

Seguridad en Bases de Datos

Prueba de Evaluación Continua, PEC 1

Enunciado

1. Responsables de la seguridad de los datos (5 puntos)

La compañía ACME tiene, entre otras, una base de datos corporativa en la que almacena los datos de sus empleados, incluyendo sus datos personales y sus sueldos. Mediante un proceso automático, se realiza una copia de seguridad mensual de la base de datos que se almacena en una cinta en un lugar seguro. Por otro lado, existe un proceso mensual que extrae un subconjunto de datos y lo envía a un sistema de archivos en un servidor para preparar el proceso de nóminas.

Teniendo en cuenta este escenario, contesta de manera argumentada las siguientes cuestiones:

1.1. Describe que roles o individuos tendrían alguna responsabilidad en la seguridad de dichos datos y cuales serían sus funciones principales.

Según el Reglamento General de Protección de Datos (RGPD) [1], deben existir tres figuras principales a la hora de tratar datos personales, vamos a describirlos y también los roles que irán asociados a cada uno y su relación con la seguridad de los datos [2].

Responsable del Tratamiento de los datos: es la persona física, jurídica, u órgano administrativo que decide sobre la finalidad, contenido y uso del tratamiento de los datos.

En este caso sería la empresa ACME S.A. como persona jurídica la Responsable del Tratamiento.

El único rol que se podría asociar al Responsable del Tratamiento es el del director de operaciones, pero éste normalmente no accederá a la base de datos ni tendrá responsabilidades sobre la seguridad de la misma, aunque responda legalmente si sus subordinados cometen errores. Sus funciones serán de más alto nivel, como dar órdenes al resto de responsables para que cumplan una nueva normativa.

Encargado del Tratamiento de los datos: persona física, jurídica u órgano administrativo que realiza el tratamiento de los datos por cuenta del responsable.

En este apartado es donde se concentran los roles que gestionarán tanto la base de datos como la información que contiene:

- **Administrador de la Base de Datos (DBA):** se encargará de todo lo relativo a la arquitectura de la base de datos. Deberá encargarse y garantizar:
 - Rendimiento con tiempos de respuesta aceptables
 - Disponibilidad de la información.
 - Pruebas de seguridad.
 - Copias de seguridad de los datos.
 - Recuperabilidad, capacidad de recuperar la información ante fallos
 - Actualizaciones de la arquitectura y las versiones del software de gestión.
- **Administrador de Sistemas:** su labor será asegurar la accesibilidad, los medios deben estar disponibles el máximo tiempo posible. Además deberá garantizar el buen funcionamiento de los sistema físicos y lógicos que darán soporte a la base de datos.
- **Responsable de Recursos Humanos:** suya es la responsabilidad de la recogida de datos personales y su inserción en la base de datos por medio de un software específico. Tienen acceso de primera mano a la información personal de los empleados.
- **Responsable de Contabilidad:** le corresponderá la elaboración de nóminas, podrá saber los datos financieros de todo el personal.

Cada Responsable de área puede tener subordinados que tendrían el mismo tipo de acceso a la información. En el caso del Administrador de la Base de Datos, pueden existir programadores de aplicaciones web con accesos más limitados (consulta, lectura y escritura).

Hemos decidido obviar los roles subordinados para centrarnos en los más básicos y representativos.

Delegado de Protección de Datos: supervisa y asesora al resto de roles para el cumplimiento del RGPD. También actúa como intermediario ante las entidades de supervisión y auditoría. Debe garantizarse su independencia en la organización, para que no haya conflictos de intereses.

Del mismo modo que el Director de Operaciones, no accederá directamente a la base de datos. Sus capacidades serán de nivel superior, como asesorar a los encargados del Tratamiento sobre las normativas vigentes o asistir en los procesos de auditoría y control.

1.2. ¿Qué medidas básicas de seguridad crees que deberían implementar cada uno de los responsables mencionados en el apartado anterior?

Todos los que traten datos personales deberían firmar contratos que incluyan cláusulas de confidencialidad sobre los datos personales [3].

Además, cada rol debe asegurar ciertas medidas de seguridad en función de su relación con la información [4].

