; y generen activos totales por valor entre cinco mil uno (5.001) y quince mil (15.000) salarios mínimos mensuales legales vigentes.

Pequeña Empresa: aquellas que tienen entre once (11) y cincuenta (50) trabajadores; y activos totales por valor entre quinientos uno (501) y menos de cinco mil (5.001) salarios mínimos mensuales legales vigentes.

Microempresa: hace referencia a las empresas con una planta de personal no superior a los diez (10) trabajadores; y que manejen activos totales por valor inferior a quinientos uno (501) salarios mínimos mensuales legales vigentes.

---

[50] DOMÍNGUEZ CHÁVEZ, Jorge. Principios Básicos de Seguridad en Bases de Datos. Jornada de Investigación, Desarrollo Socio Productivo y Vinculación Social del Departamento de Informática, 2015. 2015

[51] Ibid., p,

[52] COLOMBIA. CONGRESO DE LA REPÚBLICA. LEY 590. Por la cual se dictan disposiciones para promover el desarrollo de las micro, pequeñas y medianas empresa. Bogotá: El Congreso. 2000.

Por su parte la Comisión Económica para América Latina y el Caribe – CEPAL, "las pymes representan actores claves para incrementar el crecimiento potencial de América Latina. Estas empresas se caracterizan por una gran heterogeneidad en su acceso a mercados, tecnologías y capital humano, así como su vinculación con otras empresas, factores que afectan su productividad, capacidad de exportación y potencial de crecimiento"[53].

4.3 ANTECEDENTES

Como antecedentes para el desarrollo del presente trabajo se tomaron como referencia algunos trabajos investigativos similares, enfocados en las diferentes características y factores de la seguridad de los sistemas de gestión de bases de datos, y de la seguridad informática en general. Estos referidos sirven como fundamento teórico y metodológico, además de constituirse en punto de correlación para el planteamiento de los hallazgos obtenidos.

- ✓ Proyecto "Estudio de seguridad en bases de datos SQL y NOSQL. Gómez Mojica, Yeny Mireya. Universidad Nacional Abierta y a Distancia Escuela De Ciencias Básicas, Tecnología e Ingeniería Especialización En Seguridad Informática Bogotá D.C. 2018[54]. El objetivo central de esta investigación estuvo focalizado a identificar las diferentes vulnerabilidades que pueden presentarse en las bases de datos SQL y NoSQL que ponen en riesgo la información de las organizaciones que hacen uso de esta tecnología. Por consiguiente, se analizaron las bases de datos SQL y NoSQL para poder determinar cuál de las dos tecnologías es más conveniente para su uso en ambientes corporativos.

- ✓ Proyecto "Diseño de metodología para verificar la seguridad en aplicaciones web contra inyecciones SQL", trabajo de grado presentado por Iván Camilo Gómez en el año 2011, para optar el título de Ingeniero en Telecomunicaciones de la Universidad Militar Nueva Granada[55]. Este proyecto estableció un diseño metodológico mediante el cual se puede verificar la seguridad en aplicaciones web contra ataques denominados

[53] CEPAL. Acerca de Microempresas y Pymes. Santiago de Chile: CEPAL.
[54] GÓMEZ MOJICA, Yeny Mireya. Estudio de seguridad en bases de datos SQL y NOSQL. Trabajo para optar al título de Especialista en Seguridad de la Información. Bogotá: Universidad Nacional Abierta y A Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería. Especialización en Seguridad Informática. 2018. 92p.
[55] GÓMEZ, Iván Camilo Diseño de metodología para verificar la seguridad en aplicaciones web contra inyecciones SQL. Trabajo de grado presentado para optar el título de Ingeniero en Telecomunicaciones. Universidad Militar Nueva Granada. 2011.

inyecciones por código SQL, específicamente, en aplicaciones web que manejen bases de datos multidimensionales, favoreciendo la protección de los recursos informáticos.

- ✓ Proyecto “Modelos de encriptación en base de datos MS-SQL SERVER., presentado por William Torres Acero como requisito para optar al título de Especialista en Seguridad Informática para la Universidad Nacional Abierta y a Distancia en el año 2018[56]. Este trabajo monográfico tuvo como propósito la encontrar modelos específicos de seguridad mediante encriptación de las bases de datos MS-SQL SERVER, dado el gran campo de acción que se registra en el Colombia para este tipo de bases de datos.

4.4 ESTADO ACTUAL

Actualmente los sistemas de gestión de bases de datos son una herramienta fundamental para la administración de la información en las empresas y la evolución que estos han tenido, ha sido trascendental para el manejo seguro de la información. “Los gestores de base de datos han sido, desde los inicios de la programación de gestión hasta nuestros días, clave para ayudar al desarrollo eficiente de empresas, entes públicos y cualquier organismo que utilice datos, siguiendo en constante avance y mejora”[57].

En este contexto sostiene Marín[58] que el modelo de bases de datos relacionales, hoy posicionado en el mercado como el más utilizado, ha sufrido una serie de trasformaciones desde su aparición en 1970, hasta convertirse, en el modelo predilecto para la administración de bases de datos.

Por su parte, el sitio web *Tecnologías Información*[59]*,* señalan que los gestores difieren en precio, rendimiento, facilidad de administración de la base de datos y funcionalidad y que los principales proveedores en el mercado son: Fujitsu, Hewlett-Packard, Hitachi, IBM, Microsoft, NCR Teradata, Oracle, Progress, SAS Institute y

[56] TORRES ACERO, William. Modelos de encriptación en base de datos MS-SQL SERVER., Trabajo de grado para optar al título de Especialista en Seguridad Informática Bogotá: Universidad Nacional Abierta y A Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería. Especialización en Seguridad Informática. 2018.
[57] KYOCERA Document Solutions. Los mejores gestores de base de datos del mercado. España: Kyocera.
[58] MARÍN Rafael. Los gestores de bases de datos más usados en la actualidad. En: Revista Digital Inesem. 2019.
[59] TECNOLOGÍAS INFORMACIÓN. Sistemas de Gestión de Bases de Datos | Tipos y Clasificación.

Sybase. De igual forma, sostiene este sitio web que: “Los principales proveedores de bases de datos en Europa son Oracle, con una participación de mercado del 40.8%, IBM con 29.4% y Microsoft con 14.9%. Esto les da a las tres empresas más del 85% del mercado, y todas ellas han disfrutado de un crecimiento en los ingresos en los últimos años”.

Según Kyocera[60], los mejores gestores de base de datos y más utilizados, con licencia de pago, son Oracle, catalogado como el gestor de base de datos relacional más fiable y usado; y SQL Server, que se ubica como la competencia directa de Oracle. Mientras en el sector de los gestores con licencia gratuita, se destacan MySQL, como un gestor de simple instalación que actúa del lado del cliente (servidor) y de código abierto con licencia comercial disponible; y FireBird, conocido por ser un gestor potente y, a la vez, sencillo.

> MySQL, gestiona bases de datos relacionales, es multiusuario y el más usado dentro del software libre. Destaca por requerir de poca memoria y procesador para funcionar, dando lugar además a una mayor velocidad en sus operaciones. Es usado principalmente para el desarrollo web. Mientras FireBird, es uno de los mejores gestores de código abierto (Open Source) compatible con Windows y Linux. Entre otras funciones, da soporte completo para procedimientos almacenados, transacciones compatibles con las características ACID y métodos de acceso múltiple (nativo, Python, .NET, etc…)[61].

4.5 MARCO METODOLÓGICO

4.5.1 Tipo de Monografía: La presente monografía es de tipo compilación, bajo una modalidad descriptiva, mediante la cual se analizó información escrita sobre los sistemas de gestión de bases de datos y se establecieron características, factores de vulnerabilidad y demás aspectos que faciliten la definición de indicadores enfocados a la seguridad de los gestores, para la elección de las Pymes. Por lo anterior, se efectuó un análisis descriptivo frente a la evolución, características y factores de seguridad (amenazas, vulnerabilidades, riesgos) de los principales sistemas de gestión de bases de datos.

En este sentido, se tomaron como objetos de información, diferentes artículos teóricos o investigaciones desarrolladas sobre el tema, las cuales puntualizan en la

[60] KYOCERA Document Solutions. Op, cit.
[61] Ibid.

seguridad de los SGBD y los diferentes factores que han influido sobre la seguridad de la información.

4.5.2 **Recolección de la Información:** La recolección de la información se realizó mediante un rastreo bibliográfico teniendo en cuenta variables como:

- Características de los sistemas de gestión de bases de datos
- Seguridad de los sistemas de gestión de bases de datos
- Vulnerabilidades más comunes de los sistemas de gestión de bases de datos

4.5.3 **Fuentes de recolección de la información:** Fuentes primarias: los diferentes libros y artículos se consultaron mediante las bases de datos del sistema de biblioteca de la Universidad de Nacional Abierta y a Distancia y a través de las paginas oficiales de institutos de tecnología.

Fuentes secundarias: como fuente secundaria de información se recurrió a diferentes revistas indexadas, publicaciones de foros, congresos y demás plataformas oficiales y académicas.

5. DESARROLLO DE LOS OBJETIVOS

5.1. MUESTRA DE SISTEMAS DE GESTIÓN DE BASES DE DATOS A PARTIR DE SUS CARACTERÍSTICAS MÁS RELEVANTES

La presente investigación se focaliza en la seguridad de los sistemas de gestión de bases de datos como principal característica, para la definición de indicadores para su selección, sin embargo, se hace relevante conocer otras particularidades de los mismos, que son igual de relevantes al momento de tener que tomar la decisión sobre cual gestor es más viable que otro. En ese sentido, en el presente apartado se hace una aproximación teórica de las principales características de algunos gestores que se consideran entre los más comunes del mercado por su uso y/o comercialización.

