

ESTUDIO DE SEGURIDAD EN BASES DE DATOS SQL Y NoSQL

YENY MIREYA GOMEZ MOJICA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.

2018

ESTUDIO DE SEGURIDAD EN BASES DE DATOS SQL Y NoSQL

YENY MIREYA GOMEZ MOJICA

PROYECTO DE GRADO

DIRECTOR DE PROYECTO JULIO ALBERTO VARGAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.

2018

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Bogotá, junio de 2018

DEDICATORIA

La educación no es la respuesta a la pregunta. La educación es el medio para encontrar la respuesta a todas las preguntas.

William Allin

En primer lugar, a Dios quien me dio la vida, salud y me ha guiado, dado la fortaleza y perseverancia necesaria para alcanzar mis metas y llegar hasta este momento en la terminación de mi especialización.

Un agradecimiento especialmente a mis padres, quienes siempre están apoyándome y me inculcaron valores, principios, responsabilidades, respeto y perseverancia, motivación y mucho amor para seguir adelante.

A mis hijos, que siempre me apoyaron y me comprendieron, las cuales son unas de las razones por la cual estoy en este punto de mi vida, a puertas de este título.

AGRADECIMIENTOS

Quiero agradecer al Ingeniero Manuel Antonio Sierra Rodríguez, profesor de proyecto de grado por guiarme, corregirme y su ayuda incondicional en la elaboración de este proyecto de mi especialización.

Al profesor Salomón González García, quien con sus conocimientos me guio en el desarrollo de este proyecto.

Al director Julio Alberto Vargas, quien siempre estuvo dispuesto a colaborarme, corregirme y ofrecerme su ayuda en este proyecto.

A mi amigo por la amistad y el apoyo que me brindó durante toda esta etapa de la especialización.

A todos los profesores de la especialización que a lo largo de esta me brindaron todos sus conocimientos para mi formación académica y con ello poder formarme.

A la Universidad Nacional Abierta y a Distancia- UNAD

CONTENIDO

	pág.
RESUMEN.....	16
TITULO.....	17
0. INTRODUCCIÓN.....	18
1. PLANTEAMIENTO DEL PROBLEMA	19
1.1 DEFINICIÓN DEL PROBLEMA	19
1.2 FORMULACIÓN DEL PROBLEMA	19
2. JUSTIFICACIÓN.....	20
3. OBJETIVOS	21
3.1 OBJETIVO GENERAL	21
3.2 OBJETIVOS ESPECÍFICOS	21
4. MARCO REFERENCIAL	22
4. 1. RESEÑA HISTÓRICA.....	22
4.2. MARCO TEORICO.....	24
4.2.1 Bases de datos relacionales	24
4.2.2 Bases de datos NoSQL.	30
4.3. MARCO CONCEPTUAL.....	32
4.4. MARCO LEGAL	33
5. MARCO METODOLOGICO	35
5.1 MÉTODOLOGIA DE INVESTIGACION	35
5.1.1. Análisis..	35
5.1.2. Muestra.	35
5.2. ESTUDIO METODOLÓGICO	36
5.3 METODOLOGÍA DE DESARROLLO.....	36
6. ANÁLISIS DEL DESARROLLO DEL PROYECTO.....	38
6.1. EQUIVALENCIAS Y DIFERENCIAS ENTRE LAS BASES DE DATOS	38
6.1.1. SEGURIDAD DE LAS BASES DE DATOS SQL VS NO SQL	39
6.1.2. DESVENTAJAS EN APLICACIONES WEB NO TRANSACCIONALES	40

7. DESARROLLO DEL PROYECTO.....	42
7.1. LEVANTAR LA INFORMACIÓN DEL ESTADO ACTUAL EN BASES DE DATOS	42
7.2. DETERMINAR LAS BASES DE DATOS SQL Y NOSQL	47
7.3. DESARROLLO DEL LABORATORIO CON KALI LINUX.....	49
7.3.1 Base de Datos Relacional.....	49
7.3.2. Base de Datos No Relacional	65
8. RECOMENDACIONES Y PROPUESTA DE SEGURIDAD PARA LAS BASES DE DATOS SQL Y NOSQL	75
8.1 RECOMENDACION DE SEGURIDAD PARA BASES DE DATOS SQL.....	75
8.2 PROPUESTA DE SEGURIDAD PARA BASES DE DATOS NOSQL.....	76
8.2.1 Medidas de seguridad en bases de datos NOSQL	78
8.2.2 Cuando utilizar un tipo de base de datos:	81
8.2.3. A la hora de elegir una base de datos:.....	81
8.2.4. Pros y contras del uso de las bases de datos NoSQL :.....	81
9. RESULTADOS Y DISCUSIÓN	83
10. DIVULGACIÓN	84
CONCLUSIONES	85
RECOMENDACIONES.....	86
BIBLIOGRAFÍA.....	87
ANEXOS	¡Error! Marcador no definido.

LISTAS DE TABLAS

pág

TABLA 1. COMPARA LAS DIFERENCIAS PRINCIPALES ENTRE NOSQL Y SQL.....	39
TABLA 2. COMPARATIVO DE LAS BASES DE DATOS PRINCIPALES ENTRE SQL Y NoSQL.....	41

LISTA DE FIGURAS

	pág
FIGURA 1. MODELO DE TABLA.....	25
FIGURA 2. MODELO DE RELACIÓN DE TABLAS	26
FIGURA 3. MODELO DE VISTAS	28
FIGURA 4. MODELO DE CONSULTAS.....	28
FIGURA 5. MODELO DE FORMULARIO	29
FIGURA 6. MODELO DE INFORMES	29
FIGURA 7. MODELO DE DISTRIBUCIÓN NOSQL.....	30
FIGURA 8. MODELO DE ALMACENAMIENTO LLAVE-VALOR	32
FIGURA 9. NOSQL FRENTE A SQL.....	40
FIGURA 10. VULNERABILIDADES QUE AFECTAN LAS BASES DE DATOS EN LAS EMPRESAS.	46
FIGURA 11. CONFIGURACIÓN DE SEGURIDAD A NIVEL DE ASM	48
FIGURA 12. DESCAGA ORACLE EXPRESS EDITION 11G	49
FIGURA 13. COPIAR EL ORACLE 11.....	50
FIGURA 14. INSTALAR ALIEN LIBAIO1	50
FIGURA 15. CONVERTIR EL ARCHIVO .RPM A .DEB	50
FIGURA 16. CARGAR DATOS	51
FIGURA 17. VERIFICAR LOS PARÁMETROS	51
FIGURA 18. VERIFICAR ARCHIVO S01SHM_LOAD.....	52
FIGURA 19. PERMISOS SOBRE EL ARCHIVO S01SHM_LOAD	52
FIGURA 20. EJECUCIÓN DE COMANDOS.....	52
FIGURA 21. INSTALACIÓN EL ARCHIVO .DEB	53
FIGURA 22. CONFIGURAR PUERTOS	53
FIGURA 23. VERIFICAR EL ARCHIVO.BASHRC	53
FIGURA 24. INICIAR ORACLE 11G.....	53
FIGURA 25. AGREGAR USUARIO DBA.....	54
FIGURA 26. INICIAR CONSOLA CON EL USUARIO SYSDBA.....	54
FIGURA 27. LISTAR BASE DE DATOS	54
FIGURA 28. UBICAR METADATOS	55
FIGURA 29. USUARIOS POR DEFECTO	55
FIGURA 30. VERIFICAR USUARIOS.....	55
FIGURA 31. LISTAR PUERTOS	56
FIGURA 32. INSTALACIÓN ORACLE	56
FIGURA 33. PANTALLA INICIO PLSQL.....	57
FIGURA 34. BASE DE DATOS XE	57
FIGURA 35. RUTA DE LOS METADATOS	58
FIGURA 36. USUARIOS Y ROLES.....	58
FIGURA 37. PUERTO Y SERVICIOS.....	59
FIGURA 38. CONFIGURACIÓN DE SEGURIDAD	60

FIGURA 39. CREANDO LA BASE DE DATOS ALQUILER	60
FIGURA 40. CREAR LAS TABLAS VEHÍCULOS, CLIENTES, ALQUILER	61
FIGURA 41. POBLAR LA BASE DE DATOS	62
FIGURA 42. PROBAR LA INTEGRIDAD REFERENCIAL	63
FIGURA 43. CHEQUEO DE VULNERABILIDADES DE ORACLE	63
FIGURA 44. INSTALAR VIRTUAL BOX.....	65
FIGURA 45. CONFIGURAR LA MÁQUINA DE CASSANDRA	65
FIGURA 46. DESCARGAR JAVA.....	66
FIGURA 47. INSTALAR LA MAQUINA JAVA	66
FIGURA 48. DESCARGAR EL APACHE DE CASSANDRA	67
FIGURA 49. DESCOMPRESOR EL APACHE DE CASSANDRA.....	67
<i>FIGURA 50. CREAR VARIABLE EN JAVA Y CASSANDRA.....</i>	<i>68</i>
FIGURA 51. CONFIGURACIÓN AVANZADA DEL SISTEMA	68
FIGURA 52. CREACIÓN DE VARIABLES	68
FIGURA 53. CREACIÓN DE LA VARIABLE CASSANDRA.....	69
FIGURA 54. CREACIÓN DE LA VARIABLE JAVA	69
FIGURA 55. CREACIÓN DE CARPETAS COMMITLOG Y DATA	70
FIGURA 56. MODIFICAR ARCHIVO CASSANDRA.YAML	70
FIGURA 57. MODIFICAR LÍNEA DATA FILE DIRECTORIES.....	71
FIGURA 58. EJECUCIÓN CASSANDRA.BAT	71
FIGURA 59. INSTALAR Y CONFIGURAR EL CLIENTE	72

GLOSARIO

ATRIBUTO: son características que definen una entidad, son las propiedades individuales que tiene un objeto es diferente a otro.

API: (*Application Programming Interface*) es un conjunto de reglas y especificaciones que las aplicaciones pueden seguir para comunicarse entre ellas.

BASE DE DATOS: recursos que recopilan todo tipo de información, se guarda información ordenadamente en un programa, la información se organiza registros, campos y archivos.¹

BIG TABLE DE GOOGLE: es un técnica de base de datos creado por Google con las características de ser: de alta eficiencia y distribuido.²

CLAVE: un campo o una combinación de campos que identifica de forma única a cada fila de una tabla.

CASSANDRA: es una base de datos NoSQL distribuida y basada en un modelo de almacenamiento de «clave-valor», de código abierto que está escrita en Java.

CRUD: es el acrónimo de (*Create* (crear), *read* (leer), *updated* (modificar), *delete*(borrar)), funciones básicas de las bases de datos.

DATOS: escritura simbólica, por medio de letras o números de una recolección de información la cual consigue ser cuantitativa o cualitativa.

DOMINIO: un conjunto de valores posibles para cierto atributo.

DBMS: (*Data Base Management System*), las siglas en inglés para los Sistemas de Gestión de Bases de Datos.³

JNOS: (*JavaScript Object Notation*) es un formato para el intercambio de datos.

JOIN: admite acordar registros de tablas en una base de datos SQL.

¹ Cortes, Maria jose. Glosario Base de Datos.https://es.slideshare.net/paola584/glosario-de-base-de-datos-55560601?next_slideshow=1 En línea

² Wikipedia.Big table<https://es.wikipedia.org/wiki/BigTable>. En línea

³ <https://es.wikipedia.org/wiki/> En línea

MOTOR DE BASE DE DATOS: es una ayuda que se maneja primordialmente para acopiar, proteger y procesar los datos.⁴

NoSQL: no sólo SQL, es una extensa variedad de técnicas de gestión de bases de datos como apache cassandra, Google big table.

RDMBS: un sistema de gestión de bases de datos relacionales

SQL: el significado de las siglas en inglés Structured Query Language, lenguaje declarativo o de consulta estructurada de acceso a bases de datos relacionales.⁵

TUPLA: un registro en una fila

SEGURIDAD: es el método de proteger la información en forma íntegra y privada.

VULNERABILIDAD: es una debilidad de la técnica informática que puede ser manejada para ocasionar un daño.⁶

⁴ Technet. Motor de Base de datos SQL. [https://technet.microsoft.com/es-es/library/ms187875\(v=sql.105\).aspx](https://technet.microsoft.com/es-es/library/ms187875(v=sql.105).aspx). En línea.

⁵ SQL - RDBMS Concepts. <https://www.tutorialspoint.com/sql/sql-rdbms-concepts.htm>. En línea

⁶ Observatorio Tecnológico.

<http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3>. En línea

RESUMEN

Con este trabajo se pretende descubrir las vulnerabilidades que tienen las bases de datos SQL y NoSQL, utilizadas por las empresas para dar seguridad al gran volumen de información que debe procesar, en las actividades propias de las organizaciones.

El propósito de esta información es 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, el propósito de esta investigación es estudiar o analizar las bases de datos SQL y NoSQL y mediante la ejecución de pruebas de seguridad las cuales va a realizar utilizando herramientas de software libre a fin de comparar los resultados obtenidos y así poder determinar cuál de las dos tecnologías es más conveniente para su uso en ambientes corporativos, adicionalmente sobre las brechas de seguridad que se encuentren se realizarán recomendaciones con el fin de lograr establecer controles para la mitigación de las mismas.

TITULO

ESTUDIO DE SEGURIDAD EN BASES DE DATOS SQL Y NoSQL

0. INTRODUCCIÓN

En la actualidad la gran cantidad de la información⁷ se recolecta en bases de datos SQL o relacional entre las cuales se encuentra (mysql, Oracle, dbase), habituales por su confiabilidad y seguridad en la administración de los datos. Por la demanda de información que se maneja es necesario dirigir las bases de datos hacia la optimización, velocidad y la estabilidad para distribuir el procesamiento de la información.

Las bases de datos NoSQL integran estas nuevas exigencias de mercado y su infraestructura es más robusta y está en la nube con un sistema multiplataforma lo cual llega a ser de mayor confiabilidad

El propósito de este proyecto consiste en analizar y comparar la seguridad que ofrecen las bases de datos SQL y NoSQL, en una primera instancia se iniciará la revisión de la información general de las bases de datos relacionales y posteriormente se realiza el estudio de las BD NoSQL, para llevarlo a cabo se realiza un laboratorio donde se instala una máquina virtual con Ubuntu donde se instalan las dos bases de datos y con Kali Linux determinar cuál es más segura en la base de datos aplicando procedimientos de testeo y diagnóstico de seguridad, por medio de los cuales se busca detectar vulnerabilidades de seguridad y estudiar los riesgos que se presenta en cada una de las bases de datos analizadas para posteriormente plantear posibles soluciones.

⁷ Bases de datos. http://volaya.github.io/libro-sig/chapters/Bases_datos.html. En línea.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 DEFINICIÓN DEL PROBLEMA

Según los estudios realizados por compañías desarrolladoras de bases de datos⁸, se encontró que los activos que son atacados más frecuentemente son las bases de datos, ya que estas son donde almacena regularmente la información de las compañías, los procesos por lo general en las bases de datos se hallan alojada la información referente a los procesos más importantes de la compañía.

En el sector gobierno se maneja información significativa como los datos de los usuarios, de sus predios, matrículas y financieros que están almacenadas en las bases de datos, es importante proteger esos activos, las empresas deben buscar un equilibrio en el procesamiento de los datos, adicionalmente las bases de datos NoSQL son para empresas pymes ya que la estructura que manejan es en la nube y se requiere un procesamiento de datos más rápido. Es necesario identificar las brechas de seguridad que tiene las bases de datos

Existen las bases de datos relacionales, estas son las que usan un lenguaje estándar para su gestión y manipulación de los datos, los cuales son sensibles a los ataques y en las páginas web aparecen las bases de datos NOSQL estas no tienen esquemas, no usan SQL ni permiten joins.⁹

1.2 FORMULACIÓN DEL PROBLEMA

¿Qué tan segura se encuentra la información almacenada en las bases de datos SQL y NoSQL?

⁸ It-Insecurity. <http://insecurityit.blogspot.com.co/2010/09/bases-de-datos-inseguras-algunas.html>
En línea

⁹ Diaz Sepulveda, William. Basesdedatosnosql. <http://basesdedatosnosql.blogspot.com.co/> En línea

2. JUSTIFICACIÓN

En las organizaciones, las áreas de TI se viven enfrentando a uno de los más grandes problemas que existe actualmente, la pérdida de información que tiene que tener tres pilares, integridad, confidencial y disponibilidad y como la tecnología avanza, las metodologías que utilizan los atacantes también evolucionan y se evidencia cada día en los sistemas más vulnerabilidades, que son aprovechadas por los atacantes mientras los fabricantes las corrigen, y el personal de TI aplica los cambios necesarios para corregir la vulnerabilidad.

Es por este motivo que no se debe escatimar esfuerzos en las políticas de seguridad para proteger las bases de datos, indiferente de cual motor se utilice, se debe prestar especial atención a las medidas que se implementan y las tecnologías que se utilizan buscando que se adapte a las necesidades de cada infraestructura y el cual se encuentre dentro del alcance de la organización.

Basados en lo descrito anteriormente, se pretende realizar un estudio de seguridad de la información en las bases de datos, relacionales y no relacionales NOSQL, con el fin de definir algunos parámetros que permitan realizar la mejor elección de la base de datos para cada escenario según las condiciones específicas de cada sistema.

Se escalan horizontalmente, hacen uso de la memoria del computador, manejan grandes cantidades de consultas y transacciones a diario, lo cual es más vulnerable al ataque.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar un estudio de seguridad de la información en las bases de datos, relacionales y no relacionales NOSQL, para determinar cuál base de datos es más segura y tiene mejor capacidad.

3.2 OBJETIVOS ESPECÍFICOS

- Levantar la información del estado actual de seguridad en bases de datos relacionales y no relacionales NoSQL.
- Determinar las bases de datos SQL y NoSQL a aplicar procedimientos y diagnóstico de seguridad.
- Identificar qué tipo de base de datos es más vulnerable a los ataques informáticos.
- Presentar propuesta de solución seguridad de las bases de datos SQL y NOSQL estudiadas.

4. MARCO REFERENCIAL

4. 1. RESEÑA HISTÓRICA

El termino base de datos aparece en el año 1963 en la celebración de un congreso en California. Se empiezan a usar las bases de datos cuando surge la necesidad de almacenar información, con la aparición de las computadoras.

A continuación, los hechos más relevantes de las bases de datos.

En la década de los 60

- Las compañías dieron precios bajos para adquirir las computadoras y así utilizar los discos, con esto ya no se tenía que saber la ubicación de las bases de datos.
- Aparecen las bases de datos jerárquicas y de red donde se organizaban en árboles y listas.
- Se realizó una sociedad de IBM y la compañía American Airlines para desplegar SABRE, un sistema que operaba transacciones de reservas de los pasajeros que viajaban por la aerolínea.
- Se crea el IDS por Charles Bachman, modelo en red de base de datos.
- CODASYL (Conference on Data Systems Languages), eran industrias que regulaban los lenguajes de programación que se trabajaran a su vez en varios ordenadores, trabajaron programas como Cobol no fue posible establecer un estándar fijo.¹⁰

En la década del 70

- *Edgar Frank Codd* puntualizo sobre el modelo *relacional* y dio a conocer una serie de parámetros de los sistemas relacionado con las bases de datos, este científico desarrollo este lenguaje¹¹, al igual que algunas bases de bases de datos relacionales: ORACLE, MYSQL, SQL Server, POTGRESS, DB2, etc, con metodologías para los problemas de gestión y estructuración de la información,
- estas bases de datos tienen muchas herramientas desarrolladas, manejan un lenguaje estandarizado para su gestión en SQL.
- Con la información del señor Cood sobre las bases de datos el señor *Larry Ellison* creo una base de datos *Oracle*, fue importante por la estabilidad, servicios

¹⁰ Blog a Historia de la informática. <http://histinf.blogs.upv.es/2011/01/04/historia-de-las-bases-de-datos/> En línea

¹¹Macluskey, Historia de un Viejo Informático. La entrada en escena de Las Bases de Datos Relacionales. <https://eltamiz.com/elcedazo/2009/04/20/historia-de-un-viejo-informatico-la-entrada-en-escena-de-las-bases-de-datos-relacionales/> En línea

y que es multiplataforma, no se utilizó como base de datos relacional por problemas de rendimiento.

- IBM desarrollo una base de datos relacional más eficaz.

En la década del 80

Desarrollan SQL era un lenguaje

para consultas o accesos a la base de datos.

