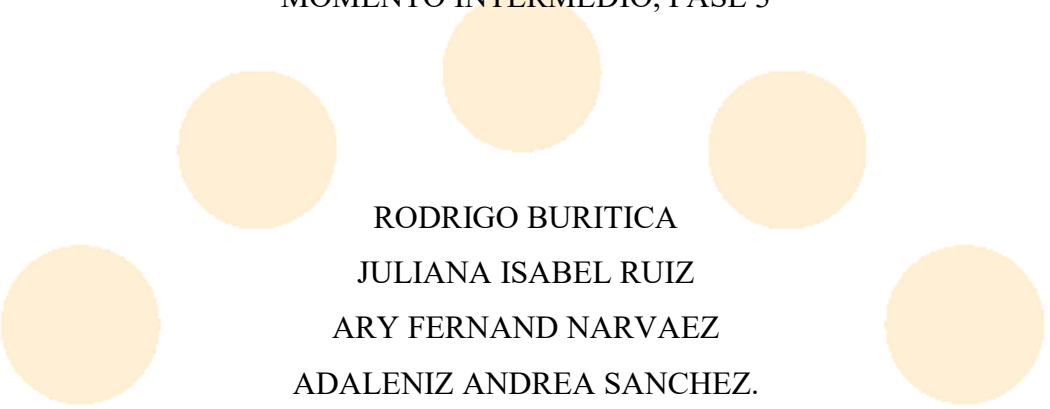
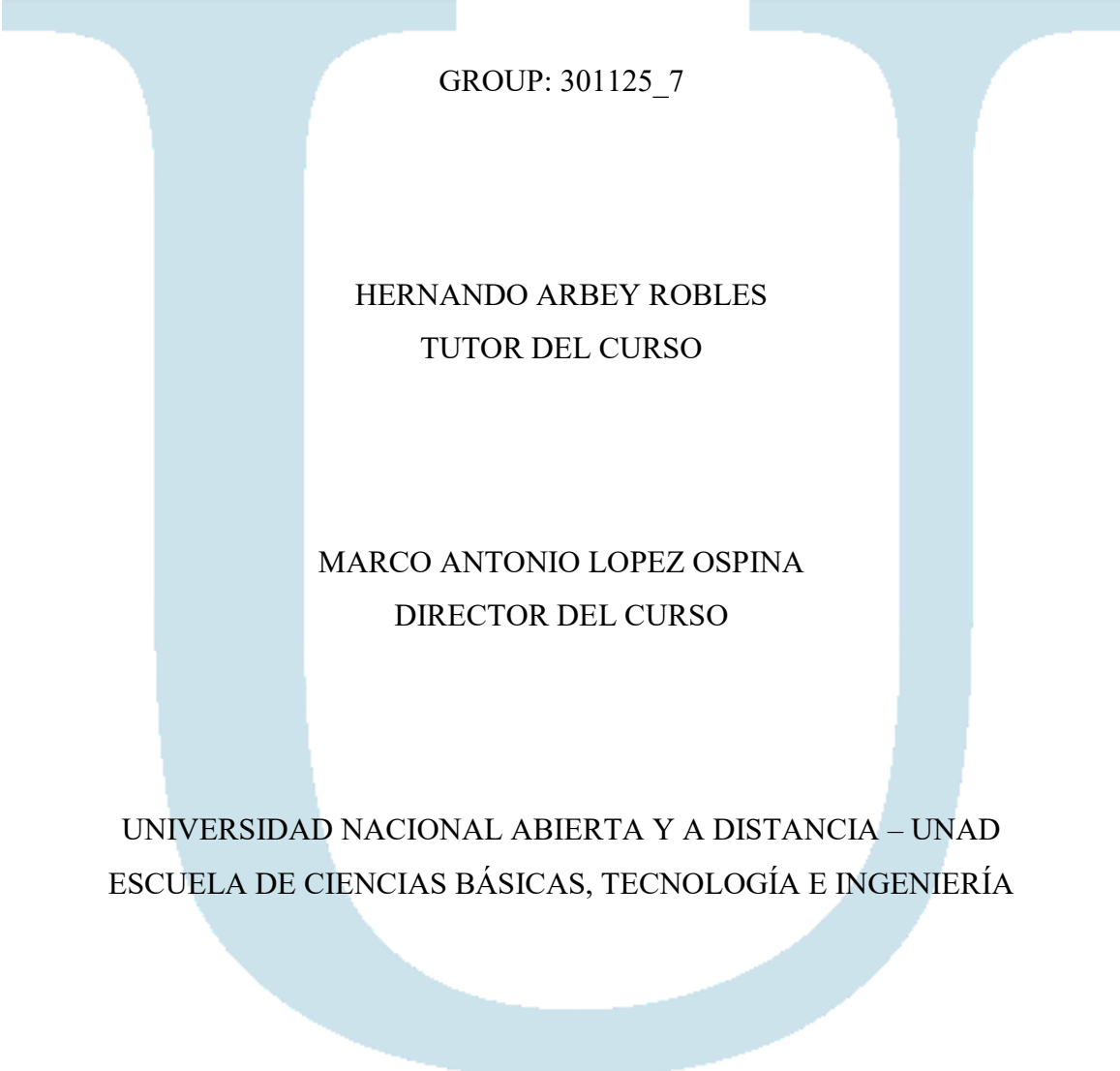


