



INGENIERÍA EN
SISTEMAS COMPUTACIONALES

.....



Tecnológico Nacional de México
Campus Felipe Carrillo Puerto
Unidad Académica Chunhuhub
Ingeniería en Sistemas Computacionales

Taller de base de datos
Tema 3.- Control de acceso

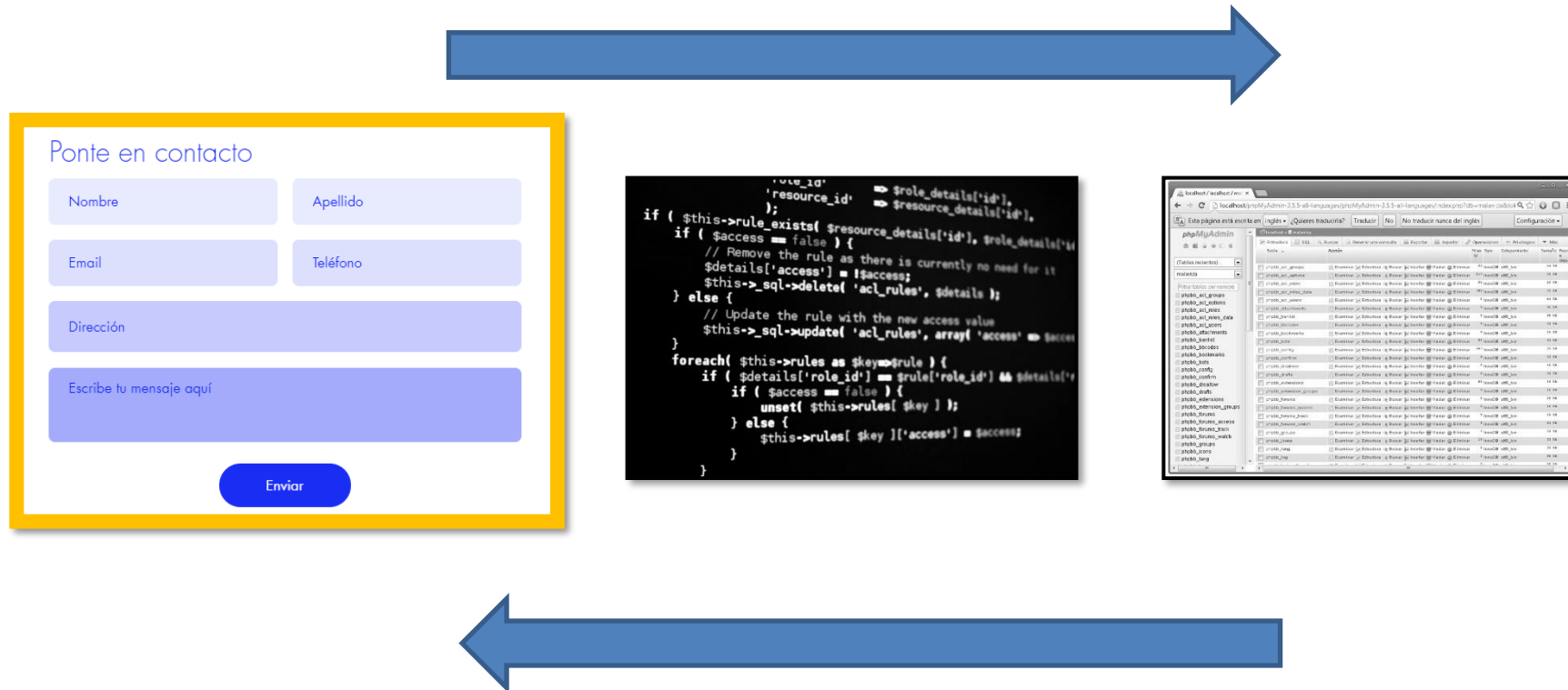
Docente: José Torres Ek

3.1 Tipos de usuario



Tipos de usuarios

Usuarios normales. Son usuarios no sofisticados que interactúan con el sistema mediante un programa de aplicación con una interfaz de formularios, donde puede rellenar los campos apropiados del formulario.