Con su método de filas, columnas y tablas las bases de datos empiezan a apostar con las bases de datos de Red y Jerárquicas, ya que eran más económicas, en este momento inician las bases de datos orientadas a objetos.

Principios década de los 90

Aparece el lenguaje *SQL (Structured Query Language)*, su constitución es para consultas de gran importancia de información, como lo eran las transacciones, las empresas realizaron mayor venta de base de datos orientada a objetos como Excel y Access.

Finales de la década de los 90

En los 90 se creó WWW "*Word Wide Web*", es una de las formas fácil de realizar consultas en las bases de datos, tiene disponibilidad permanente, cuenta con una gran capacidad de almacenamiento.

Siglo XXI.

- En este momento existen 3 compañías que lideran el mercado de las bases de datos estas son: Microsoft, Oracle y IBM.
- Google genera gran cantidad de información con internet.
- Existe gran diversidad de software que crea y operar bases de datos como es LING, de Microsoft, con código de visual estudio también está orientado a objetos.
- Visual Studio está integrado a los sistemas operativos Windows que tolera varios lenguajes de programación como son: Visual C++, Visual#, Visual J#, Visual C++, ASP.NET y Visual Basic.NET, el objetivo es diseñar aplicaciones web en la plataforma .Net, que se relaciones páginas web, estaciones y dispositivos móviles.¹²

¹² Codd, Hollerith. Historia de las bases de datos. <http://histinf.blogs.upv.es/2011/01/04/historia-de-las-bases-de-datos/En línea>

4.2. MARCO TEORICO

Una base de datos es una colección de información ordenada en registros y almacenada de forma que un programa en un ordenador que pueda seleccionar rápidamente las fracciones de datos que necesite. Las bases de datos se organizan por campos, registros y archivos. Un campo es un segmento único de información, cada registro es una unidad de información estructurada en diferentes campos o tipos de datos y un archivo es una colección de registros.

Frente a la información guardada tiene como principal ventaja recuperar exactamente la información deseada y realizar diferentes formas para modificar muchos datos en muy poco tiempo. El archivo electrónico admite realizar determinados procesos (consultar datos, ordenarlos, realizar informes).

4.2.1 Bases de datos relacionales

Las Bases de Datos han evolucionado a Métodos de Administración de Base de Datos Relacionales (RDBMS).¹³ Una base de datos es una serie de elementos organizados, se accede a tablas de los datos creados en estas. Las tablas descritas para tener acceso a estos datos se crean nuevamente de diferente manera sin reorganizar las tablas de la base. La base de datos relacional bien diseñada contiene información de un negocio o un proceso y su uso más común es para almacenar y recuperar información, mantiene la integridad de la misma, son fáciles de comprender y construir, se representan con diagramas de entidad-relación.

Las bases de datos relacionales tienen algunas características principales:

SQL

Es un Lenguaje Estructurado de Consultas actualiza, consulta y administrar base de datos relacionales, debido a estas semejanzas el modelo permite acceder a relaciones comerciales.

Tabla

Una tabla almacena datos en filas y en columnas se conforma por campos y registros lo cual son iguales a los de una hoja de cálculo.¹⁴

¹³ Pino, Diego. Los sistemas de bases de datos relacionales RDBMS. <http://diegopino.blogspot.com.co/2009/03/los-sistemas-de-bases-de-datos.html>. En línea

¹⁴ Covey Robert, Base de datos relacionales. <http://deletesql.com/viewtopic.php?f=5&t=4>. En línea

Figura 1. Modelo de tabla

Cve. cliente	Nombre	Direccion	Ciudad	Estado
1	Alfredo Godinez	Fresnillo #47	Veracruz	Veracruz
2	Gabriela Mora	El crespo #81	Guadalajara	Jalisco
3	Alejandra Avalos	Casa Mata #1	Morelia	Michoacan
4	Jaime Quintero	Miraflores #23	Uruapan	Michoacan
5	Carlos Miranda	Rio Bravo #95	Matamoros	Tamaulipas

Fuente: https://www.google.com.co/search?q=tabla+en+la+base+de+datos&espv=2&biw=1366&bih=662&source=Inms&tbm=isch&sa=X&ved=0ahUKEwiji8sTlyNrPAhUGNT4KHWnSC5MQ_AUIBigB#imgrc=LVfsIGmEa0XCtM%3A

Integridad

Es la seguridad importante que tienen los datos y la eficacia en las bases de datos. La estructura en la base de datos (DB), es administrar las acciones que se realizan en estas, resguardan las estructuras y los datos. (Llaves primarias y foráneas).

Independencia física

Son cambios ocasionales ya que en estos programas no modifican el almacenamiento físico, ni tampoco una manipulación lógica,

Independencia lógica

Se cambia el esquema de los conceptos sin afectar el programa de aplicación y no trasciende a los subconjuntos de las mismas vistas cuando modifica o elimina objetos de la base de datos.¹⁵

Flexibilidad

Es la facilidad de las diferentes vistas en función de la aplicación y los usuarios, los datos los define el usuario.

Uniformidad

La estructura de los datos uniforme que permite la concepción y manipulación de los estos por parte de los usuarios.

¹⁵ Torralba Velazco, Lucia Ángeles, Fundamentos de base de datos. <http://deletesql.com/viewtopic.php?f=5&t=4>. En línea.

Redundancia controlada

Hace parte del almacenamiento de los datos en diferentes partes, por razones técnicas o económicas.

Seguridad de acceso

Restricción de acceso a los datos no autorizados y para diferentes usuarios.¹⁸

Acceso concurrente

Es cuando varios usuarios acceden a los sistemas de base de datos (RDBMS) en forma controlada.

Dominios

Conjunto de posibles valores dentro del modelo relacional y que puede tomar un atributo, existen dominios generales son los que comprende entre un máximo y un mínimo y el dominio restringido pertenece al conjunto de valores específicos.

Clave única

Es la identificación de las claves que pertenecen a una tupla, no deben existir campos o valores que sean iguales o idénticos, cada uno es único.

Clave primaria

Una clave única es un atributo de la tabla para especificar los datos que serán relacionados con las demás tablas, se realiza por medio de claves foráneas, no debe ser NULL.

Normalización

Son reglas que se emplean del paso de un tipo entidad- relación a relacional esto permite que la base de datos sea usada de una manera eficiente.

Vistas

Muestra los atributos de otras tablas en una tabla lógica. De esta manera se obtienen datos que son de interés.¹⁹

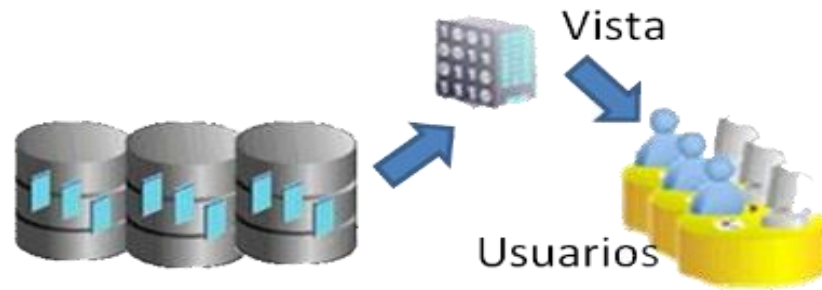
¹⁸ Drakonis. Integridad y seguridad en las bases de datos.

<https://es.slideshare.net/Drakonis11/integridad-y-seguridad-en-las-bases-de-datos-presentation>. En línea

¹⁹ PAOLA, NERLY, LINA Y YULIMA, Tecnólogo en administración documental yulipane.

<http://yulipane.blogspot.com.co/2010/09/elementos-de-una-base-de-datos.html>. En línea

Figura 3. Modelo de Vistas



Fuente: Bases de Datos y Mas. Disponible en https://www.google.com.co/search?q=vistas+en+la+base+de+datos&espv=2&biw=1366&bih=662&source=lnms&tbn=isch&sa=X&ved=0ahUKEwjf4O2-zdrPAhVlwj4KHWzDA_AQ_AUIBigB#imgsrc=Min_lioMe-ud7M%3A

Consultas

El propósito es recuperar la información que esta almacenada en las tablas, se usa para ver, cambiar y analizar datos de distintas maneras.

Figura 4. Modelo de Consultas



Fuente: Monografias.com Disponible en: https://www.google.com.co/search?q=consultas+y+formularios+en+la+base+de+datos+sql&espv=2&biw=1366&bih=662&source=lnms&tbn=isch&sa=X&ved=0ahUKEwj12JXBztrPAhWLMj4KHYMGCEoQ_AUIBygC#imgsrc=kYe1ejrHB6sYkM%3A

Formularios

Es un formato que se utiliza para adicionar, modificar o consultar información bajo criterios que personaliza el usuario, se puede tener en listas desplegadas, instrucciones, controles de desplazamiento y gráficos que ayudan a los usuarios a trabajar con los datos.

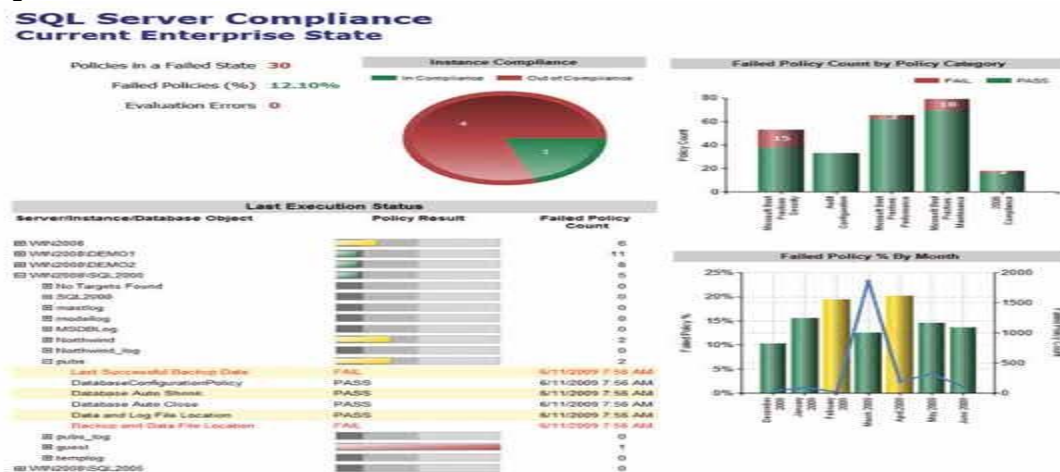
Figura 5. Modelo de Formulario

Fuente: Programando con Visual Basic.Net Disponible en: https://www.google.com.co/search?q=formularios+en+la+base+de+datos+sql&biw=1366&bih=662&espv=2&source=lnms&tbn=isch&sa=X&ved=0ahUKEwiTlv26z9rPAhVJPz4KHREGBRUQ_AUIBygC#imgrc=y1Vsy-pwtFCNfM%3A

Informes

Es el resultado de la ejecución de consultas que se ejecutan y se presenta a los usuarios de los datos que están almacenados en las bases, se puede imprimir y contiene gráficos si así están diseñados.²⁰

Figura 6. Modelo de Informes



Fuente: SQL Server: Los 10 secretos principales Disponible en: https://www.google.com.co/search?q=informes+en+la+base+de+datos+sql&biw=1366&bih=662&espv=2&source=lnms&tbn=isch&sa=X&ved=0ahUKEwiAk_ee0NrPAhVBdj4KHevTBf4Q_AUIBygC#imgrc=sAPbLgkFftweFM%3A

²⁰ MUÑOZ GOMEZ, Juan Carlos, Características principales del Modelo Relacional en las bases de datos. (<https://prezi.com/g3tx07vx2dcu/caracteristicas-principales-del-modelo-relacional-en-las-bases-de-datos/>)

4.2.2 Bases de datos NoSQL Surge en los años 90 por un empleado de Racks Pace, Eric Evans cuando evidencio el crecimiento de los registros en una base de datos, la cual es llamada relacional y distribuida, es diferente a las bases de datos relacionales que se conocen.

A medida que crece la web se evidencio que se necesitaba procesar gran cantidad de información con unas estructuras horizontales. Algunas compañías como Google, Amazon, Twitter y Facebook. Tenían retos por el manejo de los datos en las tablas, ya que las tradicionales RDBMS no solucionaban, como lo es el procesamiento de los datos más rápidamente y coherente, algunas de las características son:

Alto rendimiento

Tienen un mejor rendimiento que las bases relacionales el almacenamiento de 50GB en 0,12 milisegundos mientras que MYSQL tarda 300 segundos

Escalabilidad Horizontal.

Permite añadir, eliminar o realizar ordenamientos con elementos (Hardware) del sistema sin afectar el rendimiento, solo se tendrá que mover la nube é entornos vitalizados.

Distribuido

Logra replicar y distribuir los datos sobre los servidores permitiendo el soporte sin afectar el rendimiento²¹

Figura 7. Modelo de distribución NoSQL



Fuente: Projecte formatiu per a fomentar l'ús i millora dels mitjans socials Disponible en: https://www.google.com.co/search?q=bases+de+datos+NoSQL+big+data&espv=2&biw=1517&bih=741&source=Inms&tbn=isch&sa=X&ved=0ahUKEwiT1pjo8eLPAhWmR4KHTxDCeoQ_AUIBigB&dpr=0.9#tbn=isch&q=bases+de+datos+NoSQL+distribuido&imgdii=X1gPVaDety9G_M%3A%3BX1gPVaDety9G_M%3A%3BBAk5b7iSJEagsM%3A&imgcr=X1gPVaDety9G_M%3A

²¹ Díaz Sepúlveda, William, Bases de datos NoSQL. <http://basesdedatosnosql.blogspot.com.co/En línea>

Libertad de esquema

Permite modelar los datos; facilita la integración de lenguajes de programación orientados a objetos evitando el mapeado.

Consultas simples

No se requieren muchas instrucciones por lo que conlleva a ganar simplicidad y eficiencia.

Big Data

Los volúmenes de datos big data pueden ser manejados por NoSQL.

No DBA

Gracias al diseño para requerir menos gestión: reparación automática, distribución de datos y modelos de datos más simples, con estas características no es necesario los DBA.

Economía

Usan servidores genéricos y baratos para la administración de datos y volúmenes de transacciones.

Modelo de datos Flexibles

No depende de algún modelo específico, no existe restricciones para almacenar los datos

Consultas simples

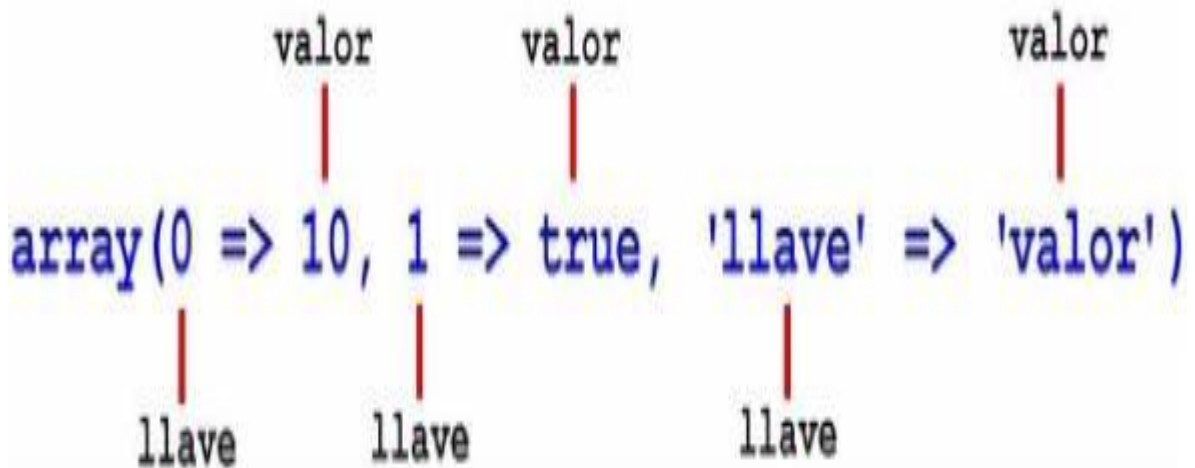
Se requieren menos instrucciones por lo que conlleva a ganar simplicidad y eficiencia.

Almacenamiento llave-valor.

Consisten en un diccionario (DHT) el cual almacena y obtiene valores mediante una clave, favoreciendo la escalabilidad y limita las consultas complejas.²²

²² Hostdimeblog, 10 características que debo conocer de las bases de datos Nosql, <http://blog.hostdime.com.co/10-caracteristicas-que-debe-conocer-de-las-bases-de-datos-nosql/> En línea

Figura 8. Modelo de almacenamiento llave-valor



Fuente: Array: ¿es posible almacenar más de un valor Disponible en: <https://www.google.com.co/search?q=almacenamiento+llave+valor&espv=2&biw=1517&bih=741&tbm=isch&tbo=u&source=univ&sa=X&ved=0ahUKEwiu5NOR8OLPAhVB6x4KHauXAYgQsAQIMA&dpr=0.9#imgrc=gX0eu-3nEG1jTM%3A>

4.3. MARCO CONCEPTUAL

Bases de datos Relacionales: son modelos que se utilizan para fabricar problemas existentes y dirigir los datos en forma dinámica, existe una relación de entidades de diagramas y vinculación de datos, se contextualiza con la relación que se realiza entre tablas y los datos que están en los registros.

Sistema Gestor de Bases de Datos (SGBD): la relación de los datos interconectados con las herramientas sistemáticas, que accede a los datos. Donde se almacena es lo que se llama base de datos. Se almacenan los datos de una empresa y se puede recuperar y guardar en forma eficiente.²³

Modelo de Datos: son las herramientas que se tiene para detallar los datos, la semántica, la relación y restricciones de contenido.

Base de Datos Relacional: es donde están contenidos los datos compartidos, los cuales existen relación de los datos que están guardados en tablas y se relacionan dos tablas, lo cual se llama modelo Relacional.

²³ Wikipedia. Sistema de gestión de base de datos. https://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_bases_de_datos. En línea

Bases de Datos Clave-Valor: son datos que se almacenan en clave –valor o también son conocidos como diccionarios, son procesados en un tiempo actual una gran cantidad de datos, fiabilidad y alta disponibilidad, con respuestas de milisegundos.

Bases de Datos Documentales: son documentos de texto utilizan datos semi-estructurales, forma de clave-valor utilizado, con estructuras como JSON.

Bases de Datos en Grafos: son nodos de grafo y su relación, la relación entre los objetos son estáticas o dinámicas, estos son datos conectados, los datos se manejan Twitter, LinkedIn y Google se modelan por grafos.

Datos Estructurados: son estructuras precisas como fechas, cadena de caracteres, con longitud definida y se guarda en tablas.

Datos Semi-estructurales: no son campos determinados, con marcadores para separar los elementos, se gestiona en forma estándar.²⁴

4.4. MARCO LEGAL

La mayoría de los países tiene leyes para castigar los delitos a los ataques de la información.

En Colombia con la ley 1273 de enero de 2009, en su primer capítulo, en los artículos

269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de

²⁴ Acenswhitepaper. Bases de datos NoSQL que son y tipos que podemos encontrar. <https://www.acens.com/wp-content/images/2014/02/bbdd-nosql-wp-acens.pdf>. En línea

información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. *El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.*

La ley en sus diferentes ítems, informa sobre los delitos informáticos, la información que se maneja en las organizaciones debe ser integridad, para evitar la alteración o robo sin autorización correspondiente para el manejo de esta y así mismo las bases de datos donde se almacena dicha información.

Para evitar estos delitos que se puede presentar con las bases de datos se debe configurar muy bien las bases de datos dando la mayor seguridad a aplicar, asignando los permisos correspondientes según el rol que maneje cada usuario.

Con los inconvenientes que se han presentado afectando la información que se maneja en las bases de datos las empresas ha tomado mayor conciencia, para tener una mayor seguridad, aplicando políticas y métodos para evitar el robo de información de los usuarios, realizando la firma de un documento de confidencialidad de la información para las personas que la manejan y es de gran ayuda esta ley ya que, si se presenta algún delito de estos, se les aplica la pena según el delito cometido el cual incurrió, pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

5. MARCO METODOLOGICO

5.1 MÉTODOLOGIA DE INVESTIGACION

Se identificarán las vulnerabilidades que se presenta en las bases de datos relacionales y no relacionales con el fin de alcanzar los objetivos de este proyecto.