Lo primero de todo sería la División de deberes, una vez cada rol tiene asignadas sus tareas, asegurarse de que tiene acceso sólo a las funciones mínimas para llevar a cabo su trabajo. De este modo se evita que un rol pueda acceder a más funcionalidades de las que tiene necesidad, evitando un posible foco de problemas.

Tanto el Administrador de la Base de Datos como el Administrador de Sistemas deben trabajar en conjunto para implementar medidas de control de acceso a la información, facilitarán así el trabajo del resto de roles en cuanto a seguridad.

A continuación algunas de las medidas para cada rol:

- Administrador de Sistemas:
 - Contraseñas para acceder al software que se comunicará con la base de datos.
 - Sistemas de Autenticación de usuarios que guarden registros de actividades de los mismos.
 - Controles biométricos para cuando haya que acceder a información sensible.
 - Encriptación de las comunicaciones tanto en la red interna como externa, recomendado el uso de certificados (SSL/TLS).
 - Firewalls y control de acceso para las comunicaciones desde el exterior.
 - Antivirus y sistemas operativos actualizados.
- Administrador de la Base de Datos:
 - Seudonimización de la información.
 - Encriptación de los ficheros de la base de datos.
 - Gestión de las claves de los usuarios, encriptado de las mismas.
 - Limitar el número de usuarios.
- Responsable de Recursos Humanos y Contabilidad: cumplir los protocolos proporcionados para el control de acceso. Extremar la precaución con el almacenamiento de contraseñas (buenas prácticas).

1.3. La compañía ha planteado contratar un servicio de Cloud Computing que permita la gestión remota de todos los datos de la compañía. De este modo, se accederá mediante un web-service para la inserción y modificación de todos los datos, y una interfaz permite la gestión de los mismos. La compañía que ofrece el servicio dice ocuparse de la seguridad de los datos, así como de realizar las copias de seguridad.

1.3.1. ¿Cómo cambia este nuevo planteamiento el anterior esquema (explica cómo cambian los roles y las responsabilidades de cada uno)?

Nota: Durante todo el apartado puede haber referencias a la empresa de Cloud Computing como “Cloud”.

El Responsable del Tratamiento sigue siendo la empresa ACME, de modo que si se produjera alguna fuga de información u otro problema que afectara a los datos, tendrían que responder por los mismos.

Sin embargo, el Encargado del Tratamiento pasaría a ser la compañía que ofrece el servicio de Cloud Computing. Por lo que ACME podría reclamarles responsabilidades si se producen problemas con los datos derivados de sus servicios.

En ACME, el rol que cambiaría de forma más significativa sería el de Administrador de Base de Datos (DBA), que perdería muchas de sus competencias, pasando a ocuparse la compañía de Cloud Computing. El DBA todavía se encargaría de posibles cambios en el diseño de la base de datos.

El Administrador de Sistemas puede verse descargado de la responsabilidad de mantener los medios físicos y lógicos para alojar la base de datos. Sigue teniendo que ocuparse de las comunicaciones y asegurando la máxima disponibilidad de los medios para la organización.

Para el personal de Contabilidad o Recursos Humanos no debería haber cambios significativos. Sus funciones serían las mismas y lo único que tendrían que hacer es adaptarse al nuevo aplicativo web.

El Delegado de Protección de Datos pasaría a ser una figura fundamental, ya que tendría que asesorar también a la compañía de Cloud Computing. Además podría ser un enlace entre ambas compañías para los asuntos relacionados con estos datos y frente a entidades de Control y Auditoría. A pesar de todo esto, sus responsabilidades para con la información no cambian.

1.3.2. Comparado con el escenario anterior, ¿qué riesgos y oportunidades crees que han aparecido?

Lo positivo es que ACME delega parte de las funciones a otra empresa, por lo que descarga a algunos de sus empleados de la carga de trabajo que supondría la base de datos [5]. Los roles que más liberación laboral aprecian son el del Administrador de la Base de Datos y el Administrador de Sistemas.

Además, los recursos y medios físicos que antes eran necesarios para sostener la infraestructura de la base de datos y las copias de seguridad, ahora se pueden usar para otros objetivos.