5.1.1. Sistemas de gestión de bases de datos relacionales

5.1.1.1. Oracle: El sistema de gestión de bases de datos Oracle, fue introducido al mercado a finales de los años 70 por Oracle Corporation. Este gestor "tiene una estructura física y una estructura lógica que se mantienen separadamente. La estructura física corresponde a los ficheros del sistema operativo: de datos (datafiles), de redo log y de control (controlfiles). La estructura lógica está formada por los tablespace y los objetos de un esquema de BD (tablas, vistas, índices)"[62]. Según la empresa de formación en TIC, NETEC, Oracle utiliza una arquitectura cliente/servidor, y aunque ha incorporado en su sistema el modelo objeto-relacional, al mismo tiempo garantiza la compatibilidad con el tradicional modelo relacional de datos. De igual forma, está considerado como un SGBD de alta eficacia, ya que permite, entre otras cosas, eliminar información redundante, modificar datos e incluso procesar preguntas. Entre sus principales características se pueden identificar las siguientes:

- ✓ Modelo relacional: los usuarios visualizan los datos en tablas con el formato filas/columnas.
- ✓ Herramienta de administración gráfica intuitiva y cómoda de utilizar.
- ✓ Control de acceso: tecnologías avanzadas para vigilar la entrada a los datos.
- ✓ Protección de datos: seguridad completa en el entorno de producción y de pruebas y gestión de copias de seguridad.

[62] PARDO, Brennero TORRES, Gabriel VERGARA, Freddy. Respaldos y recuperación sobre Oracle. Guayaquil – Ecuador. 2010.Tesis para optar al grado de Ingeniero en Sistemas Computacionales. Universidad Católica de Guayaquil. Facultad de Ingeniería, Carrera de Ingeniería en Sistemas Computacionales.

- ✓ Lenguaje de diseño de bases de datos muy completo (PL/SQL): permite implementar diseños "activos", que se pueden adaptar a las necesidades cambiantes de negocio.
- ✓ Alta disponibilidad: escalabilidad, protección y alto rendimiento para la actividad empresarial.
- ✓ Gestión de usuarios: agilidad en los trámites, reducción de costes y seguridad en el control de las personas que acceden a las aplicaciones y a los sistemas[63].

Figura 7. Características de Oracle

Fuente: NETEC. Global Knowledge. ¿Qué es Oracle? Netec.

El cifrado de datos es una de las características más importantes en la seguridad de un sistema de gestión de datos, ya que es la forma de evitar que la información sea accedida y robada. En el contexto del gestor Oracle se habla de encriptación transparente de datos TDE, como medio de respaldar la información.

[63] NETEC. *Global Knowledge.* ¿Qué es Oracle? Netec.

> Oracle Advanced Security Transparent Data Encryption (TDE), introducido en Oracle Database 10g versión 2, es la solución más avanzada del sector para la encriptación. TDE ofrece administración clave y transparencia completa de encriptación de datos de aplicaciones sensibles. El proceso de encriptación de base de datos es activado mediante el uso de comandos DDL, eliminando por completo la necesidad de cambios en las aplicaciones, la administración programática de claves, los triggers de base de datos y las visualizaciones[64].

Se detalla en el informe de Oracle que, "la encriptación de red de Oracle Advanced Security protege los datos en tránsito de la Intranet frente a las modificaciones y el espionaje de red, y Oracle Advanced Security TDE protege los datos sensibles en unidades de disco y medios de backup del acceso no autorizado, ayudando así a reducir el impacto que puede generarse a partir de la pérdida o el robo de medios"[65]

El modelo TDE realiza la encriptación de los datos antes de que se escriban en el disco y los decodifica antes de que vuelvan a la aplicación. En este sentido, el proceso de codificación y decodificación es realizado en el nivel SQL, de manera completamente transparente para las aplicaciones y los usuarios[66].

Sin embargo, Oracle, es un gestor que también tiene desventajas tales como su alto costo, lo que lo hace de uso casi que exclusivo de empresas muy grandes y multinacionales, dado que los costos de soporte técnico y mantenimiento son elevados. De igual forma, presenta vulnerabilidades en la seguridad de la plataforma, lo que hace necesario aplicar parches de seguridad.

Los investigadores chinos, Jing-Wei *et al*[67] consideran que Oracle Database es el sistema de gestión de bases de datos relacionales más popular del mundo, pero que sus problemas de seguridad están empeorando; según estos autores, las configuraciones incorrectas, las vulnerabilidades y los componentes maliciosos de terceros se convierten en los tres problemas más graves, que amenazan la seguridad de Oracle, conllevando al uso de parches de seguridad.

---

[64] ORACLE. Informe Técnico sobre Oracle Advanced Security. Informe Ejecutivo de Oracle. Junio de 2007.
[65] Ibid., p.3
[66] Ibid., p.3
[67] JING-WEI, Pan *et al*. "Un sistema mejorado de escaneo de vulnerabilidades ligero y seguridad mejorada para la base de datos Oracle", *IEEE 2019 4a Conferencia de Tecnología de Información Avanzada, Control Electrónico y Automatización (IAEAC)*, Chengdu, China, 2019, págs. 1699-1702.

Los problemas de seguridad de Oracle, son un limitante para las Pymes, según explican Jing-Wei et al[68] una gran cantidad de este tipo de empresas no tienen equipos de seguridad de red profesionales y empleados operativos de seguridad, y la base de datos Oracle generalmente está en riesgo de invasión, esta relación conlleva a deducir que Oracle no es un gestor viable para este tipo de empresas.

5.1.1.2. MySQL: El Sistema de Gestión de Base de Datos MySQL, también hace parte de la marca Oracle, dado que esta corporación compró a Sun Microsystems, quien había adquirido la patente de este gestor en 2008. Es un gestor con una arquitectura basada en un sistema cliente y servidor. "MySQL es la base de datos de código abierto más popular del mundo. Por su rendimiento, confiabilidad y facilidad de uso comprobados, MySQL se ha convertido en la opción de base de datos líder para aplicaciones basadas en la web, ya que es utilizada por propiedades web de alto perfil como Facebook, Twitter, YouTube y Booking.com. Además, es una opción extremadamente popular como base de datos integrada"[69].

Por su parte, Camps[70] manifiesta que MySQL es un sistema gestor de bases de datos con un alto rendimiento, y aunque carece de algunas características avanzadas disponibles en otros SGBD del mercado, actualmente, se constituye en una opción atractiva tanto para aplicaciones comerciales, como de entretenimiento precisamente por su facilidad de uso y tiempo reducido de puesta en marcha; además de su libre distribución en Internet bajo licencia GPL le otorgan como beneficios adicionales (no menos importantes) contar con un alto grado de estabilidad y un rápido desarrollo. "MySQL se registra como el almacenamiento de datos más utilizado para aplicaciones web debido a su velocidad en la lectura de datos"[71]. Entre sus principales características, señala las siguientes:

- ✓ Está desarrollado en C/C++.
- ✓ Se distribuyen ejecutables para cerca de diecinueve plataformas diferentes.
- ✓ La API se encuentra disponible en C, C++, Eiffel, Java, Perl, PHP, Python, Ruby y TCL.

[68] JING-WEI, Pan *et al*. "Un sistema mejorado de escaneo de vulnerabilidades ligero y seguridad mejorada para la base de datos Oracle", *IEEE 2019 4a Conferencia de Tecnología de Información Avanzada, Control Electrónico y Automatización (IAEAC)*, Chengdu, China, 2019, págs. 1699-1702.
[69] ORACLE COLOMBIA. Oracle MySQL. La base de datos de código abierto más popular del mundo. ORACLE.
[70] CAMPS PARÉ, Rafael *et al.* Op, cit., p, 235
[71] ONGO. Op. cit., p. 2

- ✓ Está optimizado para equipos de múltiples procesadores.
- ✓ Es muy destacable su velocidad de respuesta.
- ✓ Se puede utilizar como cliente-servidor o incrustado en aplicaciones.
- ✓ Cuenta con un rico conjunto de tipos de datos.
- ✓ Soporta múltiples métodos de almacenamiento de las tablas, con prestaciones y rendimiento diferentes para poder optimizar el SGBD a cada caso concreto.
- ✓ Su administración se basa en usuarios y privilegios.
- ✓ Se tiene constancia de casos en los que maneja cincuenta millones de registros, sesenta mil tablas y cinco millones de columnas.
- ✓ Sus opciones de conectividad abarcan TCP/IP, sockets UNIX y sockets NT, además de soportar completamente ODBC.
- ✓ Los mensajes de error pueden estar en español y hacer ordenaciones correctas con palabras acentuadas o con la letra 'ñ'.
- ✓ Es altamente confiable en cuanto a estabilidad se refiere[72].

En cuanto a la seguridad del gestor, Zoratti hace referencia a unos factores de MySQL, que identifica como buenas prácticas de seguridad y que se referencian a continuación.

> MySQL usa conexiones no cifradas entre el cliente y el servidor de forma predeterminada. El procedimiento de autenticación del servidor MySQL verifica tres ámbitos: nombre del cliente / dirección IP, nombre de usuario y contraseña. El servidor almacena información de privilegios en las tablas de concesión de la base de datos MySQL. El servidor MySQL lee el contenido de estas tablas en la memoria cuando se inicia. Las decisiones de control de acceso se basan en las copias en memoria de las tablas de concesión. MySQL proporciona funciones para cifrar y descifrar valores de datos. Las funciones DES permiten el cifrado utilizando el algoritmo Triple-DES[73].