5.1.1. Análisis. el estudio se realiza en empresas e internet (facebook, hadoo, twitter), debido a que las bases de datos relacionales las maneja en varias organizaciones, las bases de datos NoSQL no hay mucha información física; para perfeccionar la información obtenida se debe indagar en trabajos de grado, tesis, revistas, foros sobre temas relacionados que pueda confirmar la autenticidad de los datos encontrados en las diferentes páginas web durante la búsqueda. Frente a esta actividad se inicia a realizar una comparación de las bases de datos más utilizadas en las empresas como las políticas de uso, los procedimientos y estándares en la seguridad de las bases de datos relacionales y NoSQL.

A continuación, se relacionan las causas que origina la pérdida de información

Causas:

Errores de hardware: que las maquinas donde están instalados los motores y las bases de datos presente fallas de máquina.

Errores de software: el sistema operativo o los motores presente errores por las versiones que contiene inestabilidad.

Desastre natural: no se tenga Backups o copias de seguridad en otro lugar aparte del instalado para en caso de un desastre natural se realice una recuperación fácil de las bases de datos.

Errores humanos: que, por falta de conocimiento, mala configuración se presenten errores el cual ataquen a las bases de datos y la información.

5.1.2. Muestra. para el desarrollo de este proyecto se toma una muestra de las bases de datos una relacional y otra no relacional, con estas bases de datos se realiza un laboratorio el cual se aplicará el procedimiento sobre las bases de datos para identificar las vulnerabilidades utilizando la herramienta Kali Linux.

5.2. ESTUDIO METODOLÓGICO

Este estudio se basa en una investigación básica, aplicada y experimental cuyo objetivo es realizar procedimientos o táticas para determinar la solución viable del objetivo, aplicando los conocimientos que se adquirieron en el marco teórico y mostrar los resultados de las prácticas realizadas, probando las teorías que están relacionadas con la investigación básica, para así dar a conocer las vulnerabilidades que se identifiquen en las bases de datos relacional y no relacional, y de esta manera poder contar con argumentos para tomar una decisión acertada y elegir la tecnología más confiable.

5.3 METODOLOGÍA DE DESARROLLO

Para el desarrollo de este estudio se realizó una serie de fases para determinar el nivel de seguridad, de las bases de datos relacional y no relacional, basándose en la identificación de vulnerabilidades y ejecutando los siguientes pasos:

- Iniciar la investigación comparando las características de las bases de datos SQL y NoSQL.
- Luego se comienza con la selección de un motor de bases de datos SQL y uno de NOSQL que tengan una alta utilización en el mercado. Se realiza un estudio de la seguridad y falencias que tiene cada uno que son requeridas para aprender a escoger la mejor para su desarrollo según lo que se requiera.
- Realizar un laboratorio seleccionando un motor de bases de datos SQL y otra NOSQL, para identificar las vulnerabilidades que se presenten con Kali Linux. A continuación algunos requisitos para el desarrollo del laboratorio:

Es necesario tener una máquina virtual: Con sistema operativo, software y versión precisa para el funcionamiento de las bases de datos.

Definir las Bases de datos: una relacional y otra NoSQL.

- Versión: tomar la versión más apropiada, estable, confiable y segura para realizar las pruebas ya que se corrigieron los errores encontrados en las otras versiones inestables.
- Documentos de soporte como: El manual de instalación y funcionamiento, biblioteca de los comandos que alcanza a manejar el motor de base de datos.

- Soporte y solución de inquietudes: Foros y espacio por parte del proveedor de la base de datos para informar dudas con relación a la funcionalidad del motor.
- Ventajas/Desventajas: las posibles restricciones de uso que tienen los motores, es significativo cuando se instale o efectúe la solución.
- Realizar un análisis de los resultados del laboratorio a realizar de los dos motores de bases de datos uno SQL y otra NOSQL.
- Proporcionar unas recomendaciones de los dos motores de bases de datos uno SQL y otra NOSQL después de realizar el laboratorio.

6. ANÁLISIS DEL DESARROLLO DEL PROYECTO

Se detecta que las bases de datos SQL son más costosas y manejan mayor seguridad que las bases de datos NoSQL. Estas tienen menos rendimiento y no maneja gran volumen de información, las bases de datos NoSQL tienen más manejo de información son más rápidas no tienen soporte, no se necesitan de los DBAS, contienen mayor vulnerabilidad en el robo de información que viaja por las redes ya que mucha de esta información no está encriptada.

Todas las bases de datos son diferentes en su rendimiento y en la seguridad de la información se basa en los métodos que maneja cada una de las diferentes bases de datos relacionales y NoSQL.

6.1. EQUIVALENCIAS Y DIFERENCIAS ENTRE LAS BASES DE DATOS

Las propiedades de las dos bases de datos estándar son:

- **Arreglo:** son las relaciones y/o elementos para empezar a ver la forma de los datos, los elementos de colección, se denota en una cardinalidad que acorde a las tuplas, la colección son documentos con esquemas.
- **Restricciones No SQL:** representa los datos a dos modelos, solo hay restricción cognitiva, las restricciones son de semántica, con un esquema rígido, manipula los datos con arreglo relacional.
- **Rutinas:** existen equivalencia para recuperación y actualización, se mantiene un CRUD²⁵, las implementaciones son diferentes, los propósitos son: Consulta, Insertar, Modificar y Borrar.²⁵

²⁵ Javier. NoSQL vs SQL: Principales diferencias y cuándo elegir cada una de ellas.
<https://blog.pandorafms.org/es/nosql-vs-sql-diferencias-y-cuando-elegir-cada-una/> En línea

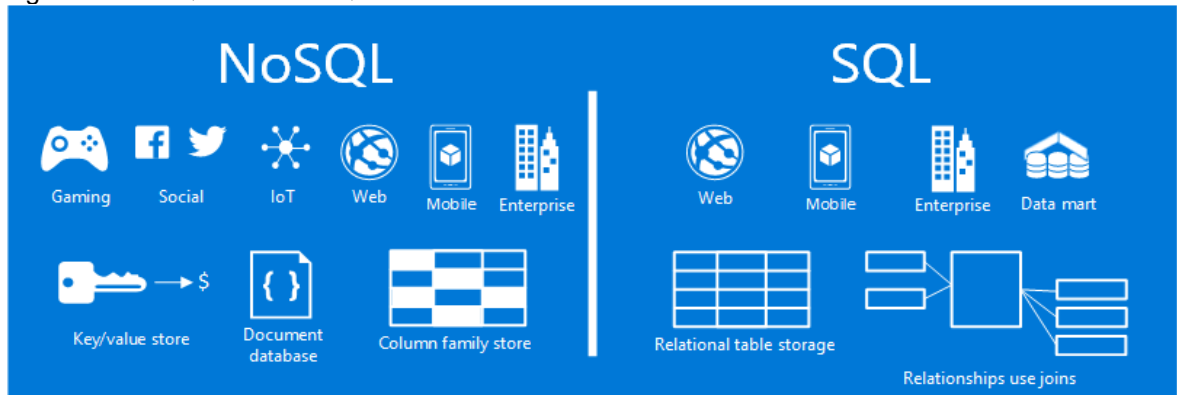
6.1.1. SEGURIDAD DE LAS BASES DE DATOS SQL VS NO SQL

Tabla 1. Compara las diferencias principales entre NoSQL y SQL

Diferencias	NoSQL	SQL
Modelo	No Relacional. Almacenar datos en documentos Json, pares clave / valor, almacenar columnas o gráficos.	Relacional. Almacena datos en una tabla.
Datos	Ofrece flexibilidad ya que no todos los registros necesitan almacenar las mismas propiedades. Nuevas propiedades se pueden agregar sobre la marcha. Las relaciones a menudo se capturan al desnormalizar los datos y presentarlos en un solo registro. Es bueno para datos semiestructura	Ideal para soluciones donde cada registro tiene las mismas propiedades. Agregar una nueva puede requerir la alteración de esquemas o el relleno de datos. Las relaciones a menudo capturan en uniones de uso para resolver las referencias en las tablas. Es bueno para datos estructurados.
Esquemas	Esquemas dinámicos o flexibles. La base de datos es independiente del esquema y el esquema es dictado por la aplicación. Esto permite agilidad y desarrollo altamente iterativo.	Esquema estricto. El esquema debe mantenerse y mantenerse sincronizado entre la aplicación y la base de datos.
Transacciones	El soporte de transacciones de ACID varía según la solución.	Admite transacciones ACID.
Consistencia	La consistencia varía según la solución, algunas soluciones tienen una consistencia sintonizable.	Fuerte consistencia apoyada.
Escala	Horizontalmente escala bien.	Escala bien verticalmente.
Procesamiento	Es rápida y confiable ya que los datos se guardan horizontalmente permite que sean elásticas.	Es rápida por su estructura que maneja.

Fuente: NoSQL frente a SQL Disponible en: <https://azure.microsoft.com/es-es/documentation/articles/documentdb-nosql-vs-sql/>

Figura 9. NoSQL frente a SQL



Fuente: NoSQL frente a SQL Disponible en: <https://azure.microsoft.com/es-es/documentation/articles/documentdb-nosql-vs-sql/>

6.1.2. Desventajas en aplicaciones web no transaccionales. las aplicaciones Web no transaccionales tienen más desventajas ya que este software es desarrollado con limitantes lo cual si se requiere realizar modificaciones no se puede realizar y en otros genera costos.

6.1.2.1. Bases GNU. es software libre, se diseña con herramientas básicas, el código es limitado para las personas, es abierto, se puede modificar cuando presente errores, contiene seguridad de las plataformas, actualización de parches y comunicaciones.

6.1.2.2. Bases de datos comerciales. el licenciamiento dependiendo de la versión tiene un costo, estas bases de datos contienen herramientas que permiten probar el rendimiento, las fallas y monitoreo, cuentan con soporte las 24 horas, el procesamiento de los datos es seguro, la configuración debe ser bien parametrizada para no tener inconvenientes, requiere ser manejado por personal especializado. SQL Server y bases de datos relacionales (RDMBS) son las bases de datos más usadas durante 20 años. La necesidad de procesar volumen y velocidad de datos ha permitido que los desarrolladores requieran un escenario que son las bases de datos NoSQL el cual se puede almacenar datos no distribuidos y heterogéneos, el almacenamiento de clave-valor, columnas y de datos de gráfico, que son populares con juegos, redes sociales y aplicaciones de Microsoft.²⁶

²⁶ Díaz, José. Que son las bases de datos? [https://blog.pandorafms.org/es/que-son-las-bases-de-datos/En línea](https://blog.pandorafms.org/es/que-son-las-bases-de-datos/En%20línea)

Tabla 2. Comparativo de las bases de datos principales entre SQL y NoSQL

Base de datos Relacionales		Base de datos NoSQL	
MySql	La administración es fácil, lo mismo que la operación, la instalación dura 15 minutos, es frecuentemente utilizado para el desarrollo Web 2,0 y Enterprise2.0.	Orientados a Documentos	Soportan diferentes formatos (JSON, XML). Se pueden cambiar esquemas sin parar las bases de datos y los desarrolladores, las cuales están Mongo DB, Couchbase Server, Mark Logic Server, ElasticSearch.
ORACLE	Para las organizaciones es abierta, su administración es simple, fácil de integrar, escalable lo cual es una ventaja para su adaptación a cambios, permite alinearse con los procesos de las organizaciones.	Orientados a Clave-Valor	Ideales cuando se accede a datos por clave. La diferencia de este tipo de base de datos radica en la posibilidad de almacenar datos, suele ser muy eficientes para las lecturas y escrituras. Ellas tienen Redis, Riak, Oracle NoSQL.
DBase	Es similar a las que existían MS/DOS dBASE 2,0, la ventana del escritorio es la combinación de diferentes programas, es fácil y entendible. Es difícil hacer que el software se vea fácil.	Orientados a Columnas	Se puede manejar claves a valores y agruparlas en arreglos y existe la necesidad de acceder a varias columnas de muchas filas. Apache Cassandra, Apache Hbase.
FileMaker Pro	Este programa de bases de datos tiene la potencia y flexibilidad para manejar todas tus funciones Su estabilidad es buena ya que es muy sencilla y también uno no se pierde.	Orientados a grafos	Detención de fraude, recomendaciones en tiempo real, la distribución que tiene columna y cada relación, Tiene Neo4j, Infinite graph.
Microsoft Access	Microsoft Access es uno de los sistemas de bases de datos relacionales más usuales para los sistemas operativos Windows, accede crear archivos de bases de datos relacionales que alcanzan a ser gestionadas por una interfaz gráfica simple.		

Fuente: El Autor

7. DESARROLLO DEL PROYECTO

Se estudiará los procedimientos y políticas estándares que se maneja en cada base de datos, lo cual se realiza una comparación de las bases de datos, las vulnerabilidades que se detectó en cada una la cual con este estudio se definirá como se puede mitigar el riesgo se presente en cada una de ellas, será necesario que se pueda integrar fácilmente y que ofrezca al programador herramientas para hacer más cómodo su trabajo.

7.1. LEVANTAR LA INFORMACIÓN DEL ESTADO ACTUAL EN BASES DE DATOS

Las bases de datos ayudan día a día a ejecutar trabajos más fáciles y rápidos, pero también presentan fallas, éstas pueden ser globales que sucede en cualquier momento, fallas del sistema como caídas leves lo cual se les denomina (crash), fallas de los medios de almacenamiento pueden ser de manera física, fallas por catástrofe están son inesperadas como desastres, temblores, derrumbes, etc.

¿Qué es una falla en una base de datos?

Cuando el software empieza a tener dificultades a la hora de mostrar el contenido de la información. Se presentan en diferente forma ya sean físicas o del sistema.

Tipo de fallas

El sistema debe tener la capacidad de recuperarse cuando se presente una falla.

Falla local: es el desborde de una transacción y solo afectan a esa transacción.

Falla global: como la caída eléctrica a la CPU, estas afectan a las transacciones que se estaban realizando en el momento que se presenta.

Falla del sistema: Son caídas leves o también conocidas como crash, pérdida de los contenidos de la memoria principal, almacenamiento temporal o buffer, no afecta las bases de datos.

Falla de almacenamiento: Cuando se destruye una parte de la base de datos lo cual se requiere recuperar con un Backup ocasionado pérdidas de algunas transacciones.

Fallas por catástrofe: se pierde la información de las bases de datos, lo cual solo se puede recuperar si se tiene una data base del Backup, a partir de la última copia que se realizó.²⁷

²⁷ De la Cruz, Juan Jose. TIPOS DE FALLAS EN BASE DE DATOS.

<https://prezi.com/zur7rjanq7ym/tipos-de-fallas-en-base-de-datos/> En Línea.

Las ventajas de las bases de datos en este momento:

- Independencia de los datos: modificar los datos sin tocar el código de los aplicativos.
- Menor redundancia: No se repiten los datos
- Integridad de los datos: Se dificulta tener inconsistencia en ellos.
- Coherencia de los datos: Recoge y almacena los datos solo una vez, si se tratan los mismos datos los resultados son más coherentes.
- Seguridad en los datos: Limitar el acceso a los usuarios, definir los roles.
- Datos más documentados: Con los metadatos se describe información de la base de datos.
- Acceso a los datos más eficiente: Por la organización de datos, el rendimiento es más rápido.
- Reducción del espacio de almacenamiento: Por la distribución que manejan los datos.

Acceso simultaneo a los datos: Se puede tener más control de los usuarios.

Desventajas de las bases de datos en este momento:

- La instalación es costosa: La administración y control en las bases de datos, pide hardware y software es costosa, aparte del mantenimiento que requiere el Sistema Gestor de Bases de Datos (SGBD).
- Personal calificado: Requiere personal calificado por la dificultad que manejan las bases de datos.
- Ausencia de estándares: Depende de los sistemas comerciales del estado.
- Implantación larga y difícil: La adaptación del personal es larga y complicada.
- No es rentable a corto plazo: Por el personal y los equipos que son costosos y tarda su operación.²⁸

Las empresas han evidenciado que los riesgos se han dado en las propias compañías, las causas son el error humano, los ataques internos, abuso de privilegios de acceso del propio personal y los códigos maliciosos y virus. Muchas empresas a pesar de conocer los riesgos cuentan con muy pocas medidas de seguridad, algunos no saben si cuentan con las garantías necesarias de seguridad por el personal que la administran ya que por error humano pueden llegar a producir algún tipo de daño en las bases de datos críticas.

El cifrado de los datos no se está realizando en todas las bases de datos, no se está tomando acciones para prevenir los ataques de inyección SQL, no se realiza la

²⁸ Blanco, Ana Lu, Ventajas y Desventajas de una Base de Datos.
<https://esbasededatos.wikispaces.com/Ventajas%20y%20Desventajas%20de%20una%20Base%20de%20Datos/> En Línea

instalación de los parches de seguridad que publican las compañías de los motores de bases de datos, no se lleva a cabo las auditorías de la seguridad de los datos.

Los principales problemas que se tiene con las bases de datos de los clientes:

- No se conocen las amenazas en las bases de datos.
- No se evidencia seguridad sobre la privacidad de los datos de los clientes y cumplimiento de la legislación de la privacidad.
- Envío de publicidad engañosa para mis clientes
- No tengo seguridad de mis bases de datos, ya que las actualizan diferentes personas y por diferentes medios sin restricción alguna.
- No se encuentran la información en las bases de datos.
- Control sobre el ingreso de datos actuales.
- La información relevante está dispersa en diferentes sistemas sin seguridad alguna.

Los SGBD reconoce derechos de acceso a nivel de: entidad, atributo y global, para los usuarios se solicita códigos con contraseñas, también se utilizan tarjetas magnéticas por reconocimiento de voz, la encriptación que se utiliza es para las contraseñas.

En el mercado se puede encontrar herramientas para la seguridad como la administración y vigilancia y otros objetivos.

A medida que los SGBD evolucionan, se va creando la necesidad de más seguridad como lo es el desarrollo orientado a objetos, tiempo de un elemento de caracterización en la información, sea más eficiente para la Data Warehouse y el mundo de Internet.

Seguridad actual en las bases de datos relacionales

- El administrador de las bases de datos es quien tiene el total de privilegios, se realiza mantenimiento de los usuarios en las bases de datos relacionales.
- Se dan privilegios a los usuarios dependiendo el tipo de rol que se maneja.
- Se diseñan políticas para las claves que se manejan.

Seguridad actual en las bases de datos NoSQL

- La autenticación es débil, las bases de datos NoSQL incorporan credenciales por defecto.
- Utiliza mecanismos complementarios ajenos a la base de datos para que la información es íntegra.
- No tiene mecanismos de cifrado ya que se maneja la información en texto plano.
- Carecen de auditoría de datos propios y robustos.
- La petición de llamado se realiza ejecutando API, habitualmente JSON o XML.

En las empresas la infraestructura de las bases de datos está sujeta a los ataques que se presentan contra la inseguridad en las bases de datos.

Vulnerabilidades en las bases de datos.

- Privilegios excesivos: Cuando se asignan muchos privilegios a un usuario y exceda a estos privilegios, crea un riesgo el cual puede ser innecesario.
- Abuso de Privilegios: Usuarios que exceden los privilegios para fines no autorizados, como información confidencial de la empresa.
- Elevación de privilegios no autorizados: Se aprovechan de las vulnerabilidades para dar privilegios altos a uno que tenía bajos privilegios.
- Vulnerabilidad de la plataforma: Las vulnerabilidades de los sistemas llevan a dar autorización a los datos y corrupción.
- Inyección de SQL: Las aplicaciones web brindan paginas dinámicas para almacenar la información, de los usuarios y la información en las bases de datos, lo cual ha creado vulnerabilidades lo cual se puede realizar un ataque de inyección ya que la información se puede enviar a bases de datos no autorizadas.
- Auditoria Débil: Las políticas débiles de las bases de datos muestran un riesgo de detección, disuasión, cumplimiento, recuperación y análisis forense. Los desarrolladores o administradores (DBA) pueden desactivar la auditoria que trae nativamente la gestión de la base de datos (DBMS), audita las capacidades que dan lugar a una adulación del rendimiento y las vulnerabilidades de los ataques que se tienen relacionados.
- Denegación del servicio: El ataque de la negación del servicio más comunes de DOS son desbordamiento de búfer, inundación en la red, corrupción en los datos, el consumo de los recursos.
- Autenticación Débil: Desde las primeras versiones hasta ahora no ha evolucionado mucho a los sistemas a usuarios múltiples, con esquemas de seguridad débil, clave débil, suplantación, ataques de fuerza bruta, ingeniería social.
- Vulnerabilidades en los protocolos: Algunas se ven afectadas por la falta de configuración en los protocolos y procesos de conexión. Ejemplo: SQL Slammer worm aprovecho la vulnerabilidad del protocolo de Microsoft SQL server para ejecutar el ataque a las bases de datos de los servidores.
- Exposición de los datos de backup: El robo de las cintas de backup de las bases de datos y cintas por falta de la seguridad propia para correos guardar la información.²⁹

29

Systems, Vulnerabilidades importantes que afectan la seguridad de bases de datos en las empresas. <http://www.onasystems.net/vulnerabilidades-importantes-afectan-la-seguridad-bases-datos-las-empresas/> En línea

Figura 10. Vulnerabilidades que afectan las bases de datos en las empresas.