En la parte negativa, hay varios aspectos a tener en cuenta. La incorporación de una empresa externa en el escenario del tratamiento de los datos supone posibles fuentes de nuevos problemas:

- Depender de un aplicativo web para insertar, modificar o gestionar los datos introduce otro punto de fallo; si no hay conexión externa, no se puede trabajar con la información. Es poco probable, pero hay que tenerlo en cuenta.
- El factor humano: otra compañía, con otras personas trabajando, que pueden cometer errores igual que los de las personas que trabajan en ACME. Cuando se habla de errores se incluye la posibilidad de espionaje industrial u otros delitos relacionados que puedan resultar en puntos débiles en la seguridad de la información.
- La seguridad de la compañía de Cloud Computing: si hay brechas en la seguridad y se consigue sustraer información sensible, se puede llegar a obtener la información de ACME.

1.3.3. ¿Qué nuevas medidas de seguridad debería implantar o exigir la compañía ACME?

Lo primero de todo por parte de ACME sería asegurarse, por contrato, de que la compañía de Cloud Computing va a responder de cualquier fallo que derivara en pérdida de datos o casos similares [6]. De modo que si ACME recibe una reclamación, pueda exigir responsabilidades si el fallo es de Cloud.

Cada vez que la compañía de Cloud Computing haga una copia de seguridad, debería hacer otra para ACME, que se almacenará en un lugar seguro bajo el control de ACME. De este modo ACME puede disponer de las copias de seguridad en caso de fallo grave de Cloud.

Garantizar que la información de ACME sea cifrada antes de ser enviada a Cloud, para que los empleados de la última no puedan ser capaces de acceder a información de ACME sin cifrar. Además también deben ser cifradas las comunicaciones entre ambas compañías.

Cloud debe controlar el acceso de sus empleados a los datos de ACME, asegurando que hay mecanismos de control que permitan saber quién accede a esa información y qué hace con ella. Tanto en el proceso de las copias de seguridad como en el mantenimiento de la base de datos.

1.3.4. ¿En qué circunstancias crees que no sería aceptable un escenario de este estilo, es decir, la compañía no podría plantearse el externalizar este tipo de servicios?

Cuando la información que manejara ACME fuera especialmente sensible o no se pudiera permitir ningún fallo ni pérdida de la misma. Por ejemplo historiales clínicos de pacientes, información fiscal sobre ciudadanos, datos gubernamentales, militares o policiales.

1.4. Crea una instancia cloud de MongoDB (Atlas) y da de alta usuarios ficticios implementando los diferentes roles que has definido en el apartado 1.1. Incluye una captura de pantalla de dichos usuarios en tu respuesta a esta pregunta.

Hemos creado un rol de MongoDB para cada uno de los agentes que habíamos enunciado. A continuación hay una captura con los roles y otra con usuarios asignados a los roles en cuestión.

UNAI'S ORG - 2019-10-13 > PROJECT 0

Database Access

MongoDB Users	MongoDB Roles
Role Name ↕	Granted Actions and Roles
Contabilidad_Responsable	read @ACME
Recursos_Humanos_Responsable	readWrite @ACME
Sistemas_Administrador	readWrite @ACME
Base_de_Datos_Administrador	useUUID @all databases (all collections) listSessions @all databases (all collections) killAnySession @all databases (all collections) connPoolStats @all databases (all collections) listDatabases @all databases (all collections) serverStatus @all databases (all collections) top @all databases (all collections) dbAdminAnyDatabase @admin readWriteAnyDatabase @admin readAnyDatabase @admin clusterMonitor @admin backup @admin enableSharding @admin

Figura 1. Roles de MongoDB con sus acciones asociadas.

UNAI'S ORG - 2019-10-13 > PROJECT 0

Database Access

MongoDB Users		MongoDB Roles
User Name ↕	Authentication Method ▲	MongoDB Roles
🔑 conta_resp	SCRAM	Contabilidad_Responsable@admin
🔑 dba	SCRAM	Base_de_Datos_Administrador@admin
🔑 rrrh_resp	SCRAM	Recursos_Humanos_Responsable@admin
🔑 sys_admin	SCRAM	Sistemas_Administrador@admin

Figura 2. Usuarios de MongoDB con sus roles asignados.

¿Cuáles de las medidas de seguridad propuestas en el apartado 12 puedes implementar en la instancia de Cloud MongoDB?

