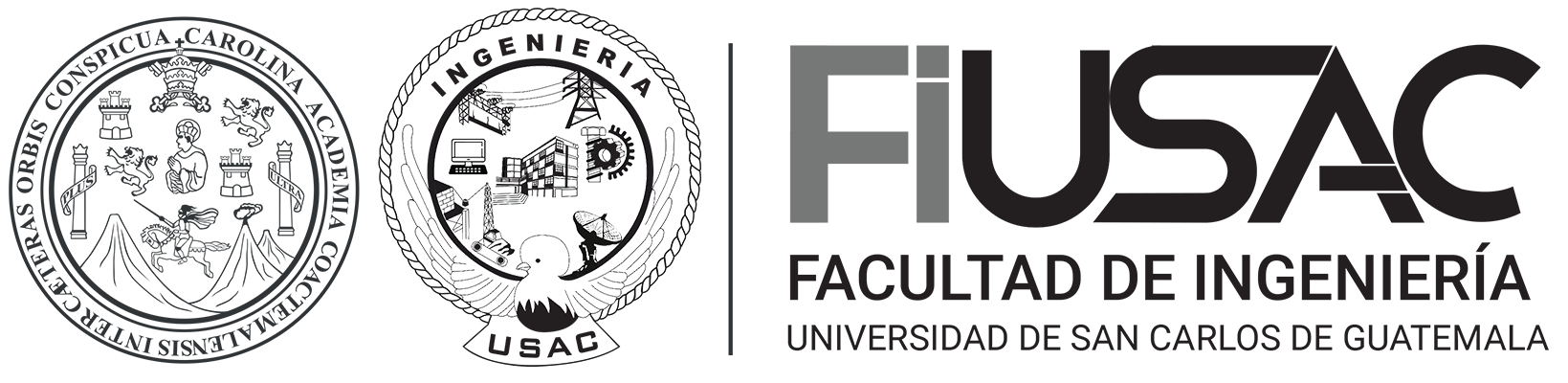
**Forma

Descripción generada automáticamente con confianza bajaUNIVERSIDAD DE SAN CARLOS DE GUATEMALA**

**FACULTAD DE INGENIERÍA**

**ESCUELA DE CIENCIAS Y SISTEMAS**

**LABORATORIO SISTEMAS DE BASES DE DATOS 1**



**TAREA 2 – SEGURIDAD EN SQL**

**NOMBRE: Alvaro Emmanuel Socop Pérez**

**CARNE: 202000194**

**FECHA: viernes, 28 de octubre de 2022**

**CONTENIDO**

**SEGURIDAD EN SQL**

**PROTOCOLOS PROCEDIMIENTOS O PRACTICAS PARA GARANTIZAR QUE UNA BASE DE DATOS SEA SEGURA**

1. **Limitar el acceso a la base de datos**

**Una parte esencial para tener control de acceso es el primer paso para mantener a los atacantes lejos de nuestra información. Por ejemplo en la facultad de INGENIERIA faltaria una restriccion de seguridad en la pagina de RegyED para que sea mas segura la recuperacion de PIN y con mayor encriptacion de datos.**

**Además de esto se debe agregar que se necesitan permisos básicos como en cualquier sistema, en este caso también se debe considerar:**

* **Limitar el acceso a los datos sensibles tanto por parte de los usuarios como de los procedimientos, es decir, que solo determinados usuarios y procedimientos estén autorizados a realizar consultas en información sensible.**
* **Limitar el uso de los procedimientos importantes solo a usuarios específicos.**
* **Evitar las concurrencias y acceso fuera del horario laboral o habitual.**

1. **Identifica los datos sensibles y los datos críticos**

**No todos los datos que almacenamos son críticos o deben ser protegidos, por lo que no tiene sentido gastar tiempo y recursos en esta información.**

**Tener control de todo diria yo.**

**También es recomendable llevar un inventario de las bases de datos de la compañía, teniendo en cuenta todas las áreas. La única forma de tener una administración prolija y no perder información es tener conocimiento y registro de todas las instancias y bases de datos de la compañía.**

**Además, el inventario resulta especialmente útil al momento de hacer un respaldo de la información, para evitar que datos críticos queden fuera del esquema.**

**3. Cifrar la información**

**Otra buena práctica es**[**utilizar algoritmos robustos**](https://www.welivesecurity.com/la-es/2016/04/27/cifrado-bases-de-datos-mysql/)**para cifrar estos datos.**