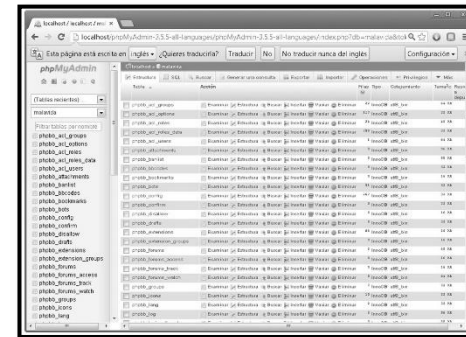
Tipos de usuarios

Programadores de aplicaciones. Son profesionales informáticos que escriben los programas de aplicación, utilizando herramientas para desarrollar interfaces de usuario que facilitan crear formularios e informes.

Ponte en contacto

Nombre	Apellido
Email	Teléfono
Dirección	
Escribe tu mensaje aquí	
Enviar	

```
        'role_id' => $role_details['id'],
        'resource_id' => $resource_details['id'],
    );
    if ( $this->rule_exists( $resource_details['id'], $role_details['id'] ) ) {
        if ( $access == false ) {
            // Remove the rule as there is currently no need for it
            $details['access'] = !$access;
            $this->sql->delete( 'acl_rules', $details );
        } else {
            // Update the rule with the new access value
            $this->sql->update( 'acl_rules', array( 'access' => $access ), $details );
        }
    }
    foreach( $this->rules as $key=>$rule ) {
        if ( $details['role_id'] == $rule['role_id'] && $details['resource_id'] == $rule['resource_id'] ) {
            if ( $access == false ) {
                unset( $this->rules[ $key ] );
            } else {
                $this->rules[ $key ]['access'] = $access;
            }
        }
    }
}
```



Tipos de usuarios

Usuarios sofisticados. Interactúan con el sistema sin programas escritos, usando el lenguaje de consulta de base de datos para hacer sus consultas. Los analistas que envían las consultas para explorar los datos en la base de datos entran en esta categoría.

Ponte en contacto

Nombre Apellido

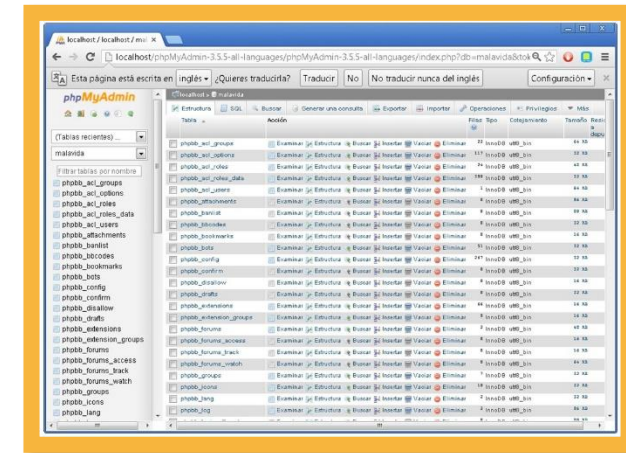
Email Teléfono

Dirección

Escribe tu mensaje aquí

Enviar

```
'role_id' => $role_details['id'],
'resource_id' => $resource_details['id'],
);
if ( $this->rule_exists( $resource_details['id'], $role_details['id'] ) {
    if ( $success == false ) {
        // Remove the rule as there is currently no need for it
        $details['access'] = !$access;
        $this->sql->delete( 'acl_rules', $details );
    } else {
        // Update the rule with the new access value
        $this->sql->update( 'acl_rules', array( 'access' => $success ) );
    }
}
foreach( $this->rules as $key=>$rule ) {
    if ( $details['role_id'] == $rule['role_id'] && $details['resource_id'] == $rule['resource_id'] ) {
        if ( $success == false ) {
            unset( $this->rules[ $key ] );
        } else {
            $this->rules[ $key ]['access'] = $success;
        }
    }
}
```



usuario	password	email	access
admin	admin	admin@localhost	1
root	root	root@localhost	1
...



