### **2. SERVIDOR WEB**

### 2.1. Instalación de los equipos

Como ya se ha explicado, se decidió cambiar el antiguo servidor a una nueva máquina puesto que el servicio que ofrecía la máquina antigua era pobre. Esto se debía a dos motivos principales: La máquina en la que residía el servidor era un 486 a 66MHz, que es poco potente y las páginas se ofrecían de forma transparente a través de una LAN interna del departamento que sobrecargaba el tráfico del servidor. Por ello, el departamento adquirió un PC formateado, que no servirá las páginas a través de ninguna LAN, donde se ha instalado el nuevo servidor. Dicho equipo tiene un procesador pentium 4 a 1,5GHz, 512 Mb de memoria RAM y 36Gb de disco duro. En principio se le iban a hacer 4 particiones, dos para Windows (sistema operativo y datos) y otras dos para Linux, pero puesto que el ordenador iba a estar funcionando como servidor no se tendría la oportunidad de reiniciar con otro sistema operativo, así que se finalmente se hicieron 2 particiones, una de 8Gb para el Sistema operativo WindowsXP y otra de 28Gb para los datos.

Tras esto era necesario elegir el sistema operativo en el que correría el servidor. Las dos alternativos que nos planteamos fueron Linux y Windows XP, al ser estos los sistemas operativos más extendidos actualmente. Linux presenta frente a Windows una mayor robustez, tiene un sistema de permisos que lo hace más seguro, es gratuito y permite un mayor control del administrador sobre el equipo. Windows se hace más sencillo ante un usuario inexperto, facilitando la elección de un administrador, presenta mejor compatibilidad con los sistemas PHP y MySQL, que se usarán en nuestro servidor, y con futuros programas que pueden ser instalados en el servidor, como por ejemplo editores de páginas web o Microsoft Office, que probablemente usará el futuro administrador, además, puesto que el diseño del portal se hace primando la seguridad (códigos php seguros, base de datos MySQL segura, opciones de php.ini y httpd.conf orientadas a seguridad) y nuestro entorno no pretende ser de máxima seguridad consideramos Windows es lo bastante seguro para nuestra aplicación. Por todo esto, se eligió Microsoft Windows XP como sistema operativo. Además se instaló las últimas actualizaciones de este sistema operativo reunidas en el service pack 2 para Windows XP.

A continuación, se solicitó conexión a Internet en la roseta en la que se conectaría nuestro ordenador. Para ello fue necesario especificar la dirección de la

12

tarjeta ethernet que poseía el equipo. Dicha dirección se consigue ejecutando el comando "ipconfig /all" o desde el símbolo del sistema "c:>route print". El centro de cálculo nos proporcionó los siguientes datos:

IP:	172.16.2.126
Máscara:	255.255.252.0
Puerta de enlace:	172.16.0.13
Direcciones DNS:	193.147.161.228,
	193.147.161.236,
	150.214.130.15,
	150.214.130.10,
	150.214.186.69
Direcciones WINS:	193.147.161.228,
	193.147.160.144

Por último, y tal como se especifíca en las instrucciones para la conexión a Internet suministradas por el centro de cáculo y adjuntadas en el Apéndice A, se ejecutaron en la línea de comandos las siguientes órdenes:

c:\>route –p add 193.147.160.0 mask 255.255.255.0 172.16.0.1 metric 1 if c:\>route –p add 193.147.161.0 mask 255.255.255.0 172.16.0.1 metric 1 if c:\>route –p add 193.147.162.0 mask 255.255.255.0 172.16.0.1 metric 1 if c:\>route –p add 193.147.163.0 mask 255.255.255.0 172.16.0.1 metric 1 if

## 2.2. Instalación de servidor Apache, PHP y MySQL

Se instala el conjunto servidor Apache, motor PHP y base de datos MySQL principalmente por ser el mismo conjunto que albergaba el servidor antiguo, lo que facilita la migración. Como ventajas, este conjunto está ampliamente desarrollado y extendido lo que hace que existan numerosas aplicaciones ya diseñadas de las que podemos beneficiarnos y se conozcan los fallos de seguridad (y por tanto sean corregidos) del conjunto. Además, el trío de programas están pensados para trabajar conjuntamente, existiendo opciones de Apache para configurar PHP directamente, órdenes PHP para trabajar con bases de datos MySQL, etc... Sin embargo, comentamos a continuación alternativas a este conjunto y las ventajas de nuestro sistema en el caso en el que se estuviera dispuesto a cambiar el portal existente.