**Cuando un atacante explota una vulnerabilidad y logra tener acceso a un servidor o un sistema, lo primero que intentará robar son las bases de datos. Son un tesoro codiciado, ya que normalmente mucho almacenamiento de valiosa información; la mejor manera de preservarla es volverla ilegible para cualquier persona que llegue a ella sin autorización.**

**2. Monitorea la actividad de tu base de datos**

**Ver bien,  y registrar las acciones y movimientos sobre los datos permite saber quién, qué, cuándo y cómo ha manipulado la información. Tener un historial completo de las transacciones asi comprendemos patrones en el acceso y modificación de los datos y así evitar fugas de información, controlar cambios fraudulentos y detectar acciones sospechosas en tiempo real.**

**La información que estas alojan es muy valiosa para la empresa y un botín codiciado para los atacantes, por lo que sin dudas merece toda tu atención.**

**5. Anonimiza las bases de datos de que no son productivas**

**Muchas empresas invierten tiempo y recursos en proteger sus bases de datos productivas, pero al momento de hacer un desarrollo o crear un entorno de pruebas, simplemente hacen una copia de la base original y comienzan a utilizarla en ambientes mucho menos controlados, exponiendo de esta manera toda la información sensible.**

**El enmascaramiento es un proceso mediante el cual se crea una versión similar, manteniendo la misma estructura que la original, pero alterando los datos sensibles para que permanezcan protegidos. A partir de esta técnica se cambian los valores respetando el formato.**

**Esta técnica es especialmente utilizada (y recomendada) para las bases de datos que forman parte de entornos de pruebas y desarrollo, ya que permite mantener la estructura lógica de los datos mientras garantiza que la información sensible del cliente no está disponible fuera del entorno de producción.**



**ROLES Y PRIVILEGIOS QUE PUEDE POSEER UN USUARIO O PERFIL**

**Para administrar con facilidad los permisos de las bases de datos, SQL Server proporciona varios roles que son las entidades de seguridad que agrupan a otras entidades de seguridad.**

**un rol puede ser creado con la siguiente seguridad:**

**\* Ninguna (Default)**

**\* Password**

**\* External**

**\* Global**

**Perfiles de Usuario**

**Los perfiles se utilizan para limitar la cantidad de recursos del sistema y de la BD disponibles para un usuario.**

|  |  |
| --- | --- |
| *Recurso* | *Descripción* |
| SESSIONES\_PER\_USER | El número de sesiones concurrentes que un usuario puede tener en una instancia. |
| CPU\_PER\_SESSION | El tiempo de CPU, en centenas de segundos, que una sesión puede utilizar. |
| CONNECT\_TIME | El número de minutos que una sesión puede permanecer activa. |
| IDLE\_TIME | El número de minutos que una sesión puede permanecer sin que sea utilizada de manera activa. |
| LOGICAL\_READS\_PER\_SESSION | El número de bloques de datos que se pueden leer en una sesión. |
| LOGICAL\_READS\_PER\_CALL | El número de bloques de datos que se pueden leer en una operación. |
| PRIVATE\_SGA | La cantidad de espacio privado que una sesión puede reservar en la zona de SQL compartido de la SGA. |
| COMPOSITE\_LIMIT | El número de total de recursos por sesión, en unidades de servicio. Esto resulta de un calculo ponderado de CPU\_PER\_SESSION, CONNECT\_TIME, LOGICAL\_READS\_PER\_SESSION y PRIVATE\_SGA, cuyos pesos se pueden variar con el comando ALTER RESOURCE COST. |