Tipos de usuarios

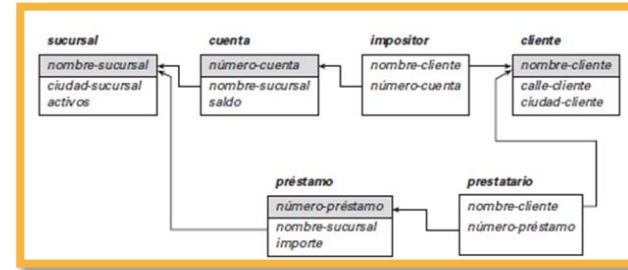
Administradores de la base de datos (ABD). Son las personas que tienen el control central del SGBD. Entre las funciones del ABD se encuentran:

- Definición del esquema de la base de datos.
- Definición de la estructura y el método de acceso.
- Modificación del esquema y la organización física.
- Concesión de autorización para el acceso a los datos.
- Mantenimiento rutinario.



Tipos de usuarios

Administradores de la base de datos (ABD). Son las personas que tienen el control central del SGBD.



Ponte en contacto

Nombre Apellido

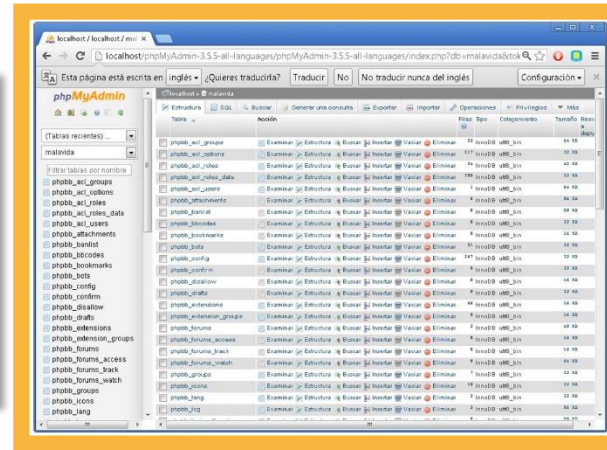
Email Teléfono

Dirección

Escribe tu mensaje aquí

Enviar

```
if ( $this->rule_exists( $resource_details['id'], $role_details['id'], $resource_id => $resource_details['id'], $role_id => $role_details['id'], $access => $access ) ) {  
    // Remove the rule as there is currently no need for it  
    $details['access'] = !$access;  
    $this->sql->delete( 'acl_rules', $details );  
} else {  
    // Update the rule with the new access value  
    $this->sql->update( 'acl_rules', array( 'access' => $access )  
    foreach( $this->rules as $key => $rule ) {  
        if ( $details['role_id'] == $rule['role_id'] ) {  
            if ( $access == false ) {  
                unset( $this->rules[ $key ] );  
            } else {  
                $this->rules[ $key ]['access'] = $access;  
            }  
        }  
    }  
}
```



phpMyAdmin

Bienvenido a phpMyAdmin

Idioma - Language

Español - Spanish

Iniciar sesión

Usuario:

Contraseña:

Continuar

```
mysql> show grants for 'parzibyte'@'localhost';  
+-----+  
| Grants for parzibyte@localhost |  
+-----+  
| GRANT USAGE ON *.* TO 'parzibyte'@'localhost' |  
| GRANT ALL PRIVILEGES ON `currental`.* TO 'parzibyte'@'localhost' |  
+-----+  
2 rows in set (0.00 sec)  
  
mysql> revoke all privileges, grant option from 'parzibyte'@'localhost';  
Query OK, 0 rows affected (0.00 sec)  
  
mysql> drop user 'parzibyte'@'localhost';  
Query OK, 0 rows affected (0.00 sec)  
  
mysql> drop database currental;
```



Entorno SQL

El entorno SQL es, simplemente, la suma de todas las partes que conforman ese entorno. Cada parte, o componente, trabaja en conjunto con otros componentes para respaldar las operaciones de SQL tales como la creación y modificación de objetos, almacenamiento y consulta de información, o modificación y eliminación de datos. En conjunto, estos componentes forman un modelo en el que un RDBMS puede basarse. Esto no significa, que los proveedores de RDBMS se adhieren estrictamente a este modelo; cuáles componentes implementan, y cómo lo hacen se deja, en su mayor parte, a la discreción de esos proveedores.