5.1.1.3. PostgreSQL: El sistema de gestión de bases de datos, PostgreSQL, usa el modelo relacional para sus bases de datos, al igual que el lenguaje SQL como lenguaje de consulta. Se caracteriza por ser un gestor de código abierto, que se destaca por diferentes factores que le han permitido competir con cualquier otro SGBD comercial:

- ✓ Está desarrollado en C, con herramientas como Yacc y Lex.

[72] CAMPS PARÉ, Rafael *et al.* Op, cit., p, 235
[73] ZORATTI, Iván "Mejores prácticas de seguridad MYSQL", *Conferencia IET 2006 sobre crimen y seguridad*, Londres, 2006, pp. 183-198.

- ✓ La API de acceso al SGBD se encuentra disponible en C, C++, Java, Perl, PHP, Python y TCL, entre otros.
- ✓ Cuenta con un rico conjunto de tipos de datos, permitiendo además su extensión mediante tipos y operadores definidos y programados por el usuario.
- ✓ Su administración se basa en usuarios y privilegios.
- ✓ Sus opciones de conectividad abarcan TCP/IP, sockets Unix y sockets NT, además de soportar completamente ODBC.
- ✓ Los mensajes de error pueden estar en español y hacer ordenaciones correctas con palabras acentuadas o con la letra 'ñ'.
- ✓ Es altamente confiable en cuanto a estabilidad se refiere.
- ✓ Puede extenderse con librerías externas para soportar encriptación, búsquedas por similitud fonética (soundex), etc.
- ✓ Control de concurrencia multi-versión, lo que mejora sensiblemente las operaciones de bloqueo y transacciones en sistemas multi-usuario.
- ✓ Soporte para vistas, claves foráneas, integridad referencial, disparadores, procedimientos almacenados, subconsultas y casi todos los tipos y operadores soportados en SQL92 y SQL99.
- ✓ Implementación de algunas extensiones de orientación a objetos. En PostgreSQL es posible definir un nuevo tipo de tabla a partir de otra previamente definida[74].

Por su parte, la empresa *Todo PostgreSQL*, publicó en 2018[75] un artículo de ventajas y desventajas sobre el gestor, en el cual hace una descripción más profunda de algunas características que posee, definiéndolas de la siguiente manera:

- ✓ Se puede instalar en todos los equipos que se requieran. Independientemente de la plataforma y la arquitectura que se use, PostgreSQL está disponible para los diferentes SO, Unix, Linux y Windows, en 32 y 64 bits. Esto hace de PostgreSQL un sistema multiplataforma y también hace que sea más rentable con instalaciones a gran escala.
- ✓ Gran escalabilidad**:** Nos permite configurar PostgreSQL en cada equipo según el hardware. Por lo que es capaz de ajustarse al número de CPU y a la cantidad de memoria disponible de forma óptima**.** Con ello logramos una mayor cantidad de peticiones simultáneas a la base de datos de forma correcta.
- ✓ Estabilidad y confiabilidad**:** Tiene más de 20 años de desarrollo activo y en constante mejora. No se han presentado nunca caídas de la base de datos**.** Esto es debido a su capacidad de establecer un entorno de Alta disponibilidad y gracias a Hot-Standby**,** que permite que los clientes puedan

[74] GINESTÁ MARC Gibert y PÉREZ MORA, Oscar. Bases de datos en PostgreSQL. En: Bases de datos. 1ra ed. Barcelona: Universitat Oberta de Catalunya. 2005

[75] SEGOVIA, José. Ventajas y Desventajas de PostgreSQL. Todo PostgreSQL. 2018.

realizar consultas de solo lectura mientras que los servidores están en modo de recuperación o espera. Así pueden hacer tareas de mantenimiento o recuperación sin bloquear completamente el sistema.

Al igual que todos los gestores, PostgreSQL también tiene ciertas limitaciones como las enmarca Camps o desventajas como las define Segovia

- ✓ Puntos de recuperación dentro de transacciones. Actualmente, las transacciones abortan completamente si se encuentra un fallo durante su ejecución. La definición de puntos de recuperación permitirá recuperar mejores transacciones complejas.
- ✓ No soporta tablespaces para definir dónde almacenar la base de datos, el esquema, los índices, etc.
- ✓ El soporte a orientación a objetos es una simple extensión que ofrece prestaciones como la herencia, no un soporte completo[76].

Sumado a esto, "es relativamente lento en inserciones y actualizaciones en bases de datos pequeñas, PostgreSQL está diseñado para ambientes de alto volumen. Esto hace que la velocidad de respuesta pueda parecer lenta en comparación con bases de datos de pequeño tamaño. La sintaxis de algunos de sus comando o sentencias puede llegar a no ser intuitiva si no tienes un nivel medio de conocimientos en lenguaje SQL"[77].

En cuanto al cifrado de datos, PostgreSQL hace uso del módulo "pgcrypto" el cual proporciona funciones criptográficas para este gestor, de la mano de los siguientes algoritmos: MD5, SHA1, SHA224 / 256/384/512, Blowfish, AES, DES / 3DES / CAST5, Encriptación sin procesar, Cifrado simétrico PGP, Cifrado de clave pública PGP[78].

Por su parte cuando se habla de cifrado a nivel de archivo de base de datos Kumar[79] hace referencia a métodos como el cifrado de disco completo y cifrado de archivos a nivel de sistema, para proteger los datos en reposo. El cifrado completo o parcial del disco se constituye en una de las mejores maneras de proteger los datos. Mediante este sistema se protege a cada archivo, y también protege el almacenamiento temporal que puede contener partes de estos archivos. Mientras el cifrado de archivos a nivel de sistema o cifrado de archivos/directorios, protege los archivos individuales o los directorios cifrándolos por el sistema mismo de archivos.

[76] GINESTÁ y PÉREZ. Op, cit., p, 310.
[77] SEGOVIA, Op, cit.
[78] POSTGRESQL. Documentación, PostgreSQL 12. Pgcrypto. 2020.
[79] KUMAR, Vibhor. Postgres y cifrado de datos transparente (TDE). 2015

5.1.1.4 SQL Server: El sistema de gestión de base de datos *Microsoft SQL Server* es un gestor de tipo relacional (RDBMS) producido por la multinacional Microsoft, como alternativa a otros potentes sistemas gestores de bases de datos, tales como son Oracle, Sybase ASE, PostgreSQL o MySQL. Este gestor maneja como su principal lenguaje de consulta Transact-SQL, una aplicación de las normas ANSI / ISO estándar Structured Query Language (SQL)[80].

Afirma Parada[81], que entre las características del gestor SQL Server sobresalen la alta disponibilidad al permitir un gran tiempo de actividad y una conmutación más rápida. Todo esto sin sacrificar los recursos de memoria del sistema. Pero quizá su característica más destacada es que ofrece una solución robusta que se integra a la perfección con la familia de servidores Microsoft Server. De igual forma, este sistema de gestión, cuenta con características como: soporte de transacciones, escalabilidad, estabilidad y seguridad, soporte de procedimientos almacenados, incluye también un potente entorno gráfico de administración, que permite el uso de comandos DDL y DML gráficamente, permite trabajar en modo cliente-servidor, donde la información y datos se alojan en el servidor y las terminales o clientes de la red solo acceden a la información, permite administrar información de otros servidores de datos.

En cuestiones de seguridad, SQL Server usa claves de cifrado para proteger los datos, las credenciales y la información de conexión que se almacena en una base de datos servidor. Según información de Microsoft[82] SQL Server tiene dos tipos de claves: *simétricas* y *asimétricas*. Las claves simétricas utilizan la misma contraseña para cifrar y descifrar los datos. Las claves asimétricas usan una contraseña para cifrar los datos (denominada clave *pública*) y otra para descifrarlos (denominada clave *privada*). En SQL Server, las claves de cifrado incluyen una combinación de claves públicas, privadas y simétricas que se utilizan para proteger la información confidencial. SQL Server utiliza la clave para cifrar los datos confidenciales, el sistema operativo crea las claves públicas y privadas, y éstas se utilizan para proteger la clave simétrica. Para cada instancia de SQL Server que almacena datos confidenciales en una base de datos se crea un par de claves pública y privada[83].

De otro lado, según datos del portal de Microsoft, el SGBD SQL Server permite elegir entre varios algoritmos, incluidos AES de 128 bits, AES de 192 bits y AES de 256 bits, los cuales se implementan mediante la API Windows Crypto.

---

80 PARADA, Miguel. Qué es SQL Server. 2019. OpenWebinars.
81 Ibid.
82 MICROSOFT. SQL Server y claves de cifrado de base de datos (motor de base de datos). 2017.
83 Ibid.

5.1.2. Sistemas de gestión de bases de datos no relacionales

5.1.2.1. MongoDB: MongoDB es un sistema de gestión de base de datos NoSQL de tipo documento, es decir, es un gestor que almacena datos en forma de documentos tipo JSON (JavaScript Object Notation). MongoDB abarca las características de accesibilidad, confiabilidad y escalabilidad en el contexto de grandes volúmenes de datos, termino conocido recientemente como “Big Data”.

> En MongoDB existen dos modelos de representación para las relaciones entre documentos: referencias y documentos embebidos. La relación por referencia consiste en que en los documentos existe un campo que identifica a otro documento que contiene datos específicos, también se lo denominan modelos de datos normalizados por el hecho de que con la referencia se obtendrá toda la información del documento. […] En cuanto a sistemas Operativos, MongoDB es soportado para sistemas UNIX, OS X [124] y Windows. Los lenguajes de programación que soporta son: C, C++, Java, C#, .NET, Java, Node.js, Perl, PHP, Python, Ruby, Scala. Para manipular base de datos MongoDB con estos lenguajes existen “manejadores” (drivers) para cada uno de ellos que son utilizados como librerías adicionales[84].

