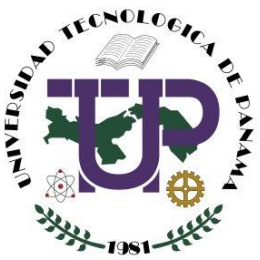
Universidad Tecnológica de Panamá

Facultad de Ing. de Sistemas Computacionales

Departamento de Sistemas de Información



Carrera: Licenciatura en Ingeniería en Sistemas de información

Cursado: Bases de Datos II

Profesor: Ing. Henry Lezcano

Investigación Final | Administración y Autentificación de Usuarios

Estudiantes:

Rolando Riley [8-972-1033]
Johel Batista [8-914-587]
Andrés Villareal [8-970-1267]
Miguel Pinilla [8-975-2460]

Grupo: 1IF-131

Fecha de Entrega: 10-11-2022

República de Panamá, II Semestre Académico 2022

Índice de Contenidos

Contenidos de la Investigación

Comentarios Iniciales

Uno de los problemas más grande que se presentan como una amenaza, a pesar de que la información “Data, en inglés”, se ha convertido en el “oro” del Siglo XXI; se convierte en la protección de la misma ante los ataques, así como accesos no deseados por parte de personas que no se encuentran autorizadas para acceder a los recursos críticos de cualquier empresa u organización, cuestión que incluso ha llevado a la pérdida de millones de dólares, como lo fue (Según la versión oficial), el tema de los mal llamados “Panama Papers”, dónde hubo un acceso no autorizado a la Base de Datos de una de las firmas de abogados más grandes del país, Mossack Fonseca, en la que se extrajeron más de 2.60TB de información de sus servidores.

Para esto, comienza a tomar auge un área altamente lucrativa para aquellos que la dominan en sobremanera como lo es la Seguridad Informática, quienes son los encargados de llevar la Protección de los Datos y la Información en contra a los accesos no autorizados, así como protegerlos para que se mantengan los principios de Integridad e Inmutabilidad en cada uno de ellos.

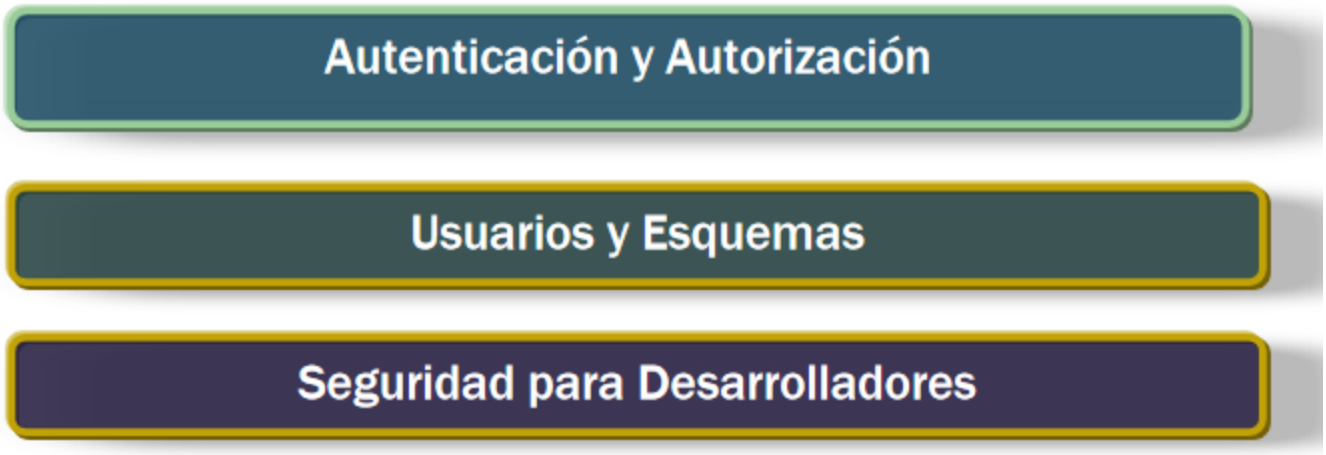


Figura N°1: Elementos Esenciales de la Protección de la Información (Universidad Don Bosco, 2022)

Conceptos como la Encriptación de Datos, Prácticas de la Gestión de Claves, e incluso el uso de elementos propios de la migración que se está dando en la Web 3.0 como la

Tokenización de los accesos y las autorizaciones de estos, que permiten el desarrollo de múltiples plataformas de gestión de la información.