Casi todas son posibles, las que dependen de los medios físicos en la parte del cliente, como los controles biométricos, no dependen de MongoDB y supondremos que se podrían implementar.

A continuación una lista de las medidas con posibilidades de implementación:

- Encriptación de las comunicaciones: la conexión a la base de datos está protegida con certificados por (SSL/TLS) a través de https [7].
- Contraseñas para acceder al software que se comunicará con la base de datos y gestión de las claves de los usuarios: se encriptan por medio de funciones de “hashing” con “salt” (SCRAM) [8] o con certificados (SSL/TLS).
- Firewalls y control de acceso para las comunicaciones desde el exterior: MongoDB tiene una lista de direcciones IP permitidas (“whitelist”) para el acceso a la base de datos.
- Antivirus y sistemas operativos actualizados. En la parte del cliente la tenemos, suponemos que también está en la parte del servidor.
- Sistemas de Autenticación de usuarios que guarden registros de actividades de los mismos: hay una lista de todas las acciones que se van llevando a cabo sobre el proyecto y las bases de datos.
- Seudonimización de la información y encriptación de los ficheros de la base de datos: los ficheros del servidor están encriptados, además permite añadir otra capa de seguridad con nuestras propias claves de encriptado.
- Limitar el número de usuarios: tenemos control sobre la creación de los mismos, además hay un límite al número de conexiones a la base de datos.

2. Arquitecturas de bases de datos (5 puntos)

En primer lugar, es necesario instalar una versión de Oracle 12c.

Hemos utilizado Windows 10 de 64 bits con un procesador i7-7800X Quad Core con CPUs a 3.50 Ghz y 16GB de RAM.

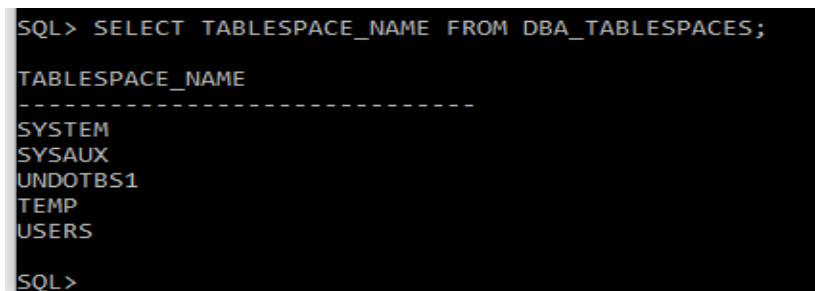
Tras la instalación, contestad a las siguientes cuestiones:

2.1. ¿Qué bases de datos (tablespaces) hay creadas por defecto?

Hay 5 bases de datos que se crean por defecto [9]:

- SYSTEM: Contiene el diccionario de datos de toda la base de datos.
- SYSAUX: Componentes opcionales de la base de datos (auxiliar de SYSTEM).
- UNDOTBS1: Información de antes de realizar cambios, para poder deshacer los mismos.
- TEMP: Almacenan información con poco tiempo de vida, como tablas globales temporales o resultados cortos de procesar sentencias SQL.
- USERS: Guarda objetos y datos permanentes de los usuarios.

Para visualizarlas hemos usado la sentencia SQL: “SELECT tablespace_name FROM dba_tablespaces;”



```
SQL> SELECT TABLESPACE_NAME FROM DBA_TABLESPACES;
TABLESPACE_NAME
-----
SYSTEM
SYSAUX
UNDOTBS1
TEMP
USERS
SQL>
```

Figura 3. Tablespaces creados por defecto.

2.2. ¿Dónde se encuentran los metadatos del sistema de base de datos? ¿Qué tablas destacarías?

Los metadatos son el diccionario de datos, describen las estructuras de la base de datos. Se componen de un número de tablas y vistas, que dependiendo de la versión pueden llegar hasta el millar.

Están almacenados principalmente en la tabla SYSTEM, aunque algunos componentes se encuentran en la tabla SYSAUX [10], esas dos tablas serían las más destacadas.

2.3. ¿Qué usuarios de base de datos crea por defecto? ¿Qué permisos tienen dichos usuarios?

Por defecto se crean 36 usuarios. La mayoría de ellos están bloqueados.