**Fuente: obtenido de infor.uva.es.**

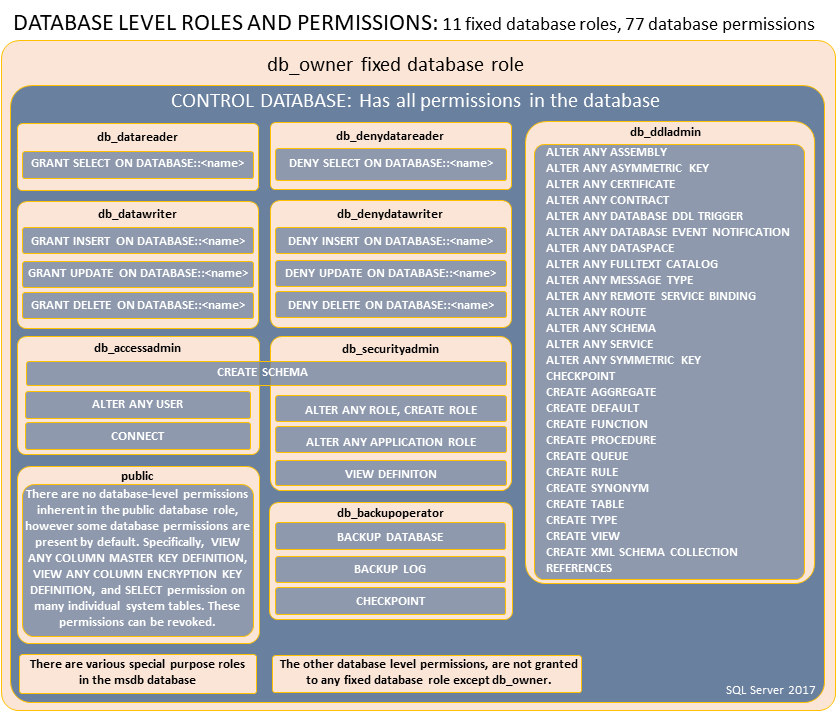
**Lista Completa de Privilegios en Oracle**

|  |  |
| --- | --- |
| Privilegio | Significado |
| Base de datos y sistema | |
| ALTER DATABASE | Modificar la base de datos (privilegio de gran capacidad administrativa) |
| ALTER SYSTEM | Modificar los parámetros del sistema |
| AUDIT SYSTEM | Auditar la base de datos |
| Usuarios, roles, privilegios y perfiles | |
| CREATE USER | Crear usuarios pudiendo indicar tablespace por defecto, cuotas y perfiles |
| ALTER USER | Modificar al usuario. Permite cambiar la contraseña y modo de autentificación, tablespace por defecto, cuota de uso de disco, roles y el perfil del usuario |
| DROP USER | Borrar usuario |
| CREATE PROFILE | Crear perfiles |
| ALTER PROFILE | Modificar perfiles |
| DROP PROFILE | Borrar perfiles |
| CREATE ROLE | Crear roles |
| ALTER ANY ROLE | Modificar roles |
| GRANT ANY ROLE | Conceder roles |
| GRANT ANY PRIVILEGE | Conceder privilegios de sistema |
| Extraído de fuente Oracle hoy | |

**Roles fijos de base de datos**

**roles fijos de base de datos y sus funcionalidades.**

|  |  |
| --- | --- |
| Nombre del rol fijo de base de datos | Descripción |
| db\_owner | Los miembros del rol fijo de base de datos **db\_owner** pueden realizar todas las actividades de configuración y mantenimiento en la base de datos y también pueden quitar la base de datos en dropSQL Server. (En SQL Database y Azure Synapse, algunas actividades de mantenimiento requieren permisos de nivel de servidor y los roles **db\_owners** no las pueden realizar). |
| db\_securityadmin | Los miembros del rol fijo de base de datos **db\_securityadmin** pueden modificar la pertenencia a roles únicamente para roles personalizados y administrar permisos. Los miembros de este rol pueden elevar potencialmente sus privilegios y se deben supervisar sus acciones. |
| db\_accessadmin | Los miembros del rol fijo de base de datos **db\_accessadmin** pueden agregar o quitar el acceso a la base de datos para inicios de sesión de Windows, grupos de Windows e inicios de sesión de SQL Server . |
| db\_backupoperator | Los miembros del rol fijo de base de datos **db\_backupoperator** pueden crear copias de seguridad de la base de datos. |
| db\_ddladmin | Los miembros del rol fijo de base de datos **db\_ddladmin** pueden ejecutar cualquier comando del lenguaje de definición de datos (DDL) en una base de datos. Los miembros de este rol pueden elevar potencialmente sus privilegios manipulando el código que puede ejecutarse con privilegios elevados y se deben supervisar sus acciones. |
| db\_datawriter | Los miembros del rol fijo de base de datos **db\_datawriter** pueden agregar, eliminar o cambiar datos en todas las tablas de usuario. |
| db\_datareader | Los miembros del rol fijo de base de datos **db\_datareader** pueden leer todos los datos de todas las tablas y vistas de usuario. Los objetos de usuario pueden existir en cualquier esquema, excepto *sys* e *INFORMATION\_SCHEMA*. |
| db\_denydatawriter | Los miembros del rol fijo de base de datos **db\_denydatawriter** no pueden agregar, modificar ni eliminar datos de tablas de usuario de una base de datos. |
| db\_denydatareader | Los miembros del rol fijo de base de datos **db\_denydatareader** no pueden leer datos de las tablas y vistas de usuario dentro de una base de datos. |