Entorno SQL

El entorno SQL se compone de varios tipos de componentes, cada tipo de componente realiza una función específica dentro del entorno SQL.

Tipo de componente	Descripción
Identificador de autorización	Un identificador representa a un usuario o un rol al que se le concede privilegios de acceso a objetos o información dentro del entorno SQL. Un usuario es una cuenta individual de seguridad que puede representar a un individuo, una aplicación o un servicio del sistema. Un rol es un conjunto de privilegios predefinidos que se asignan a un usuario o a otro rol.



3.2 Creación de usuarios



Creación de usuarios

Cuando se instala MySQL se tiene un nombre de usuario y una contraseña. Estas credenciales iniciales otorgarán acceso root o control total de todas las bases de datos y tablas.

Mediante un usuario podemos permitir el acceso a una base de datos y asignar permisos según se necesite.

Por ejemplo, si se tiene que contratar desarrolladores para trabajar con algunas bases de datos, pero no se desea darles la capacidad de eliminar o modificar cualquier información confidencial.



Crear un usuario

La instrucción para crear un usuario tiene la siguiente estructura:

```
CREATE USER 'tiendacel'@'localhost' IDENTIFIED BY 'fgh123k99';
```

Los valores editables son:

```
CREATE USER 'tiendacel'@'localhost' IDENTIFIED BY 'fgh123k99';
```



Nombre del usuario que
queremos crear



Contraseña para el usuario
que estamos creando



3.3 Privilegios a usuarios



Tipos de privilegios que se pueden asignar a un usuario

Privilegios de datos

No	Privilegio	Descripción
1	SELECT	Permite a los usuarios crear una base de datos o una tabla
2	INSERT	Permite a los usuarios recuperar datos
3	UPDATE	Permite a los usuarios agregar nuevos registros a las tablas
4	DELETE	Permite a los usuarios modificar entradas en los registros existentes en tablas
5	FILE	Permite importar y exportar datos de y hacia un archivo



Tipos de privilegios que se pueden asignar a un usuario

Privilegios de estructura		
No	Privilegio	Descripción
1	CREATE	Permite crear nuevas bases de datos y tablas
2	ALTER	Permite a los usuarios alterar la estructura de las tablas existentes.
3	INDEX	Permite a los usuarios crear y eliminar índices
4	DROP	Permite a los usuarios eliminar bases de datos y tablas
5	CREATE TEMPORARY TABLES	Permite a los usuarios la creación de tablas temporales
6	SHOW VIEW	Permite a los usuarios llevar a cabo las consultas SHOW CREATE VIEW



Tipos de privilegios que se pueden asignar a un usuario

Privilegios de estructura

No	Privilegio	Descripción
7	CREATE ROUTINE	Permite a los usuarios crear el almacenamiento de rutinas
8	ALTER ROUTINE	Permite a los usuarios alterar y eliminar las rutinas almacenadas.
9	EXECUTE	Permite a los usuarios ejecutar las rutinas almacenadas
10	CREATE VIEW	Permite a los usuarios crear nuevas vistas
11	TRIGGER	Permite a los usuarios crear y eliminar un disparador



Tipos de privilegios que se pueden asignar a un usuario

Privilegios de administración		
No	Privilegio	Descripción
1	GRANT	Permite añadir usuarios y privilegios
2	SUPER	Permite la conexión, incluso si el número máximo de conexiones se ha alcanzado
3	PROCESS	Permite ver los procesos de todos los usuarios
4	RELOAD	Permite volver a cargar los parámetros del servidor y limpiar los cachés del servidor
5	SHUTDOWN	Permite desconectar el servidor
6	SHOW DATABASES	Concede acceso a la lista completa de bases de datos



Tipos de privilegios que se pueden asignar a un usuario

Privilegios de administración

No	Privilegio	Descripción
7	LOCK TABLES	Permite poner candados a las tablas para el proceso actual
8	REPLICATION CLIENTE	Da el derecho al usuario para preguntar dónde están los esclavos/maestros
9	REPLICATION SLAVE	Necesario para los esclavos de replicación
10	CREATE USER	Permite crear, eliminar y cambiar el nombre de las cuentas de usuario.