BASE DE DATOS AVANZADA
MOMENTO INTERMEDIO, FASE 3



RODRIGO BURITICA
JULIANA ISABEL RUIZ
ARY FERNAND NARVAEZ
ADALENIZ ANDREA SANCHEZ.



GROUP: 301125_7

HERNANDO ARBEY ROBLES
TUTOR DEL CURSO

MARCO ANTONIO LOPEZ OSPINA
DIRECTOR DEL CURSO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

JUNIO 2016

INTRODUCCIÓN

Mediante el desarrollo de esta actividad el estudiante identifica las amenazas a las cuales está expuesta la base de datos, conoce e implementa los diferentes niveles de seguridad que se pueden aplicar a los usuarios que van a acceder a la base de datos.

Se le indica como generar copias de seguridad, como restaurar una base de datos.

Todo esto son herramientas que se le brindan al estudiante con el fin de mejorar sus conocimientos y que los trabajos implementados sean más seguros para el cliente final.

OBJETIVO

” Una base de datos nos permite acomodar, ordenar y tener libre acceso de la información, sea cual fuere”. Y con este fin se pretende afianzar el aprendizaje de los contenidos, este momento inicial nos invita a realizar una práctica de las temáticas propuestas en las Unidades de Bases de Datos Avanzada y a través del foro no solo interactuar sino también retroalimentar y multiplicar el conocimiento de estos contenidos. Se espera cumplir con los objetivos planteados en la guía y en la rúbrica.

PREGUNTAS ORIENTADAS

○ **Pregunta 1. ¿Qué entiende por seguridad en Bases de Datos?**

Hablando de seguridad se puede implementar en diferentes puntos, puede ser a nivel del servidor, de la aplicación, desde el motor de base de datos y otros.

Pero si del motor de base de datos se puede tener seguridad:

A nivel de Autenticación: saber quién se autentica, desde donde. En otra palabra información de la sesión.

A nivel de Autorización: se concede, revoca y se deniega permisos, se configura roles y se puede restringir el acceso a datos específicos de la base de datos.

A nivel de Cifrado de Datos: donde se puede cifrar archivos de datos o de transacciones, se puede cifrar columnas, datos, claves y procedimiento almacenados.

A nivel de Seguridad de Conexión: se restringe y protege el acceso configurando firewall en el servidor y se puede cifrar las conexiones que se realicen al motor de base de datos.

A nivel de Auditoria: guardar trazo de las transacciones realizadas en el motor, muchas veces se olvida de este punto y es importante tener la configurado las herramientas que permitan una auditoria dentro de la base de datos..

○ **Pregunta 2. Mencione 4 Amenazas en el entorno de bases de Datos, justifique su respuesta**

Protocolos de copia de seguridad mal diseñados, que no aseguren una restauración del sistema en tiempos admisibles.

Incorrecta o pobre definición de los niveles de acceso por tipos de usuarios, permitiendo el ingreso o manipulación de los datos por quienes no deberían estar autorizados. A éste

problema puede sumársele una pobre política de contraseñas, que permita el uso de contraseñas débiles, afectando los niveles de seguridad del acceso a los datos.

Vulnerabilidad a nivel del servidor, donde incompletos protocolos de seguridad pueden permitir el ingreso de intrusos o software peligroso.