Sustentan Moreno et al[85] que MongoDB, está escrito en C++ y es multiplataforma, de código abierto y gratuito. Explican también, que su nombre proviene de la palabra en inglés Humongous, que significa literalmente "algo realmente grande", y se refiere a su capacidad de gestionar cantidades enormes de datos. Entre las principales características de este gestor señalan lo siguiente:

- ✓ Basado en el motor V8 de Google Chrome para JavaScript. Facilidad de aprendizaje por basarse en este lenguaje.
- ✓ Almacenamiento flexible basado en JSON sin necesidad de definir esquemas previamente.
- ✓ Alto rendimiento para consultas y actualizaciones.
- ✓ Consultas flexibles basadas en documentos.
- ✓ Soporte para creación de índices a partir de cualquier atributo, lo que facilita mucho su uso para porque no es necesario definir procesos Map-Reduce.
- ✓ Alta capacidad de crecimiento, replicación y escalabilidad: puedes escalar horizontalmente simplemente añadiendo máquinas baratas sin ver afectado el rendimiento ni complicar la gestión.
- ✓ Soporte para almacenamiento independiente de archivos de cualquier tamaño basado en GridFS.

---

[84] DELLA CROCE, Lisandro y SALINAS, Jorge Adrián. Flexibilidad en Bases de Datos NoSQL sobre ambientes Web Mining. Argentina. 2016. Tesina. Universidad de la Plata. Facultad de Informática. Licenciatura en Sistemas.

[85] MORENO ARBOLEDA, Francisco; QUINTERO RENDÓN, Juan y RUEDA VÁSQUEZ, Robinson. Una Comparación de Rendimiento Entre Oracle y Mongodb / a Performance Comparison between Oracle and Mongodb. *Ciencia e Ingeniería Neogranadina*, *26*(1), 109–129. 2016

> La principal ventaja de MongoDB es que se trata de un modelo NoSQL orientado a documentos que intenta mejorar los tiempos de respuesta con respecto al modelo relacional cuando se trabajan con datos no estructurados que crecen de manera exponencial. En cuanto a soporte al desarrollador es opensource, soporta variedad de lenguajes de programación; así como también diversas herramientas adicionales propias para mejorar la administración de base de datos orientada a documentos. MongoDB contiene algunas limitaciones, la más relevante es que no permite el manejo de transacciones y no asegura completamente ACID. Tampoco permite almacenar documentos mayores a 16MB[86].

En cuanto a las características de seguridad que incluyen el cifrado de datos, MongoDB maneja tres formas o tipos de cifrado: admite TLS / SSL (Seguridad de la capa de transporte / Capa de sockets seguros) para cifrar todo el tráfico de red; para el para el cifrado en reposo, el modo de cifrado predeterminado que utiliza MongoDB Enterprise es el AES256-CBC (o Estándar de cifrado avanzado de 256 bits en modo de encadenamiento de bloques cifrados) a través de OpenSSL. AES-256 usa una clave simétrica; es decir, la misma clave para cifrar y descifrar texto; y finalmente, el cifrado de nivel de campo, el cual posibilita a los usuarios tener campos cifrados en el servidor (almacenados en la memoria, en registros del sistema, en reposo y en copias de seguridad), que se representan como texto cifrado, lo que los hace ilegibles para cualquier parte que no tenga acceso de cliente o las claves necesarias para descifrar los datos[87].

Moreno et al[88] explican que las bases de datos documentales como MongoDB se utilizan para multitud de tareas, pero fundamentalmente cuando necesitan flexibilidad en la definición de los datos, sencillez a la hora de acceder a éstos, gran rendimiento y posibilidad de crecer muy rápido**.** En este sentido, se hace importante resaltar la apreciación de esto autores, cuando afirman que bases de datos como MongoDB, no entran a sustituir a las bases de datos tradicionales, como SQL Server, Oracle o MySQL, sino que las complementan para ciertos tipos de aplicaciones especializadas. Finalmente, se puede decir, que MongoDB puede utilizarse para casi cualquier cosa para la que utilizarías SQL Server o MySQL, pero sin la rigidez que presentan este tipo de bases de datos.

---

[86] DELLA CROCE, Lisandro. Op, cit. p,

[87] MONGODB. MongoDB 4.2 agrega transacciones distribuidas, cifrado a nivel de campo, operador Kubernetes actualizado y más a la base de datos líder, moderna y de propósito general. MongoDB. 2019.

[88] MORENO ARBOLEDA, Francisco; QUINTERO RENDÓN, Juan y RUEDA VÁSQUEZ, Robinson. Una Comparación de Rendimiento Entre Oracle y Mongodb / a Performance Comparison between Oracle and Mongodb. *Ciencia e Ingeniería Neogranadina*, *26*(1), 109–129. 2016

5.1.2.2. Cassandra: El sistema de gestión de base de datos Cassandra, maneja un lenguaje CQL (Lenguaje de Consulta Cassandra)**,** es un gestor con un sistema de código abierto distribuido, puede manejar grandes cantidades de datos a través de muchos servidores. “Es una base de datos distribuida NoSQL de código abierto, escrita en Java. Es un ajuste ideal para mantener una gran cantidad de datos estructurados y no estructurados debido a su capacidad para escalar elásticamente y linealmente. Debido a la elasticidad lineal de Cassandra, el rendimiento aumenta con el aumento en el número de nodos en el clúster”[89].

> Cassandra es una base de datos NoSQL que almacena datos en formas tabulares no relacionadas. Cassandra trabaja en el concepto de "consulta a la vez" y "consulta en una mesa". Cassandra es una base de datos distribuida, orientada a columnas, NoSQL con alta escalabilidad, alta disponibilidad y proporciona un alto rendimiento sin un solo punto de falla. Cassandra es la mejor opción para las empresas que necesitan confiabilidad, alta disponibilidad y rendimiento muy rápido. Tiene un rendimiento de escritura muy bueno y un buen rendimiento de lectura con un esquema flexible, y utiliza el modelo de datos de Google de Big Table para el almacenamiento de datos y el concepto de distribución de datos de Amazon Dynamo[90]

En cuanto a las características de esta aplicación, PowerData, las identifica así:

- ✓ Arquitectura escalable: gracias a un diseño masterless, en el que todos los nodos son iguales, lo que ofrece simplicidad operativa y fácil escalabilidad horizontal.
- ✓ Diseño activo de principio a fin: ya que en todos los nodos se puede escribir y leer**.**
- ✓ Rendimiento a escala lineal: la posibilidad de añadir nodos sin tener que frenar el ritmo produce aumentos en el rendimiento.
- ✓ Disponibilidad continua: elimina los puntos únicos de fallo y proporciona un tiempo de actividad constante.
- ✓ Detección de fallos y recuperación transparente: para nodos que no pueden ser fácilmente restaurados o reemplazados.
- ✓ Modelo de datos flexible y dinámico: que soporta tipos de datos modernos para lectura y escritura rápida.
- ✓ Protección de datos sólida: un diseño de registro de confirmación evita la pérdida de datos y construye copias de seguridad para facilitar la restauración a la vez que se mantienen los datos protegidos y seguros.
- ✓ Consistencia de los datos sintonizable: de esta forma, Cassandra base de datos ofrece apoyo a la consistencia de los datos en un clúster ampliamente distribuido.

---

[89] RAMESH, Dharavath, SINHA, Ashay y SINGH, Suraj., "Modelado de datos para datos discretos de series de tiempo usando Cassandra y MongoDB", *3a Conferencia Internacional sobre Avances Recientes en Tecnología de la Información (RAIT)* 2016, Dhanbad, 2016, pp. 598-601.

[90] PANDEY Shivendra Kumar and SUDHAKAR, "Context based Cassandra query language," 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Delhi, 2017, pp. 1-7.