Los únicos que empiezan desbloqueados son “SYSTEM” y “SYS”.

La sentencia SQL para obtenerlos sería: “SELECT username FROM dba_users;”

```
SQL> SELECT USERNAME FROM DBA_USERS;

USERNAME
-----
SYS
SYSTEM
XS$NULL
OJVMSYS
LBACSYS
OUTLN
SYS$UMP
DBSNMP
APPOSSYS
DBSFUSER
GGSYS

USERNAME
-----
ANONYMOUS
```

Figura 4. Primeros 11 usuarios por defecto.

Los privilegios de los roles comunes se almacenan en la tabla “dba_sys_privs” se pueden obtener con la sentencia SQL: “SELECT * FROM dba_sys_privs;” [11].

A continuación una captura con los privilegios del usuario “SYSTEM”:

```
SQL> SELECT * FROM DBA_SYS_PRIVS WHERE GRANTEE = 'SYSTEM';

GRANTEE PRIVILEGE                                ADM COM INH
-----
SYSTEM CREATE MATERIALIZED VIEW                  NO YES NO
SYSTEM CREATE TABLE                            NO YES NO
SYSTEM UNLIMITED TABLESPACE                   NO YES NO
SYSTEM GLOBAL QUERY REWRITE                     NO YES NO
SYSTEM MANAGE ANY QUEUE                         YES YES NO
SYSTEM ENQUEUE ANY QUEUE                       YES YES NO
SYSTEM SELECT ANY TABLE                       NO YES NO
SYSTEM DEQUEUE ANY QUEUE                       YES YES NO

8 filas seleccionadas.

SQL>
```

Figura 5. Privilegios del usuario “SYSTEM”

2.4. ¿Qué puertos tiene a la escucha? ¿Cuál es la función de cada uno de los procesos a la escucha? ¿Cómo pueden desactivarse?

En el puerto 5500 se encuentra el Oracle Enterprise Manager Database Express: una interfaz web que permite varias gestiones con la base de datos; como listar los usuarios y sus privilegios o visualizar estadísticas de rendimiento.

En el puerto 49152 está el servicio OraMTS, que permite el uso de las bases de datos de Oracle como recursos por el Coordinador de transacciones distribuidas de Microsoft (MSDTC). El servicio OraMTS no está creado por defecto.

En el puerto 1521 está el Listener de Oracle, que espera conexiones de clientes y gestiona el tráfico de dichas conexiones con el servidor de la base de datos. Se puede desactivar desde la línea de comandos con la instrucción “lsnrctl STOP [nombre_listener]” [12].

Además de estos, hay otros puertos para componentes de Oracle [13], pero al no estar activos en nuestra instalación, los vamos a obviar.

2.5. ¿En qué directorio se encuentran los binarios? ¿Y los archivos de datos?

Los binarios están en la carpeta “/bin” situada dentro de la estructura de la base de datos. En nuestro caso la ruta es “C:\app\unai\virtual\product\12.2.0\dbhome_1\bin”.