**Fuente: Obtenido de pagina oficial de Microsoft.**

**Roles especiales para SQL Database y Azure Synapse**

**solo existen en la base de datos maestra virtual.**

|  |  |
| --- | --- |
| Nombre de rol | Descripción |
| dbmanager | Puede crear y eliminar bases de datos. Un miembro del rol dbmanager que crea una base de datos se convierte en el propietario de dicha base de datos, lo que permite que el usuario se conecte a ella como el usuario dbo. El usuario dbo tiene todos los permisos de base de datos en la base de datos. Los miembros del rol dbmanager no necesariamente tienen permiso para acceder a las bases de datos que no son de su propiedad. |
| db\_exporter | *Solo se aplica a grupos de SQL dedicados de Azure Synapse Analytics (anteriormente SQL DW).* Los miembros del rol de base de datos fijo **db\_exporter** pueden realizar todas las actividades de exportación de datos. Los permisos concedidos a través de este rol son CREATE TABLE, ALTER ANY SCHEMA, ALTER ANY EXTERNAL DATA SOURCE, ALTER ANY EXTERNAL FILE FORMAT. |
| loginmanager | Puede crear y eliminar inicios de sesión en la base de datos maestra virtual. |

**Roles de msdb**

|  |  |
| --- | --- |
| Nombre de rol de msdb | Descripción |
| **db\_ssisadmin**  **db\_ssisoperator**  **db\_ssisltduser** | Los miembros de estos roles de base de datos pueden administrar y utilizar SSIS. Las instancias de SQL Server que se actualizan desde una versión anterior podrían contener una versión anterior del rol cuya denominación se realizaba al usar Servicios de transformación de datos (DTS) en lugar de SSIS. Para obtener más información, consulte [Roles de Integration Services (servicio SSIS)](https://learn.microsoft.com/es-es/sql/integration-services/security/integration-services-roles-ssis-service?view=sql-server-ver16). |
| **dc\_admin**  **dc\_operator**  **dc\_proxy** | Los miembros de estos roles de base de datos pueden administrar y utilizar el recopilador de datos. Para obtener más información, consulte [Data Collection](https://learn.microsoft.com/es-es/sql/relational-databases/data-collection/data-collection?view=sql-server-ver16). |
| **PolicyAdministratorRole** | Los miembros del rol de base de datos **db\_ PolicyAdministratorRole** pueden realizar todas las actividades de mantenimiento y configuración en las condiciones y directivas de Administración basada en directivas. Para obtener más información, vea [Administrar servidores mediante administración basada en directivas](https://learn.microsoft.com/es-es/sql/relational-databases/policy-based-management/administer-servers-by-using-policy-based-management?view=sql-server-ver16). |
| **ServerGroupAdministratorRole**  **ServerGroupReaderRole** | Los miembros de estos roles de base de datos pueden administrar y utilizar grupos de servidores registrados. |
| **dbm\_monitor** | Se crea en la base de datos **msdb** cuando se registra la primera base de datos en el Monitor de creación de reflejo de la base de datos. El rol **dbm\_monitor** no tiene miembros hasta que un administrador del sistema asigna usuarios al rol. |