En primer lugar tenemos una base de datos de software libre (SQL) frente a otras bases de datos de pago como Access u Oracle. Frente a Postgre SQL (otra base de datos de software libre) tenemos una ventaja y es que Postgre SQL crea automáticamente un campo identificador siempre que se añade una línea a una tabla, lo que provoca que en la tabla de usuarios existan dos campos que identifiquen unívocamente un usuario, lo que provoca fallos en la seguridad.

En segundo lugar tenemos el lenguaje PHP cuyas ventajas son: Es muy adecuado para trabajar con MySQL. Es de software libre (frente por ejemplo a ASP). PHP oculta el código al cliente (frente a HTML o Java).

Por último, Las ventajas del servidor Apache son: Es de software libre (frente a IIS o Sun). Es especialmente compatible con PHP. Finalmente, debido a la extensión del paquete Apache, PHP, MySQL, se hace posible que esté muy actualizado y mejorado.

A continuación se describe la instalación del nuevo servidor.

En primer lugar, se instaló el servidor Apache versión 1.3.26 en d:/PFC/Apache (descargándolo de <u>www.apache.org</u>). Tras ejecutar el instalable se modificó el archivo de configuración httpd.conf tal y como se especificaba en [8], adaptando algunas de dichas modificaciones a nuestro entorno. En concreto se configuró de la siguiente forma:

Se especificó:

- ServerRoot "D:\PFC\Apache". Esta opción indica el directorio raiz del servidor Apache.
- BindAdress 172.16.2.126. Que es la dirección IP de nuestro servidor.
- ServerAdmin <u>fbarrero@gte.esi.us.es</u>. que es el e-mail del administrador de nuestro sistema.
- ServerName localhost. El nombre que recibe nuestro servidor.
- DocumentRoot "D:/PFC/www/" y <Directory "D:/PFC/www/">. El directorio donde estarán todas las páginas web.
- ServerSignature Off. Para no responder con la versión del servidor a peticiones ftp, mensajes de error...
- Options *indexes* FollowSymLinks. Borrando la palabra Indexes si se accede a un directorio que no tenga una página index.html o index.php en nuestro servidor no se muestra la estructura de directorios para elegir una página alternativa.

Se añadió:

- ServerTokens ProductOnly. Esta opción evita que el servidor envíe su versión en respuesta a una orden php.
- Para proteger los directorios config se añade.
   </Directory>

```
<Directory "D:/PFC/www/CSED/config/">
Deny from all
</Directory>
```

```
<Directory "D:/PFC/www/LIE/config/">
Deny from all
</Directory>
```

 Se añade la opción index.php para que pueda haber páginas de inicio php.

```
IfModule mod_dir.c>
DirectoryIndex index.html index.php
```

• Se añade lo siguiente para proteger los archivos con extensión .inc.

```
<Files ~ "\.inc$">
Order allow,deny
Deny from all
Satisfy all
</Files>
```

• Se añade lo siguiente para que el servidor apache trabaje conjuntamente con PHP.

```
LoadModule php4_module D:/PFC/php/sapi/php4apache.dll
AddModule mod_php4.c
AddType application/x-httpd-php .php
```

En el apéndice B se encuentra el listado definitivo de httpd.conf, donde se han marcado las variaciones explicadas en negrita.

A continuación se descargó PHP versión 4.2.2. Se copió la carpeta descargada a d:\PFC\php, php4ts.dll a windows/system32 (donde se encuentran las librerías .dll en los sistemas operativos Windows) y se modificó php.ini-dist tal y como se especificaba en el [8]. Sin embargo, el archivo php.ini se instaló en una ubicación diferente (c:\Windows) de la especificada en dicho proyecto (d:\pfc\apache) para que funcionara correctamente ya que tras la migración no se modificó el archivo mysql.ini por no ser necesario y en ese caso era más sencillo copiar php.ini en la ubicación por defecto.

Seguidamente, se descargó el servidor MySQL versión 3.23.52 y se ejecutó el archivo de "setup", instalándolo todo en d:\PFC\mysql.

Además se ha instalado en dicha máquina el antivirus Trend Micro Internet Security, cuyo número de serie lo suministra la Universidad de Sevilla. En las opciones del antivirus se ha desactivado el Cortafuegos o Firewall para que se pueda acceder al servidor sin problemas.

Por último, se ejecutó el comando Msconfig.exe para eliminar la autocarga al inicio de apache y de MySQLadmin.