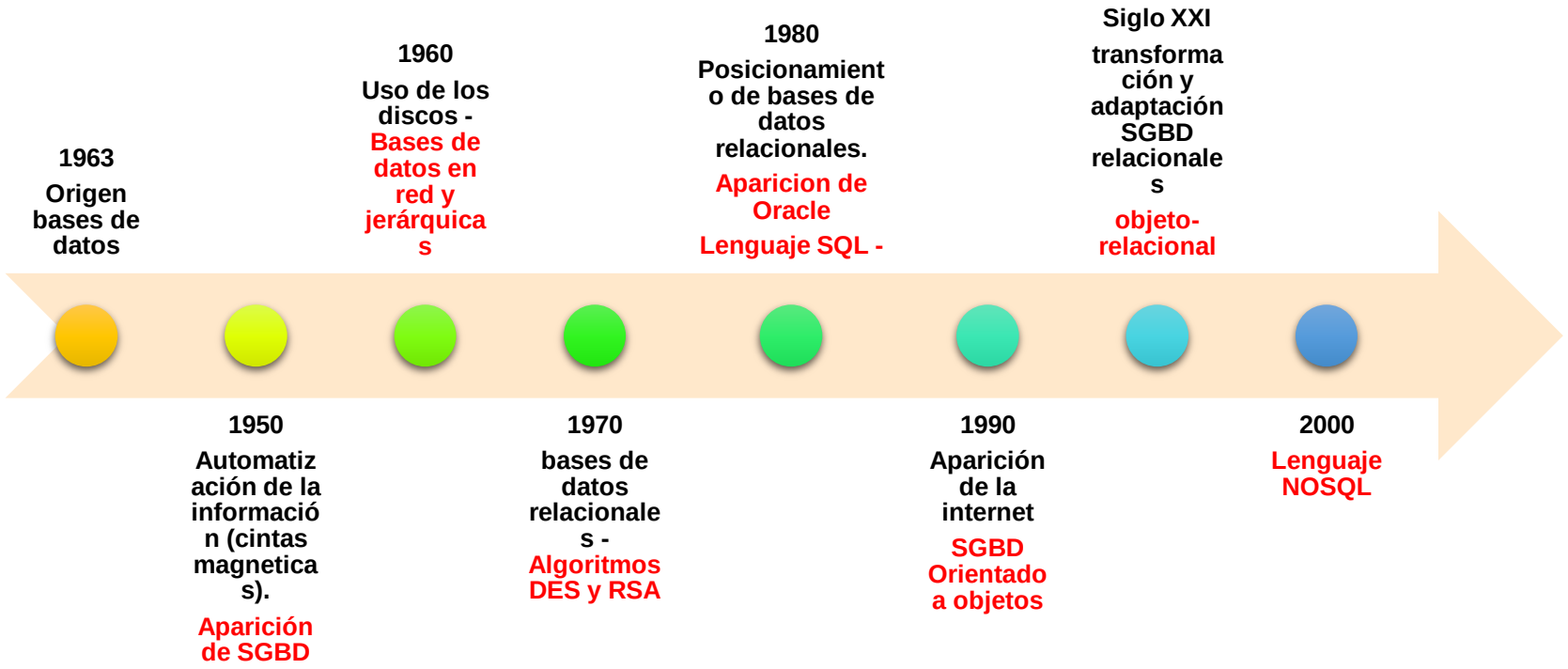
- ✓ Replicación de datos multi-centro: se trata de un centro de datos transversal (en diferentes zonas geográficas) que recibe el el apoyo de múltiples zonas de disponibilidad en la nube tanto para escritura como para lectura.
- ✓ Compresión de datos: garantiza que los datos se comprimirán hasta un 80% sin que ello suponga un gasto de recursos.
- ✓ CQL (Lenguaje de Consulta Cassandra): un lenguaje similar a SQL que consigue que la transición desde una base de datos relacional sea muy sencilla[91].

El cifrado de datos de este gestor se realiza mediante conexiones SSL - Secure Socket Layer. Este método de ciframiento se constituye en un protocolo criptográfico utilizado para proteger las comunicaciones entre ordenadores. "Cassandra proporciona comunicación segura entre un cliente y un clúster de base de datos, y entre nodos en un clúster. La habilitación del cifrado SSL garantiza que los datos en vuelo no se vean comprometidos y se transfieran de forma segura. El cifrado de cliente a nodo y de nodo a nodo se configura de forma independiente. Las herramientas de Cassandra (cqlsh, nodetool, DevCenter) se pueden configurar para usar el cifrado SSL. Los controladores DataStax se pueden configurar para asegurar el tráfico entre el controlador y Cassandra"[92].

[91] POWERDATA. Cassandra base de datos: agilidad y rendimiento a prueba de fallos. 2016
[92]DATASTAX. Asegurando a Cassandra.

5.2 IDENTIFICACIÓN DEL PROCESO EVOLUTIVO QUE HAN TENIDO LOS GESTORES DE BASES DE DATOS EN CUANTO A LA CARACTERÍSTICA DE SEGURIDAD.

Figura 8: Línea de tiempo de los gestores de bases de datos en cuanto a la característica de seguridad.



Fuente: Elaboración Propia

La seguridad se constituye en un factor relevante en el contexto de los sistemas de gestión de bases de datos y generalmente se asocia a la certeza, falta de riesgo o contingencia, sin embargo, conviene aclarar que esa certeza no es absoluta y que los riesgos son un factor que siempre están presente, independiente de las medidas que se tomen, por lo que se debe hablar de niveles de seguridad. En ese sentido, la seguridad informática se constituye en un conjunto de políticas encaminadas a obtener altos niveles de seguridad en los sistemas informáticos.

Y en cuanto a esta característica de la seguridad los gestores de bases de datos han idos mejorando paulatinamente de acuerdo a las nuevas exigencias que comprende garantizar la integridad de la información, en la sociedad moderna, mediatizada y globalizada. En ese sentido, han tenido una evolución paulatina que inicia con el surgimiento de las bases de datos en 1963, la concepción de los SGBD en la década de los 50 y pasa por el surgimiento de diferentes innovaciones tecnológicas que han posibilitado la concepción de los sistemas de gestión de bases de datos actuales.

Según Hernández[93] los primeros sistemas de bases de datos aparecieron a finales de los cincuenta. Y surgieron como respuesta a la complejidad que suponía, para la época, el creciente número de datos y de usuarios, para almacenar en un juego de ficheros. los cuales, aunque almacenaban grandes cantidades de datos y durante un largo periodo, no garantizaban generalmente que los datos no se perdían ante fallos bastante triviales, y se basaban casi exclusivamente en recuperación por copia de seguridad. Es así, como la aparición de estos sistemas, evolucionados de la metodología de los ficheros, comenzaron a brindar a las compañías la posibilidad de aplicar soluciones mecánicas más baratas y eficientes.

“Los Sistemas de Gestión de Bases de Datos (SGBD), que convierten el acceso a los datos y su gestión en una aplicación cerrada ("caja negra"), interponiéndose entre los usuarios y los ficheros, y haciéndose cargo de todos los problemas de explotación, mantenimiento y comprobación de los datos. De esta manera el usuario pierde de vista todos los detalles relativos al almacenamiento físico de los de los datos tratando con ellos sólo a través de un lenguaje conceptual sencillo”[94].

Ya para la década de los 60, empiezan a aparecer distintos modelos de datos para describir la estructura de la información en una base de datos; y se conocen entonces, el

[93] HERNÁNDEZ ORALLO, José. La Disciplina de los Sistemas de Bases de Datos. Historia, Situación Actual y Perspectivas. Universidad Politécnica de Valencia. 2002.
[94] QUINTAS RIPOLL, Luis. Sistemas De Gestión de Bases de Datos. EOI. 2010.

modelo jerárquico y en red, para el almacenamiento de datos, que para esa época fueron llamados “lenguajes de programación de tercera generación”.

> El modelo jerárquico no tiene una historia demasiado bien documentada. Se deriva de los sistemas de gestión de información de los cincuenta y los sesenta. En 1968, IBM introdujo el sistema IMS, derivado del programa Apollo de la NASA sobre sus System/360, basado en el modelo jerárquico. Este modelo fue adoptado por muchos bancos y compañías de seguros que todavía los utilizan en algún caso hoy en día. Los sistemas de base de datos jerárquicos todavía se pueden encontrar en algunos departamentos de instituciones públicas y hospitales para gestionar el inventario y la contabilidad, aunque la renovación provocada por el efecto 2000 ha eliminado prácticamente su uso, así como el reciclaje de los expertos en estos sistemas a otros más modernos[95].

Después del surgimiento de los modelos jerárquico y red, comienza un puente entre estos, y el nacimiento del modelo relacional. En los años 70, Edgar F. (Ted) Codd, investigador de IBM, “propuso que los sistemas de bases de datos deberían presentarse a los usuarios con una visión de los datos organizados en estructuras llamadas relaciones. Las relaciones se definen como conjuntos de tuplas, no como series o secuencias de objetos, con lo que el orden no es importante”[96]. Surge en la época del 70, también, la criptografía moderna, con la aparición de los algoritmos de cifrado DES y RSA. “La criptografía actual se inicia a mediados de la década de los 70’s. No es hasta la invención del sistema conocido como DES (Data Encryption Standard) en 1976 que se da a conocer ampliamente, principalmente en el sector industrial y comercial. Posteriormente se crea el sistema RSA (Rivest, Shamir, Adleman) en 1978, de ahí en adelante se da el comienzo de la criptografía en un gran número de aplicaciones”[97]

Ya para la década de los 80 se da la estandarización o posicionamiento del modelo relacional. en 1980, la ACM (Association for Computer Machinery) otorgaba a Codd el “Turing Award”, uno de los premios más prestigiosos en el campo de la informática. El modelo relacional era imparable.”[98]. de igual forma, en el año 1986, el lenguaje SQL produjo una auténtica explosión de los SGBD relacionales. Durante este tiempo Structured Query Language (SQL) comenzó a ser el modelo de la

[95] HERNÁNDEZ ORALLO, Op, cit. p., 3
[96] Ibid., p., 6
[97] FRANCO BORRE, David Antonio MOYA VILLA, Yasmin. Seguridad en bases de datos distribuidas utilizando agentes móviles. Cartagena de Indias: 2005. P., 122. Tesis de Magister En Ciencias Computacionales. Instituto Tecnológico y de Estudios Superiores de Monterrey - Universidad Autónoma de Bucaramanga. Campus Unitecnologica.
[98] HERNÁNDEZ ORALLO, Op, cit. p., 6

industria con bases de datos relacionales con su sistema de tablas pudieron competir con las bases de datos de red y las jerárquicas.

Al principio de la década de los 90 surgen los primeros Sistemas de Gestión de Bases de Datos Orientados a Objetos (SGBDOO, o simplemente, SGBDO), los cuales empiezan a tener éxito en el momento de ejecutar datos complejos en los lugares donde las bases de datos relacionales no podían desenvolverse con una manera eficaz. Estos sistemas empezaron a aparecer en el mercado, a partir de compañías como Objectivity. En este modelo la información sobre una entidad se almacena como un objeto persistente y no como una fila en una tabla. Esto, en principio, lo hace más eficiente en términos de requerimientos de espacio y asegura que los usuarios puedan manipular los datos sólo de las maneras en las que el programador haya especificado. De igual forma, para esa época, se da la creación del World Wide Web, lo cual llega a facilitar la consulta de las bases de datos[99].