**EXTRA EXTRA!**

**vistas y las funciones que se usan para trabajar con los roles de nivel de base de datos.**

|  |  |  |
| --- | --- | --- |
| Característica | Tipo | Descripción |
| [sp\_helpdbfixedrole (Transact-SQL)](https://learn.microsoft.com/es-es/sql/relational-databases/system-stored-procedures/sp-helpdbfixedrole-transact-sql?view=sql-server-ver16) | Metadatos | Devuelve la lista de los roles fijos de base de datos. |
| [sp\_dbfixedrolepermission (Transact-SQL)](https://learn.microsoft.com/es-es/sql/relational-databases/system-stored-procedures/sp-dbfixedrolepermission-transact-sql?view=sql-server-ver16) | Metadatos | Muestra los permisos de un rol fijo de base de datos. |
| [sp\_helprole (Transact-SQL)](https://learn.microsoft.com/es-es/sql/relational-databases/system-stored-procedures/sp-helprole-transact-sql?view=sql-server-ver16) | Metadatos | Devuelve información acerca de los roles de la base de datos actual. |
| [sp\_helprolemember (Transact-SQL)](https://learn.microsoft.com/es-es/sql/relational-databases/system-stored-procedures/sp-helprolemember-transact-sql?view=sql-server-ver16) | Metadatos | Devuelve información acerca de los miembros de un rol de la base de datos actual. |
| [sys.database\_role\_members (Transact-SQL)](https://learn.microsoft.com/es-es/sql/relational-databases/system-catalog-views/sys-database-role-members-transact-sql?view=sql-server-ver16) | Metadatos | Devuelve una fila por cada miembro de cada rol de base de datos. |
| [IS\_MEMBER (Transact-SQL)](https://learn.microsoft.com/es-es/sql/t-sql/functions/is-member-transact-sql?view=sql-server-ver16) | Metadatos | Indica si el usuario actual es miembro del grupo de Microsoft Windows o del rol de base de datos de SQL Server especificados. |
| [CREATE ROLE (Transact-SQL)](https://learn.microsoft.com/es-es/sql/t-sql/statements/create-role-transact-sql?view=sql-server-ver16) | Get-Help | Crea un rol de base de datos nuevo en la base de datos actual. |
| [ALTER ROLE (Transact-SQL)](https://learn.microsoft.com/es-es/sql/t-sql/statements/alter-role-transact-sql?view=sql-server-ver16) | Get-Help | Cambia el nombre o la pertenencia de un rol de base de datos. |
| [DROP ROLE (Transact-SQL)](https://learn.microsoft.com/es-es/sql/t-sql/statements/drop-role-transact-sql?view=sql-server-ver16) | Get-Help | Quita un rol de la base de datos. |
| [sp\_addrole (Transact-SQL)](https://learn.microsoft.com/es-es/sql/relational-databases/system-stored-procedures/sp-addrole-transact-sql?view=sql-server-ver16) | Get-Help | Crea un rol de base de datos nuevo en la base de datos actual. |
| [sp\_droprole (Transact-SQL)](https://learn.microsoft.com/es-es/sql/relational-databases/system-stored-procedures/sp-droprole-transact-sql?view=sql-server-ver16) | Get-Help | Quita un rol de base de datos de la base de datos actual. |
| [sp\_addrolemember (Transact-SQL)](https://learn.microsoft.com/es-es/sql/relational-databases/system-stored-procedures/sp-addrolemember-transact-sql?view=sql-server-ver16) | Get-Help | Agrega un usuario de base de datos, un rol de base de datos, un inicio de sesión de Windows o un grupo de Windows a un rol de base de datos en la base de datos actual. Todas las plataformas, excepto Sistema de la plataforma de análisis (PDW) y Azure Synapse, deben usar ALTER ROLE en su lugar. |
| [sp\_droprolemember (Transact-SQL)](https://learn.microsoft.com/es-es/sql/relational-databases/system-stored-procedures/sp-droprolemember-transact-sql?view=sql-server-ver16) | Get-Help | Quita una cuenta de seguridad de un rol de SQL Server de la base de datos actual. Todas las plataformas, excepto Sistema de la plataforma de análisis (PDW) y Azure Synapse, deben usar ALTER ROLE en su lugar. |
| [GRANT](https://learn.microsoft.com/es-es/sql/t-sql/statements/grant-transact-sql?view=sql-server-ver16) | Permisos | Agrega el permiso a un rol. |
| [DENY](https://learn.microsoft.com/es-es/sql/t-sql/statements/deny-transact-sql?view=sql-server-ver16) | Permisos | Deniega un permiso a un rol. |
| [REVOKE](https://learn.microsoft.com/es-es/sql/t-sql/statements/revoke-transact-sql?view=sql-server-ver16) | Permisos | Quita los permisos concedido o denegados anteriormente. |