Sin embargo, al final de todo, lo cual será el objeto de este trabajo investigativo, son Las personas, los Procesos internos de la Empresa/Organización y la Tecnología.

Cuentas de Usuario Bloqueadas y No Bloqueadas

Para efectos del Cursado de Sistemas de Bases de Datos II, en el Segundo Semestre Académico del Año 2022, dónde se ha impartido utilizando el lenguaje de Base de Datos PL/SQL, utilizaremos este como un elemento esencial de la investigación en curso, por lo que procederemos a describir ciertas tareas básicas de administración que se tienen que realizar para Gestionar los Usuarios de una Base de Datos PL/SQL:

- **Creación de Usuarios de Base de Datos**: A manera de que se vayan a crear usuarios en la base de datos, se debe conectar como usuario ADMIN, a través de cualquier herramienta de cliente SQL, sin embargo, una de las más utilizadas, ya sea en CLI (Command Line Interface) es SQLPLUS, mientras que a través del uso de una GUI (Graphical User Interface), Oracle recomienda el uso de SQL Developer, que en estos momentos se encuentra en su versión 16.
    - Al ejecutar la sentencia ***CREATE USER johel IDENTIFIED by contraseña;** así como GRANT CREATE SESSION TO johel; esto hace que se cree un nuevo usuario con privilegios de conexión a la Base de Datos, a lo que este puede ejecutar consultas, sin embargo, al no tener acceso de administrador total, se requieren temas como el otorgar privilegios adicionales al usuario en cuestión, lo cual es un tema que abordaremos posteriormente grosso modo.

Un tema de suma relevancia al momento de crear usuarios en una Base de Datos de tipo PL/SQL (Extrapolables a cualquier motor de Bases de Datos, es la creación de contraseñas seguras para sus usuarios, de manera que se han diseñado ciertas reglas de complejidad de contraseña por defecto:

- Todas las contraseñas deben poseer entre un mínimo de 12 y 30 caracteres de longitud, así como se debe incluir una letra en Mayúsculas, otra en Minúsculas y un Carácter Numérico.
- No se puede encontrar dentro de la contraseña, el nombre de usuario. Por ejemplo, si el nombre del usuario en cuestión es “johel”, la contraseña no podría ser “Johel273”, ya que esta a pesar del uso de las mayúsculas y minúsculas, incluye el nombre del usuario.
- Adicional a ello, es importante que, si se desea desbloquear la cuenta de un usuario específico en la Base de Datos, se debe conectar a ella como usuario ADMIN y ejecutar el siguiente comando: *ALTER USER username IDENTIFIED by contrasena ACCOUNT UNLOCK*

- **Eliminación de Usuarios en la Base de Datos**: Este es un tema especialmente prioritario al momento de asegurar los accesos, así como la autenticación de la Base de Datos, ya que se espera que únicamente las personas autorizadas son las que puedan acceder a esta. Sin embargo, resulta importante reconocer que se vuelve una amenaza para la seguridad de la Empresa/Organización, al momento en el que por ejemplo se despide a un colaborador que tenía acceso a la Base de Datos, ya que, si sus accesos no han sido desactivados previamente a la notificación del despido, se pueden presentar situaciones complejas.
    - En PL/SQL, el proceso para eliminar un usuario de la Base de Datos requiere que nos conectemos como usuario ADMIN a través de cualquier herramienta de cliente SQL, se tiene que ejecutar la siguiente sentencia SQL:
        - *DROP USER nombre_usuario CASCADE;*
        - Esto hace que al nombre_usuario se elimine como usuario de la Base de Datos, así como se eliminan todos los objetos y datos que hayan sido creados o sean propiedad de él, por lo que debe manejarse con alto cuidado y verificación.
- **Gestión de Privilegios de Usuarios de Bases de Datos:** Existe un rol de Base de Datos predefinido en PL/SQL que se denomina DWROLE. El mismo se