> Alrededor de la mitad de los ochenta, algunas aplicaciones exigían mayor expresividad en los datos con los que trabajaban. Por ejemplo, las bases de datos médicas, las bases de datos multimedia y algunas bases de datos científicas requerían mayor flexibilidad en la manera en la que los datos se representaban y eran accedidos. Coincidiendo con la entrada de los lenguajes orientados a objetos como Smalltalk o C++ en el ámbito industrial, los investigadores se plantearon transportar estas ideas a las bases de datos y permitir que el tipo de datos marcara cómo se representaba y se manipulaba dependiendo de los métodos que se definían para dicho tipo o clase[100].

Para comienzos del siglo XXI, surge el modelo objeto-relacional el cual se constituye en una mezcla entre el modelo relacional y el orientado a objetos, “se define como una extensión objetual del modelo relacional, permitiendo la definición de nuevos tipos y de relaciones de herencia, entre otras cosas. Permite a las organizaciones continuar usando sus sistemas existentes y sus datos, sin realizar prácticamente cambios y les permiten empezar a utilizar gradualmente características orientadas a objetos, especialmente si se hace en conjunción con aplicaciones desarrolladas en entornos también orientados a objetos”[101]

En el año 2009, comienza a surgir el movimiento NoSQL, como consecuencia al crecimiento de datos; es decir, desde la entrada en vigencia de la Internet, se da un cambio drástico en el tratamiento de las bases de datos, dando lugar a multitud de nuevas formas de almacenamiento de la información, con partes y estructuras

[99] Ibid., p., 9
[100] Ibid., p., 9
[101] FRANCO BORRE, Op, cit. p., 16

comunes, y características propias y únicas que las diferencia de las demás; atendiendo a esto, empieza a concebirse el termino de bases de datos no relacionales o NoSQL, como una tecnología de base de datos moderna pensada desde las limitaciones de las bases de datos relacionales, es decir, con el propósito de superar los problemas de escalabilidad, alto rendimiento, modelado de datos, distribución de datos y disponibilidad continua, al momento de admitir datos voluminosos[102].

Desde los inicios de los gestores de bases de datos hasta la actualidad, se puede observar en perspectiva el cambio de los sistemas de gestión de bases de datos. "Inicialmente se trataba de software muy caro, sobre grandes y costosos ordenadores. Actualmente existen sistemas de gestión de bases de datos para ordenadores personales, muchos de ellos económicos o incluso gratuitos. Esta tendencia al abaratamiento y disminución en tamaño físico de los sistemas contrasta con la cada vez mayor capacidad, potencia y prestaciones de los SGBD. Sólo median menos de 30 años desde el primer sistema de gestión relacional, el "System R", cuyo primer prototipo podía almacenar 8MB de datos hasta los terabytes usuales hoy en día en cualquier organización discreta"[103].

5.3. Indicadores para la selección adecuada de un gestor de bases de datos bajo un escenario propuesto.

Con el propósito de definir unos indicadores que faciliten la toma de decisiones en un escenario propuesto, se realiza una caracterización de los gestores de bases de datos antes descritos, fundamentando dicha determinación en unos aspectos comunes entre los diferentes SGBD, tales como tipo de licencia, lenguaje de consulta, cifrado de datos, rendimiento, algoritmo de cifrado y arquitectura. En ese sentido, se esboza la siguiente tabla.

[102] HERRANZ GÓMEZ, Raúl. Bases de Datos NOSQL: Arquitectura y ejemplos de aplicación. Leganés: 2014. P., 159. Tesis de Ingeniería Informática. Departamento de Informática. Universidad Carlos III de Madrid.

[103] HERNÁNDEZ ORALLO, Op, cit. p., 15

Tabla 1: Caracterización de SGBD

SGBD	Lenguaje de consulta SQL/NoSQL	Tipo de licencia	Algoritmo de cifrado	Arquitectura	Rendimiento
ORACLE	SQL	Pago/ alto costo	3DES, AES (128, 192 y 256 bits)	Cliente/Servidor	Alta Escalabilidad
SQL SERVER	SQL	Pago/ alto costo	AES de 128 bits, AES de 192 bits y AES de 256 bits	Cliente/Servidor	Alta escalabilidad
MYSQL	SQL	Gratuito/ código abierto	Triple-DES, AES	Cliente/Servidor	Baja escalabilidad
POSTGRESQL	SQL	Gratuito	MD5, SHA1, SHA224 / 256/384/512, Blowfish, AES, DES / 3DES / CAST5	Cliente/Servidor	Variable
MONGODB	NoSQL orientada a documentos	Gratuito/Código abierto	AES256-CBC - TLS / SSL	Maestro – Esclavo	Alta escalabilidad/ Horizontal
CASSANDRA	NoSQL orientada a columnas	Gratuito**/**Código abierto distribuido	SSL	Peer-to-Peer	Alta escalabilidad

Fuente: Elaboración Propia

Para realizar un análisis comparativo con respecto a la caracterización de los diferentes sistemas de gestión de bases de datos, en un escenario propuesto, se procede a evaluar cada una de estas características dándoles una puntuación de 1 a 5 puntos, y finalmente realizando una sumatoria general que permita identificar que gestor alcanza mayor representatividad de acuerdo a las necesidades de las MIPYMES. Para ellos se evaluarán las características de acuerdo a un escenario básico para una MIPYMES:

Una mediana empresa, con un flujo de información básico, pero confidencial, por lo cual se necesita respaldo y seguridad en el almacenamiento de los datos y con un número aproximado de 100 colaboradores o usuarios. Por lo cual para fundamentar la evaluación de elección del SGBD, se priorizarán características como el tipo de licencia, el algoritmo de cifrado y el lenguaje de consulta, a los cuales se les asignarán puntos de la siguiente manera:

Tipo de licencia: Gratuita (5 puntos), Paga (1 punto).

Lenguaje de consulta: SQL (5 punto), NoSQL (1punto).

Algoritmo de cifrado: AES y/o 3DES (5) TLS/SSL u otro (1)
Arquitectura: Cliente/servidor (5 puntos), otro (1 punto).

Rendimiento: Alta escalabilidad (5) Baja escalabilidad (1) Variable (3)

Tabla 2: Normalización de los datos

SGBD	**Lenguaje de consulta SQL/NoSQL**	**Tipo de licencia**	**Algoritmo de cifrado**	**Arquitectura**	**Rendimiento**
ORACLE	5	1	5	**5**	**5**
SQL SERVER	5	1	5	**5**	**5**
MYSQL	5	5	5	**5**	**1**
POSTGRESQL	5	5	5	**5**	**3**
MONGODB	1	5	4	1	5
CASSANDRA	1	5	1	1	5

Fuente: Elaboración propia

Una vez evaluadas las características de los SGBD, se procede a asignar indicadores porcentuales de acuerdo a las características principales elegidas para el caso propuesto, de la siguiente manera: Tipo de licencia: 30%, Algoritmo de cifrado: 30%, Lenguaje de consulta: 20%, Arquitectura: 10% y Rendimiento: 10%.

Tabla 3: Índices porcentuales de las características de los SGBD

SGBD	Lenguaje de consulta 20%	Tipo de licencia 30%	Algoritmo de cifrado 30%	Arquitectura 10%	Rendimiento 10%	Puntaje final
ORACLE	1.0	0,3	1,5	0,5	0,5	3.8
SQL SERVER	1.0	0,3	1,5	0,5	0,5	3.8
MYSQL	1.0	1.5	1,5	0,5	0,1	4.6
POSTGRESQL	**1.0**	**1.5**	**1,5**	**0,5**	**0,3**	**4.8**
MONGODB	0,2	1.5	1,2	0,1	0,5	3.5
CASSANDRA	**0,2**	**1.5**	**0,3**	**0,1**	**0,5**	**2.6**

Fuente: Elaboración propia

El análisis comparativo de las características de los gestores arroja como resultado a PostgreSQL, como el gestor con mayor puntuación, con un 4,8 % de acuerdo a los aspectos priorizados por las necesidades del caso propuesto para una mediana empresa, seguido de MySQL con un 4,6% y características realmente muy similares a las de PostgreSQL. Estos índices indican que un gestor con licencia de código abierto, con un lenguaje SQL que se caracteriza por ser práctico al momento de la consulta, y recomendado para sistemas que requieren transacciones de varias filas. Así como también es un lenguaje que ofrece soporte y variedad de herramientas toda vez que tiene mucho más tiempo en el mercado. En cuando a la seguridad, es un gestor con un método de encriptación soportado en el algoritmo AES y 3DES

Es importante resaltar, que Oracle y SQLServer, son también una excelente opción, solo que representan incremento en los costos, dado que sus licencias son pagas y requieren de personal especializado y permanente para su administración lo que implicaría una mayor inversión para una mediana empresa que por su funcionalidad se acopla bien a un SGBD de código abierto que le garantice respaldo de su información.

De igual forma, no quiere decir que Cassandra y MongoDB sean una mala opción. Lo que se pretende con la fijación de estos indicadores es proporcionar a la MiPyMes una herramienta práctica para comparar teniendo en cuenta sus prioridades. Es así, como Cassandra y MongoDB no representan una elección conveniente para este escenario propuesto, toda vez que la empresa no tiene la necesidad de un flujo de información elevado que requiera alta escalabilidad y rendimiento. Las bases de datos NoSQL se constituyen en un modelo diferente que ofrece ventajas y soluciones a problemas que poseen las bases de datos relacionales, más no son su reemplazo.