#### 2.3. Migración del servidor

Puesto que los archivos httpd.conf y php.ini ya estaban modificados tras su creación, la migración consistió principalmente en dos tareas. En primer lugar, copiar en la carpeta d:\pfc\www todos los archivos del portal (.html, .php, imágenes, manuales, etc..) respetando la estructura de directorios, teniendo que obtener los archivos de dos ubicaciones distintas (woody y apache) mediante ftp y cambiar las rutas de los enlaces que hacían referencia a un servidor o a otro. En segundo lugar, migrar la base de datos MySQL. Sin embargo, el archivo migración.sql resultante de la copia de la base de datos, como se verá a continuación, no se generaba correctamente y ello generó numerosos problemas. Ello nos forzó a probar diversas opciones numerosas veces y de distinta forma sin resultado satisfactorio. Finalmente, se corrigió el error en dicho archivo y todo funcionó. La migración se realizó siguiendo las indicaciones en [8]:

Primero, mediante telnet o directamente en el servidor apache, se entró en el directorio mysql\bin y se copió la base de datos con el comando *mysqldump -uroot - "Contraseña" --opt --all-databases > migracion.sql*. Tras instalar el servidor MySQL 3.23.52 se ejecutó en modo línea de comando *d:\PFC\mysql\bin>mysqld --standalone* para iniciar el servidor MySQL.

A continuación nos conectamos a mysql como usuario anónimo (mysql.exe) y se borró todo lo que había (*drop database mysql*; *drop database test*).

Por último, se ejecutó la migración con el comando *mysql>* source *migracion.sql.* 

La primera vez que se ejecutó dicha orden se copió todo como estaba previsto excepto la tabla db. Para solucionar el problema fue necesario modificar el archivo que había sido generado automáticamente. Se encontró una error de sintaxis en una de las sentencias SQL y se corrigió. A continuación (Ilustración 5) se muestra una pequeña porción del código de dicho archivo (un 20%) para dar una pequeña idea de la complejidad de encontrar dicho error de sintaxis.

16

Ilustración 5. - Porción del código del volcado de la base de datos MySQL.

# 2.4. Modificaciones del portal

Sobre el servidor antiguo se han realizado las siguientes modificaciones que agrupamos en modificaciones a la organización del portal y de los archivos, modificaciones al aspecto del portal y modificaciones a la programación:

#### Modificaciones a la organización del portal y de los archivos:

- Se ha agrupado el portal en su totalidad en un mismo servidor, en lugar de tener las páginas html en uno y las páginas php en otro.
- Puesto que las páginas web se encontraban en dos servidores distintos existían gran cantidad de enlaces de una máquina a la otra. Se han cambiado todos esos enlaces por rutas relativas dentro del mismo servidor. Se han cambiado todos los <u>http://gte.us.es/~fbarrero/</u> por "./../" Esto mejorará enormemente la portabilidad del actual servidor.
- Se ha añadido un hipervínculo al temario de la asignatura Laboratorio de Instrumentación Electrónica desde su portal. Dichas páginas existían pero extrañamente no había forma de acceder a ellas.
- Se ha añadido un hipervínculo a la sección cuestionario de autoevaluación desde el portal de la asignatura Complementos de Sistemas Electrónicos Digitales (Ilustración 6). . Dichas páginas existían pero extrañamente no había forma de acceder a ellas.
- Se ha añadido un hipervínculo al portal del laboratorio virtual (al igual que existía en el portal de la asignatura Laboratorio de Instrumentación Electrónica) desde el portal de la asignatura Complementos de Sistemas Electrónicos Digitales (Ilustración 6).
- Se han corregido algunos hipervínculos del tipo "volver al inicio" del conjunto de páginas del Laboratorio de Instrumentación Electrónica que apuntaban extrañamente a la página de inicio de Complementos de Sistemas Electrónicos Digitales.
- Se ha cambiado el hipervínculo que desde el portal del laboratorio virtual accedía al laboratorio remoto creado con LabVIEW. Para poder modificar dicho hipervínculo es necesario usar el editor de páginas web Dreamweaver, programa con el que fueron creadas las páginas.
- Se ha arreglado el acceso al mundo virtual creado con VRML al que no se podía acceder.
- Se han eliminado en la base de datos MySQL, los permisos lab\_virtual (de la base de datos de usuarios\_lie) y superusuario (de la base de datos usuarios\_csed) que eran innecesarios.
- Se han creado tres usuarios (Ilustración 7): Root (Pwd: "Contraseña"), que es el administrador del portal. Monitor1 (Pwd: "Contraseña"), que tiene los permisos de los monitores, es decir, no puede editar o borrar usuarios ni crear otros monitores o roots (Para ello, al crearlos es

importante no darles los permisos usuarios\_edit o usuarios\_del). Invitado (Pwd: *"Contraseña"*), creado con la intención de tener una cuenta con la que mostrar el portal web a cualquier persona interesada en el tema sin tener por qué ser un alumno.