Fuente: Vulnerabilidades que afectan las bases de datos en las empresas. Disponible en: <http://www.onasystems.net/vulnerabilidades-importantes-afectan-la-seguridad-bases-datos-las-empresas/>

Seguridad de las bases de datos NoSQL

Estas bases de datos NoSQL tienen debilidades genéricas, para cada implementación se debe realizar las medidas necesarias para la seguridad.

Autenticación: Es una de las debilidades de que tienen las bases de datos NoSQL, incorporar credenciales por defecto o sin que se realice autenticación.

Integridad de los datos: Lo importante es la disponibilidad y el rendimiento de los datos.

Confidencialidad y cifrado en el almacenamiento: se almacena en texto plano, la mayoría es necesario confiar el cifrado en capa de aplicación.

Auditoria de datos: No tienen auditoria de datos.

Seguridad en las comunicaciones: No tiene cifrado ni protocolo SSL.

Cuando se realiza las peticiones y llamadas se hace invocando la API corresponde a formateada según una convención común, normalmente JSON o XML, la posibilidad de inyección y riesgos son mayores que las bases de datos relacionales.

Las bases de datos Nosql no tiene seguridad ya que fueron diseñada por lo rápidas y ágiles que resultado a estas son inseguras posee riesgos y falencias.

7.2. DETERMINAR LAS BASES DE DATOS SQL Y NOSQL

Por ello, se debe evaluar una serie de parámetros, de la que se puede deducir cuál de estos almacenes es el mejor para nuestro caso

Las bases que se escoge para el desarrollo del estudio son:

Bases de datos relacional SQL

- **Oracle**

Es un sistema de bases de datos relacional, diseñado por Oracle Corporación, completo y robusto, tiene soporte de transacciones, estabilidad, estabilidad, multiplataforma y la desventaja es su valor.

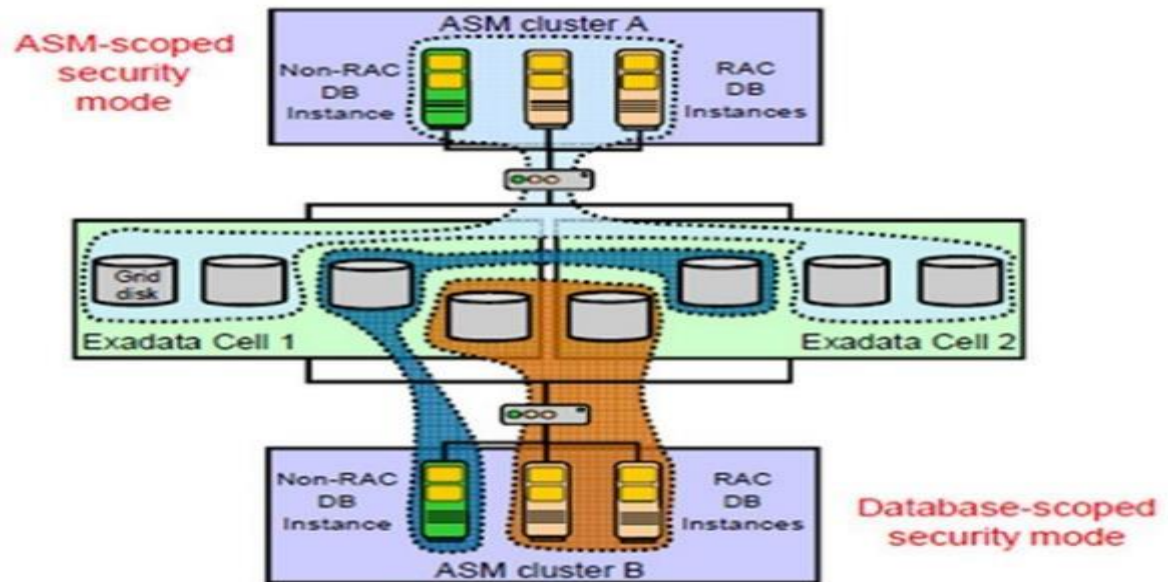
Seguridad de base de datos: Las bases de datos tienen accesos limitados "Grid Disk", se tiene que usar un archivo "cellkey.ora" por cada base de datos. En Oracle el clúster de ASM y las bases de datos pueden ingresar "Grid Disk", es una seguridad abierta.

¿Cuándo se debe implementar la seguridad en un "Oracle Exadata Database Machine"?

- Un Cluster ASM puede compartir un "Grid Disk" en una "Exadata Cell" para que se almacene dos bases de datos una sencilla y otra en Cluster.
- Denegar que los ambientes de pruebas ingresen a los ambientes de producción.
- Cuando el ciclo de vida perturba "Exadata Cell", porque se tienen varios ambientes de Ti en un mismo "Oracle Exadata Database Machine".
- Evitar la corrupción en las bases de datos.
- Las bases de datos que manejan el clúster no pueden acceder a los "Grid Disk", que también utilicen clúster.³⁰

³⁰ Gomez, Deiby. Oracle Exadata Database Machine: Seguridad a Nivel de ASM y de Base de Datos. <http://www.oracle.com/technetwork/es/articles/database-performance/seguridad-asm-base-de-datos-parte1-2166616-esa.html>/En línea

Figura 11. Configuración de Seguridad a nivel de ASM



Fuente: Configuración de Seguridad a nivel de ASM Disponible en:

<http://www.oracle.com/technetwork/es/articles/database-performance/seguridad-asm-base-de-datos-parte1-2166616-esa.html>

Uno de los mecanismos de las bases de datos Oracle es realizado en forma discrecional es la asignación de permisos para acceder a los objetos.

Cada usuario debe tener un dominio para el ingreso a las bases de datos, un rol, un password para identificar la persona que tiene permisos para empezar conexión con la base de datos, debe tener asignado un espacio y recursos a en la base de datos para utilizar.

Los privilegios tienen que ser a las bases de datos de los sistemas, a los objetos y las sentencias en SQL. Estos privilegios se deben asignar a un rol no a un usuario, con los permisos respectivos según se defina en cada rol. De esta forma se tiene un control de manejo sobre la base de datos según el rol, este permite fácilmente la asignación de permisos sobre la base de datos según el rol que se tenga.

Los usuarios pueden utilizar el default tablespace según el permiso que tenga el rol para crear los objetos según la asociación que tenga el rol.

Se debe asignar recursos a cada usuario, como son las secciones concurrentes que puede utilizar, se debe tener el limitante, como lo es el password, el número de intentos fallidos para la utilización de la base de datos.

- **Cassandra**

Es una base de datos de código abierto. Lo inicio Facebook para resolver problemas con el rendimiento del motor de búsqueda, la comunicación entre usuarios, con un gran volumen de datos y con una calidad excelente. Configuración de explotación escalable, horizontal y económica.

La seguridad en esta base de datos es muy primitiva.

La base de datos Cassandra suministra copias de seguridad y da instantaneidad en los datos, copia de seguridad en línea.

Crea un enlace hard con una nueva SSTable en línea.

Tiene una arquitectura Peer-to-Peer: Tiene un patrón y un esclavo si uno de los nodos falla la otra toma el rol de coordinador en un query ya que la información almacenada está en los dos. Los datos están distribuidos en el clúster por un token único por fila con la función hash, los datos se replican en los nodos con políticas que se definan.

La confidencialidad y cifrado de almacenamiento la tecnología Transparent data encryption esta no cuenta con un cifrado integrado.

La seguridad de las comunicaciones se opcional en el uso de SSL y el cifrado.³¹

7.3. DESARROLLO DEL LABORATORIO CON KALI LINUX

A continuación, los pasos para el desarrollo del laboratorio.

7.3.1 Base de Datos Relacional

1. Instalar una máquina virtual con Ubuntu lo cual se descarga del siguiente link:

<https://www.virtualbox.org/wiki/Downloads>

2. Instalar el gestor de bases de datos y realizar lo siguiente:

Descargar el archivo. rpm de la página oficial de ORACLE, (requiere tener o crear usuario), en siguiente link:

<http://www.oracle.com/technetwork/database/database-technologies/express-edition/downloads/index.html>

Figura 12. Descarga Oracle Express Edition 11g

Oracle Database Express Edition 11g Release 2

Thank you for accepting the License Agreement; you may now download this software.

- 📄 Oracle Database Express Edition 11g Release 2 for Windows x64
- Unzip the download and run the DISK1/setup.exe
- 📄 Oracle Database Express Edition 11g Release 2 for Windows x32
- Unzip the download and run the DISK1/setup.exe
- 📄 Oracle Database Express Edition 11g Release 2 for Linux x64
-Unzip the download and the RPM file can be installed as normal

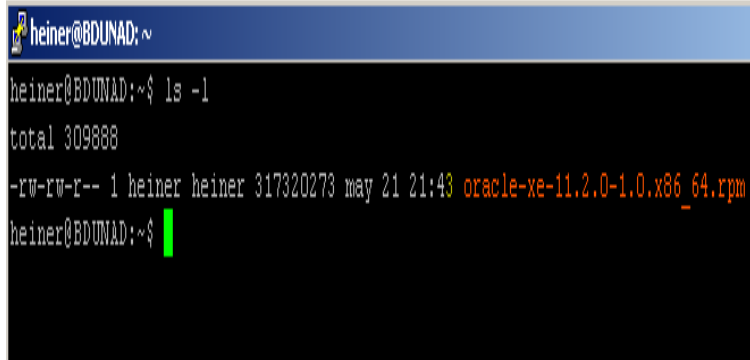
Fuente: El Autor

³¹ Hewitt, Eben. Apache Cassandra. https://es.wikipedia.org/wiki/Apache_Cassandra/En_Línea

Instalacion en Linux

Copiar en el servidor Linux Ubuntu que utilizara para la instalación.

Figura 13. Copiar el Oracle 11



```
heiner@BDUNAD:~  
heiner@BDUNAD:~$ ls -l  
total 309888  
-rw-rw-r-- 1 heiner heiner 317320273 may 21 21:43 oracle-xe-11.2.0-1.0.x86_64.rpm  
heiner@BDUNAD:~$
```

Fuente: El Autor

Instalar los paquetes lien libaio1 unixodbc con el siguiente comando:

apt-get install alien libaio1 unixodbc

Figura 14. Instalar alien libaio1



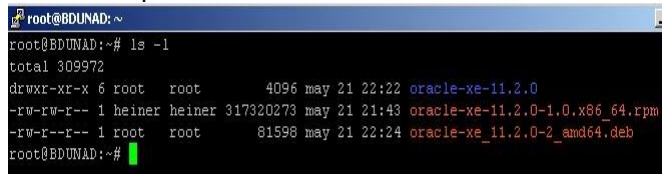
```
root@BDUNAD:~  
root@BDUNAD:~# apt-get install alien libaio1 unixodbc  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
Se instalarán los siguientes paquetes extras:  
binutils build-essential cpp cpp-4.8 debhelper debugedit dh-apparmor  
dpkg-dev fakeroot g++ g++-4.8 gcc gcc-4.8 gcc-4.8-base gettext  
intltool-debian libalgorithm-diff-perl libalgorithm-diff-xs-perl  
libalgorithm-merge-perl libasan0 libasprintf-dev libatomic1 libc-dev-bin  
libc6-dev libclocale-is14 libcroc3 libdpkg-perl libfakeroot
```

Fuente: El Autor

Convertir el archivo .rpm a .deb (utilizado por Ubuntu), con el siguiente comando:

alien --scripts -d oracle-xe-11.2.0-1.0.x86_64.rpm

Figura 15. Convertir el archivo .rpm a .deb



```
root@BDUNAD:~  
root@BDUNAD:~# ls -l  
total 309972  
drwxr-xr-x 6 root root 4096 may 21 22:22 oracle-xe-11.2.0  
-rw-rw-r-- 1 heiner heiner 317320273 may 21 21:43 oracle-xe-11.2.0-1.0.x86_64.rpm  
-rw-r--r-- 1 root root 81598 may 21 22:24 oracle-xe_11.2.0-2_amd64.deb  
root@BDUNAD:~#
```

Fuente: El Autor

Crear el archivo chkconfig y agregar las siguientes líneas:


```
#!/bin/bash
# Oracle 11gR2 XE installer chkconfig hack for Ubuntu
file=/etc/init.d/oracle-xe
if [[ ! `tail -n1 $file | grep INIT` ]]; then
echo >> $file
echo '### BEGIN INIT INFO' >> $file
echo '# Provides: OracleXE' >> $file
echo '# Required-Start: $remote_fs $syslog' >> $file
echo '# Required-Stop: $remote_fs $syslog' >> $file
echo '# Default-Start: 2 3 4 5' >> $file
echo '# Default-Stop: 0 1 6' >> $file
echo '# Short-Description: Oracle 11g Express Edition' >> $file
echo '### END INIT INFO' >> $file
fi
update-rc.d oracle-xe defaults 80 01
Cambiar los permisos al archive creado.
```

Se estable los siguientes parámetros al Kernel para que pueda ser usada la BD ORACLE, en el archivo /etc/sysctl.d/60-oracle.conf

```
# Oracle 11g XE kernel parameters
fs.file-max=6815744
net.ipv4.ip_local_port_range=9000 65000
kernel.sem=250 32000 100 128
kernel.shmmax=536870912
```

Enseguida cargar los datos de los parámetros del kernel.

Figura 16. Cargar datos

```
root@BDUNAD:/etc/sysctl.d#
root@BDUNAD:/etc/sysctl.d# service procps start
procps stop/waiting
root@BDUNAD:/etc/sysctl.d# █
```

Fuente: El Autor

Verificar los nuevos parametros cargados de la siguiente forma:

Figura 17. Verificar los parámetros

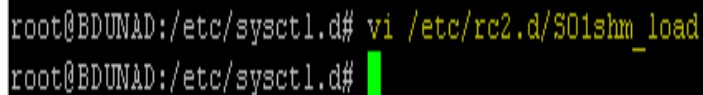
```
procps stop/waiting
root@BDUNAD:/etc/sysctl.d# sysctl -q fs.file-max
fs.file-max = 6815744
root@BDUNAD:/etc/sysctl.d# █
```

Fuente: El Autor

Crear el archivo S01shm_load que servirá como el punto de montaje para ORACLE. Enseguida agregar los siguientes datos:

```
#!/bin/sh
case "$1" in
start) mkdir /var/lock/subsys 2>/dev/null
      touch /var/lock/subsys/listener
      rm /dev/shm 2>/dev/null
      mkdir /dev/shm 2>/dev/null
      mount -t tmpfs shmfs -o size=2048m /dev/shm ;;
*) echo error
  exit 1 ;;
esac
```

Figura 18. Verificar archivo S01shm_load



```
root@BDUNAD:/etc/sysctl.d# vi /etc/rc2.d/S01shm_load
root@BDUNAD:/etc/sysctl.d#
```

Fuente: El Autor

Se cambia los permisos del archivo creado anteriormente

Figura 19. Permisos sobre el archivo S01shm_load



```
-rwxr-xr-x 1 root root 256 may 21 22:46 S01shm_load
```

Fuente: El Autor

Ejecutar los siguientes comandos para asegurar la correcta instalación de ORACLE sobre Ubuntu Server.

```
ln -s /usr/bin/awk /bin/awk
mkdir /var/lock/subsys
touch /var/lock/subsys/listener
```

Figura 20. Ejecución de comandos



```
root@BDUNAD:/etc/rc2.d# ln -s /usr/bin/awk /bin/awk
root@BDUNAD:/etc/rc2.d# mkdir /var/lock/subsys
root@BDUNAD:/etc/rc2.d# touch /var/lock/subsys/listener
root@BDUNAD:/etc/rc2.d#
```

Fuente: El Autor

Proceder con la instalación del archivo .deb que contiene el motor ORACLE.

Figura 21. Instalación el archivo .deb

```
root@BDUNAD:/home/heiner/Disk1# dpkg --install oracle-xe_11.2.0-2_amd64.deb
(Leyendo la base de datos ... 63727 ficheros o directorios instalados actualmente.)
Preparing to unpack oracle-xe_11.2.0-2_amd64.deb ...
Unpacking oracle-xe (11.2.0-2) ...
Configurando oracle-xe (11.2.0-2) ...
Executing post-install steps...
Adding system startup for /etc/init.d/oracle-xe ...
/etc/rc0.d/K01oracle-xe -> ../init.d/oracle-xe
/etc/rc1.d/K01oracle-xe -> ../init.d/oracle-xe
/etc/rc6.d/K01oracle-xe -> ../init.d/oracle-xe
/etc/rc2.d/S80oracle-xe -> ../init.d/oracle-xe
/etc/rc3.d/S80oracle-xe -> ../init.d/oracle-xe
/etc/rc4.d/S80oracle-xe -> ../init.d/oracle-xe
/etc/rc5.d/S80oracle-xe -> ../init.d/oracle-xe
```

Fuente: El Autor

Después configurar los puertos de escucha de ORACLE al igual que la contraseña de los usuarios SYS y SYSTEM.

Figura 22. Configurar puertos

```
Specify a port that will be used for the database listener [1521]:1521
Specify a password to be used for database accounts. Note that the same
password will be used for SYS and SYSTEM. Oracle recommends the use of
different passwords for each database account. This can be done after
```

Fuente: El Autor

Ingresar las siguientes variables de entorno al archivo. bashrc.

```
export ORACLE_HOME=/u01/app/oracle/product/11.2.0/xe
export ORACLE_SID=XE
export NLS_LANG=`$ORACLE_HOME/bin/nls_lang.sh`
export ORACLE_BASE=/u01/app/oracle
export LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH
export PATH=$ORACLE_HOME/bin:$PATH
```

Figura 23. Verificar el archivo.bashrc

```
root@BDUNAD:/home/heiner/Disk1# vi ~/.bashrc
root@BDUNAD:/home/heiner/Disk1#
```

Fuente: El Autor

Iniciar ORACLE 11gR2

Figura 24. Iniciar Oracle 11g

```
root@BDUNAD:/home/heiner/Disk1# service oracle-xe start
Oracle Database 11g Express Edition instance is already started
```

Fuente: El Autor

Ahora agregar un usuario dba a la base de datos

Figura 25. Agregar usuario DBA

```
root@BDUNAD:/home/heiner/Disk1# usermod -a -G dba heiner
root@BDUNAD:/home/heiner/Disk1#
```

Fuente: El Autor

Ingresa por consola con el usuario sysdba

Figura 26. Iniciar consola con el usuario sysdba

```
root@BDUNAD:/home/heiner/Disk1# sqlplus sys as sysdba

SQL*Plus: Release 11.2.0.2.0 Production on Dom May 22 00:05:49 2016

Copyright (c) 1982, 2011, Oracle. All rights reserved.

Enter password:

Connected to:
Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production

SQL>
```

Fuente: El Autor

Ya se tiene el motor instalado en Ubuntu Server de forma correcta, ahora realizar los siguientes pasos:

a) Listar las bases de datos que se crea por defecto.

Figura 27. Listar base de datos

```
SQL> SELECT NAME FROM v$databases;

NAME
-----
XE

SQL>
```

Fuente: El Autor

Por defecto ORACLE instalada la base de datos **XE**

b) Ubicar los metadatos del sistema de base de datos

Figura 28. Ubicar Metadatos

```
root@BDUNAD:/u01/app/oracle/oradata# pwd
/u01/app/oracle/oradata
root@BDUNAD:/u01/app/oracle/oradata# ls -l
total 4
drwxr-xr-x 2 oracle dba 4096 may 21 23:46 XE
root@BDUNAD:/u01/app/oracle/oradata#
```

Fuente: El Autor

Los metadatos son almacenados en la ruta **/u01/app/oracle/oradata**

c) Usuarios que se crean por defecto en la instalación.

Figura 29. Usuarios por defecto

```
SQL> SELECT USERNAME FROM DBA_USERS;

USERNAME
-----
SYS
SYSTEM
ANONYMOUS
APEX_PUBLIC_USER
APEX_040000
XS$NULL
OUTLN
FLOWS_FILES
MDSYS
CTXSYS
XDB

USERNAME
-----
HR
```

Fuente: El Autor

Por defecto crea 12 cuentas de usuario como se puede observar en la imagen anterior.