Malas prácticas de programación en el software cliente, que puedan dejar puertos o conexiones abiertas, u ocasionar procesos que afecten la integridad de la base de datos

- **Pregunta 3. En MySQL cuáles son los niveles distintos de privilegios, justifique su respuesta**

En MySQL los niveles de privilegios son:

- Globales => nivel más alto entre los niveles de privilegios. Se aplica a todas las bases de datos y a todos los objetos contenidos en cada base de datos del servidor.
- De base de datos => aplica a una base de datos puntual, incluyendo todos los objetos contenidos en la misma.
- De tabla => aplica a una tabla puntual y por ende a todas sus columnas.
- De columna => aplica para una columna de terminada dentro de una tabla específica.
- De rutina => aplica para los procedimientos almacenados.
- **Pregunta 4. Mencione 3 Mecanismos de recuperación usados por SMDB, justificando su respuesta**
 - Técnica de paginación en la sombra: se realiza un seguimiento en páginas antiguas en las Bases de Datos y han utilizado un directorio sombra. NO DESHACER / NO REHACER
 - Algoritmo de recuperación ARIES: este tiene una particularidad de utilizar el método ROBAR / NO FORZAR para escribir, lo que requiere:
 - Hacer el registro antes de la escritura
 - Realizar la repetición del histórico durante el proceso de REHACER
 - Realización de registros de los cambios durante el proceso DESHACER
 - Recuperación en sistemas multibases de Datos: este mecanismo lleva acabo 2 procesos o niveles.

- Gestor de recuperación global
- Gestor de recuperación locales

Contiene 2 fases en el protocolo de confirmación:

- Cuando el participante falla
- Exitoso o fallo.

Se utiliza los mecanismos de recuperación para restaurar al estado coherente, más reciente inmediatamente anterior al momento del fallo el cual irán guardados en el registro del Sistema



EVIDENCIA DE LAS PRACTICAS REALIZADAS

PRACTICA: JULIANA RUIZ

CREACIÓN DE USUARIOS:

CREACIÓN DE USUARIOS

Hernando Robles

```
CREATE USER 'hrobles'@'localhost' IDENTIFIED BY 'hr@613s';
```

Adaleniz Sanchez

```
CREATE USER 'asanchez'@'localhost' IDENTIFIED BY '@d@13n1s';
```

Rodrigo Buritica

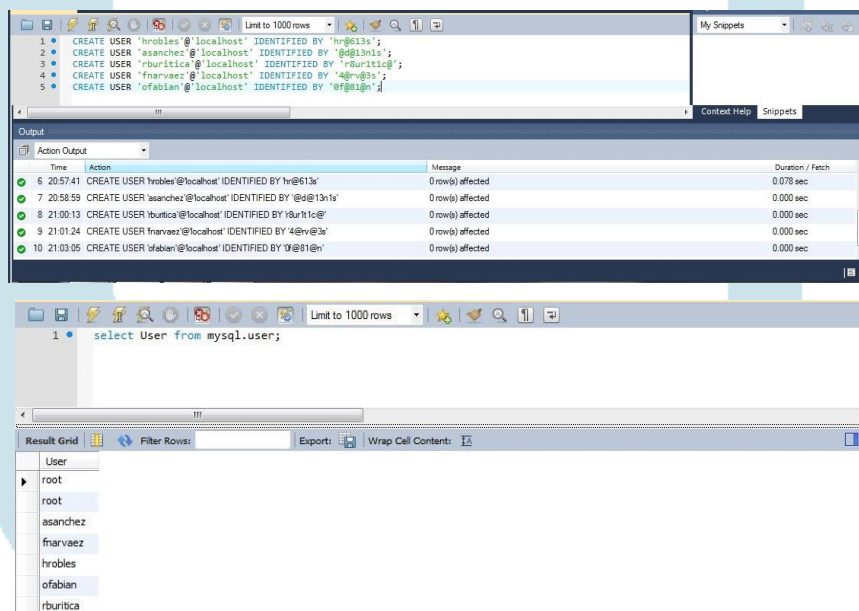
```
CREATE USER 'rburitica'@'localhost' IDENTIFIED BY 'r8ur1t1c@';
```

Ary Fernando Narvaez

```
CREATE USER 'fnarvaez'@'localhost' IDENTIFIED BY '4@rv@3s';
```

Omar Fabian Castillo

```
CREATE USER 'ofabian'@'localhost' IDENTIFIED BY '0f@81@n';
```