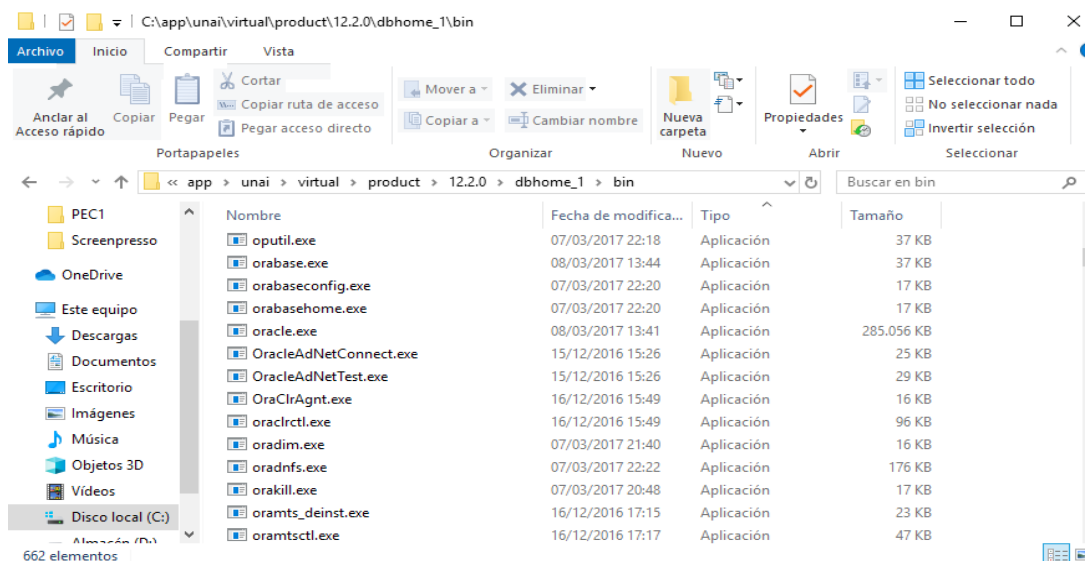


Figura 6. Binarios de la base de datos.

Los archivos de datos, con extensión DBF, están en la carpeta “oradata\[nombre base de datos]” de la instalación de la base de datos. La ruta en nuestra máquina es “C:\app\unai\virtual\oradata\orclglb”. Además, dentro de cada carpeta de la imagen hay una estructura similar.

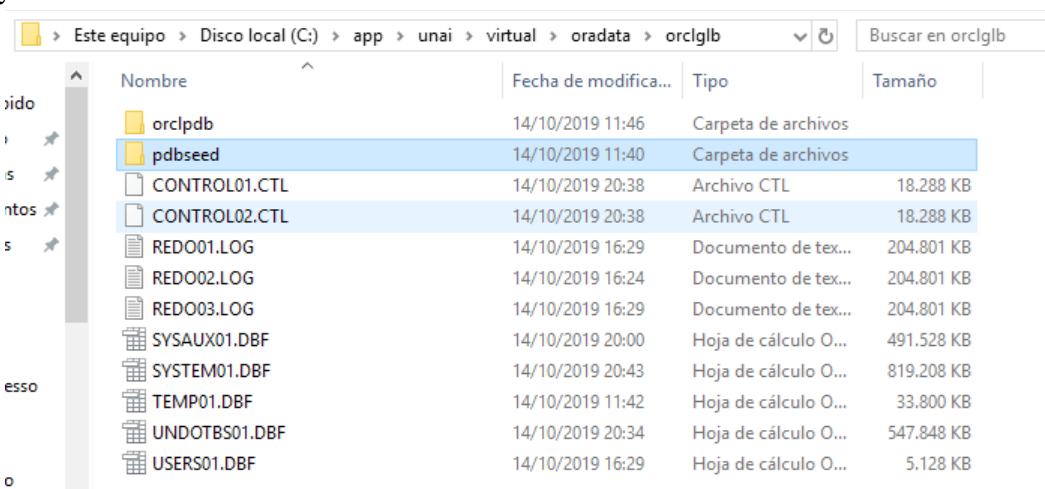


Figura 7. Archivos de Datos.

2.6. ¿Con qué permisos se ejecuta el proceso de base de datos en el sistema?

El proceso “oracle.exe” se ejecuta como un servicio por el usuario “OracleServiceORCLGLB”, con una prioridad normal.

2.7. ¿Qué opciones de configuración, en cuanto a seguridad, se ofrecen durante la instalación?

El primer cuadro de diálogo de la instalación nos permite introducir nuestro correo electrónico para recibir información sobre los problemas de seguridad y actualizaciones de seguridad.

Unos pasos más tarde nos permite configurar una contraseña para el administrador de la base de datos Global.

En segundo lugar, vamos a instalar Mongo DB.

2.8 Compara las opciones de seguridad disponibles durante la instalación de Mongo DB con las que has descrito en la pregunta 2.7.

A diferencia de Oracle, durante la instalación no se ha instado a crear una contraseña para el administrador.

La única seguridad que se proporciona durante la instalación es la de poder crear el servicio de la base de datos como un usuario local o de dominio y especificar las credenciales. En nuestro caso lo hemos creado como un servicio de red.

2.9 ¿Qué puertos tiene por defecto a la escucha? ¿Cuál es la función de cada uno de los procesos a la escucha? ¿Cómo pueden desactivarse?