Figura 30. Verificar usuarios

```
USERNAME          USER_ID PASSWORD
-----
ACCOUNT_STATUS    LOCK_DAT EXPIRY_D
-----
DEFAULT_TABLESPACE  TEMPORARY_TABLESPACE  CREATED
-----
PROFILE            INITIAL_RSRC_CONSUMER_GROUP
-----
EXTERNAL_NAME
-----
PASSWORD E AUTHENTI
-----
```

Fuente: El Autor

- a) Listar puertos y servicios de Oracle, para la revisión se puede usar la aplicación nmap

Figura 31. Listar puertos

```
Starting Nmap 6.40 ( http://nmap.org ) at 2016-05-22 01:30 COT
Nmap scan report for 192.168.182.134
Host is up (0.0000050s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
1521/tcp   open  oracle

Nmap done: 1 IP address (1 host up) scanned in 2.68 seconds
root@BDUNAD:/u01/app/oracle/oradata#
```

Fuente: El Autor

ORACLE tiene a la escucha el puerto 1521, el cual fue configurado en el proceso de instalación.

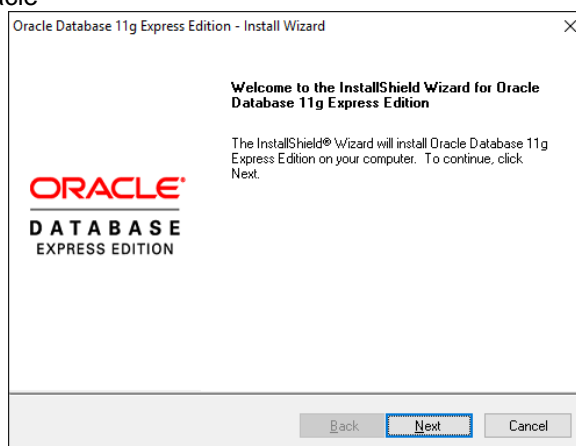
- b) Opciones de seguridad durante la instalación.

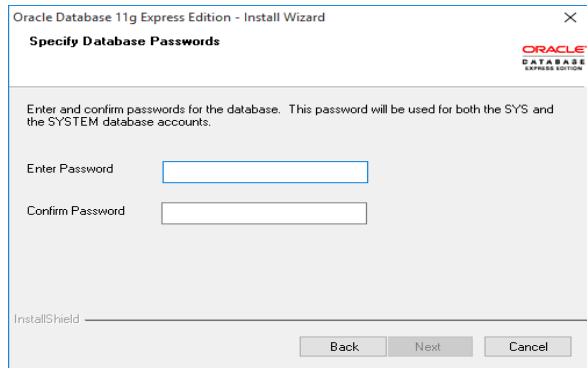
En el proceso de instalación ORACLE solicita proporcionar una contraseña para los usuarios SYS y SYSTEM, la cual deberá ser lo suficientemente segura y compleja, de tal forma que no pueda ser detectada por algún programa de explotación.

Instalacion en Windows

Instalar la versión express 11g, en una maquina Windows.

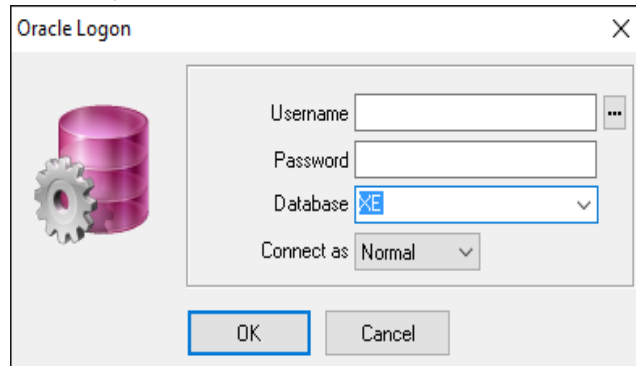
Figura 32. Instalación Oracle





Fuente: El Autor

Figura 33. Pantalla inicio PLSQL



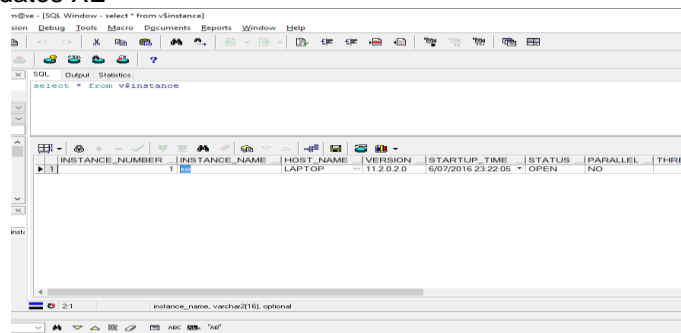
Fuente: El Autor

Instalar el PLSQL, para ver de forma gráfica la base de datos.

a. Bases de datos creadas por defecto

Por defecto se crea una base de datos llamada XE, como se muestra en la siguiente captura.

Figura 34. Base de datos XE



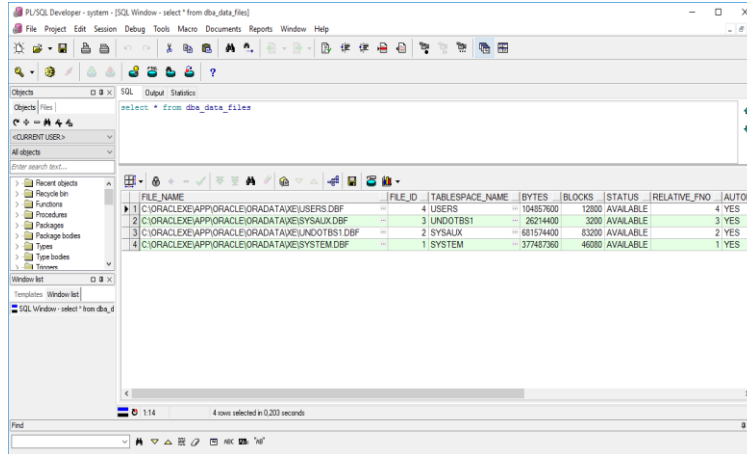
Fuente: El Autor

b. Ruta metadatos del sistema de base de datos

La ruta en la que se almacena los datos está dentro de la instalación de Oracle.

La ruta es: C:\ORACLEXE\APP\ORACLE\ORADATE\XE\

Figura 35. Ruta de los metadatos



The screenshot shows the PL/SQL Developer interface with a query window displaying the following data:

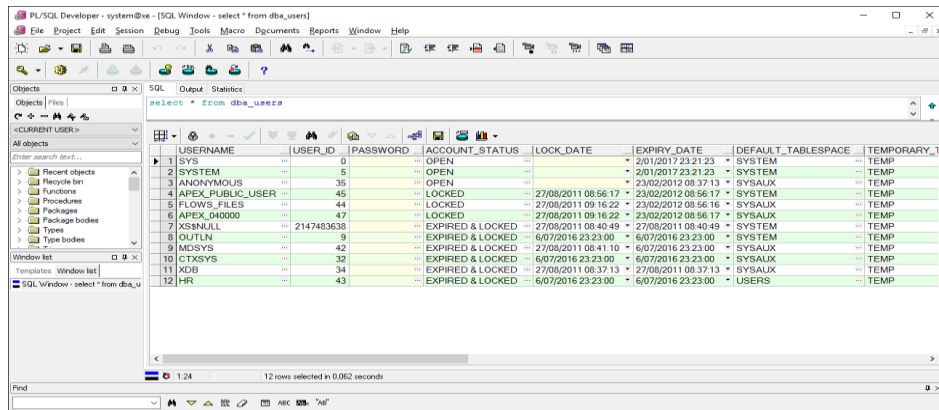
FILE_NAME	FILE_ID	TABLESPACE_NAME	BYTES	BLOCKS	STATUS	RELATIVE_FNO	AUTOEXT
C:\ORACLEXE\APP\ORACLE\ORADATE\XE\USERS.DBF	4	USERS	104857600	12800	AVAILABLE	4	YES
C:\ORACLEXE\APP\ORACLE\ORADATE\XE\SYSTEM.DBF	3	UNDO_TBS1	26214400	3200	AVAILABLE	3	YES
C:\ORACLEXE\APP\ORACLE\ORADATE\XE\UNDOTBS1.DBF	2	SYSAUX	681574400	8320	AVAILABLE	2	YES
C:\ORACLEXE\APP\ORACLE\ORADATE\XE\SYSTEM.DBF	1	SYSTEM	377487360	46080	AVAILABLE	1	YES

Fuente: El Autor

c. Usuarios creados por defecto.

Por defecto se crea 12 usuarios, dentro de los cuales se encuentra SYSTEM, el cual es superusuario. También se encuentra sys, HR, estos son lo que cuentan con más privilegios.

Figura 36. Usuarios y roles



The screenshot shows the PL/SQL Developer interface with a query window displaying the following data:

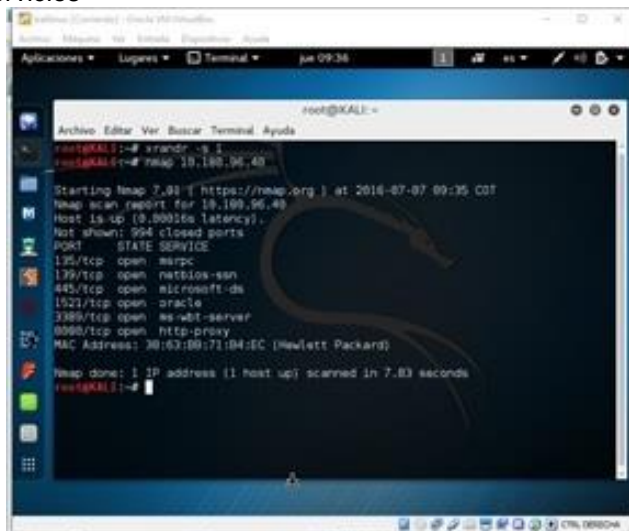
USERNAME	USER_ID	PASSWORD	ACCOUNT_STATUS	LOCK_DATE	EXPIRY_DATE	DEFAULT_TABLESPACE	TEMPORARY
1 SYS	0		OPEN		2/01/2017 23:21:23	SYSTEM	TEMP
2 SYSTEM	5		OPEN		2/01/2017 23:21:23	SYSTEM	TEMP
3 ANONYMOUS	35		OPEN		23/02/2012 08:37:13	SYSAUX	TEMP
4 APEX_PUBLIC_USER	45		LOCKED	27/08/2011 08:56:17	23/02/2012 08:56:17	SYSAUX	TEMP
5 FLOWS_FILES	44		LOCKED	27/08/2011 09:16:22	23/02/2012 08:56:16	SYSAUX	TEMP
6 APEX_040000	47		LOCKED	27/08/2011 09:16:22	23/02/2012 08:56:17	SYSAUX	TEMP
7 XSNNULL	2147483638		EXPIRED & LOCKED	27/08/2011 08:40:49	27/08/2011 08:40:49	SYSTEM	TEMP
8 OUTLN	9		EXPIRED & LOCKED	6/07/2016 23:23:00	6/07/2016 23:23:00	SYSTEM	TEMP
9 MDSYS	42		EXPIRED & LOCKED	27/08/2011 08:41:10	6/07/2016 23:23:00	SYSAUX	TEMP
10 CTXSYS	32		EXPIRED & LOCKED	6/07/2016 23:23:00	6/07/2016 23:23:00	SYSAUX	TEMP
11 MDSYS	34		EXPIRED & LOCKED	27/08/2011 08:37:13	27/08/2011 08:37:13	SYSAUX	TEMP
12 HR	43		EXPIRED & LOCKED	6/07/2016 23:23:00	6/07/2016 23:23:00	USERS	TEMP

GRANTEE	GRANTED_ROLE	ADMIN_OPTION	DEFAULT_ROLE
1 SYS	ROLE SET PASSWORD	YES	YES
2 SYS	ROLE ADMIN	YES	YES
3 SYS	IMP_FULL_DATABASE	YES	YES
4 DBA	SCHEDULER_ADMIN	YES	YES
5 DBA	DATAUMP_IMP_FULL_DATABASE	NO	YES
6 SYSTEM	AG_ADMINISTRATOR_ROLE	YES	YES
7 EXECUTE_CATALOG_ROLE	HR_ADMIN_EXECUTE_ROLE	NO	YES
8 HR_ADMIN_ROLE	HR_ADMIN_EXECUTE_ROLE	NO	YES
9 DBA_CATALOG_ROLE	SELECT_CATALOG_ROLE	YES	YES
10 APPL_MONITOR	RESOURCE	YES	YES
11 SYS	APPL_ADMINISTRATOR_ROLE	YES	YES
12 SYS	APPL_ADMINISTRATOR_ROLE	YES	YES
13 SYS	DELETE_CATALOG_ROLE	YES	YES
14 DBA	DELETE_CATALOG_ROLE	YES	YES
15 DBA	EXECUTE_CATALOG_ROLE	YES	YES
16 HR	RESOURCE	NO	YES
17 SYS	DBA	YES	YES

Fuente: El Autor

d. puertos y servicios de Oracle.

Figura 37. Puerto y servicios



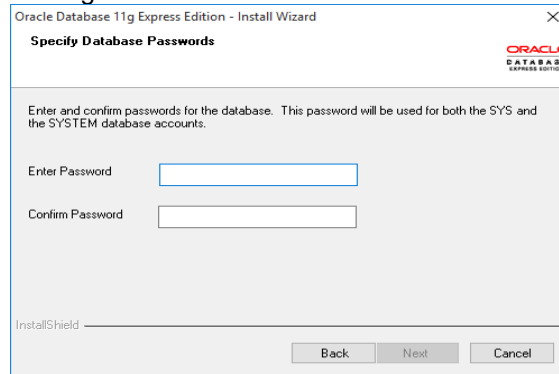
Fuente: El Autor

Los puertos que utilizar Oracle en la instalación por defecto son 1521 correspondiente al listener y el 8080 que corresponde al servicio http.

e. Configuración de seguridad

Durante la instalación de la versión express edition, el único parámetro de seguridad que se configura y es obligatorio es el password del usuario system.

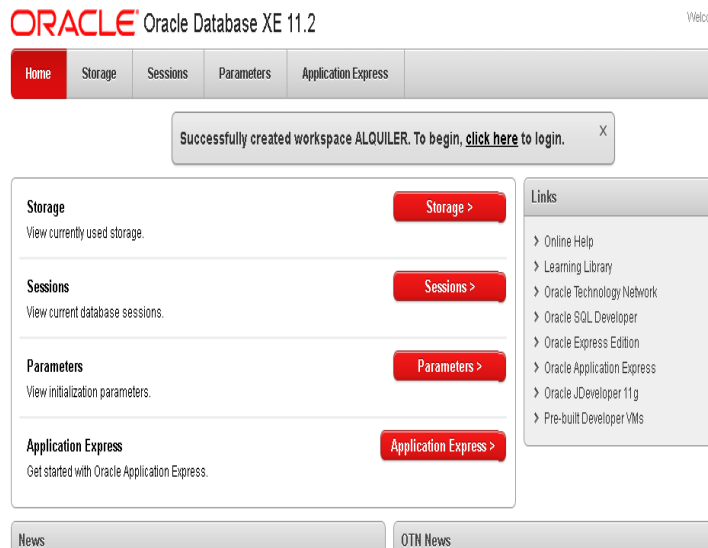
Figura 38. Configuración de seguridad



Fuente: El Autor

1. Diseñar y crear una base de datos relacional que sirva para la gestión y procesos un negocio de Alquiler de vehículos a extranjeros.

Figura 39. Creando la base de datos ALQUILER



Fuente: El Autor

Figura 40. Crear las tablas Vehículos, Clientes, Alquiler

VEHICULOS										
Table	Data	Indexes	Model	Constraints	Grants	Statistics	UI Defaults	Triggers	Dependencies	SQL
Add Column	Modify Column	Rename Column	Drop Column	Rename	Copy	Drop	Truncate	Create Lookup Table		
Column Name	Data Type	Nullable	Default	Primary Key						
PLACA	VARCHAR2(10)	No	-	1						
MARCA	VARCHAR2(20)	Yes	-	-						
REFERENCIA	VARCHAR2(20)	Yes	-	-						
MODELO	NUMBER(5,0)	Yes	-	-						
SOAT	VARCHAR2(10)	Yes	-	-						
TECNICOMECANICA	VARCHAR2(10)	Yes	-	-						
ESTADO	VARCHAR2(10)	Yes	-	-						1 - 7

CLIENTES										
Table	Data	Indexes	Model	Constraints	Grants	Statistics	UI Defaults	Triggers	Dependencies	SQL
Add Column	Modify Column	Rename Column	Drop Column	Rename	Copy	Drop	Truncate	Create Lookup Table		
Column Name	Data Type	Nullable	Default	Primary Key						
PASAPORTE	VARCHAR2(30)	No	-	1						
NOMBRES	VARCHAR2(20)	Yes	-	-						
APELLIDOS	VARCHAR2(30)	Yes	-	-						
NACIONALIDAD	VARCHAR2(50)	Yes	-	-						
TELÉFONO_CELULAR	NUMBER(10,0)	Yes	-	-						
TARJETA_CRÉDITO	NUMBER(20,0)	Yes	-	-						1 - 6

[Download](#)

ALQUILER										
Table	Data	Indexes	Model	Constraints	Grants	Statistics	UI Defaults	Triggers	Dependencies	SQL
Add Column	Modify Column	Rename Column	Drop Column	Rename	Copy	Drop	Truncate	Create Lookup Table		
Column Name	Data Type	Nullable	Default	Primary Key						
NUMERO_ALQUILER	NUMBER(10,0)	No	-	1						
PASAPORTE	VARCHAR2(20)	Yes	-	-						
PLACA	VARCHAR2(10)	Yes	-	-						
HORAS	NUMBER(3,0)	Yes	-	-						
VALOR_HORA	NUMBER(10,0)	Yes	-	-						1 - 5

Fuente: El Autor

Figura 41. Poblar la base de datos

CLIENTES

Row updated. X

Table **Data** Indexes Model Constraints Grants Statistics UI Defaults Triggers Dependencies SQL

Query
Count Rows
Insert Row

EDIT	PASAPORTE	NOMBRES	APELLIDOS	NACIONALIDAD	TELÉFONO_CELULAR	TARJETA_CREDITO
	AS9885SA	ORLANDO	BOCHEMA	ARGENTINA	3145474586	874125
	AS97AS84	JAVIER	BENAVIDEZ	ESPAÑA	3205874198	888523
row(s) 1 - 2 of 2						

[Download](#)

VEHICULOS

Row created. X

Table **Data** Indexes Model Constraints Grants Statistics UI Defaults Triggers Dependencies SQL

Query
Count Rows
Insert Row

EDIT	PLACA	MARCA	REFERENCIA	MODELO	SOAT	TECHNOMECANICA	ESTADO
	BT487F	TOYOTA	COROLLA XEI	2006	VIGENTE	VIGENTE	ACTIVO
	NM1708	MAZDA	ALEGRO	2009	VIGENTE	VIGENTE	ACTIVO
row(s) 1 - 2 of 2							

ALQUILER

Row created. X

Table **Data** Indexes Model Constraints Grants Statistics UI Defaults Triggers Dependencies SQL

Query
Count Rows
Insert Row

EDIT	NUMERO_ALQUILER	PASAPORTE	PLACA	HORAS	VALOR_HORA
	1	AS97AS84	BT487F	5	10000
row(s) 1 - 1 of 1					

Fuente: El Autor

Figura 42. Probar la integridad referencial

The screenshot shows the Oracle database's 'Create Row' form for the 'ALQUILER' table. The form fields are filled with the following values: Numero Alquiler: 2, Pasaporte: SAS5544, Placa: BRA87G, Horas: 4, and Valor Hora: 9000. Below the form, a yellow error message is displayed: 'error ORA-02231: integrity constraint (ALQUILER.ALQUILER_FK) violated - parent key not found'. The interface includes 'Cancel', 'Create', and 'Creat' buttons.

Fuente: El Autor

Realiza un chequeo de vulnerabilidades al servidor de la base de datos, usar la aplicación de KALI Linux (máquina virtual usada en las prácticas) para análisis de vulnerabilidades.