Asignar todos los privilegios a usuarios

La instrucción para asignar todos los permisos a un usuario tiene la siguiente estructura:

```
GRANT ALL PRIVILEGES ON * . * TO 'tiendacel'@'localhost';  
FLUSH PRIVILEGES;
```

Los valores editables son:

```
GRANT ALL PRIVILEGES ON * . * TO 'tiendacel'@'localhost';  
FLUSH PRIVILEGES;
```



Nombre del usuario al que
asignaremos todos los permisos



Asignación de privilegios por separado a usuarios

La instrucción para asignar todos los permisos a un usuario tiene la siguiente estructura:

```
GRANT CREATE, SELECT ON * . * TO 'tiendacel'@'localhost';
```

Los valores editables son:

```
GRANT CREATE, SELECT ON * . * TO 'tiendacel'@'localhost';
```



Se escribe los permisos
individuales separados por comas



Nombre del usuario al que
asignaremos los permisos



Quitar todos los privilegios a un usuario

La instrucción para quitar todos los permisos a un usuario tiene la siguiente estructura:

```
REVOKE ALL PRIVILEGES ON * . * FROM 'tiendacel'@'localhost'
```

Los valores editables son:

```
REVOKE ALL PRIVILEGES ON * . * FROM 'tiendacel'@'localhost'
```



Nombre del usuario al que
quitarémos todos los permisos



Quitar privilegios por separado a un usuario

La instrucción para quitar todos los permisos a un usuario tiene la siguiente estructura:

```
REVOKE DELETE, UPDATE ON *.* FROM 'tiendacel'@'localhost';
```

Los valores editables son:

```
REVOKE DELETE, UPDATE ON *.* FROM 'tiendacel'@'localhost';
```



Se escribe los permisos individuales separados por comas



Nombre del usuario al que quitaremos los permisos



Eliminar un usuario

La instrucción para eliminar un usuario tiene la siguiente estructura:

```
DROP USER 'tiendacel'@'localhost';
```