En el puerto 27017 está el proceso principal de la base de datos, que espera conexiones de clientes. Para desactivarlo habría que detener el servicio.

Existe la posibilidad de activar los puertos 27018 y 27019 [14], pero con nuestra configuración no es así

2.10 ¿Con qué permisos se ejecuta MongoDB en el sistema?

El servicio de red se ejecuta con permisos de usuario normal.

2.11 ¿En qué directorio se encuentran los binarios? ¿Y los archivos de datos?

Los binarios están en la ruta que viene por defecto, en nuestra máquina es “C:\Program Files\MongoDB\Server\4.2\bin”.

Nombre	Fecha de modifica...	Tipo	Tamaño
bsondump.exe	09/08/2019 5:05	Aplicación	13.544 KB
mongo.exe	09/08/2019 5:25	Aplicación	22.770 KB
mongocryptd.exe	09/08/2019 5:38	Aplicación	13.682 KB
mongod.exe	09/08/2019 5:37	Aplicación	35.504 KB
mongodcrypt.exe	09/08/2019 5:39	Aplicación	10.770 KB
mongodump.exe	09/08/2019 5:06	Aplicación	20.914 KB
mongoexport.exe	09/08/2019 5:06	Aplicación	20.546 KB
mongofiles.exe	09/08/2019 5:06	Aplicación	20.472 KB
mongoimport.exe	09/08/2019 5:06	Aplicación	20.796 KB
mongoldap.exe	09/08/2019 5:38	Aplicación	10.946 KB
mongorestore.exe	09/08/2019 5:06	Aplicación	21.382 KB
mongos.exe	09/08/2019 5:36	Aplicación	18.174 KB
mongostat.exe	09/08/2019 5:06	Aplicación	20.097 KB
mongotop.exe	09/08/2019 5:06	Aplicación	19.667 KB

Figura 8. Binarios de MongoDB.

En cuanto a los archivos de datos, en la instalación nos dejan configurar la localización, hemos dejado el que viene por defecto. En nuestro caso “C:\Program Files\MongoDB\Server\4.2\data”

Nombre	Fecha de modifica...	Tipo	Tamaño
diagnostic.data	14/10/2019 21:52	Carpeta de archivos	
journal	14/10/2019 21:13	Carpeta de archivos	
_mdb_catalog.wt	14/10/2019 21:48	Archivo WT	36 KB
collection-0--5466001323503814062.wt	14/10/2019 21:14	Archivo WT	20 KB
collection-2--5466001323503814062.wt	14/10/2019 21:14	Archivo WT	20 KB
collection-4--5466001323503814062.wt	14/10/2019 21:48	Archivo WT	36 KB
collection-8--5466001323503814062.wt	14/10/2019 21:48	Archivo WT	20 KB
collection-10--5466001323503814062.wt	14/10/2019 21:49	Archivo WT	36 KB
index-1--5466001323503814062.wt	14/10/2019 21:14	Archivo WT	20 KB
index-3--5466001323503814062.wt	14/10/2019 21:14	Archivo WT	20 KB
index-5--5466001323503814062.wt	14/10/2019 21:28	Archivo WT	20 KB
index-6--5466001323503814062.wt	14/10/2019 21:48	Archivo WT	36 KB
index-9--5466001323503814062.wt	14/10/2019 21:48	Archivo WT	20 KB
index-11--5466001323503814062.wt	14/10/2019 21:48	Archivo WT	20 KB

Figura 9. Archivos de Datos de MongoDB.

Por último, veamos cuales deberían ser los criterios para decantarse por uno u otro tipo de base de datos:

2.12 Completa la siguiente tabla:

Base de Datos	Principales características	¿En qué casos deberíamos considerar su uso?	Aspectos de seguridad más relevantes a tener en cuenta
Oracle	Muchas versiones. Muchas plataformas. Autenticación diversa.	Producto muy veterano. Buen soporte. Variedad de productos. Mucho software que da funcionalidades extras.	TNS Listener puede estar desprotegido. Oracle Intelligent Agent no necesita autenticación y da información útil Históricamente vulnerable a inyecciones SQL.
Mongo DB	Usa Javascript en vez de procedimientos. No tiene diccionario de datos. Escrita en C++. Fácil de administrar.	Aplicaciones pequeñas o con poca carga. Entornos de estudio.	Por defecto se instala sin autenticación por contraseña. Cualquier usuario tiene acceso de lectura a toda la base de datos. No hay encriptación de datos.
HP Vertica	Separa la computación del almacenaje. Arquitectura Cloud.	Manejo de grandes cantidades de información que crecen rápidamente. Mejor respuesta a consultas que las bases relacionales.	Problemas con alta concurrencia. Hay un proceso que no requiere autenticación y permite ejecutar código arbitrario remotamente.
Neo4j	Código Abierto. Gestiona bases de datos de gráficos.	Rendimiento constante de tiempo real. Diccionario de datos flexible.	No hay distribución de la información, cada nodo necesita todos los datos.
Elastic Search	Código Abierto. Trabaja sobre JSON en HTTP. Fácilmente escalable.	Tiempos de respuesta casi óptimos. Publicación de documentos rápida para poder hacer búsquedas sobre ellos.	Vulnerable a Cross Site Request Forgery (CSRF). No trae por defecto una estructura de autenticación y validación.

Bibliografía y Enlaces

1. Reglamento General de Protección de Datos

[Consulta: 12 de Octubre de 2019].

<<https://www.boe.es/doue/2016/119/L00001-00088.pdf>>

2. Puestos y responsabilidades del personal de base de datos

[Consulta: 12 de Octubre de 2019].

<<https://es.slideshare.net/rumus1000/puestos-y-responsabilidades-del-personal-de-base-de-datos>>

3. What Is Database Security And Why Is It Important?

[Consulta: 12 de Octubre de 2019].

<<https://www.gasystems.com.au/database-security-important/>>

4. Puestos y responsabilidades del personal de base de datos (Presentación).

[Consulta: 12 de Octubre de 2019].

<<https://dzone.com/articles/10-common-database-security-issues>>

5. Puestos y responsabilidades del personal de base de datos (Presentación).

[Consulta: 12 de Octubre de 2019].

<<https://www.datacenterknowledge.com/archives/2016/06/09/why-outsource-application-and-database-management>>

6. Reglamento General de Protección de Datos Y listado de empresas de protección de datos.

[Consulta: 12 de Octubre de 2019].

<<https://rgpd.es/>>

7. La guía final ¿Qué son SSL,TLS y HTTPS?

[Consulta: 13 de Octubre de 2019].

<<https://www.websecurity.symantec.com/es/es/security-topics/what-is-ssl-tls-https>>

8. How to Use SCRAM-SHA1 as Authentication Method in MongoDB.

[Consulta: 13 de Octubre de 2019].

<<https://medium.com/mongoaudit/how-to-use-scrum-sha1-as-authentication-method-in-mongodb-580f7251168>>

9. Oracle Help Center. Database 2 Day DBA. - 6.1.6 About Tablespaces.

[Consulta: 14 de Octubre de 2019].

<<https://docs.oracle.com/database/121/ADMQS/GUID-F05EE514-FFC6-4E86-A592-802BA5A49254.htm#ADMQS12053>>

10. The Architecture of the Data Dictionary.

[Consulta: 14 de Octubre de 2019].

<http://www.dba-oracle.com/concepts/data_dictionary.htm>

11. How to Show All Oracle Database Privileges for a User.

[Consulta: 14 de Octubre de 2019].

<<https://chartio.com/resources/tutorials/oracle-user-privileges--how-to-show-all-privileges-for-a-user/>>

12. Oracle Net Listener Configuration

[Consulta: 14 de Octubre de 2019].

<<https://docs.oracle.com/en/database/oracle/oracle-database/12.2/ntcli/creating-the-oramts-service-for-microsoft-transaction-server.html#GUID-E35C0875-1632-4A95-9CAD-94B09972F15B>>

13. Port Numbers and Protocols of Oracle Components

[Consulta: 14 de Octubre de 2019].

<<https://docs.oracle.com/database/121/RILIN/ports.htm#RILIN1181>>

14. Default MongoDB Port.

[Consulta: 14 de Octubre de 2019].

<<https://docs.mongodb.com/manual/reference/default-mongodb-port/>>