Figura 43. Chequeo de Vulnerabilidades de Oracle

```
root@kali:~# sqlmap -u 192.168.1.5:8080/apex/f?p=4950:1012511876033985
{1.0-dev-nongit-201605080a89}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 15:21:51

[15:21:51] [INFO] testing connection to the target URL
[15:21:52] [INFO] checking if the target is protected by some kind of WAF/IPS/ID
S
[15:21:52] [INFO] heuristics detected web page charset 'ascii'
[15:21:52] [CRITICAL] heuristic detected that the target is protected by some k
ind of WAF/IPS/IDS
do you want sqlmap to try to detect backend WAF/IPS/IDS? [y/N] y
[15:21:54] [WARNING] dropping timeout to 10 seconds (i.e. '--timeout=10')
[15:21:54] [INFO] using WAF scripts to detect backend WAF/IPS/IDS protection
```

```
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
[15:21:54] [WARNING] dropping timeout to 10 seconds (i.e. '--timeout=10')
[15:21:54] [INFO] using WAF scripts to detect backend WAF/IPS/IDS protection
[15:21:54] [WARNING] no WAF/IDS/IPS product has been identified
[15:21:54] [INFO] testing if the target URL is stable
[15:21:55] [WARNING] target URL is not stable. sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison' and provide a string or regular expression to match on
[15:22:01] [INFO] testing if GET parameter 'p' is dynamic
[15:22:01] [CRITICAL] connection dropped or unknown HTTP status code received. Try to force the HTTP User-Agent header with option '--user-agent' or switch '--random-agent'. sqlmap is going to retry the request(s)
[15:22:02] [INFO] confirming that GET parameter 'p' is dynamic
[15:22:02] [INFO] GET parameter 'p' is dynamic
[15:22:02] [WARNING] heuristic (basic) test shows that GET parameter 'p' might not be injectable
[15:22:02] [INFO] testing for SQL injection on GET parameter 'p'
[15:22:02] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[15:22:02] [WARNING] reflective value(s) found and filtering out
[15:22:02] [INFO] testing 'MySQL >= 5.0 boolean-based blind - Parameter replace'
[15:22:02] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause'
```

```
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
[15:22:02] [INFO] testing for SQL injection on GET parameter 'p'
[15:22:02] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[15:22:02] [WARNING] reflective value(s) found and filtering out
[15:22:02] [INFO] testing 'MySQL >= 5.0 boolean-based blind - Parameter replace'
[15:22:02] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause'
[15:22:02] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[15:22:02] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause'
[15:22:03] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[15:22:03] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace'
[15:22:03] [INFO] testing 'MySQL inline queries'
[15:22:03] [INFO] testing 'PostgreSQL inline queries'
[15:22:03] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[15:22:03] [INFO] testing 'MySQL > 5.0.11 stacked queries (SELECT - comment)'
[15:22:03] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[15:22:03] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[15:22:03] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[15:22:03] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SELECT)'
[15:22:03] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[15:22:04] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind'
[15:22:04] [INFO] testing 'Oracle AND time-based blind'
[15:22:04] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[15:22:04] [WARNING] using unescaped version of the test because of zero knowledge of the back-end DBMS. You can try to explicitly set it using option '--dbms'
[15:22:05] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[15:22:06] [WARNING] GET parameter 'p' is not injectable
[15:22:06] [CRITICAL] all tested parameters appear to be not injectable. Try to increase '--level'/'--risk' values to perform more tests. Also, you can try to rerun by providing either a valid value for option '--string' (or '--regexp') If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could retry with an option '--tamper' (e.g. '--tamper=space2comment')
[15:22:06] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 1 times, 404 (Not Found) - 1 times
[*] shutting down at 15:22:06
root@kali:~#
```

```
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
[15:22:03] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[15:22:03] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[15:22:03] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SELECT)'
[15:22:03] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[15:22:04] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind'
[15:22:04] [INFO] testing 'Oracle AND time-based blind'
[15:22:04] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[15:22:04] [WARNING] using unescaped version of the test because of zero knowledge of the back-end DBMS. You can try to explicitly set it using option '--dbms'
[15:22:05] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[15:22:06] [WARNING] GET parameter 'p' is not injectable
[15:22:06] [CRITICAL] all tested parameters appear to be not injectable. Try to increase '--level'/'--risk' values to perform more tests. Also, you can try to rerun by providing either a valid value for option '--string' (or '--regexp') If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could retry with an option '--tamper' (e.g. '--tamper=space2comment')
[15:22:06] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 1 times, 404 (Not Found) - 1 times
[*] shutting down at 15:22:06
root@kali:~#
```

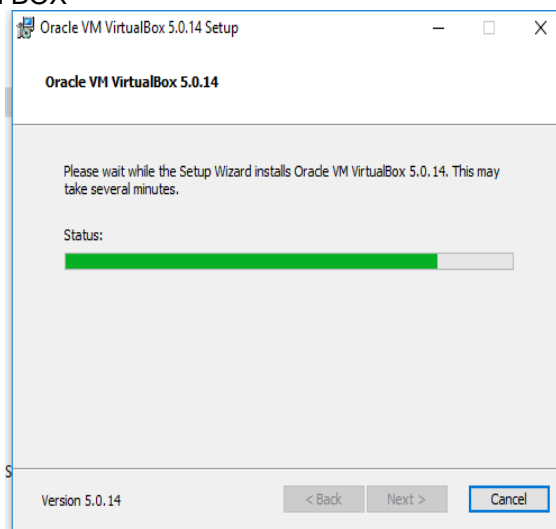
Fuente: El Autor

Realizar algún tipo de inyección o enumeración sobre la URL que administra el motor de ORACLE es casi imposible, ya que posee unas características de seguridad muy avanzadas.

7.3.2. Base de Datos No Relacional

Instalar una máquina virtual descargar del siguiente link:
<https://www.virtualbox.org/wiki/Downloads>

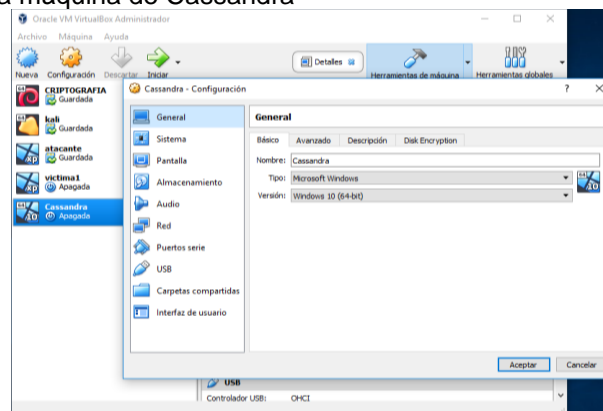
Figura 44. Instalar Virtual BOX



Fuente: El Autor

Configurar la máquina virtual con sistema operativo Windows 10

Figura 45. Configurar la máquina de Cassandra



Fuente: El Autor

Instalar Cassandra pero para instalar se debe colocar primero Java lo cual se descarga del siguiente link: <http://www.java.com/es/download/>

Figura 46. Descargar Java



Fuente: El Autor

Instalar la maquina Java

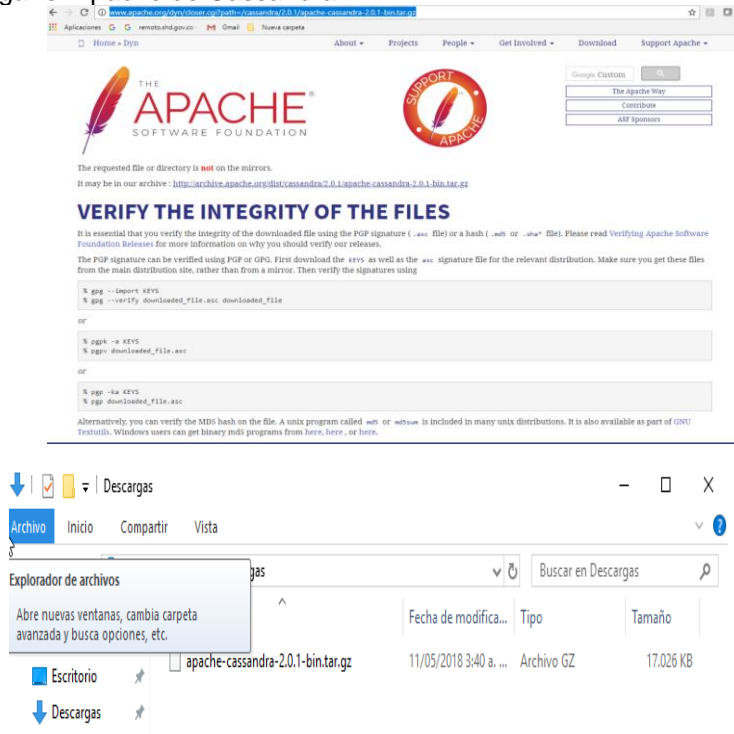
Figura 47. Instalar la maquina Java



Fuente: El Autor

Instalar el gestor de bases de datos Cassandra se puede descargar del siguiente link:
<http://www.apache.org/dyn/closer.cgi?path=/cassandra/2.0.1/apache-cassandra-2.0.1-bin.tar.gz>

Figura 48. Descargar el Apache de Cassandra

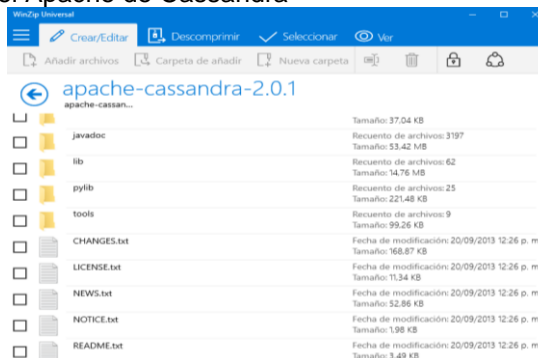


Fuente: El Autor

Descomprimir el archivo apache-cassandra-2.1.19-bin.tar.gz en una carpeta llamada cassandra.

C:\cassandra

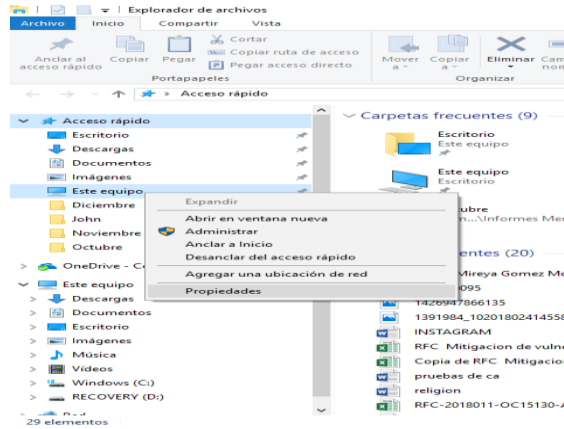
Figura 49. Descomprimir el Apache de Cassandra



Fuente: El Autor

Luego se crea una variable para java y otra para cassandra en el sistema se realiza dando clic derecho en Equipo y luego Propiedades

Figura 50. Crear variable en java y cassandra



Fuente: El Autor

Ir a la configuración avanzada del sistema dando clic

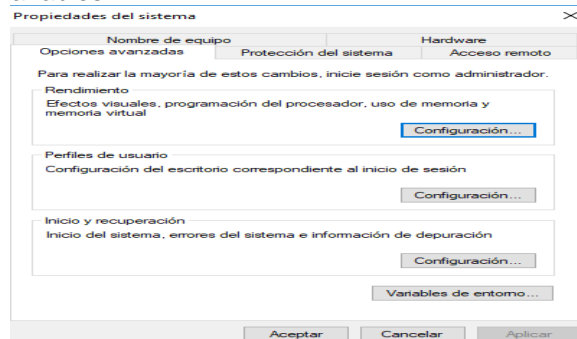
Figura 51. Configuración avanzada del sistema



Fuente: El Autor

La creación se realiza dando clic en variables de entorno

Figura 52. Creación de variables



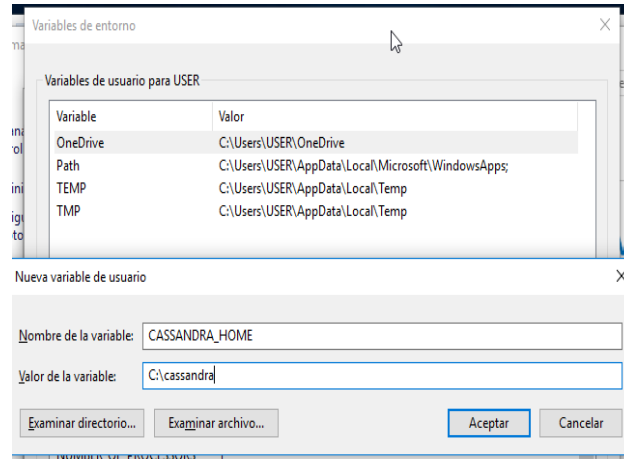
Fuente: El Autor

La primera que se crea es la de Cassandra

En el nombre de la variable: CASSANDRA_HOME

El Valor de la variable: C:\cassandra

Figura 53. Creación de la variable Cassandra



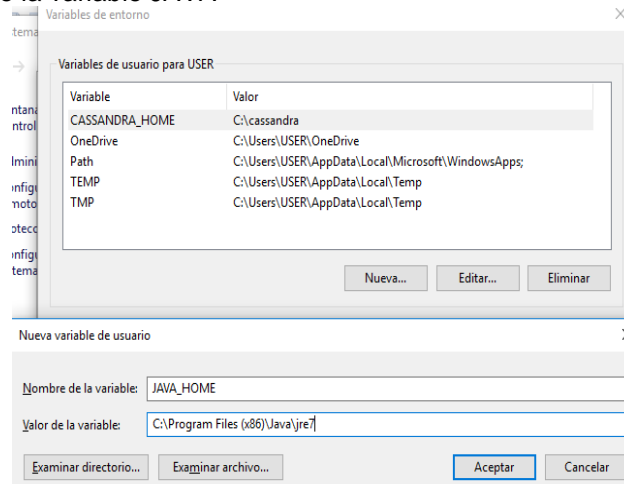
Fuente: El Autor

Luego crear la variable de Java:

En variable de entorno: Nombre de la variable: JAVA_HOME

El valor de la variable: C:\Program Files (x86)\Java\jre7

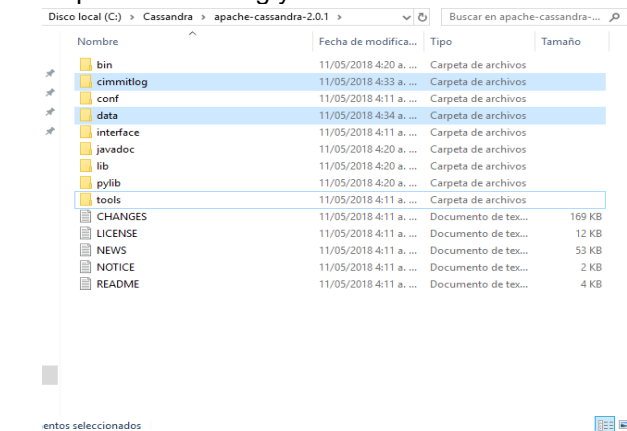
Figura 54. Creación de la variable JAVA



Fuente: El Autor

De donde se extraen los archivos de Cassandra crear dos carpetas, una carpeta se debe llamar commitlog y la otra carpeta data.

Figura 55. Creación de carpetas commitlog y data

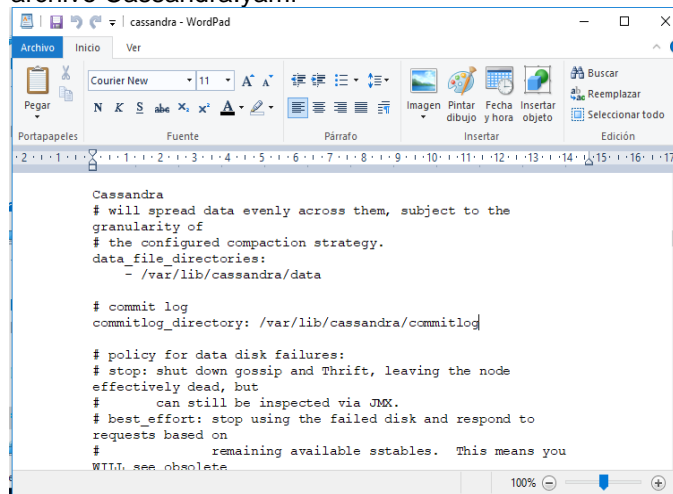


Fuente: El Autor

Modificar el archivo C:\cassandra\conf\cassandra.yaml

Ir a la línea # commit log commitlog_directory: /var/lib/cassandra/commitlog
Modificar por # commit log commitlog_directory: C:/cassandra/commitlog

Figura 56. Modificar archivo Cassandra.yaml



Fuente: El Autor

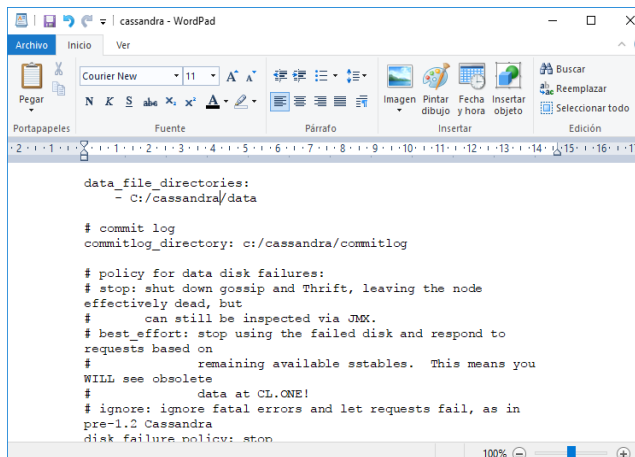
Y también en la línea data_file_directories: - /var/lib/cassandra/data
Modificar por data_file_directories: - C:/cassandra/data

Figura 57. Modificar línea data file directories

```
data_file_directories:
  - /var/lib/cassandra/data

# commit log
commitlog_directory: c:/cassandra/commitlog

# policy for data disk failures:
# stop: shut down gossip and Thrift, leaving the node
effectively dead, but
# can still be inspected via JMX.
# best_effort: stop using the failed disk and respond to
requests based on
# remaining available sstables. This means you
WILL see obsolete
# data at CL.ONE!
# ignore: ignore fatal errors and let requests fail, as in
pre-1.2 Cassandra
disk_failure_policy: stop
```

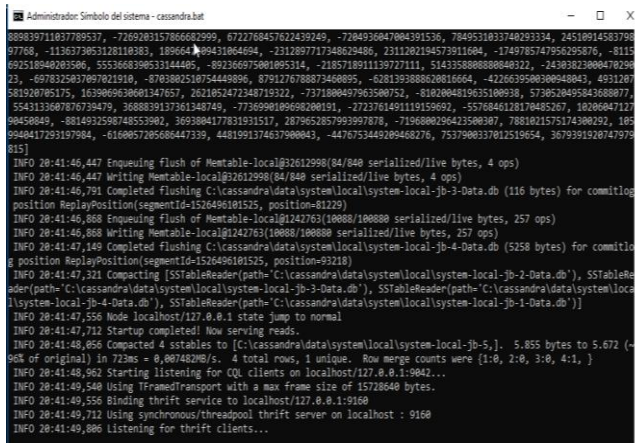


The screenshot shows a WordPad window titled 'cassandra - WordPad'. The text content is identical to the one in the previous block, but the path for 'data_file_directories' has been changed from '/var/lib/cassandra/data' to 'C:/cassandra/data'. The rest of the configuration, including the commit log directory and disk failure policy, remains the same.