ASIGNAR NIVELES DE PRIVILEGIOS POR USUARIO

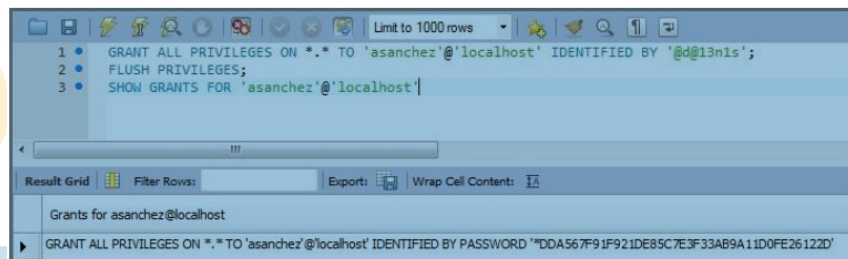
Todos los Privilegios

```
GRANT ALL PRIVILEGES ON *.* TO 'asanchez'@'localhost' IDENTIFIED BY  
'@d@13n1s';
```

```
FLUSH PRIVILEGES;
```

Verificación de privilegios a usuarios

```
SHOW GRANTS FOR 'asanchez'@'localhost'
```



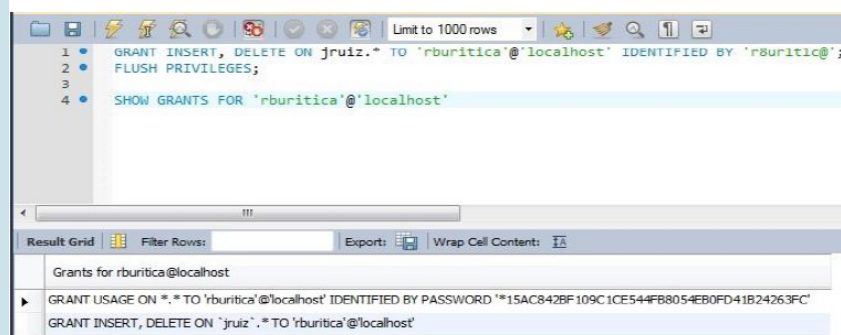
Privilegios a nivel de Base de Datos

```
GRANT INSERT, DELETE ON jrui.* TO 'rburitica'@'localhost' IDENTIFIED BY  
'r8ur1t1c@';
```

```
FLUSH PRIVILEGES;
```

Verificación de privilegios a usuarios

```
SHOW GRANTS FOR 'rburitica'@'localhost'
```



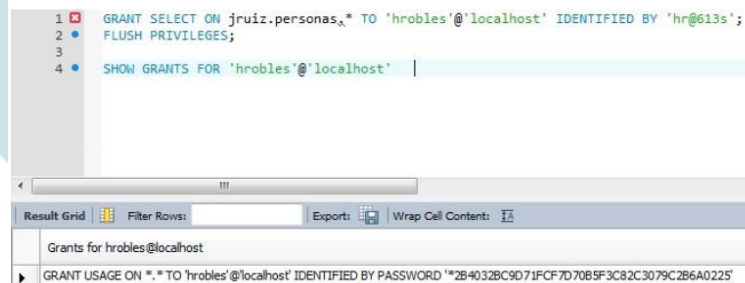
Privilegios a nivel de Tabla

```
GRANT SELECT ON jrui.personas.* TO 'hroble'@'localhost' IDENTIFIED BY  
'hr@613s';
```

```
FLUSH PRIVILEGES;
```

Verificación de privilegios a usuarios

```
SHOW GRANTS FOR 'hroble'@'localhost'
```

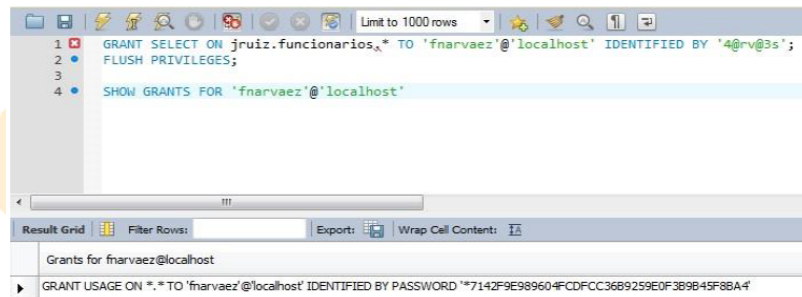



```
GRANT SELECT ON jruiz.funcionarios.* TO 'fnarvaez'@'localhost' IDENTIFIED BY '4@rv@3s';
```