encarga de proporcionar los privilegios necesarios para la mayoría de los usuarios de la Base de datos, algunos de los privilegios que son otorgados a un usuario en cuestión, son la siguiente lista de sentencias SQL:

- *CREATE ANALYTIC VIEW*
- *CREATE ATTRIBUTE DIMENSION*
- *ALTER SESSION*
- *CREATE HIERARCHY*
- *CREATE JOB*
- *CREATE MINING MODEL*
- *CREATE PROCEDURE*
- *CREATE SEQUENCE*
- *CREATE SESSION*
- *CREATE SYNONYM*
- *CREATE TABLE*
- *CREATE TRIGGER*
- *CREATE TYPE*
- *CREATE VIEW*
- *READ,WRITE ON directory DATA_PUMP_DIR*

Cuentas de Usuario y su Reestablecimiento

Los usuarios en general a nivel de PL/SQL se encuentran bloqueados al momento de fracasar sus diferentes intentos de inicio de sesión a través del subprograma conocido como “Identity Manager”, una de las causales que puede ser tomada en cuenta a razón de que un usuario quede bloqueado; es que este llegue a superar el número permitido de inicios de sesión fallidos, los cuales generan que las cuentas se bloqueen en cuestión, que manejan causales como las siguientes:

1. Los usuarios que superan el máximo de intentos fallidos de inicio de sesión con una contraseña quedarán bloqueados en todas las interfaces que existan de Identity Manager de Oracle, no excluyendo a la de recuperación de contraseña.

2. Los usuarios que superan el número máximo de intentos fallidos de inicio de sesión con una pregunta específica asignada por ellos mismos podrán autenticarse en todas las interfaces del subprograma de Identity Manager, con la debida excepción de las rutinas de recuperación de contraseña.

En estos casos, se conoce que el único capaz de hacerlo en una base de datos Oracle PL/SQL, vendría siendo el Administrador o aquel usuario que tenga todos los privilegios y permisos que hemos mencionado con anterioridad.

Por ejemplo, estas son las capacidades adecuadas que puede aplicar las operaciones siguientes al momento del bloqueo de una cuenta:

- **Actualizar**: Se pueden actualizar los datos generales de la cuenta, sin embargo, esto afectará directamente a los recursos y objetos que se encuentren en ella.
- **Cambiar o Reinicializar la Contraseña**: Este es el enfoque común, ya que en caso tal de que un usuario no recuerde su contraseña y la haya perdido por “N” motivo que pueda llegar a ser, se reconoce que la misma puede ser cambiada directamente por el Administrador o incluso, si la Base de Datos se encuentra conectada a internet en el servidor que está alojada, se le puede enviar un mal a este usuario con un Enlace Único, para el restablecimiento de su cuenta.
- **Inhabilitar o Habilitar**: De extrema importancia, ya que como fue mencionado en los comentarios iniciales de esta investigación por el autor de esta, se reconoce que muchas veces se presentarán casos de uso en los que se por un motivo específico, se deba inhabilitar automáticamente los accesos a un usuario X, pero en otro, habilitarlos.
- **Renombrar**
- **Desbloquear la Cuenta**