Fuente: El Autor

Luego ejecutar el archivo cassandra.bat del directorio c:\cassandra.bat

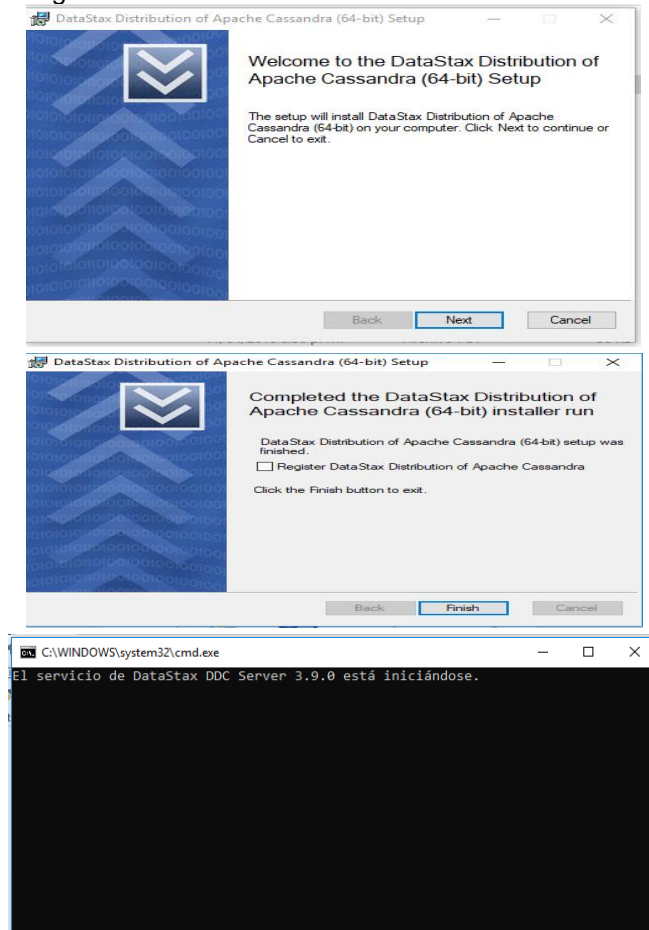
Figura 58. Ejecución cassandra.bat



The screenshot shows a command prompt window titled 'Administrador: Símbolo del sistema - cassandra.bat'. The output displays various system information, including IP addresses and MAC addresses, followed by Cassandra startup logs. Key log messages include: 'INFO 20:41:46,447 Enqueuing flush of Memtable-local[822612998]...', 'INFO 20:41:46,447 Writing Memtable-local[822612998]...', 'INFO 20:41:46,791 Completed flushing C:\cassandra\data\system\local\system-local-jb-3-Data.db...', 'INFO 20:41:47,311 Compacting [SSTableReader(path='C:\cassandra\data\system\local\system-local-jb-2-Data.db')...]', and 'INFO 20:41:47,712 Startup completed! Now serving reads.'

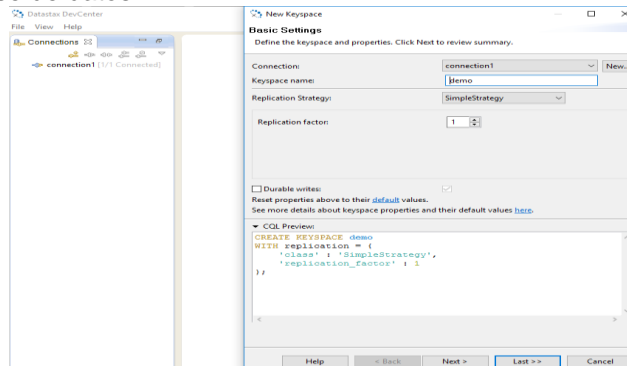
Fuente: El Autor

Figura 59. Instalar y configurar el cliente



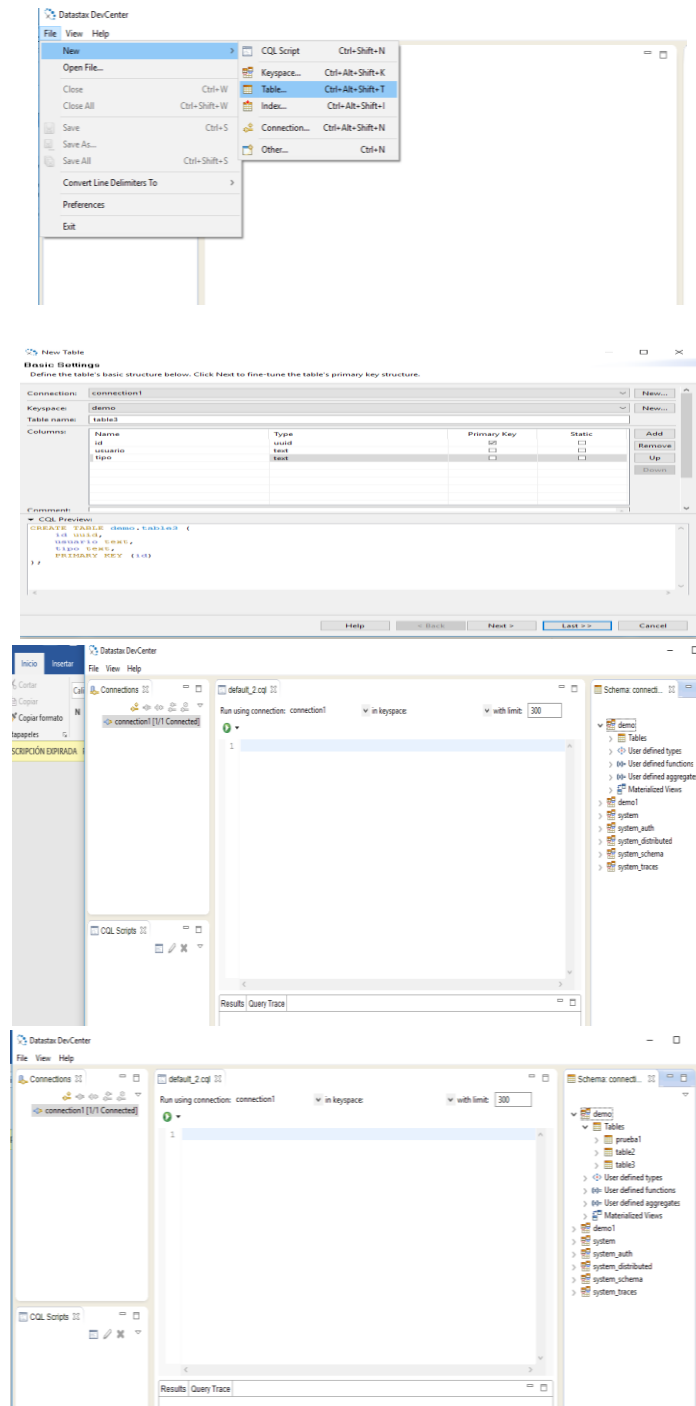
Fuente: El Autor

Figura 60. Crear la base de datos



Fuente: El Autor

Figura 61. Crear las tablas con datos



Fuente: El Autor

Figura 62. Vulnerabilidades de Cassandra

```
root@kali:~# sqlmap -u 192.168.1.5:8080/apex/?p=4950:1012511876033985
{1.0-dev-hongit-201605080a89}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon-
sible for any misuse or damage caused by this program

[*] starting at 15:21:51

[15:21:51] [INFO] testing connection to the target URL
[15:21:52] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[15:21:52] [INFO] heuristics detected web page charset 'ascii'
[15:21:52] [CRITICAL] heuristics detected that the target is protected by some k
ind of WAF/IPS/IDS
do you want sqlmap to try to detect backend WAF/IPS/IDS? [y/N] y
[15:21:54] [WARNING] dropping timeout to 10 seconds (i.e. '--timeout=10')
[15:21:54] [INFO] using WAF scripts to detect backend WAF/IPS/IDS protection
```

Fuente: El Autor

8. RECOMENDACIONES Y PROPUESTA DE SEGURIDAD PARA LAS BASES DE DATOS SQL Y NOSQL

Las bases de datos admiten mejorar la calidad de las técnicas informáticas y que estas sean más rápidas y eficaces.

Cada día se hace más importante la seguridad en la información que se maneja en las bases de datos con información de personas, que exige más protección y confidencialidad sobre los datos que se almacenan en las bases de datos.

8.1 RECOMENDACION DE SEGURIDAD PARA BASES DE DATOS SQL

La seguridad en los datos involucra controlar las acciones prohibidas que coloquen en riesgo su divulgación, estabilidad e integridad. Esto se realiza por medio de mecanismos para controlar el acceso y manejo de los datos, sin alterar los definidos en el modelo según los requisitos del sistema o la aplicación. Las recomendaciones de seguridad son:

El esquema de seguridad

- Existen tecnologías y servicios de seguridad para acceder a la información.
- Una de las causas importantes de la información es que no se tenga pérdida de esta por causas como: errores de hardware y software, desastre natural, errores humanos.
- Se debe prevenir la pérdida de información realizando backup de las bases de datos, realizando una copia en cintas y en custodia en un lugar externo o datacenter, si en algún momento se requiere restaurar la base de datos, es más fácil con el backup que se tiene, este se debe realizar a diario ya que la base de datos crece todos los días por la cantidad de registros, para acceder al backup solo al personal con permisos y con los roles permitidos como lectura, escritura, modificación.
- Tener un control de los recursos que se tiene para el manejo de la información como lo es impresoras, CPU, medios de almacenamiento y de exportación, por estos medios se puede extraer información importante de la compañía.
- Las capacidades de log-on debe ser único en la red, para realizar la autenticación, cada usuario debe tener su usuario y clave en la red, la política es que no se presta el usuario y clave a ninguna persona para evitar pérdida de información.
- Tener archivos con encriptación para el almacenamiento en sistemas NTFS, mejor protección de información.
- La seguridad IP dar elementos para protección de las redes como Windows IP Security, para evitar una forma de fraude o extracción de la información.

- Con tarjetas inteligentes realizar protocolos y servicios asociados para la autenticación, esta es otra forma de asegurar la información que existe en las bases de datos.
- Tener tecnología de clave pública con información criptográfica.

Previsiones de seguridad a las vulnerabilidades:

- Privilegios excesivos: restringir privilegios de las rutinas solo para los datos necesarios, con el diseño de buenas políticas de concentración.
- Abuso de Privilegios: Tener la solución con la política de control de acceso para los datos, como la ubicación, el tiempo, el volumen de los datos recuperados e identificar los usuarios que abusan de los privilegios, aplicarles las leyes de protección de la información.
- Elevación de privilegios no autorizados: El Exploits de elevación de privilegios se puede derrotar con el control de acceso por consulta, auditorias y sistemas de prevención (IPS) esta última puede identificar la amenaza de la seguridad web dentro de una operación.
- Vulnerabilidad de la plataforma: Se puede utilizar herramientas IPS para identificar y bloquear los ataques que se presenten a las bases de datos.
- Inyección de SQL: Realizar auditorías, controles, detectar consultas no autorizadas, rutinas almacenadas.
- Auditoria Débil: Auditoria de las bases de datos en la red, recopilación de datos detalladamente y no debe causar demora o impacto.
- Denegación del servicio: Expandir un IPS y controles de velocidad, para que los usuarios individuales tomen mayor recurso.
- Autenticación Débil: Se debe tener mecanismos de autenticación integrados con la infraestructura del directorio AD y la seguridad web, escabilidad y factibilidad del uso.
- Vulnerabilidades en los protocolos: Tener un análisis y validación de las comunicaciones de SQL para asegurarse de que no están malformados, los protocolos, para así prevenir pérdidas o daños en las bases de datos.
- Exposición de los datos de backup: Copias de seguridad cifrada, las bases de datos no deberían permitir realizar copias sin la información no está cifrada.
- No permitir que esta información sea manipulada por personas que no están autorizadas.

8.2 PROPUESTA DE SEGURIDAD PARA BASES DE DATOS NOSQL

La característica principal de seguridad en una base de datos es confidencial, íntegra y disponibilidad. El estudio realizado se evidencio que a la gran diversidad

de bases de datos NoSQL que existe, no tienen mayor seguridad, el contenido es vulnerable a ataques, para esto se debe aplicar medidas para prevenir ataques. Una de las pautas de seguridad para aplicar en las bases de datos NoSQL, es crear una política teniendo en cuenta el ciclo PHVA que se conforma:

- Planear: especificar objetivos y eficacia de la política y como se van a lograr, recoger las opiniones de las bases de datos, plasmar en un documento las opiniones para tener en cuenta para realizar la política. Como política se debe definir el correcto funcionamiento de las bases de datos, con los parámetros de seguridad en la base de datos para que la información siempre este integra, confidencialidad y disponible, aplicarla en el servidor donde está alojada la base de datos. Con la norma ISO 27001 la seguridad de la información es: “la preservación de la confidencialidad (solo los autorizados pueden acceder a la información), integridad (la información y métodos que se utilizan son exactos) y disponibilidad (los usuarios autorizados pueden acceder a la información).
- Hacer: gestionar los activos de la información con controles como la responsabilidad de los activos, la clasificación de la información, inventario, propiedad y uso de los activos, clasificar la información con directrices y etiquetada, realizar un levantamiento de información de la infraestructura física donde está la base de datos (información, persona, software, hardware, servicios), la información es pública o privada., identificar los riesgos, amenazas y vulnerabilidades a la que está expuesta la base de datos.
- Verificar: la medición de los controles establecidos, ejecutar un seguimiento y la eficacia, desarrollar normas y procedimientos de la política establecida, documentar el procedimiento de los controles establecidos, verificar que se cumpla, realizar una auditoría constante de los sobre la política para verificar su cumplimiento.
- Actuar: con el análisis de la auditoría, tomar las respectivas medidas sobre los controles, procedimiento y normas que se tiene y que ha fallado, realizar las correcciones respectivas en la política, darla a conocer a los usuarios que interactúan con la base de datos.³²

Con el ciclo PHVA, es la primera forma para realizar y tener en cuenta en la seguridad de las bases de datos NoSQL, otra forma es cifrar los datos que procesa con estrategias de réplica así se evitara alarmas por accesos indebidos a la información que contiene las bases de datos, esto no quiere decir que con el solo cifrado ya están protegidas las bases, se tienen que realizar todos los procesos posibles para tener una base de datos segura.

³² Ibid, pág. 2

8.2.1 Medidas de seguridad en bases de datos NOSQL con la diversidad de las bases de datos NoSQL se debe tener en cuenta las debilidades genéricas que presentan e implementar las medidas necesarias para su seguridad las cuales son:

- **Autenticación** muchas de las bases de datos presentan debilidad en la autenticación, estas bases de datos traen por defecto credencial, no traen autenticación. Dependiendo del software siempre se debe configurar y revisar la autenticación de los usuarios a las bases de datos, para lo cual se debe tener claves robustas.
- **Integridad de los datos** en las bases de datos se tiene presente el rendimiento y la disponibilidad, no se tiene presente la integridad de los datos. Para mitigar esto se debe utilizar otros mecanismos adicionales y ajenos a las bases de datos para certificar la integridad.
- **Cifrado y confidencialidad en el almacenamiento** actualmente el almacenamiento de los datos se efectúa en texto plano, una de las bases que lo realiza en forma diferente es Cassandra con el método Transparent data encryption, no contiene cifrado integrado. Esta función la puede realizar la capa de aplicación o por el sistema de ficheros.
- **Backup permanentes** la inexactitud de medidas de seguridad causa que intrusos ataquen maliciosamente las bases de datos, se conoce como la demanda del rescate, lo cual pueden borrar, cambiar y robar, el cambio de los permisos en las bases de datos, para mitigar esto se deben realizar backup de las bases periódicamente.
- **Protección de la Infraestructura** muchos de los ataques que se realizan a las bases de datos NoSQL son por los puertos que están habilitados, con un software especializado realizar escaneo de los puertos ya que por este medio ven las vulnerabilidades para realizar los ataques, se debe tener una buena configuración de la infraestructura y un firewall IP.
- **Encriptación en la transmisión y almacenamiento de contraseñas** el no utilizar encriptación en las conexiones que existe entre el cliente y el servidor de base de datos, hace que los usuarios y contraseñas puedan ser "sniffeados" con ciertas herramientas. Se debe habilitar, configurar e encriptar TLS/SSL para las conexiones de clientes y servidor a la base de datos.

- **Cifrado en la transmisión** muchas de estas bases de datos no manejan un cifrado en la transmisión de los datos, si efectúa un ataque a la red, se puede perder datos de las bases de datos. Par mitigar esto se debe manejar un cifrado de datos de cliente servidor para evitar la pérdida de los datos almacenados.
- **Seguridad en las comunicaciones** en las bases de datos NoSQL el cifrado y protocolo SSL habitualmente se halla deshabilitado por defecto, es necesaria habilitarla y realizar una configuración específica en la instalación.
- **Auditoria de datos** la gran cantidad de bases de datos NoSQL escasean de componentes propios y robustos de auditoría de datos, a la hora de detectar un posible ataque se realiza por observación de eventos sobre registros precisos. Se debe monitorear las bases de datos para evitar ataques
- **Vulnerabilidades tradicionales en las bases de datos** tener en presente que en las bases de datos NoSQL, las llamadas y peticiones se hacen invocando la API, regularmente JSON o XML. Las posibilidades de inyección y los riesgos, al manejar una API con lenguaje procedimental, son de mayor riesgo que las bases de datos relacionales. Con (data-sharing), se puede realizar una evaluación de riesgos, realizar más eficientemente y efectivamente la seguridad en la información que manejan las empresas.

Otros aspectos de la seguridad para que se apliquen en las bases de datos ya sean relacionales y NoSQL.

Las bases de datos tienen debilidades en común ya sean relacionales o NoSQL para prevenirlas se deben implementar las medidas de seguridad necesarias las cuales son:

- Seguridad de las redes: se debe utilizar un firewall IP, para el resguardo de las bases de datos NoSQL, se utiliza estableciendo IP para adicionar la relación con el firewall, son reglas en los sistemas en las bases de datos, para que se pueda acceder desde una maquina o servicios en la nube.
- Configurar los protocolos: HTTPS, SSL y Cifrado TLS para interrelacionar con las bases de datos se debe tener estos protocolos.
- Controles físicos, naturales y de acceso a las instalaciones: previniendo la pérdida, daño de las bases de datos por alguna falla física o natural.
- Aspectos legales, sociales y éticos: se deben aplicar para proteger las bases de datos.
- Diseñar políticas en la organización: para acceso a la información, las cuales se deben divulgar a los empleados para que ayuden a prevenir los ataques y riesgos que se puedan presentar en las bases de datos.

- Controlar el sistema operativo: se debe evitar los riesgos que puedan causar alguna vulnerabilidad del sistema operativo.
- Identificar a los usuarios autorizados: se debe validar la solicitud de ingreso con un código que se autentique al cual se crea un hash, para verificarlo con el de la solicitud que se requiere, si el hash creado anteriormente coincide con el ingresado está autorizado al ingreso, también se puede tener una clave maestra, un token, o con alguna de estas tecnologías como la huella, voz, retina de ojo, se puede identificar las personas que acceden a las bases de datos.
- Usuarios con privilegios: con una clave maestra, se puede asignar recursos y permisos en la base de datos, dependiendo el perfil, se debe asignar de esta forma para que solo acceda el personal autorizado, un token está ligado a una base de datos y este usuario tiene unos accesos como son (lectura, escritura, modificación), es una autenticación para del usuario a los recursos de la base de datos.
- SGBD: perfiles de usuario, vistas, restricciones de uso de vistas, etc.
- Monitoreo permanente de las bases de datos NoSQL: para identificar rápidamente alguna vulnerabilidad que se presente.
- La información sea confidencialidad, la integridad y la disponibilidad.
- Identificar la sensibilidad (configurando tablas o datos sensibles): que se tengan en las bases de datos NoSQL.
- Evaluar las vulnerabilidades: y la configuración que se tienen en la infraestructura donde están alojadas las bases de datos NoSQL.
- Auditar permanentemente las bases de datos NoSQL y el uso no autorizado de los recursos como lo es la lectura, modificación, destrucción de datos.
- Mecanismos de protección: tienen que ser simples, uniformes y en capas básicas del sistema, para esto existen soluciones que ayudan con el cifrado y protección en las bases de datos.
- Para aplicaciones en la nube se puede utilizar arquitecturas web, es para varios equipos se llama Software as a Service (SaaS).
- Cliente con desarrollo de herramientas contiene varios lenguajes para que se cree nuevas aplicaciones este se llama Plataforma as a Service (PaaS)
- El IaaS es donde esta los servicios de SaaS y PaaS
- La infraestructura es un servicio (IaaS) es donde está el proceso (CPU) y la capacidad de almacenamiento, se realiza a través de una red privada o internet.

Aplicando procedimientos y políticas sobre la información que se manejan en las empresas y en las bases de datos, se está protegiendo y dando seguridad al activo más valioso tanto en las empresas como a las personas el cual corresponde a la información que está contenida en las bases de datos. Cuando se escoja una de estas bases de datos NoSQL, según la jerarquía, se pueden aplicar estas pautas de seguridad en las bases de datos y así proteger la información que contiene y evita ataques de otras personas. Con las bases de datos NoSQL se deberá robustecer a seguridad.