En función de esto, la evaluación de las características es un proceso que debe ser proporcional, como se ha manifestado anteriormente, a las necesidades de las empresas, y de acuerdo a ello se deben variar los índices porcentuales que se plantean para la selección.

6. CONCLUSIONES

Después de realizar un análisis conceptual a las características de los SGBD, enfatizando en la seguridad de estos, se establece que la forma de cifrar datos es un aspecto clave de la seguridad de las bases de datos, toda vez que garantiza el respaldo de este bien valioso que es la información; sin embargo, mediante el estudio se pudo comprender que no hay seguridad absoluta o estándar, por lo cual no existe un gestor de bases de datos hermético a las vulnerabilidades y ataque maliciosos presentes en la web.

Todos los sistemas de gestión de bases de datos constan de sistemas de encriptación e Integridad de los datos, no obstante, estos pueden ser penetrados por ciberataque, los cuales se ha vuelto muy común en las bases de datos, dado que se puede obtener información privada o en su defecto controlar el servidor. Por consiguiente, la seguridad, en el contexto de los sistemas de gestión de bases de datos, es un tema que mantiene en constantemente evolución, innovación y búsqueda de calidad, en función de las expectativas de la sociedad de la información y la virtualidad.

En este sentido, la elección de un sistema de gestión de bases de datos es un proceso que está ligado a las necesidades informacionales de cada organización y que se determina de acuerdo a características de costo, estructura, y seguridad. Por lo tanto, debe ser un proceso estratégico, fundamentado en conocimientos profesionales y documentados.

Finalmente, las características de los SGBD se convierten en elementos claves que se pueden usar como indicadores en un ejercicio de evaluación y elección bajo un escenario propuesto o ciertos parámetros determinantes. En el caso de este proyecto, en donde el énfasis estuvo mediado por la seguridad de la información para MiPymes, los indicadores seleccionados fueron: tipo de licencia, lenguaje de consulta, cifrado de datos, rendimiento, algoritmo de cifrado y arquitectura. Mediante estos indicadores y de acuerdo a los aspectos priorizados por las necesidades del caso propuesto para una mediana empresa, se destaca PostgreSQL, como el gestor con mayor puntuación.

7. RECOMENDACIONES

Una vez concluido este proceso de investigación monográfico, en el cual se establecieron índices porcentuales para la elección de sistemas de gestión de bases de datos para el contexto de las PYMES, se recomienda a estas:

- Identificar sus prioridades en cuanto a necesidades de almacenamiento, gestión y administración de su información. Esto les permitirá tener claro que gestor de bases de datos es pertinente para sus transacciones.

- Priorizar la seguridad de la información como un elemento fundamental para su accionar organizacional, toda vez que está se constituye en un activo de gran valor para los propósitos organizacionales; así como también se constituye en un objetivo de ataques y amenazas.

- Analizar las diferentes propuestas de Gestores de bases de datos existentes en el mercado, dado que la propuesta presentada en este documento, fue diseñada solo con una muestra de los gestores más comerciales o comunes en el mercado.

BIBLIOGRAFÍA

ANGUIANO MORALES, Jorge. Características y tipos de bases de datos. [En Línea] Argentina: IBM. 2014. [citado 17-03-2020] Disponible en: https://www.ibm.com/developerworks/ssa/data/library/tipos_bases_de_datos/index.html

BENÍTEZ, Miguel y ARIAS, Ángel. Curso de introducción a la administración de bases de datos. [En Línea] IT Campus Academy. 2015. P, 283. [citado 09-03-2020] Disponible en: https://books.google.es/books?hl=es&lr=&id=NUSiCgAAQBAJ&oi=fnd&pg=PA1&dq=concepto+de+bases+de+datos+2015&ots=mqNLr9EA2Q&sig=no2Jp-3EJrUbOJEBdwe-OuANzC0#v=onepage&q=concepto%20de%20bases%20de%20datos%202015&f=false

CAMPS PARÉ, Rafael *et al.* Bases de datos. 1ra ed. Barcelona: Universitat Oberta de Catalunya. 2005

CAPACHO PORTILLA, José Rafael, y NIETO BERNAL, Wilson. Diseño de Base de Datos. [En Línea] Barranquilla: Universidad del Norte, 2017. [citado 09-03-2020] Disponible en: http://eds.a.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/ebookviewer/ebook/bmxlYmtfXzE2OTAwNDlfX0FO0?sid=6546fb9f-6150-43ce-a8f4-9b5285a7be93@sdc-v-sessmgr02&vid=0&format=EB

CEPAL. Acerca de Microempresas y Pymes. Antiago de Chile: CEPAL. [citado 26-03-2020] Disponible en: https://www.cepal.org/es/temas/pymes/acerca-microempresas-pymes

CHICKERUR, Satyadhyan; GOUDAR, Anoop y KINNERKAR, Ankita "Comparación de la base de datos relacional con la base de datos orientada a documentos (MongoDB) para aplicaciones de Big Data", *octava conferencia internacional de 2015 sobre ingeniería avanzada de software y sus aplicaciones (ASEA)*, Jeju, 2015, pp. 41-47. [citado 18-03-2020] Disponible en: https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/document/7433067/authors#authors

COLOMBIA. CONGRESO DE LA REPÚBLICA. LEY 590. Por la cual se dictan disposiciones para promover el desarrollo de las micro, pequeñas y medianas empresa. Bogotá: El Congreso. 2000.

DATASTAX. Asegurando a Cassandra. [citado 24-04-2020] Disponible en: https://docs.datastax.com/en/archived/cassandra/3.0/cassandra/configuration/secureIntro.html

DELLA CROCE, Lisandro y SALINAS, Jorge Adrián. Flexibilidad en Bases de Datos NoSQL sobre ambientes Web Mining. Argentina. 2016. Tesina. Universidad de la Plata. Facultad de Informática. Licenciatura en Sistemas. [citado 09-03-2020] Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/59099/Documento_completo__.%20y%20Salinas,%20J.%20A.pdf-PDFA.pdf?sequence=3&isAllowed=y

DINI, Marco y STUMPO, Giovanni (coords.), “Mipymes en América Latina: un frágil desempeño y nuevos desafíos para las políticas de fomento”, [En Línea] Documentos de Proyectos (LC/TS.2018/75), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2018. [citado 09-03-2020] Disponible en: https://repositorio.cepal.org/bitstream/handle/11362/44148/1/S1800707_es.pdf

DHARAVATH, Ramesh, KUMAR ,Jain y KUMAR, Chiranjeev. "Implementación de atomicidad y aislamiento de instantáneas para transacciones de varias filas en bases de datos distribuidas orientadas a columnas usando RDBMS", *2012 Conferencia Internacional sobre Comunicaciones, Dispositivos y Sistemas Inteligentes (CODIS)*, Kolkata, 2012, pp. 298-301. [citado 25-03-2020]

EL CRONISTA. Seguridad informática en riesgo: cada vez más empresas sufren ciberataques, Argentina. 2017. [citado 25-04-2020] Disponible en: https://www.cronista.com/negocios/Seguridad-informatica-en-riesgo-cada-vez-mas-empresas-sufren-ciberataques-20170529-0022.html

FAJARDO DÍAZ, Carmen Elizabeth. Análisis de los riesgos de Seguridad de la Información de un aplicativo de gestión documental líder en el mercado colombiano. Trabajo para optar al título de Especialista en Seguridad de la Información. Bogotá: Institución Universitaria Politécnico Grancolombiano. Facultad de Ingeniería y Ciencias Básicas. Especialización En Seguridad de la Información. 2017. [citado 18-04-2020] Disponible en: http://repository.poligran.edu.co/bitstream/handle/10823/995/3.%20Documento%20Final%20Opci%c3%b3n%20de%20grado%20II.pdf?sequence=1&isAllowed=y

FRANCO BORRE, David Antonio MOYA VILLA, Yasmin. Seguridad en bases de datos distribuidas utilizando agentes móviles. Cartagena de Indias: 2005. P., 122. Tesis de Magister En Ciencias Computacionales. Instituto Tecnológico y de Estudios Superiores de Monterrey - Universidad Autónoma de Bucaramanga. Campus Unitecnologica. [citado 25-04-2020] Disponible en: https://biblioteca.utb.edu.co/notas/tesis/0030676.pdf

GIMENO, Vicente Alfonso. La influencia de las nuevas tecnologías de la información y las comunicaciones y su repercusión en las estrategias empresariales. La banca online y su aplicación en las cooperativas de crédito. 2015. Tesis Doctoral. Universidad de Valencia. Facultada de Economía. Departamento de Dirección de

Empresas. [citado 09-03-2020] Disponible en: https://www.tesisenred.net/bitstream/handle/10803/52170/alfonso.pdf

GINESTÁ, MARC Gibert y PÉREZ MORA, Oscar. Bases de datos en PostgreSQL. En: Bases de datos. 1ra ed. Barcelona: Universitat Oberta de Catalunya. 2005

GÓMEZ, Iván Camilo Diseño de metodología para verificar la seguridad en aplicaciones web contra inyecciones SQL. Trabajo de grado presentado para optar el título de Ingeniero en Telecomunicaciones. Universidad Militar Nueva Granada. Facultad de Ingeniería. 2011. [citado 18-04-2020] Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/7212/GomezGonzalezIvanCamilo2012.pdf?sequence=2&isAllowed=y

GÓMEZ MOJICA, Yeny Mireya. Estudio de seguridad en bases de datos SQL y NOSQL. Trabajo para optar al título de Especialista en Seguridad de la Información. Bogotá: Universidad Nacional Abierta y A Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería. Especialización en Seguridad Informática. 2018. 92p. [citado 18-04-2020] Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/21429/4/52488191

HERNÁNDEZ ORALLO, José. La Disciplina de los Sistemas de Bases de Datos. Historia, Situación Actual y Perspectivas. Universidad Politécnica de Valencia. 2002.