Los valores editables son:

```
DROP USER 'tiendacel'@'localhost';
```



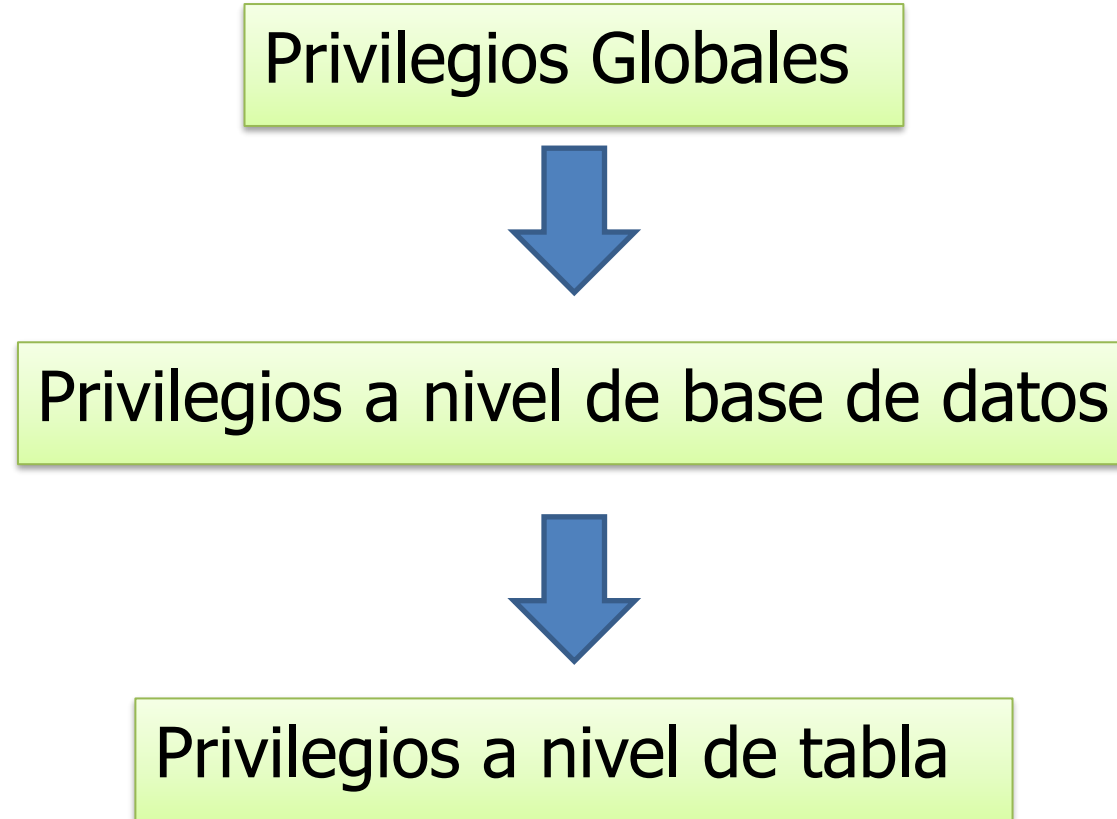
Nombre del usuario que
eliminaremos



Jerarquía de privilegios



Jerarquía de privilegios



Asignar una contraseña al usuario root



Usuario root por defecto

Para añadir una contraseña al usuario root desde phpmyadmin:

- Hacer clic en la opción: Cuentas de usuario
- Hacer clic en la opción: Editar privilegios (del usuario root con servidor localhost)



The screenshot shows the phpMyAdmin interface. The 'Cuentas de usuarios' tab is selected. Below the tabs, there are two buttons: 'Vista global de las cuentas de usuario' and 'Grupos de usuario'. The main heading is 'Vista global de las cuentas de usuario'. Below this is a table with the following columns: 'Nombre de usuario', 'Nombre del servidor', 'Contraseña', 'Privilegios globales', 'Grupo de usuario', 'Conceder', and 'Acción'.