• Se ha añadido al archivo "httpd.conf" del servidor woody las líneas:

ProxyPass /fbarrero http://172.16.2.126/fbarrero

ProxyPassReverse /fbarrero http://172.16.2.126/fbarrero

De esta forma, el servidor woody (que tiene una IP pública) realiza las peticiones de las páginas al servidor apache de forma transparente al cliente y éste puede, por tanto, acceder a dicho servidor que no tiene una dirección IP accesible.

 Se ha añadido una contraseña BIOS ("Contraseña") y se ha definido un usuario administrador (usuario:alvaro, contraseña: "Contraseña") para iniciar sesión en windows, para así aumentar la seguridad del servidor contra ataques presenciales.

#### Modificaciones al aspecto del portal:

 Se ha uniformizado el formato de las páginas del portal. En concreto se ha cambiado el aspecto de toda la sección Laboratorio virtual (Ilustración 8).

### Modificaciones a la programación:

- Se ha añadido una comprobación de contraseña (login) a la entrada de los portales del laboratorio virtual a los que se podía acceder sin estar autentificado. Para ello, se ha creado un nuevo permiso en las tablas de permisos de usuarios\_csed y usuarios\_lie llamado "laboratorio".
- Se ha protegido el directorio *config* tal y como estaba previsto en [8], ya que existía un error entre lo explicado en [8] y lo que finalmente se realizó. Esta diferencia pudo haberse provocado en uno de los proyectos posteriores en los que se modificaron muchas opciones.
- Se ha añadido el carácter @, en la función conectar() del archivo config.php. Dicho carácter evita la muestra de warnings cuando hay algún problema en la conexión con la base de datos MySQL, lo que podría relevar información importante, como los datos con que se conecta el portal a la base de datos.

- Se añaden a los portales de herramientas administrativas una opción de creación de usuarios específica para monitores (usuarios especiales que pueden crear nuevos usuarios, aunque no otros monitores ni administradores). Dicha opción es una nueva página php denominada usuarios\_mon.php. Para acceder a dicha página basta con tener el permiso usuarios\_add que tendrán los monitores y el administrador.
- Se ha simplificado la administración de los permisos que los monitores pueden otorgar a los usuarios. Tan sólo es necesario cambiar una línea de código claramente identificada y explicada en el archivo usuarios\_mon.php. Actualmente los monitores solo pueden dar permisos de lectura para acceder a los servicios del portal.

```
//Ahora especificamos que permisos no queremos mostrar en gestion de
//usuarios para monitores
    if ($key!=admin_tool && $key!=cuestionario_w && $key!=dudas_w &&
$key!=encuesta_w && $key!=monitores_w && $key!=notas_w &&
$key!=noticias_w){
```

 Se modifica la creación de usuarios específica para el administrador (archivo usuarios.php) para que sea más sencillo crear monitores o usuarios (añadiendo la opción de otorgar permisos de creación, edición y eliminación de usuarios que estaban deshabilitados: usuarios\_add, usuarios\_edit, usuarios\_del). Ahora para acceder a la página usuarios.php será necesario tener el permiso usuarios\_edit que sólo tendrá el administrador.

```
// next($row); recuperamos los permisos usuarios del, add, list y
//edit.
// next($row);
// next($row);
// next($row);
```

- En la sección Laboratorio virtual se ha añadido una sección denominada instrucciones donde están los archivos necesarios para los alumnos; para visualizar el laboratorio remoto, para visualizar el mundo VRML, el programa para compilar programas para el DSK y un tutorial para hacer prácticas remotas. (Ilustración 9)
- Por último se ha modificado el archivo *borrar\_todas\_encuestas.php* de forma que al borrar las encuestas se reinicialicen los flags que controlan que un alumno no pueda rellenar las encuestas más de una vez. Esto antes no ocurría y un alumno sólo podía rellenar las encuestas una vez

independientemente de que estas se hubieran borrado y por tanto no tuvieran ningún resultado.

```
mysql_select_db($db_usuarios, $id) or die ("Fallo al conectar con db
de users");
for ($prof=1; $prof<=3; $prof++) {
    $sql = "UPDATE permisos SET encuesta".$prof."=0 WHERE
user='".$_SESSION['user']."'";
    mysql_query($sql ,$id) or die ("Fallo al marcar encuesta hecha
    en los permisos de usuario");</pre>
```



Ilustración 6.- Nuevo menu del portal CSED.