HERRANZ GÓMEZ, Raúl. Bases de Datos NOSQL: Arquitectura y ejemplos de aplicación. Leganés: 2014. P., 159. Tesis de Ingeniería Informática. Departamento de Informática. Universidad Carlos III de Madrid. Disponible en: https://core.ac.uk/download/pdf/44310803.pdf

INSTITUTO NACIONAL DE CIBERSEGURIDAD. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? España: CIBER. 2017. [citado 25-03-2020] Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

INCIBE. Gestión de riesgos. Una guía de aproximación para el empresario. España: INCIBE. [citado 25-03-2020] Disponible en: https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf

JING-WEI, Pan *et al*. "Un sistema mejorado de escaneo de vulnerabilidades ligero y seguridad mejorada para la base de datos Oracle", *IEEE 2019 4a Conferencia de Tecnología de Información Avanzada, Control Electrónico y Automatización (IAEAC)*, Chengdu, China, 2019, págs. 1699-1702. [citado 25-03-2020] Disponible

en: https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/document/8997534

KYOCERA Document Solutions. Los mejores gestores de base de datos del mercado. España: Kyocera. [citado 18-04-2020] Disponible en: https://www.kyoceradocumentsolutions.es/es/smarter-workspaces/insights-hub/articles/los-mejores-gestores-de-base-de-datos-del-mercado.html

KUMAR, Jitender; GARG, Varsha. "Security analysis of unstructured data in NOSQL MongoDB database," *2017* International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN), Gurgaon, 2017, pp. 300-305. [citado 25-03-2020] Disponible en: https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/document/8284495

KUMAR, Vibhor. Postgres y cifrado de datos transparente (TDE). 2015. [citado 18-04-2020] Disponible en: https://www.enterprisedb.com/es/blog/postgres-and-transparent-data-encryption-tde

MANNINO, Michael. Administración de bases de datos. Diseño y desarrollo de aplicaciones. 3ra ed. México. McGraw Hill. 2007. [citado 25-03-2020] Disponible en: http://www.ebooks7-24.com.bibliotecavirtual.unad.edu.co/stage.aspx?il=&pg=&ed=

MARÍN Rafael. Los gestores de bases de datos más usados en la actualidad. En: Revista Digital Inesem. 2019. [citado 18-04-2020] Disponible en: https://revistadigital.inesem.es/informatica-y-tics/los-gestores-de-bases-de-datos-mas-usados/

MICROSOFT. SQL Server y claves de cifrado de base de datos (motor de base de datos). 2017. [citado 18-04-2020] Disponible en: https://docs.microsoft.com/es-es/sql/relational-databases/security/encryption/sql-server-and-database-encryption-keys-database-engine?view=sql-server-ver15

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía para la Implementación de Seguridad de la Información en una MIPYME. Bogotá: MinTic. 2016.

MONGODB. MongoDB 4.2 agrega transacciones distribuidas, cifrado a nivel de campo, operador Kubernetes actualizado y más a la base de datos líder, moderna y de propósito general. MongoDB. 2019. [citado 25-04-2020] Disponible en: https://www.mongodb.com/press/mongodb-42-adds-distributed-transactions-field-level-encryption-updated-kubernetes-operator-and-more-to-the-leading-modern-general-purpose-database

MORENO ARBOLEDA, Francisco; QUINTERO RENDÓN, Juan y RUEDA VÁSQUEZ, Robinson. Una Comparación De Rendimiento Entre Oracle Y Mongodb / a Performance Comparison between Oracle and Mongodb. *Ciencia e Ingeniería Neogranadina*, *26*(1), 109–129. 2016. [citado 25-03-2020] Disponible en: https://doi-org.bibliotecavirtual.unad.edu.co/10.18359/rcin.1669.

NETEC. *Global Knowledge.* ¿Qué es Oracle? Netec. [citado 25-03-2020] Disponible en: https://www.netec.com/que-es-oracle

ORACLE COLOMBIA. Oracle MySQL. La base de datos de código abierto más popular del mundo. ORACLE. [citado 25-03-2020] Disponible en: https://www.oracle.com/co/mysql/

ORACLE. Informe Técnico sobre Oracle Advanced Security. Informe Ejecutivo de Oracle. Junio de 2007. https://www.oracle.com/technetwork/es/database/enterprise-edition/documentation/oracle-advanced-security-11g-426368-esa.pdf

PARDO, Brennero TORRES, Gabriel VERGARA, Freddy. Respaldos y recuperación sobre Oracle. Guayaquil – Ecuador. 2010.Tesis para optar al grado de Ingeniero en Sistemas Computacionales. Universidad Católica de Guayaquil. Facultad de Ingeniería, Carrera de Ingeniería en Sistemas Computacionales.

PARADA, Miguel. Qué es SQL Server. 2019. OpenWebinars. [citado 25-04-2020] Disponible: https://openwebinars.net/blog/que-es-sql-server/

PATIL, Mayur; HANNI, Akkamahadevi; TEJESHWAR, Ch and PATIL, Priyadarshini "A qualitative analysis of the performance of MongoDB vs MySQL database based on insertion and retriewal operations using a web/android application to explore load balancing — Sharding in MongoDB and its advantages," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, 2017, pp. 325-330. [citado 17-03-2020] Disponible en: https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/document/8058365

PORTAFOLIO. El secuestro de información desangra a las empresas del país. Bogotá: Portafolio.2019. [citado 25-04-2020] Disponible en: https://www.portafolio.co/negocios/empresas/ciberataques-a-las-empresas-en-colombia-525729

POSTGRESQL. Documentación, PostgreSQL 12. Función Pgcrypto. 2020. https://www.postgresql.org/docs/current/pgcrypto.html#id-1.11.7.34.7

QUINTAS RIPOLL, Luis. Sistemas De Gestión de Bases de Datos. EOI. 2010.

RAMESH, Dharavath, SINHA, Ashay y SINGH, Suraj., "Modelado de datos para datos discretos de series de tiempo usando Cassandra y MongoDB", *3a Conferencia Internacional sobre Avances Recientes en Tecnología de la Información (RAIT)*, 2016, Dhanbad, 2016, pp. 598-601. [citado 26-03-2020] Disponible en: https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/document/7507966

REASONWHY. Qué consecuencias puede tener un ciberataque para tu empresa. Madrid: REASONWHY. 2017. https://www.reasonwhy.es/actualidad/digital/que-consecuencias-puede-tener-un-ciberataque-para-tu-empresa-2017-05-15

RODRÍGUEZ GONZÁLEZ, María Elena. Gestión de datos: bases de datos y sistemas gestores de bases de datos. Barcelona: Editorial UOC, 2013. [citado 15-03-2020] Disponible en: https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3219201

SÁNCHEZ, Jorge. Diseño Conceptual de Bases de Datos. California: Creative Commons, 2014. [citado 09-03-2020] Disponible en: https://s3.amazonaws.com/academia.edu.documents/34140268/disenoBD.pdf?response-content-disposition=inline%3B%20filename%3DLos_contenidos_de_este_documento_estan_p.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20200317%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20200317T231652Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=4e582e34cc23c2f53ebdcfd0ea327a2d0a1b4f2ebf3474a3864e9aa0e89bfd32

SEGOVIA, José. Ventajas y Desventajas de PostgreSQL. Todo PostgreSQL. 2018. [citado 25-03-2020] Disponible en: https://todopostgresql.com/ventajas-y-desventajas-de-postgresql/.

SIGNIFICADOS. Significado de Vulnerabilidad. [citado 25-03-2020] Disponible en: https://www.significados.com/vulnerabilidad/

TAMAYO ÁLZATE, Alonso y DUQUE MÉNDEZ, Néstor Darío. Mecanismos de seguridad e integridad en un sistema de bases de datos. En: *Rev Departamento de Ciencias*. Universidad Nacional. 2001. [citado 25-03-2020] Disponible en: http://bdigital.unal.edu.co/58107/1/mecanismosdeseguridadeintegridad.pdf

TECNOLOGÍAS INFORMACIÓN. Sistemas de Gestión de Bases de Datos | Tipos y Clasificación. [citado 18-04-2020] Disponible en: https://www.tecnologias-informacion.com/gestionbasedatos.html

TREVIÑO VILLALOBOS, Marlen, et al. Una comparación de rendimiento entre MongoDB, ArangoDB y CouchBase para la operación lectura sobre bases de datos geográficas. En: IEEE. 2018. [citado 09-03-2020] Disponible en: https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/stamp/stamp.jsp?tp=&arnumber=8596387

TORRES ACERO, William. Modelos de encriptación en base de datos MS-SQL SERVER., Trabajo de grado para optar al título de Especialista en Seguridad Informática Bogotá: Universidad Nacional Abierta y A Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería. Especialización en Seguridad Informática. 2018.

UNIVERSIDAD INTERNACIONAL DE VALENCIA*. Los principales tipos de base de datos.* [En Línea] VIU. *2018.* [citado 15-03-2020] Disponible en: https://www.universidadviu.com/los-principales-tipos-base-datos/

ZORATTI, Iván "Mejores prácticas de seguridad MYSQL", *Conferencia IET 2006 sobre crimen y seguridad*, Londres, 2006, pp. 183-198. [citado 25-03-2020] Disponible en: https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/document/4123759