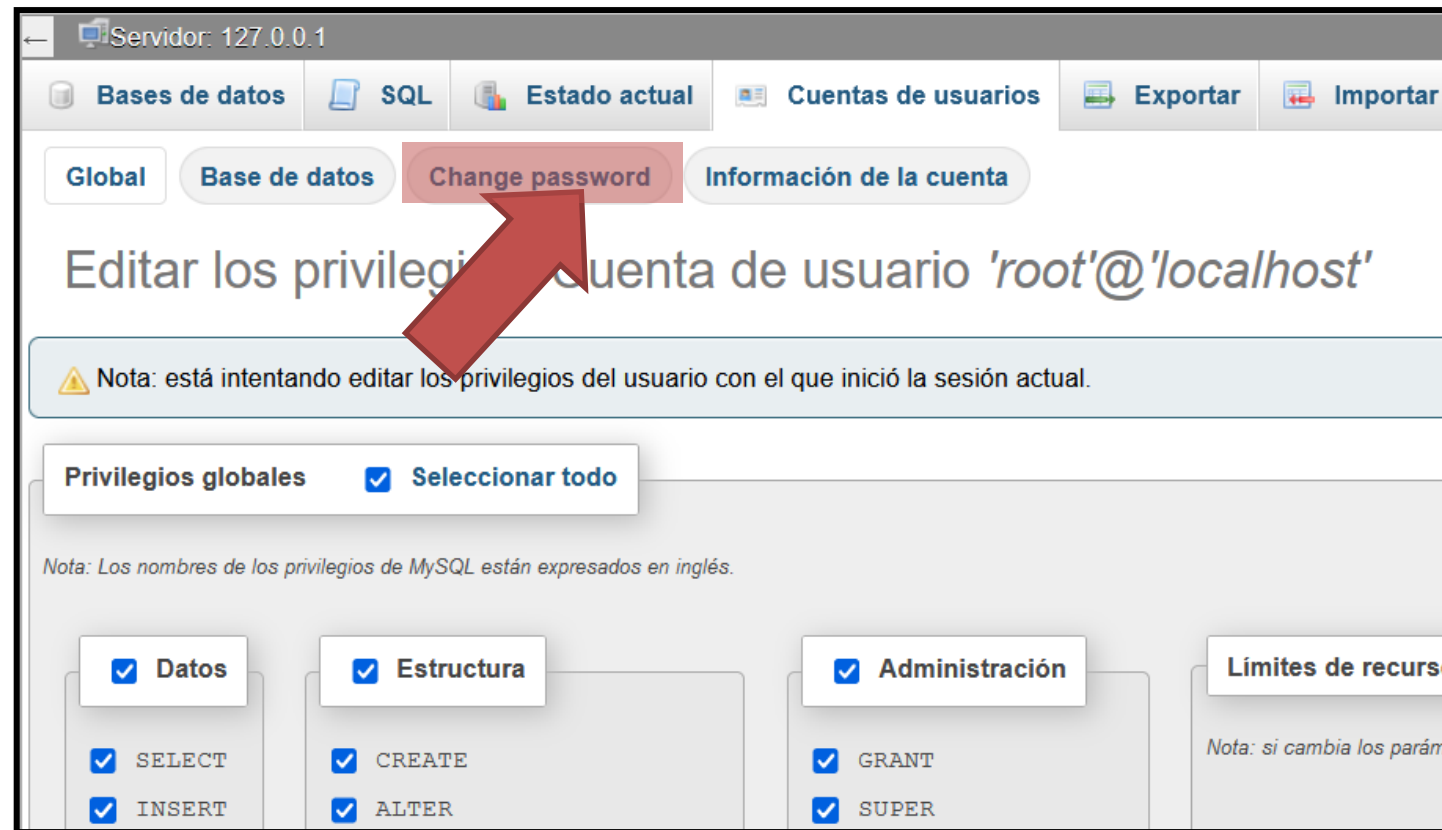
Nombre de usuario	Nombre del servidor	Contraseña	Privilegios globales	Grupo de usuario	Conceder	Acción
<input type="checkbox"/> cualquiera	%	No	USAGE		No	Editar privilegios Exportar
<input type="checkbox"/> pma	localhost	No	USAGE		No	Editar privilegios Exportar
<input type="checkbox"/> root	127.0.0.1	No	ALL PRIVILEGES		Sí	Editar privilegios Exportar
<input type="checkbox"/> root	:::1	No	ALL PRIVILEGES		Sí	Editar privilegios Exportar
<input type="checkbox"/> root	localhost	No	ALL PRIVILEGES		Sí	Editar privilegios Exportar

At the bottom, there is a 'Seleccionar todo' checkbox and a text label 'Para los elementos que están marcados:' followed by an 'Exportar' button.



Usuario root por defecto

- Hacer clic en la opción: Cambiar contraseña



Usuario root por defecto

- Escribir la nueva contraseña
- Confirmar la nueva contraseña
- Hacer clic en el botón Continuar

Global Base de datos Change password Información de la cuenta

Editar los privilegios: Cuenta de usuario 'root'@'localhost'

⚠ Nota: está intentando editar los privilegios del usuario con el que inició la sesión actual.

Cambio de contraseña

☐ Sin contraseña

☒ Contraseña:

Ingresar: Strength:

Debe volver a escribir:

Hashing de la contraseña: Autenticación de MySQL nativo ▼

Generar contraseña Generar

Continuar



Usuario root por defecto

- Para el caso de XAMPP, hay que modificar el archivo **config.inc.php** que se encuentra en la carpeta phpMyAdmin de la carpeta de instalación de XAMPP (la ruta puede variar dependiendo de la instalación de XAMPP)

Este parámetro debe tener el valor: cookie

```
18  /* Authentication type and info */
19  $cfg['Servers'][$i]['auth_type'] = 'cookie';
20  $cfg['Servers'][$i]['user'] = 'root';
21  $cfg['Servers'][$i]['password'] = '';
22  $cfg['Servers'][$i]['extension'] = 'mysqli';
23  $cfg['Servers'][$i]['AllowNoPassword'] = false;
24  $cfg['Lang'] = '';
```

Este parámetro debe tener el valor: false



Asignación de privilegios a nivel global



Asignación de privilegios a nivel de base de datos



Asignación de privilegios a nivel de tabla



3.4 Roles