FLUSH PRIVILEGES;

Verificación de privilegios a usuarios

```
SHOW GRANTS FOR 'fnarvaez'@'localhost'
```

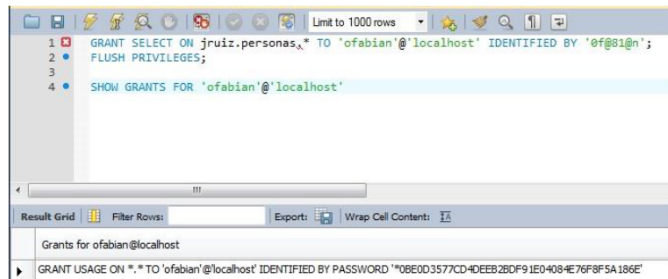


```
GRANT SELECT ON jruiz.personas.* TO 'ofabian'@'localhost' IDENTIFIED BY '0f@81@n';
```

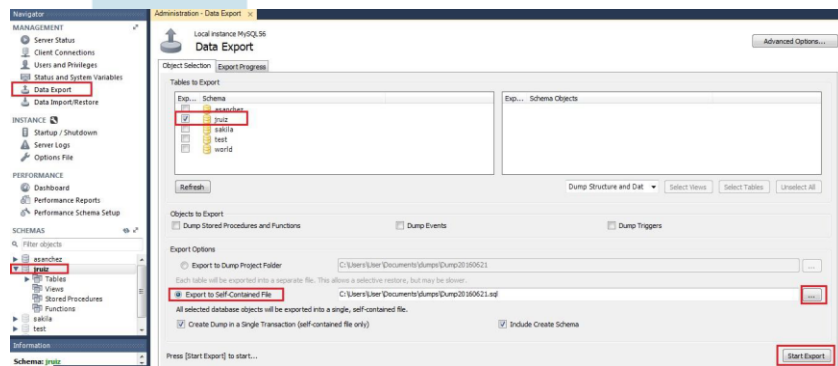
FLUSH PRIVILEGES;

Verificación de privilegios a usuarios

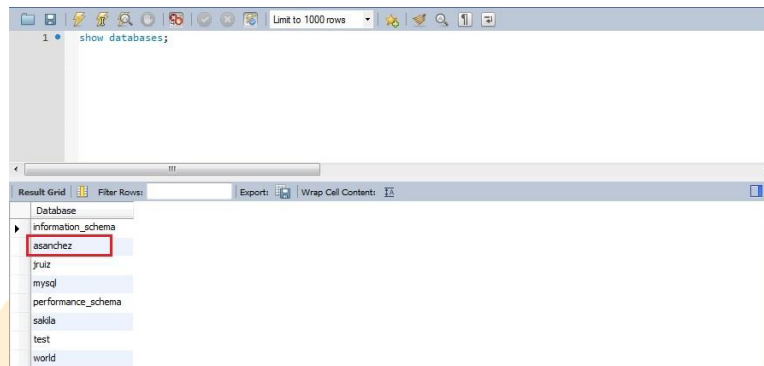
```
SHOW GRANTS FOR 'ofabian'@'localhost'
```



EXPORTACIÓN BASE DE DATOS



RESTAURACIÓN BASE DE DATOS ADALENIZ SANCHEZ



PRACTICA: ADALENIZ SANCHEZ

DEFINICIÓN DE LOS USUARIOS

- GLOBALES: Adaleniz Sánchez y Hernando Arbey Robles
- De base de datos: Juliana Isabel Ruiz
- De tabla: Rodrigo Buritica
- De columna: Omar Fabián Castillo
- De rutina: Arby Fernando Narvaez

CREACION DE USUARIOS

```
CREATE USER 'adaleniz.sanchez'@'localhost' IDENTIFIED BY '@ad1128418584';
```

```
CREATE USER 'hernando.robles'@'localhost' IDENTIFIED BY '@har123456';
```

```
CREATE USER 'juliana.rius'@'localhost' IDENTIFIED BY '@jr123456';
```

```
CREATE USER 'rodrigo.buritica'@'localhost' IDENTIFIED BY '@rb123456';
```

```
CREATE USER 'omar.fabian'@'localhost' IDENTIFIED BY '@o123456';
```