Editar	Borrar	Nombre	Usuario	Última modif.	admin_tool	administrador	chpass	cuestionario_r	cuestionario_w
1	×	Cualquier invitado	invitado	14/06/2005 - 11:20:17	0	0	0	1	0
1	×	monitor	monitor1	04/08/2005 - 16:28:10	1	0	1	1	0
1	×	Administrador	root	15/03/2004 - 13:01:05	1	1	1	1	1

Ilustración 7.- Tipos de usuarios creados.

🚈 Laboratorio Virtual - Microso	ft Internet Explorer		8 ×
Archivo Edición Ver Favori	tos Herramientas Ayuda		-
	: • • • • • • • • • • • • • • • • • • •		
Dirección 🙋 http://www.gte.us.e	s/fbarrero/CSED/laboratorio/laboratorio.php	- 6	⇒Ir
D.I.E.			×
Departamento de Ingeniería Electrónica	Complementos de Sistemas Electrónicos Digitales		
	El Laboratorio Virtual de Instrumentación Electrónica es una herramienta creada para poder realizar prácticas de forma remota desde cualquier ordenador. También ofrece la posibilidad de conocer el laboratorio y familiarizarte con el material que manejarás durante el curso.		
Non-	Visita virtual visita el Laboratorio de Instrumentacion del L-2		
	Práctica Virtual Realiza una de las prácticas del laboratorio sin moverte de tu casa		
Y	Contactar Para cualquier duda contacta con el Webmaster		
15	Enlaces Aquí encontrarás enlaces a páginas y programas de interés		
	Instrucciones LEER MUY IMPORTANTE		
	Página optimizada para resolución 1024x768		
			7
E Listo		r 47	
📴 Inicio 🗍 💽 🍪 🖼 🚍 🗠	🛛 🥁 🐉 📑 📋 🛄 Alvaro_Ybarra_Memoria   @ ]Laboratorio Virtual - M 💆 Microsoft PhotoDraw - [u]	• 15 1	6:38

Ilustración 8.- Nuevo formato de la sección Laboratorio virtual.



Ilustración 9.- Nueva sección "instrucciones".

# 2.5. Estado actual del servidor (Sistema de directorios)

A continuación describimos el actual sistema de directorios para facilitar la futura administración del servidor. Se harán continuas referencias a las páginas del portal de forma que cuando se desee cambiar alguna de ellas se sepa que archivos hay que modificar.

- D:PFC/Apache Carpeta donde se encuentra instalado Apache y todos sus archivos.
- D:PFC/PHP Carpeta donde se encuentra instalado PHP y todos sus archivos.
- D:PFC/MySQL Carpeta donde se encuentra instalado MySQL y todos sus archivos.
- D:PFC/Moodle\_data Carpeta donde se guardan los archivos subidos a los cursos moodle. En concreto el curso sobre C3x es la carpeta 6.
- D:PFC/www/fbarrero/CSED Al igual que D:PFC/www/fbarrero/LIE, carpetas donde se encuentran los portales de ambas asignauras. A continuación nos centraremos en la descripción de la carpeta CSED pues LIE es muy similar.
- ./CSED/index.html Página principal del portal.
- ./CSED/footer.html pie de página que se llama desde otras páginas del portal.
- ./CSED/admin Carpeta en la que están todos los archivos de las herramientas administrativas. Los nombres de dichos archivos, excepto *index.php* que es la página que muestra el menú con las diferentes herramientas administrativas, son lo bastante claros como para reflejar claramente a que parte de la herramienta administrativa se refieren.
- ./CSED/autoevaluación Carpeta en la que se encuentran los archivos de la sección "Cuestionario de autoevaluación": *Autoevaluacion.php* donde se les presenta el cuestionario y *solucion.php* donde se les muestra el resultado de dicho cuestionario.
- ./CSED/config Carpeta protegida donde se encuentra el archivo *config.php*. En dicho archivo se establecen: e-mail del administrador, nombres de los profesores de la asignatura (que se usarán, por ejemplo, en la encuesta), flag de notas publicadas, usuarios de la base de datos MySQL, bases de datos asociadas a cada servicio del portal y por último, las funciones comunes a todos los archivos ".php".
- ./CSED/descarga\_temario Carpeta donde se encuentran los archivos de la sección "Acceso al temario" cuya página principal es temario.html. Las páginas temario\_html.htm, descarga\_temario.php, descarga\_practicas.html y descarga\_presentaciones.html son las páginas principales de cada una de las

cuatro secciones a las que se accede desde *temario.html*. La página *fondo\_descarga\_temario.html* es el fondo común de todas ellas.