Usuarios Predeterminados de la Base de Datos

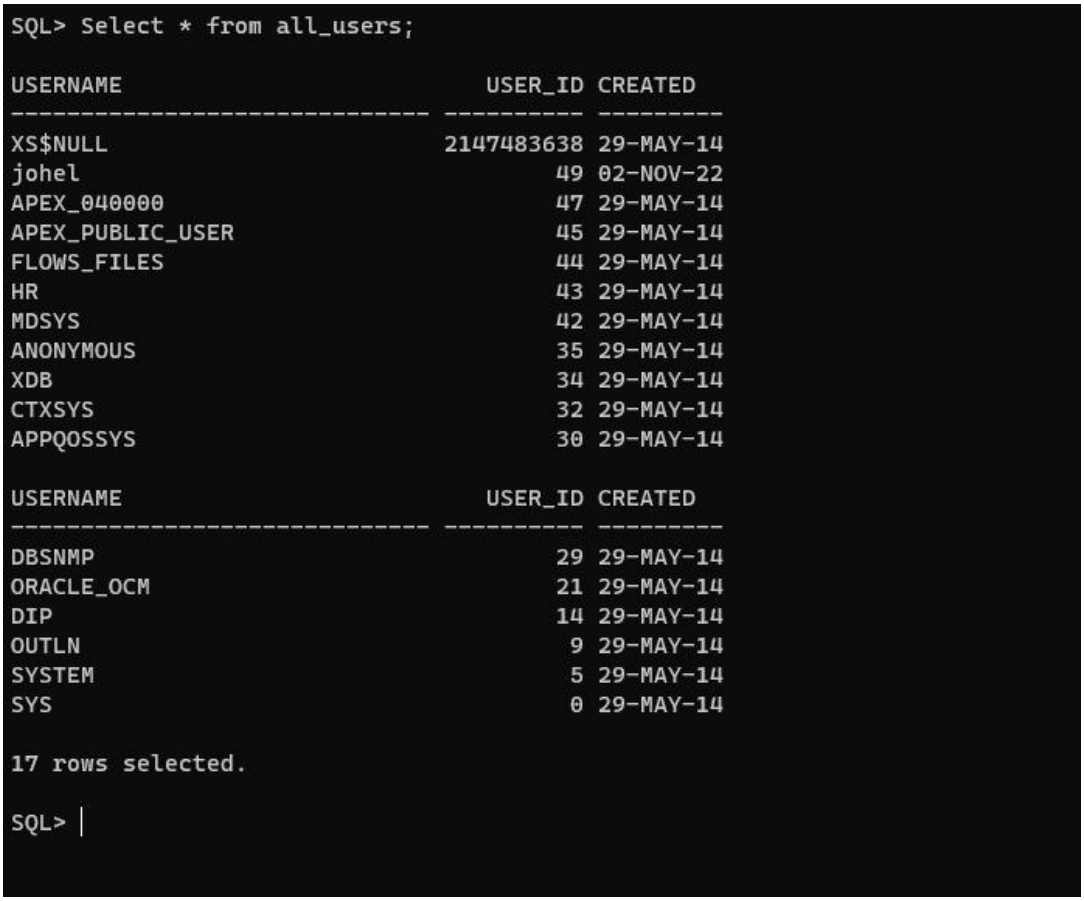
Existen algunos usuarios que al momento de la instalación del motor de Bases de Datos de Oracle PL/SQL, se proceden a crear de manera automática y a ellos se les otorga el rol de DBA (DataBase Administrator), ya que son usuarios administrados por el mismo sistema, como veremos a continuación; sin embargo, el acceso a cada uno de ellos, especialmente en el entorno gráfico, se convierte en uno de los principales problemas que se pueden presentar, a manera de asegurar la Base de Datos.