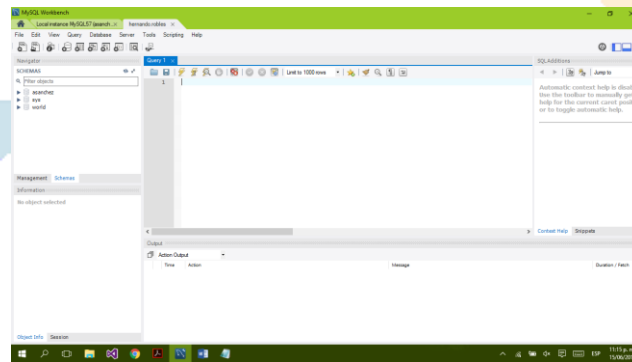
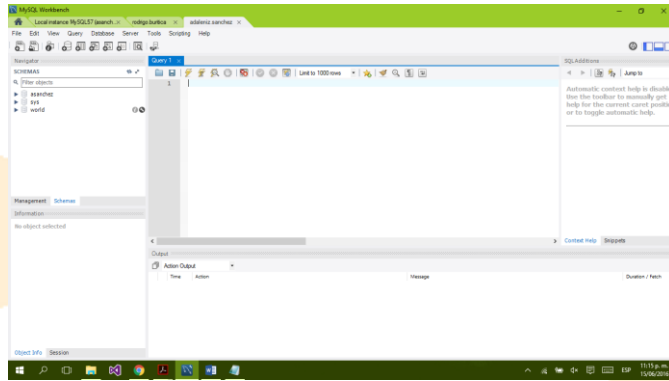
```
CREATE USER 'fernando.narvaez'@'localhost' IDENTIFIED BY '@fn123456';
```

ASIGNACIÓN DE ROLES

GLOBALES

```
GRANT ALL PRIVILEGES ON * . * TO 'adaleniz.sanchez'@'localhost';
```

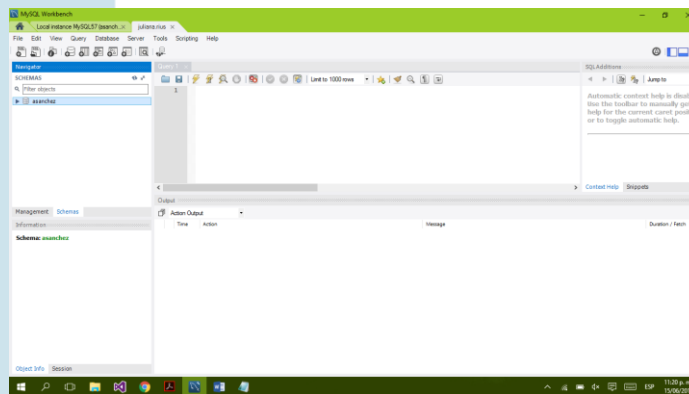
```
GRANT ALL PRIVILEGES ON * . * TO 'hernando.robles'@'localhost';
```



BASE DE DATOS

GRANT ALL ON asanchez.* TO 'juliana.rius'@'localhost';

GRANT SELECT, INSERT, CREATE, DROP, DELETE, UPDATE ON
asanchez.* TO 'juliana.rius'@'localhost';



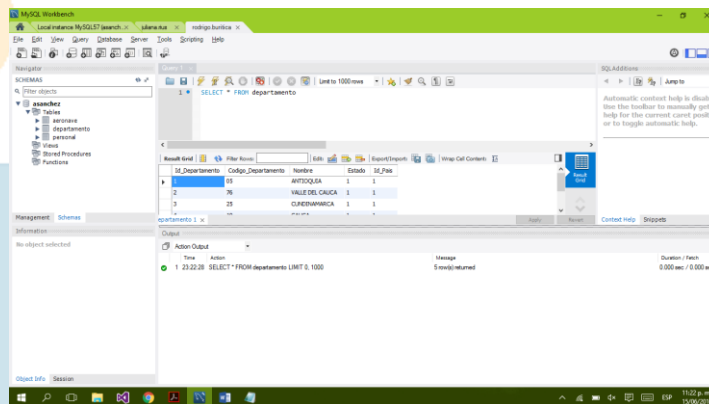
TABLA

GRANT ALL ON asanchez.departamento TO 'rodrigo.buritica'@'localhost';