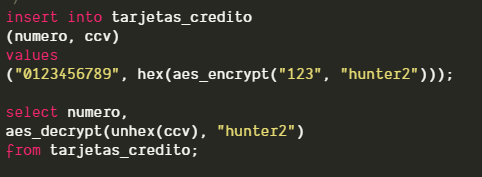
**TIPOS DE ENCRIPTACION**

**MYSQL: SHA1 Y SHA2**

**MySQL permite cifrar y descifrar datos utilizando el algoritmo AES a través de las funciones aes\_encrypt y aes\_decrypt**

**aes\_encrypt("texto\_plano", "clave") Y: aes\_decrypt("texto\_cifrado", "clave")**

**al encriptar se devuelven datos binarios, así que hay que definir (dentro de la tabla) el tipo de dato como BLOB**

****

**si la encriptación de datos es distinta por usuario haz que la clave sea algo como un hash con su contraseña, o cosas de esas. Si la encriptación es general, usa la misma clave para todos, pero mantenla en un lugar seguro.**

**ORACLE:**

**El cifrado de datos transparente de Oracle admite dos modos de cifrado: el cifrado de espacios de tabla de TDE y el cifrado de columnas de TDE. El cifrado de espacios de tabla de TDE se utiliza para cifrar tablas de aplicaciones completas.**

**Los algoritmos de encriptación de datos que Oracle soporta son los siguientes:**

* **Algoritmos DES**
* **Triple DES**
* **Texto

  Descripción generada automáticamenteRSA (el más rápido actualmente)**

**Oracle, como en el módulo Advanced Security en versiones Enterprise nos garantiza un nivel alto de seguridad.**

**El Estándar de Cifrado Avanzado (Advanced Encryption Standard, AES), también conocido como Rijndael, el cual es su nombre original, es una especificación establecida en 2001 para el cifrado de datos electrónicos.**

**SQL SERVER:**

**SQL Server ofrece dos maneras de encriptar los datos:**

1. **Encriptación de Datos Transparente (Transparent Data Encryption, TDE)**

**permite encriptar una base de datos complete. TDE protege la base de datos contra accesos no autorizados a los discos duros o copias de seguridad en las cuales la base de datos está almacenada. Cuando ENCRIPTA datos muestra problemas de desempeño resultando en un uso significativamente incrementado de CPU durante, por ejemplo, operaciones de copia de seguridad.**

1. **Encriptación de Copia de Seguridad**

**La encriptación de copias de seguridad SQL Server soporta la encriptación de copias de seguridad de base de datos directamente desde el motor de la base de datos. En el caso de la característica de Encriptación de Copia de Seguridad, es realizada sólo cuando se hace una copia de seguridad y cuando se restaura una base de datos, por tanto, no hay problemas de desempeño.**

La primera capa de jerarquía es la Clave Maestra de Servicio (Service Master Key, SMK). La Clave Maestra de Servicio es generada automáticamente durante la instalación de SQL Server y almacenada en la base de datos maestra del sistema.

La siguiente capa es una Clave Maestra de Base de Datos (Database Master Key, DMK) de a base de datos maestra.

**BIBLIOGRAFÌA**

<https://www.welivesecurity.com/la-es/2017/09/05/consejos-bases-de-datos-seguras/>

<https://learn.microsoft.com/es-es/sql/relational-databases/security/authentication-access/database-level-roles?view=sql-server-ver16>

s, V. (2022, 18 agosto). *Roles de nivel de base de datos - SQL Server*. Microsoft Learn. Recuperado 19 de septiembre de 2022, de <https://learn.microsoft.com/es-es/sql/relational-databases/security/authentication-access/database-level-roles?view=sql-server-ver16>

<http://marcosreyeszeta.blogspot.com/2009/10/privilegios-roles-y-perfiles.html>

*Jorge Sánchez. Manual de Administración de Bases de Datos. Administración de usuarios en Oracle Database*. (s. f.). Recuperado 19 de septiembre de 2022, de <https://jorgesanchez.net/manuales/abd/control-usuarios-oracle.html>

<https://parzibyte.me/blog/2019/06/01/cifrado-datos-mysql-aes/#:~:text=MySQL%20permite%20cifrar%20y%20descifrar,las%20funciones%20aes_encrypt%20y%20aes_decrypt%20.&text=De%20esta%20manera%20podemos%20proteger%20y%20asegurar%20datos%20utilizando%20AES>.

<https://docs.aws.amazon.com/es_es/AmazonRDS/latest/UserGuide/Appendix.Oracle.Options.AdvSecurity.html>