- ./CSED/descarga\_temario/tema1 (2,3,4) Carpetas donde se encuentran los archivos ".html" a los que se accede desde *temario\_html.htm* (temario en formato html)
- ./CSED/descarga\_temario/ficheros Carpeta donde se encuentran los archivos
   ".pdf" a los que se accede desde descarga\_temario.php (temario en formato pdf para descarga).
- ./CSED/descarga\_temario/practicas\_seminarios Carpeta donde se encuentran los archivos ".pdf" y ".zip" a los que se accede desde descarga\_practicas.html (prácticas y seminarios en formato pdf y zip para descarga).
- ./CSED/descarga\_temario/presentaciones Carpeta donde se encuentran los archivos ".zip" a los que se accede desde descarga\_presentaciones.html (presentaciones en formato zip para descarga).
- ./CSED/dudas Carpeta en la que se encuentran los archivos de la sección "Tablón de dudas": *tabladudas.php* donde se muestra el tablón completo de las dudas y *consultadudas.php* donde se responde a la petición de consulta de una duda en concreto.
- ./CSED/encuesta Carpeta en la que se encuentran los archivos de la sección "Encuesta de calidad": *encuesta.php* donde se muestra la encuesta tomando las preguntas de la base de datos y *tomadatos.php* donde una vez rellenada la encuesta, se selecciona el profesor sobre el que está realizada, se envían los datos a la base de datos y se guarda que el alumno ya ha realizado una encuesta sobre ese profesor.
- ./CSED/foro Carpeta en la que se encuentran los archivos de la sección "Foro".
- ./CSED/images Carpeta donde se encuentran las imágenes usadas en todo el portal.
- ./CSED/info\_asignatura Carpeta donde se encuentran los archivos de la sección "Información general de la asignatura": Principalmente tenemos el archivo *info.html* que en parte del mismo accede a los dos archivos ".pdf" contenidos en la misma carpeta.
- ./CSED/laboratorio Carpeta donde se encuentran los archivos de la sección "Laboratorio virtual": *laboratorio.php* es la página principal, *instrumentos.php*, *contactar.php*, *enlaces.php* e *instrucciones.php* son las páginas de las secciones correspondientes. *button9.swf* a *button14.swf* son los botones flash creados con

dreamweaver que deben estar en la misma carpeta que la página en la que se encuentran.

- ./CSED/laboratorio/downloads Carpeta donde se encuentran los archivos que se pueden descargar *instrucciones.php*.
- ./CSED/laboratorio/dswmedia Carpeta donde se encuentran los archivos de Macromedia Director con manuales de los equipos a los que se accede desde instrumentos.php.
- ./CSED/laboratorio/images Carpeta con las imágenes de la sección "Laboratorio virtual".
- ./CSED/laboratorio/vrml Carpeta donde se encuentran los archivos de la visita virtual al laboratorio realizada con VRML.
- ./CSED/login Carpeta en la que se encuentra el archivo *login.php* al que se accede siempre que se abre una página protegida y aún no estamos autentificados.
- ./CSED/manuales Carpeta en la que se encuentran páginas "html" con manuales de los equipos de instrumentación. En estos momentos dichas páginas no estan en uso pero por su utilidad se han dejado entre las carpetas del portal.
- ./CSED/msg Carpeta en la que se encuentran las dos páginas que dan mensajes de error: *Err\_db\_connection.html* si no hemos podido conectar con la base de datos y *Err\_noprivs.php* si no tenemos suficientes privilegios (tras *login.php*) para acceder a una sección.
- ./CSED/notas Carpeta en la que se encuentran los archivos de la sección "Publicación de notas": la sección mostrará la página *notas.php* si está activado el flag de notas publicadas y *notas\_np.php* en caso contrario.
- ./CSED/noticias Carpeta en la que se encuentran los archivos de la sección "Noticias": *noticias.php* donde se muestra el tablón completo de las noticias y *consultanoticias.php* donde se responde a la petición de consulta de una noticia en concreto.