GRANT SELECT, INSERT, CREATE, DELETE, UPDATE ON
asanchez.departamento TO 'rodrigo.buritica'@'localhost';

GRANT ALL ON asanchez.personal TO 'rodrigo.buritica'@'localhost';
GRANT SELECT, INSERT, CREATE, DELETE, UPDATE ON
asanchez.personal TO 'rodrigo.buritica'@'localhost';

GRANT ALL ON asanchez.aeronave TO 'rodrigo.buritica'@'localhost';
GRANT SELECT, INSERT, CREATE, DELETE, UPDATE ON
asanchez.aeronave TO 'rodrigo.buritica'@'localhost';



COLUMNA

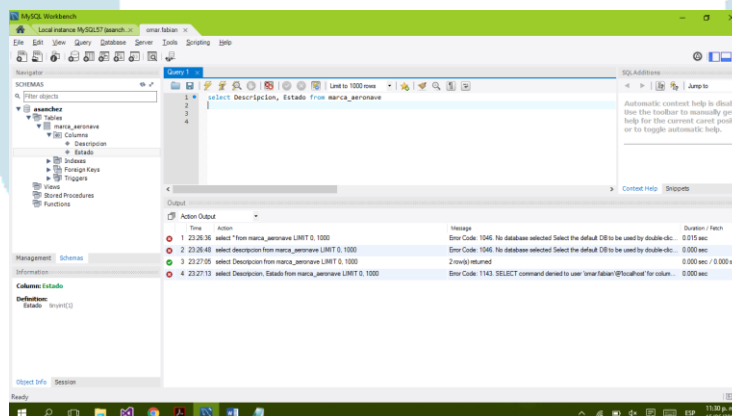
GRANT SELECT (descripcion), INSERT (descripcion,estado) ON
asanchez.marca_aeronave TO 'omar.fabian'@'localhost';

Errores:

Error 1: no habia seleccionada la base de datos

Error 2: en vez de nombrar las columnas puse el *

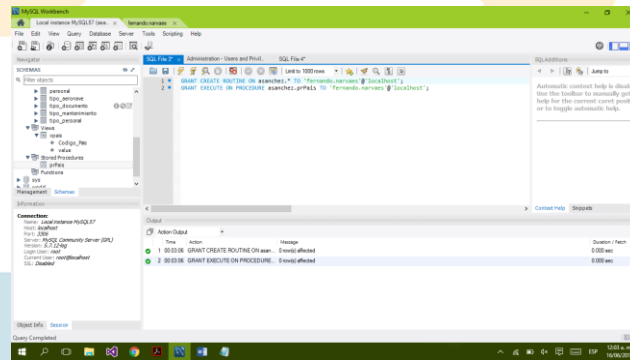
Error 3: solo puedo consultar la columna descripcion y estoy intentando
consultar ambas columnas.



RUTINA

GRANT CREATE ROUTINE ON asanchez.* TO
'fernando.narvaez'@'localhost';

GRANT EXECUTE ON PROCEDURE asanchez.prPais TO
'fernando.narvaez'@'localhost';



CONCLUSIONES

Se toma un poca más de conciencia en la importancia de delimitar el acceso a la base de datos por cada usuario que va a tener acceso a la misma, evitando de esto modo un manejo inadecuado de los datos, o prevenir que se eliminen datos o tablas importantes para el proceso del sistema.

Se conoce un poco más sobre los diferentes niveles de seguridad que se puede aplicar a la base de datos, las diferentes variables que nos pueden hacer vulnerables.

Se aprende a realizar copias de seguridad en MySQL, a restaurar bases de datos, a limitar por niveles de seguridad el acceso a la base de datos por usuario.

REFERENCIAS BIBLIOGRAFIA

Se utilizaron los tutoriales publicados en el entorno de conocimiento, Unidad 3: gestion de seguridad en base de datos:

Villalobos, Johnny. 2012. Principios básicos de seguridad en base de datos

InfoSecuity. 2013. Las 10 grandes amenazas de seguridad en las bases de datos.

Oracle. 2014. MySql 5.0. Manual de referencia, Capitulo 5, Administración de la base de datos.

Pozo, Salvador. 2005. Lenguaje SQL usuarios y privilegios .