8.2.2 Cuando utilizar un tipo de base de datos cuando la información cumple el rol más importante en el negocio se debe escoger la base de datos más apropiada, para ello tener en cuenta algunos aspectos:

- No se puede dar posibilidad de error en los datos por esta razón se deben utilizar base de datos relacional.
- Cuando se tienen maquinas con bajo rendimiento se de utilizar base de datos No SQL
- El análisis de datos es muy grande, las distribuciones son variables se debe utilizar NoSQL.
- Captura y procesado de eventos. No SQL
- Cuando los motores complejos se requieren tiendas online No SQL

8.2.3. A la hora de elegir una base de datos existen muchas bases de datos a la hora de elegir se debe tener en cuenta unos aspectos importantes los cuales son:

- Los servicios para cuantos clientes son y si son de forma concurrente.
- Que datos y tamaños se van a trabajar
- Se necesita implementar trabajos en “catch” para que estén en la base de datos
- Como va a ser el tiempo de respuesta.
- Si mi base de datos aumenta como la voy a escalar
- Para que el tiempo de indisponibilidad sea mínimo como la monitoreo.
- Que base de datos voy a escoger
- Cuando hay problemas como se va a trabajar

8.2.4. Pros y contras del uso de las bases de datos NoSQL en un ambiente organizacional las bases de datos NoSQL en los ambientes organizacionales cumplen un papel importante ya que en estas se guardan la información del negocio para ellos se deben analizar los pros y contras que tiene:

Pros

El procesamiento de datos es más rápido que las bases de datos relacionales. Las NoSQL son rápidas porque los datos que se manejan son simples, no posee requerimientos técnicos en los sistemas NoSQL, son flexibles para los que desarrollan.

Aparte de ser rápidas, son confiables, rápidas y no tienen costos. Se escalan horizontalmente por esta razón son elásticas.

Distribuye la carga en varios hosts o en varias máquinas a medida que esta va creciendo.

Contras

Con respecto a las bases de datos relacionales la utilizan para su negocio con cierta precisión, las restricciones de transacciones ACID para todos los datos y las NoSQL no tienen esas garantías para su rendimiento puede realizarse daños en las bases de datos.

9. RESULTADOS Y DISCUSIÓN

Este estudio de la seguridad en las bases de datos relacional y NoSQL, se tomó dos bases de datos de las cuales se revisó su seguridad actual, los procedimientos y las políticas que se estandarizaran en cada una de las bases de datos, se recomienda cómo se puede tener más seguridad y mitigar los riesgos de los registros o información que se almacena en las bases de datos ya sea relacional o no relacional.

Se evidencio que las bases de datos NoSQL son eficientes y contienen más capacidad de almacenamiento, pero no tienen tanta seguridad como las bases de datos relacionales, se debe aplicar políticas y procedimientos cuando se escoja una base de datos NoSQL, más si la información se encuentra en la nube.

Al escoger una base de datos se debe tener en cuenta varios aspectos como lo es la velocidad, capacidad de almacenamiento, procedimientos, políticas y seguridad que maneje, en el mercado ya existen herramientas como token y software especial para aplicar la seguridad a las bases de datos y la protección de la información.

La infraestructura que se tiene para las bases de datos es importante para aplicar la seguridad, contar con personal especializado, con políticas claras, procedimientos que se apliquen y se conozca por el personal que interactúa con las bases de datos y la información de las organizaciones, también realizar periódicamente auditorias para identificar los riesgos que se tenga para corregir a tiempo.

Las bases de datos SQL y NoSQL se van a seguir utilizando y desarrollando por varios años más. Con las bases de datos NoSQL son más rápidas y los datos pueden crecer más sin tener inconvenientes de espacio, estos atraen costos que las bases de datos SQL las tienen. Las garantías que ofrece NoSQL valen la pena para varias de las aplicaciones que se manejan.

10. DIVULGACIÓN

Este estudio es un apoyo para muchas entidades y personal que manejan bases de datos, se entregara a la universidad para que sea almacenado en el repositorio para consulta y en internet, para que se tenga en cuenta a la hora de escoger una base de datos que maneje información sensible.

CONCLUSIONES

- Se realizó el estudio de las bases de datos relacionales y no relacionales donde se detectó que las bases de datos relacionales tienen más seguridad según su configuración y en cuanto a las bases de datos no relacionales manejan una mayor capacidad de almacenamiento por su forma horizontal y elástica.
- La organización según su actividad del negocio está a través de internet o aplicaciones en la nube, necesitan otorgar sistemas e infraestructuras con procesos, procedimientos y políticas adecuadas para proteger su información, dar continuidad al negocio.
- Al momento de la configuración de las bases de datos, definir un sistema de seguridad, políticas y estándares que aseguren la confidencialidad de los datos del sistema instalado.
- Se debe tener bases de datos relacionales y no relacionales, útiles con protección de los datos o registros que se manejan, para que la información este con los pilares integra, confidencialidad y disponible.
- Para las bases de datos no relacionales se presenta una propuesta sobre la seguridad que se debe tener y aplicar en estas bases de datos, en la actualidad se está almacenando gran cantidad de información por medio de las redes sociales que se maneja, estas no reemplazaran las bases de datos relacionales, solo quieren brindar más rapidez, eficacia en el manejo y respuesta de la información, por los medios donde se maneja se debe tener seguridad para mitigar los riesgos que se presente con estas bases de datos.
- Contar con la infraestructura y el personal capacitado para maneje las bases de datos en las organizaciones contando con las herramientas necesarias para la seguridad de las bases de datos.

RECOMENDACIONES

- Se debe socialización el proyecto “Estudio de seguridad en bases de datos SQL y NoSQL” para poder escoger una base de datos para la información que manejan las entidades.
- Algunas propuestas de cómo se puede llegar a tener más seguridad de las bases de datos relacionales y no relacionales que se pueden aplicar para evitar las vulnerabilidades.
- Implementar un Sistema de Gestión de Seguridad, para que la información de las bases de datos está protegida y tener personal capacitado.
- Realizar las respectivas políticas y auditorias permanentes cada 3 meses para evidenciar si se tiene vulnerabilidades de las bases de datos y la infraestructura donde está instalada.
- Tener backup diario y en custodia con cifrado de datos para evitar la pérdida de la información sensible que se maneja.
- Se debe autorizar al personal entrenado y con la capacidad para manejar las bases de datos y así mitigar los riesgos que se presente.
- Capacitar a las personas del área de sistemas TIC, en seguridad en las bases de datos.
- Este estudio es un apoyo para muchas entidades y personal que manejan bases de datos, se entregara a la universidad para que sea colocado en el repositorio para consulta, para que se tenga en cuenta a la hora de escoger una base de datos e información sensible.

BIBLIOGRAFÍA

ALVAREZ, Sara, Desarrollo Web, Estructura del modelo relacional, [5 de septiembre de 2007], [En línea], [Citado 03 de noviembre de 2016], Disponible en: (<http://www.desarrolloweb.com/articulos/estructura-modelo-relacional.html>)

ARAYA, Daniel, Recuperación de fallas en Bases de Datos [En Línea], [27 de octubre del 2014], [Citado el 25 de abril de 2017] Disponible en: (https://prezi.com/2ddr-lqrxwo_/recuperacion-de-fallas-en-bases-de-datos/)

BLAT, Fernando, Bigtable el servicio de base de datos NoSQL con el que Google quiere dominar los Big Data, [2017], [En línea], [Citado el 23 de abril de 2017], Disponible en: (<https://unpocodejava.wordpress.com/2012/07/12/un-poco-de-cassandra/>).

BUSSINES SCHOOL, Inesem, Redes y Sistemas, Los gestores de bases de datos más usados, [En línea], [Citado el 17 de octubre de 2016] Disponible en: (<http://revistadigital.inesem.es/nuevas-tecnologias/los-gestores-de-bases-de-datos-mas-usados/>).

CABALLERO, Alonso, Curso Virtual de Hacking Ético. Consultor Hacking Ético Lima Perú: 2016

CADENA, Edison, Transcripción de Seguridad en Aplicaciones con bases de Datos NOSQL y sus diferencias, [10 de Julio de 2015], [En línea], [Citado 20 de octubre de 2016], Disponible en: presentación Prezi, (https://prezi.com/fg2pjped0_xs/seguridad-en-aplicaciones-con-bases-de-datos-nosql-y-su-dife/)

CAMPS PARE, Rafael, PEREZ MORA, Oscar, MARTIN ESCOFET, Carme, CASILLAS SANTILLAN, Luis Alberto. Software libre, Bases de Datos [En línea] [Citado el 03 de marzo de 2017] disponible en: (<http://www.uoc.edu/masters/oficiales/img/913.pdf>)

CODD, Hollerith, Universidad politécnica de Valencia, Historia de las Bases de Datos, [4 DE ENERO DE 2011], [En línea], [Citado 12 de noviembre de 2016],

Disponible en: (<http://histinf.blogs.upv.es/2011/01/04/historia-de-las-bases-de-datos/>)

CORDOBA ESPINOSA, Rosa Fernanda, Cusco Sarango Bernardo Esteban, Análisis Comparativo entre bases de datos relacionales con bases de datos no relacionales, [2013, Cuenca-Ecuador, tesis], [En línea], [Citado 03 de noviembre de 2016], Disponible en: (<http://www.dspace.ups.edu.ec/bitstream/123456789/6977/1/UPS-CT003639.pdf>)

CORDOBA ESPINOSA, Rosa, Cuzco Sarango Bernardo, Análisis Comparativo de bases de datos relacionales y No relacionales, tesis, [2013], [En línea], [Citado 18 de Noviembre de 2016], Disponible en: (<http://dspace.ups.edu.ec/bitstream/123456789/6977/1/UPS-CT003639.pdf>)
CUNI, David, empresa & economía, Bases de datos más utilizadas, [23 de febrero de 2012], [En línea], [Citado 10 de noviembre de 2016], Disponible en: (<http://empresayeconomia.republica.com/aplicaciones-para-empresas/bases-de-datos-mas-utilizadas.html>)

DATAPRIX, Orígenes y Antecedentes de las Bases de Datos, [2013], [En línea], [Citado 12 de noviembre de 2016], Disponible en: (<http://www.dataprix.com/24-origenes-antecedentes-las-bases-datos>)

DEVELOPER, Network, Autenticación en SQL Server [2017], [En Línea], [Citado el 26 de abril de 2017] Disponible en ([https://msdn.microsoft.com/es-es/library/bb669066\(v=vs.110\).aspx](https://msdn.microsoft.com/es-es/library/bb669066(v=vs.110).aspx)).

DRAGONIS11, Integridad y Seguridad en las Bases de Datos, [En Línea], [Citado el 28 de febrero de 2017] disponible en: (<https://es.slideshare.net/Drakonis11/integridad-y-seguridad-en-las-bases-de-datos-presentation>)

GARZON ARISTIZABAL, Danny Alejandro, Creación, implementación y evaluación de la política de seguridad de base de datos para los ambientes de producción del instituto colombiano para la evaluación de la educación "icfes", [En línea], [Citado el 06 de mayo de 2017], Disponible en: <http://repository.udistrital.edu.co/bitstream/11349/2424/1/Garz%C3%B3nAristizabaIDannyAlejandro2015.pdf>

GOMEZ ROBLES, Deiby, Oracle Exadata Database Machine: Seguridad a nivel de ASM y de Base de Datos, [En Línea], [Citado el 27 de febrero de 2017] disponible en: (<http://www.oracle.com/technetwork/es/articles/database-performance/seguridad-asm-base-de-datos-parte1-2166616-esa.html>)

LEON, Blaustein, León, Falta seguridad en bases de datos, según encuesta de Oracle, [2016], [En línea], [Citado el 29 de abril de 2017], Disponible en: <http://searchdatacenter.techtarget.com/es/cronica/Falta-seguridad-en-bases-de-datos-segun-encuesta-de-Oracle>

MICROSOFT, Azure, Como puedo proteger mi base de datos NoSQL, [En línea], [Citado el 12 de mayo de 2017], Disponible en: <https://docs.microsoft.com/es-es/azure/documentdb/documentdb-nosql-database-security>

Ministerio de Tecnologías de la Información y las Comunicaciones, ley 1273 de [2009], [En línea], [Citado 12 de noviembre de 2016], Disponible en: (<http://www.mintic.gov.co/portal/604/w3-article-3705.html>)

MOSCOSO, Ivan, Bases de datos relacionales, El Rincón del Vago, en Salamanca desde [1998], Republica dominicana, documento,[En línea], [Citado 10 de noviembre de 2016] Disponible en:(<http://html.rincondelvago.com/base-de-datos-relacional.html>)

MUÑOZ GOMEZ, Juan Carlos, Características principales del Modelo Relacional en las bases de datos, [8 de octubre de 2012], Bogotá, presentación, [En línea],[Citado 03 de noviembre de 2016] Disponible en: (<https://prezi.com/g3tx07vx2dcu/caracteristicas-principales-del-modelo-relacional-en-las-bases-de-datos/>)

NEVADO CABALLERO, María Victoria, Introducción a las Bases de Datos Relacionales, [En línea], [Citado el 28 de abril de 2017], Disponible en: https://books.google.com.co/books?id=0lUpB1lNUdIC&pg=PA22&lpg=PA22&dq=seguridad+actual+en+bases+datos+relacionales&source=bl&ots=sJ0UK6w-OR&sig=5Z9G-xqjCaXBz7_PBGdgBVsBJG4&hl=es-419&sa=X&ved=0ahUKEwie0KzL2MnTAhVHQCYKHRdhBDAQ6AEIUzAH#v=onepage&q&f=false

ONASYSTEM, Vulnerabilidades importantes que afectan la seguridad de bases de datos en las empresas, [En línea], [Citado el 29 de abril de 2017], Disponible en: <http://www.onasystems.net/vulnerabilidades-importantes-afectan-la-seguridad-bases-datos-las-empresas/>

OPENREPOSITORIO, NoSQL: futuro de almacenamiento de datos [En línea], [Citado 17 de noviembre de 2016], Disponible en: (<http://repositorioacademico.upc.edu.pe/upc/bitstream/10757/552364/1/tesis+medina+-+mendoza.pdf>)

PANDORA, Javier, NOSQL vs SQL. Diferencias y cuando elegir cada una, [18 de Noviembre de 2015], [En línea], [Citado 13 de noviembre de 2016], Disponible en: (<https://blog.pandorafms.org/es/nosql-vs-sql-diferencias-y-cuando-elegir-cada-una>)

PEREZ, Victoria, NoSQL =No Security [En Vivo] [Septiembre 17 de 2016], [En línea], [Citado el 04 de marzo de 2017] Disponible en: (<http://www.dragonjar.org/nosql-nosecurity-seguridad-en-bases-de-datos-no-relacionales.shtml>)

POTOLOMEIO, Bases de datos relacionales, [2 014], [En línea],[Citado 30 de octubre de 2016] Bogotá, Disponible en: (<http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/907/A5.pdf?sequence=5>)

QUINATO A MOROCHO, Fabio Enrique, Bases de datos NoSQL en computación en la nube, [En línea], [Citado el 12 de mayo de 2017], Disponible en: <https://prezi.com/fugbqylmoezv/bases-de-datos-nosql-en-computacion-en-la-nube/>

SALAZAR CARDENAS, José Edwin, análisis comparativo de dos bases de datos sql y dos bases de datos no sql, [2014, Pereira, proyecto,] [En línea], [Citado 25 de Octubre de 2016] Disponible en: (<http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/5119/0057565S161.pdf?sequence=1>)


UNIVERSIDAD Católica de Colombia, diseño y elaboración de prácticas de laboratorio para la enseñanza de los conceptos fundamentales de bases de datos no relacionales – nosql, [11, mayo, 2015, Bogotá, tesis], [En línea], [Citado 24 de octubre de 2016] Disponible en:

(<http://repository.ucatolica.edu.co/bitstream/10983/2470/1/TRABAJO%20DE%20GRADO.pdf>)

VILLALOBOS MURILLO, Johnny. Principios Básicos de Seguridad en Bases de Datos, [13/01/2012], [En línea], [Citado el 20 de octubre, 2016], Disponible en: (<http://revista.seguridad.unam.mx/numero-12/principios-basicos-de-seguridad-en-bases-de-datos>)

ANEXOS

ANEXO A

	FORMATO
RESUMEN ANALÍTICO EN EDUCACIÓN – RAE	
Código:	Versión: 01
Fecha de Aprobación:	Página 1 de 3

1. Información General	
Tipo de documento	Trabajo de Grado
Acceso al documento	Universidad Nacional Abierta y a Distancia
Título del documento	Estudio de seguridad en bases de datos SQL y NoSQL
Autor(es)	GOMEZ, Yeny
Publicación	Bogotá. Universidad Nacional Abierta y a Distancia, 2017.
Palabras Claves	Base de datos, Clave, Motor de base de datos, SQL, NoSQL, Tupla, datos, seguridad, vulnerabilidad, RDMBS, DBMS, dominio.
Descripción	<p>Las bases de datos son importantes por el contenido que contiene como lo es la información se debe garantizar la integridad, disponibilidad y confiabilidad de la misma, la base de datos crece cada día puede ser vulnerables a ataques.</p> <p>Con este estudio se planteó objetivos correspondientes a la seguridad que deben tener las bases de datos relacionales y NoSQL, para esto se da las recomendaciones de seguridad en las bases de datos SQL y una propuesta para las bases de datos NoSQL, lo cual garantizara su arquitectura en el manejo de la información.</p>
Fuentes	31 Fuentes
Contenido	A través de este proyecto, se realiza un estudio sobre los conceptos que con lleva a la toma de decisiones sobre las bases de datos que tiene las organizaciones según la necesidad, los antecedentes, los conceptos sobre estas bases de datos, las leyes que no se pueden violar, los métodos que se utilizan sobre las diferentes bases de datos y la comparación de las mismas si es relacional y NoSQL, se <i>identifica qué tipo de base de datos es más vulnerable a</i>

	<p><i>los ataques informáticos, la evolución que han tenido las bases de datos.</i></p> <p>La metodología que se sigue para identificar la seguridad de las bases de datos, el análisis de las diferentes bases de datos y el desarrollo sobre las dos bases de datos que se tomó para realizar el laboratorio, en el cual se evidencian las vulnerabilidades que presenta cada una de estas bases de datos y se dan las recomendaciones y propuestas a aplicar en las bases de datos, los resultados que se tiene del estudio que se realizó, las conclusiones y recomendaciones del desarrollo de la seguridad de las bases de datos relacionales y NoSQL, como es la divulgación del estudio realizado.</p>
Metodología	<p>El estudio se enmarco en los procesos, métodos y políticas que se debe tener en las bases de datos según su tipo si son relacionales y NoSQL, lo más importante en las organizaciones es la información, que sea disponible, confiable e integra para los usuarios y las personas que manejan estas bases de datos, las diferencias que existen en las bases de datos relacionales y NoSQL, cual es la mejor para que las entidades las manejen.</p> <p>El laboratorio que se realizo fue a una base de datos relacionales y una base de datos NoSQL, las características de la infraestructura, las vulnerabilidades que tienen y los roles que se maneja en las bases de datos.</p> <p>Se da a conocer las recomendaciones, propuestas para aplicar a las base de datos sobre la seguridad que se debe tener a la hora de escoger una base de datos.</p>
Conclusiones	<p>Se realizó el estudio de las bases de datos relacionales y no relacionales donde se detectó que las bases de datos relacionales tienen más seguridad según su configuración y en cuanto a las bases de datos no relacionales manejan una mayor capacidad de almacenamiento por su forma horizontal y elástica.</p> <p>Al momento de la configuración de las bases de datos, definir un sistema de seguridad, políticas y estándares que aseguren la confidencialidad de los datos del sistema instalado.</p> <p>Se debe tener bases de datos relacionales y no relacionales, útiles con protección de los datos o registros que se manejan, para que la información este con los pilares integra, confidencialidad y disponible.</p> <p><i>Contar con la infraestructura y el personal capacitado para maneje las bases de datos en las organizaciones contando</i></p>

	<p><i>con las herramientas necesarias para la seguridad de las bases de datos.</i></p> <p><i>Para las bases de datos no relacionales se presenta una propuesta sobre la seguridad que se debe tener y aplicar en estas bases de datos, en la actualidad se está almacenando gran cantidad de información por medio de las redes sociales que se maneja, estas no reemplazaran las bases de datos relacionales, solo quieren brindar más rapidez, eficacia en el manejo y respuesta de la información, por los medios donde se maneja se debe tener seguridad para mitigar los riesgos que se presente con estas bases de datos.</i></p>
--	---

Elaborado por:	Gómez Mojica Yeny Mireya
Revisado por:	Vargas Julio Alberto

Fecha de elaboración del Resumen:	07	06	2018
--	----	----	------