- **Usuario SYS**: Maneja una contraseña por defecto que es "CHANGE_ON_INSTALL", es decir que se incita a que el usuario en cuestión, proceda a cambiarla automáticamente al momento de realizar la instalación, de forma que se puedan evitar brechas de seguridad.
    - Importante es reconocer que las tablas y vistas del Diccionario de Datos de la Base de Datos, se encuentran almacenadas en el Esquema (Schema en inglés) para el usuario SYS. Estas Tablas y Vistas son fundamentales para el funcionamiento de nuestra Base de Datos, ya que permiten mantener la Integridad del Diccionario de Datos, estas tablas son únicamente manipuladas por la base de datos.
        - Jamás se deben modificar o crear tablas en el Schema del usuario SYS.
- **Usuario SYSTEM**: Maneja una contraseña por defecto al momento de la instalación QUE ES "MANAGER", por lo que también se recomienda cambiarlo de manera automática al momento de su instalación.
    - Dicho usuario, es utilizado principalmente para la creación de tablas y vistas adicionales que se encargan de mostrar información administrativa de la Base de Datos, especialmente tablas internas y vistas que se utilizan por varias opciones, así como herramientas de la misma Base de Datos Oracle.

- Una buena práctica en general es el no uso del Schema SYSTEM para almacenar tablas o cualquier objeto general que sea de interés para usuarios no administrativos dentro de ella.

Es importante resaltar, que ninguno de los dos ejemplos de usuarios anteriormente mencionados, ni los que se encuentran en la Segunda Tabla de la siguiente imagen en cuestión (DBSNMP, ORACLE_OCM, DIP, OUTLN, SYSTEM, SYS), pueden ser utilizados, ya que representan la integridad como tal de la instalación de PL/SQL, he ahí su buen uso e importancia.

Una buena práctica, resulta en no trabajar bajo ninguno de estos usuarios, sino como se muestra en la Primera Tabla, con usuarios creados, en muchos de los casos por el DBA (Database Administrator), como lo es en este caso el usuario '*johel*.



```
SQL> Select * from all_users;

USERNAME                          USER_ID CREATED
------------------------------ ---------- ---------
XS$NULL                        2147483638 29-MAY-14
johel                                  49 02-NOV-22
APEX_040000                            47 29-MAY-14
APEX_PUBLIC_USER                       45 29-MAY-14
FLOWS_FILES                            44 29-MAY-14
HR                                     43 29-MAY-14
MDSYS                                  42 29-MAY-14
ANONYMOUS                              35 29-MAY-14
XDB                                    34 29-MAY-14
CTXSYS                                 32 29-MAY-14
APPQOSSYS                              30 29-MAY-14

USERNAME                          USER_ID CREATED
------------------------------ ---------- ---------
DBSNMP                                 29 29-MAY-14
ORACLE_OCM                             21 29-MAY-14
DIP                                    14 29-MAY-14
OUTLN                                   9 29-MAY-14
SYSTEM                                  5 29-MAY-14
SYS                                     0 29-MAY-14

17 rows selected.

SQL>
```

Figura N°2: En la segunda tabla se muestran todos los usuarios predeterminados que se encuentran cargados en cualquier tipo de Base de Datos PL/SQL

Comentarios Finales

Como observamos en la Investigación presentada anteriormente, el Manejo de Usuarios se convierte en un elemento primordial al momento no solamente del Diseño Conceptual o Lógico de una Base de Datos, sino que puede llegar a generar problemas en su desarrollo final, implementación y despliegue en servidores; lo que conllevaría a múltiples inconvenientes, que pueden ser traspasados casos de negocio en el que se ponga en riesgo la infraestructura crítica de la Empresa/Organización.

La minimización del riesgo a nivel de accesos de usuarios autorizados y no autorizados comienza directamente al momento en el que se establecen las conexiones iniciales a la Base de Datos, ya que hoy en día existen múltiples herramientas, como por ejemplo Identity Manager que han sido desarrolladas por la Unidad Funcional de Cloud en ORACLE, que permiten verificar ingresos no deseados o incluso intentos por fuerza bruta, que últimamente son los más comunes, incluyendo inyecciones SQL.