# 2.6. Seguridad en el servidor apache

En primer lugar se comentará brevemente el modo en que se controla la autentificación de usuarios. Dicho sistema se describe en detalle en [8]. Se plantean tres alternativas: Autentificación basada en apache, autentificación basada en Apache con módulo de acceso a MySQL y autentificación basada en código PHP. Para la

primera existen mecanismos basados en la definición de ficheros ".htacces" que permiten proteger directorios y subdirectorios pero ello conlleva que el portal dependa del servidor web subyacente (Apache), y que se modifiquen en tiempo real ficheros de sistema sin que exista un control de acceso a estos provocando colisiones. El segundo sistema, usando MySQL, provee dicho control de acceso pero de nuevo el portal es dependiente del servidor web. Por último se plantea la opción elegida, autentificación basada en código PHP, para ello las páginas PHP acceden al servidor MYSQL con dos tipos de usuarios (de lectura o de lectura y escritura) según las necesidades de la función codificada en PHP (por ejemplo, leer usuarios() se conectaría como usuario de sólo lectura). En todas las páginas PHP existe un código común que lee los permisos del usuario que quiere acceder a una de esas páginas (si no se ha autentificado aun se conecta a la página. Se ha comprobado que todas las páginas del portal (hay páginas creadas en otros proyectos fin de carrera) sigan esta política y en el caso de no ser así se ha subsanado el error.

A continuación explicamos resumidamente (se explica en detalle en [8]) dos tipos de ataques comunes y la protección que contra ellos existe. Ambos son de naturaleza similar. El primero "SQL-inject" consiste en que mediante el uso de caracteres especiales (",',/,etc) se pueden ejecutar sentencias MySQL desde cualquier entrada de datos del portal, por ejemplo, en la autentificación de usuarios. El segundo "Cross Site Scripting" consiste en introducir líneas de código que puedan ser interpretadas por el navegador en lugares donde otros usuarios puedan acceder, por ejemplo, introducir en el foro un código html que pida autentificarse al usuario y que envía la información al autor del código. Igualmente se puede evitar este problema evitando la escritura de caracteres especiales que forman parte de códigos específicos (<html>, </html>, etc). Ambos ataques se contrarrestan con las funciones filtro\_numerico(), filtro\_alfanumerico() y sanitize\_vars() que filtran los caracteres que el usuario introduce.

Contra los ataques físicos o presenciales, es decir, un alumno que físicamente acceda a la sala donde se halla ubicado el servidor, se han tomado las siguientes medidas:

Se ha activado una contraseña de BIOS (*"Contraseña"*) que al ser ésta cargada pide autentificación. Esto evita que se pueda reiniciar el ordenador e iniciar desde un disco de arranque, lo que permitiría acceder a los archivos de sistema de windows que no se encuentran protegidos por permisos.

También hay establecida una contraseña windows para inicio de sesión (en nuestro caso como administrador (usuario:alvaro contraseña: *"Contraseña"*)). Además

26

tras unos minutos de inactividad, se vuelve a mostrar la pantalla de inicio de sesión, siendo necesario colver a autentificarse, sin que esto afecte a los programas en ejecución (servidor apache y MySQL). Esto evita que cualquiera que acceda físicamente al ordenador pueda realmente alterar algo en él.

Por último, reflejamos algunas medidas tomadas para resolver detalles de seguridad de diversa índole:

- Ahora el servidor se puede desconectar de la LAN interna del departamento, de forma que se crea una zona desmilitarizada (DMZ) segura, que evita el acceso a la red interna del departamento si el servidor apache fuera comprometido desde Internet.
- Se ha protegido el directorio *config.php* en los que se almacena información muy importante, en concreto, los dos tipos de usuario y sus contraseñas con las que las páginas PHP acceden a la base de datos MySQL.
- Se ha añadido a las sentencias MySQL "mysql\_connect" en las funciones de conectar a la base de datos conectar() y conectar\_admin.() de los archivos config.php, el carácter @, quedando "@mysql\_connect". De esta forma, si hay algún error en la conexión con la base de datos, no se mostrarán warnings, que en general revelan información potencialmente peligrosa, como la ubicación de la base de datos, nombre del usuario que se está intentando conectar, etc...
- Se han configurado en el archivo "httpd.conf" de apache las siguientes opciones: ServerSignature Off. Para no responder con la versión del servidor a peticiones ftp, mensajes de error... Options indexes FollowSymLinks. Borrando la palabra Indexes si se accede a un directorio que no tenga una página index.html o index.php en nuestro servidor no se muestra la estructura de directorios para elegir una página alternativa. ServerTokens ProductOnly. Esta opción evita que el servidor envíe su versión en respuesta a una orden php.

