La seguridad en las bases de datos es un asunto crucial. Deberíamos aplicar siempre los siguientes principios generales:

- Validar los datos para asegurarnos de que antes de salir de PHP son del tipo que se espera en MySQL.
- Sanear los datos para asegurarnos de que antes de salir de PHP tienen el formato que espera MySQL (por ejemplo, las fechas en formato YYYY-MM-DD).
- Limitar la longitud de los datos. No permitir que se introduzcan textos demasiado largos en la base de datos si no es estrictamente necesario; podrían ser códigos maliciosos.
- Escapar todas las cadenas de caracteres con mysql_real_scape_string.
- Usar un usuario para la conexión de PHP que posea los privilegios mínimos para realizar las operaciones que necesitemos.
- No almacenar datos que realmente no sea necesario. Por ejemplo, no almacenar un número de tarjeta de crédito si no se va a usar en el futuro.
- No almacenar los datos redundantemente. Si en el futuro es necesario modificarlos costará más mantener la base de datos actualizada, y puede llevar a tener datos no coherentes (corrupción de información.)
- Si sólo se necesita saber si un dato se ha escrito correctamente (por ejemplo una contraseña), pero no se necesita saber exactamente cuál es ese dato, almacenarlo hasheado en la base de datos (por ejemplo con MD5).
- Para almacenar datos sensibles, considerar posibilidad de encriptarlos previamente en PHP (librería Mcrypt)

- **Envio de consultas con datos seguros**

La función mysql_real_escape_string() debe usarse siempre para hacer seguros los datos antes de enviar una consulta a MySQL y evitar, en lo posible, inyecciones SQL .

string **mysql_real_escape_string** (string $dato [, resource $conexión])

Escapa caracteres especiales en $dato, teniendo en cuenta el conjunto de caracteres en uso de la conexión, para que sea seguro usarla en mysql_query().

El conjunto de caracteres se puede establecer con la función mysql_set_charset() con la que se indica qué codificación utilizará PHP para los datos que envíe a través de conexión.

bool **mysql_set_charset** (string $charset [, resource $conexión])

```
<?php   //                                                    Ej. Inyección de SQL
$a = $_POST['user'];   //  sea  $a='ana'
$b = $_POST['key'];    //  sea $b = " '  OR  '1' = '1"
....                                  //  suponemos abierta conexión a BD
....
$orden= "select * from users where user='$a'  and clave='$key' ";
mysql_query($orden);
...
?>
```

La orden enviada es: **select * from users where user='ana' and clave ='' OR '1'='1'**

```
<?php   //                                                    Ej. Quitar imyeccion SQL
$a = $_POST['user'];   //  sea  $a='ana'
$b = $_POST['key'];    //  sea $b = " '  OR  '1' = '1"
....        //  suponemos abierta conexión a BD
....
mysql_set_charset('utf8', $conexion);  //  Establece codificacion utf8 para envio/recepcion de datos a Server Mysql
mysql_real_escape_string($a, $conexion);  //  Sanea datos a usar en la consulta
mysql_real_escape_string($b, $conexion);
$orden= "select * from users where user='$a'  and clave='$key' ";
mysql_query($orden);
...
?>
```

La orden enviada es: **select * from users where user='ana' and clave =' \' OR \'1\'=\'1'**

- Crear una base de datos llamada BIBLIOTECA , y en ella crea una tabla llamada **libros** , con el cotejamiento latin1_spanish_ci que implica el juego de caracteres ANSI, con los campos

id autonumerico

titulo texto

autor texto

```
mysql> create database biblioteca;

mysql> create table biblioteca.libros (
            id int auto_increment, titulo varchar(50), autor varchar(50),
                primary key id)  COLLATE  'latin1_spanish_ci';
```

- Crear documento HTML que muestre un formulario con dos campos de texto llamados titulo y autor, cuyo action sea el script procesar_libros1.php, y un enlace al script consultar_libros. Guarda el archivo en utf-8 y añade el header que así se lo indica al navegador

```
<html><head><title>Entrada Libros</title>
<meta http-equiv='Content-type' content='text/html; charset=utf-8'/> </head>
        <body>  <form action='procesar_libros1.php'>
                    Título: <input type='text' name='titulo' id='id_titulo'/><br />
                    Autor:  <input type='text' name='autor' id='id_autor'/><br />
                    <input type='submit'  value='Enviar'  />
                </form>
                echo "<p><center><a href='consultar_libros.php'>Ver libros</a></center></p>";
          </body>
</html>
```

- Crear script **procesar_libros1.php**, que guarde los datos recibidos en tabla libros y muestre en pantalla el id del libro introducido. Guarda el archivo en ANSI.

```
<html><head><title>Registra libros</title>
<meta http-equiv='Content-type' content='text/html; charset=ISO-8859-1'/>  </head>
<body>
<?php
  if ( isset($_REQUEST['titulo'])) { $titulo=$_REQUEST['titulo'];  }   else  { die('Se requiere un título');   }
  if ( isset($_REQUEST['autor'])) {  $autor=$_REQUEST['autor']; }    else  { die('Se requiere un autor');  }

 $conexion=mysql_connect('localhost','root','') or die (mysql_error());
        echo "Recibe:------ $titulo------$autor <br>";
  mysql_set_charset('latin1' , $conexion);     // Establece conjunto de caracteres para diálogo con BD
 mysql_select_db('biblioteca');
// convierte datos recibidos de UTF-8  a ANSI  y muestra el resultado
   $titulo=mysql_real_escape_string(iconv('UTF-8','ISO-8859-1',$titulo));
   $autor=mysql_real_escape_string (iconv('UTF-8','ISO-8859-1',$autor));
   echo "Datos tras la conversión : ------ $titulo------$autor <br>";
// Registra nueva fila en libros y muestra valores registrados
   $consulta="INSERT INTO libros(titulo, autor) VALUES ('$titulo', '$autor'); ";
   $resultado=mysql_query($consulta)  or  die (mysql_error());
   echo mysql_insert_id($conexion).' - '.$titulo.' - '.$autor.'<br>';
 mysql_close($conexion);
echo "<p><center><a href='lib_entrar.html'>Nuevo libro</a></center></p>";
?>
```

- Crear script **consultar_libros.php**, que recorra y muestre los datos de la tabla libros . Guarda el archivo en ANSI

```
<html><head><title>Consulta Libros</title>
<meta http-equiv='Content-type' content='text/html;  charset=ISO-8859-1'/>  </head>
<body>
<?php
  $conexion=mysql_connect('localhost','root','') or die (mysql_error());
  mysql_set_charset('latin1',$conexion);
  mysql_select_db('biblioteca');            $consulta="SELECT * FROM libros; ";
 $resultado=mysql_query($consulta) or die (mysql_error());
  while($fila=mysql_fetch_array($resultado,MYSQL_ASSOC)){
       foreach($fila as $indice=>$valor) {   echo $indice.':'.$valor.'<br />';  }
  }
 mysql_close($conexion);
echo "<p><center><a href='lib_entrar.html'>Nuevo libro</a></center></p>";
?>
```