A continuación, presentamos las principales amenazas que existen para la integridad referencial y general de una Base de Datos como tal:

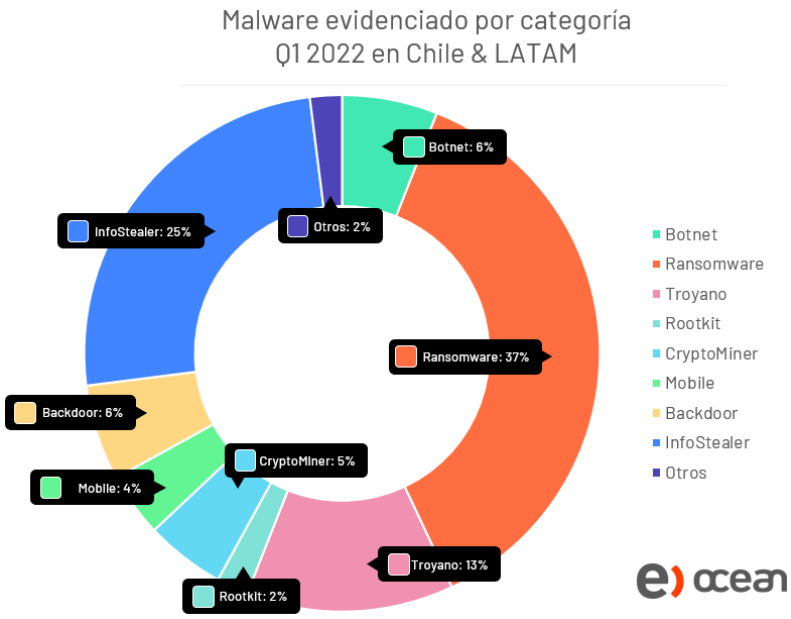


Figura N°3: Gráfico de Principales Amenazas en Q1 2022 (Fuente: ENTEL Ocean)

Se vuelve de vital importancia, que siendo ORACLE PL/SQL uno de los motores de Bases de Datos más utilizados para transacciones de alta redundancia por su reconocida fiabilidad e integridad en entornos empresariales; imperativo es el aseguramiento de ¿Quiénes tienen los accesos? ¿Quiénes tienen los permisos? ¿Cómo se tiene control acerca de lo que ve el usuario final o no, que es por ello que una buena prática es la de

evitar que se vea cualquier tipo de código, sino que todo lo requerido por las Unidades Funcionales del Negocio, se muestre a través de una “Vista”.

Bibliografía

1. "Oracle autonomous database en infraestructura de exadata dedicada". Oracle Help Center. https://docs.oracle.com/es-ww/iaas/autonomous-database/doc/managing-database-users.html (accedido el 9 de noviembre de 2022).
2. H. Paredes. "Usuario SYS y SYSTEM - ORACLE". Blog | hadsonpar. http://blog.hadsonpar.com/2016/02/usuario-sys-y-system-oracle.html (accedido el 9 de noviembre de 2022).
3. "Diseño de seguridad de una base de datos". Universidad de Don Bosco, El Salvador. https://www.udb.edu.sv/udb_files/recursos_guias/informatica-ingenieria/base-de-datos-i/2019/i/guia-12.pdf (accedido el 8 de noviembre de 2022).
4. "Seguridad de datos: En qué consiste y qué es importante en tu empresa". PowerData - Especialista en Gestión de Datos | MDM | Big Data | Cloud | Data Warehouse. https://www.powerdata.es/seguridad-de-datos (accedido el 9 de noviembre de 2022).
5. "Desbloqueo de cuentas de usuario (guãa del administrador de negocio de sun identity manager 8.1)". Moved. https://docs.oracle.com/cd/E19957-01/821-0062/byaee/index.html (accedido el 10 de noviembre de 2022).
6. "Usuarios bloqueados en Oracle". Informaticadas. http://informaticadasdecadadia.blogspot.com/2014/02/usuarios-bloqueados-en-oracle.html (accedido el 10 de noviembre de 2022).