### 2.7. Migración rápida del servidor actual

Este apartado resume como a partir de la copia de seguridad entregada con el presente proyecto fin de carrera se puede reinstalar el servidor en su totalidad en la

misma u otra máquina. Se explicará de forma sencilla y resumida a modo de manual para el futuro administrador del sistema.

- Para instalar Apache ejecutar el archivo "apache\_1.3.33-win32-x86no\_src.exe" de la carpeta "copia de seguridad apache/ instalables". Elegir instalarlo en "d:\PFC". En el resto de opciones se puede poner cualquier cosa pues se modificarán más tarde.
- Copiar el archivo "httpd.conf" de la "copia de seguridad apache" en "d:\PFC\Apache\conf\" sobrescribiendo el existente.
- Para instalar PHP copiar la carpeta "php-4.2.2-Win32" de la carpeta "copia de seguridad apache/ instalables" en "d:\PFC\" y renombrarla como "php". Copiar el archivo "php4ts.dll" de "d:\PFC\php\" en c:\WINDOWS\System32\".
- 4. Copiar el archivo "php.ini" de la "copia de seguridad apache" en "c:\WINDOWS\".
- Copiar la carpeta "copia de seguridad apache/ www" (las páginas del portal) en "d:\PFC\".
- Para instalar MySQL ejecutar el archivo "setup.exe" de la carpeta "mysql-3.23.52-win" de la carpeta "copia de seguridad apache/ instalables". Elegir instalarlo en "d:\PFC\mysql\" creando la carpeta nueva "mysql".
- La estructura debe quedar: En "D:\" la carpeta "PFC". En dicha carpeta, las carpetas "Apache", "www", "mysql", "php".
- 8. Ejecutar el comando "msconfig" (menu "ejecutar" de windows) y eliminar la carga al inicio de apache y de mysqladmin.
- Copiar en "d:\PFC\mysql\" el archivo "mysql.bat" de la "copia de seguridad apache" y crear en el escritorio un acceso directo al archivo "apache.exe" de la carpeta "Apache" y otro a "mysql.bat".
- 10. Para inciar el servidor apache ejecutar el archivo "apache.exe" de la carpeta "Apache" o bien ejecutar el acceso directo del escritorio.
- 11. Para iniciar el servidor MySQL ejecutar en línea comando en la ubicación "d:\PFC\mysql\bin" el comando "mysqld --standalone" o bien ejecutar el archivo "mysql.bat" del escritorio que ejecuta dichas órdenes.
- 12. Para migrar la base de datos, en primer lugar copiar en "d:\PFC\mysql\bin" el archivo "migration.sql" de la "copia de seguridad apache". Después conectarse a la base de datos ejecutando en línea comando en "d:\PFC\mysql\bin" el comando "mysql". Para poder

conectarse a la base de datos es necesario que el servidor MySQL esté iniciado (paso 10). Borrar a continuación las bases de datos existentes ejecutando en "mysql>" los comandos "drop database mysql;" y "drop database test;". Ejecutar en línea de comando en "d:\PFC\mysql\bin" el comando "mysql>source migration.sql". Salir de la base de datos con "mysql>exit;".

13. Cada vez que se reinicie el ordenador es necesario volver a iniciar los servidores Apache y MySQL siguiendo los pasos 10 y 11.

A continuación explicamos algunos procesos básicos y de uso común.

- Para conectar a la base de datos MySQL (para hacer cambios de estructura) debemos ejecutar en línea de comando en "d:\PFC\mysql\bin" el comando "mysql –uroot – "Contraseña"".
- Para desconectar el servidor MySQL ejecutar en línea de comando en "d:\PFC\mysql\bin" el comando "mysqladmin –uroot –"Contraseña" shutdown".
- 3. Para hacer una copia de la base de datos actual (si ha sufrido cambios) ejecutar en línea de comando en "d:\PFC\mysql\bin" el comando "mysqldump –uroot "Contraseña" --opt --all-databases > migracion.sql". En "d:\PFC\mysql\bin\" se habrá creado el archivo migración.sql, que habrá que editar y eliminar la palabra resaltada de la frase "KEY user (user))" (se puede buscar con la herramienta de buscar del menu edición pues tan sólo aparece en un lugar).