La seguridad informática en el trabajo con la plataforma *Moodle*

Luisa María Romero-Moreno
Universidad de Sevilla

La seguridad informática en el trabajo con la plataforma *Moodle*

Computer Security in Working with the Moodle Platform

Luisa María Romero-Moreno
Universidad de Sevilla
mariaro@us.es

Recibido: 7 de julio de 2010
Aceptado: 26 de noviembre de 2010

Resumen

El trabajo presenta los aspectos de seguridad de la plataforma *Moodle*. Es sabido que los Sistemas Virtuales de Formación impregnan el mundo académico (Campus Virtuales) pero cada día más el de la empresa (Formación Continua). Las plataformas *eLearning* se nos presentan como herramientas adecuadas en estos contextos. Apostamos por el software libre y dentro de él por la plataforma que a día de hoy constituye un auténtico referente en el ámbito de la formación. Pero nos parece fundamental que profesores y tutores puedan tener la seguridad de que sus ficheros están debidamente protegidos. Analizaremos como aprovechar los niveles de seguridad de la herramienta y como configurarla para obtener los resultados esperados.

Palabras clave: eLearning, Campus Virtuales, Aprendizaje Colaborativo, Software Libre

Abstract

This paper presents the security aspects of *Moodle* platform. It is known that the Virtual Training Systems impregnate the academic world (Virtual Campus) but faster and faster the company's (Continuing Training). The platforms eLearning are presented as suitable tools in these contexts. Here we focus on free software and especially on the platform that today is a real landmark in the area of Virtual Training. But it seems essential that teachers and tutors can be safe that their files are protected. In what follow we will analyze how to take advantage of the security levels and how to configure the tool to obtain the expected results.

Keywords: eLearning, Virtual Campus, Collaborative Learning, Free Software.

Referencia bibliográfica: Romero-Moreno, Luisa María (2010). La seguridad informática en el trabajo con la plataforma *Moodle*. *Revista de Humanidades*, 17, p. 169-190. ISSN 1130-5029

1. INTRODUCCIÓN

En este artículo trataremos la seguridad en *Moodle,* pues es sabido que este aspecto está cobrando cada vez más importancia en las aplicaciones informáticas. De hecho la Seguridad Informática se está convirtiendo en una disciplina académica en auge.

Es bien conocido que los Sistemas Virtuales de formación están cobrando cada día mayor protagonismo, en la enseñanza a distancia (imprescindibles), en el ámbito de la universidad en general (campus virtuales asociados a todas ellas) y de una manera considerable en el contexto de las empresas (formación continua de sus profesionales). Pero los profesores y tutores de los cursos y enseñanzas necesitan trabajar con seguridad y tener la certeza de que sus herramientas están a salvo de *ataques informáticos* no deseados.

La seguridad, en este contexto, se encarga de activar mecanismos de protección para los ficheros (Britain, 2004: 39). En particular, se trata de *proteger la información* dejando la responsabilidad del acceso a la misma y su secuenciación en el tiempo en manos de los administradores de las aplicaciones, de *proteger la infraestructura computacional* que trata de que los sistemas y herramientas trabajen satisfactoriamente y prevean situaciones de emergencias (fallos) y de *proteger a los usuarios* administrando concienzudamente los perfiles y permisos.

2. ASPECTOS BÁSICOS DE SEGURIDAD

La plataforma tiene varios niveles de seguridad que deben tenerse en cuenta, desde ella y desde el servidor se pueden configurar algunos aspectos básicos para tener un nivel aceptable de protección ante amenazas. Se dispone de un enlace donde se puede analizar la seguridad y sus posibles soluciones http://moodle.org/security/ [29].

El administrador principal debe ser el responsable de la seguridad de la plataforma. Veremos las configuraciones básicas en los niveles más delicados: servidor, autenticación, contraseñas y roles.

2.1 La seguridad del servidor

El servidor es independiente de la plataforma, es función del administrador del sistema tener bien configurado el servidor donde está alojada.

Para establecer un buen nivel de seguridad en el servidor basta con disponer de:

- Un antivirus actualizado
- Control sobre las actualizaciones del Sistema Operativo, especialmente contra *rootkis* (software para esconderse a sí mismo o a otras herramientas) y *exploits* (software desarrollado para automatizar errores) que podrían dañar el equipo
- Control sobre servicios de Internet abiertos que no vayan a usarse
- Contraseñas complejas y diferentes para *MySQL*, administrador de sistemas y administrador de la plataforma

- Separación entre la carpeta de Datos de *Moodle* y la plataforma principal e imposibilidad de acceso vía web

- Configurar el servidor web (Apache, IIS, etc.) para que impida el acceso a direcciones IP no autorizadas (si se trabaja con red privada)

2.2. La seguridad en autenticación

Los métodos de autenticación de un nuevo usuario pueden ser de diversos, usando la autenticación por defecto de *Moodle* o usando un *plugin* compatible con la plataforma como *Shibboleth*, *LDAP*, etc. En la figura que sigue podemos ver que hay varias maneras de autenticación del usuario, ya hemos comentado la creación de cuentas manual, basadas en email y no hay uso de *login* (inicio sesión). De estas el nivel más seguro es el que contempla la creación de cuentas de forma manual, el administrador será el encargado de darlas de alta. Con esto se evita el acceso de *bots* (programa informático que realiza distintos cometidos y que trata de simular a un humano) y *spam* porque tenemos control absoluto de quienes son los admitidos a la plataforma. Es la opción más recomendada para grupos pequeños de uso pero puede ser un trabajo tedioso para plataformas masivas, así que la opción recomendada será la autenticación basada en email bien configurado.

Para una buena gestión de autenticación basada en *email* es recomendable seguir estos pasos:

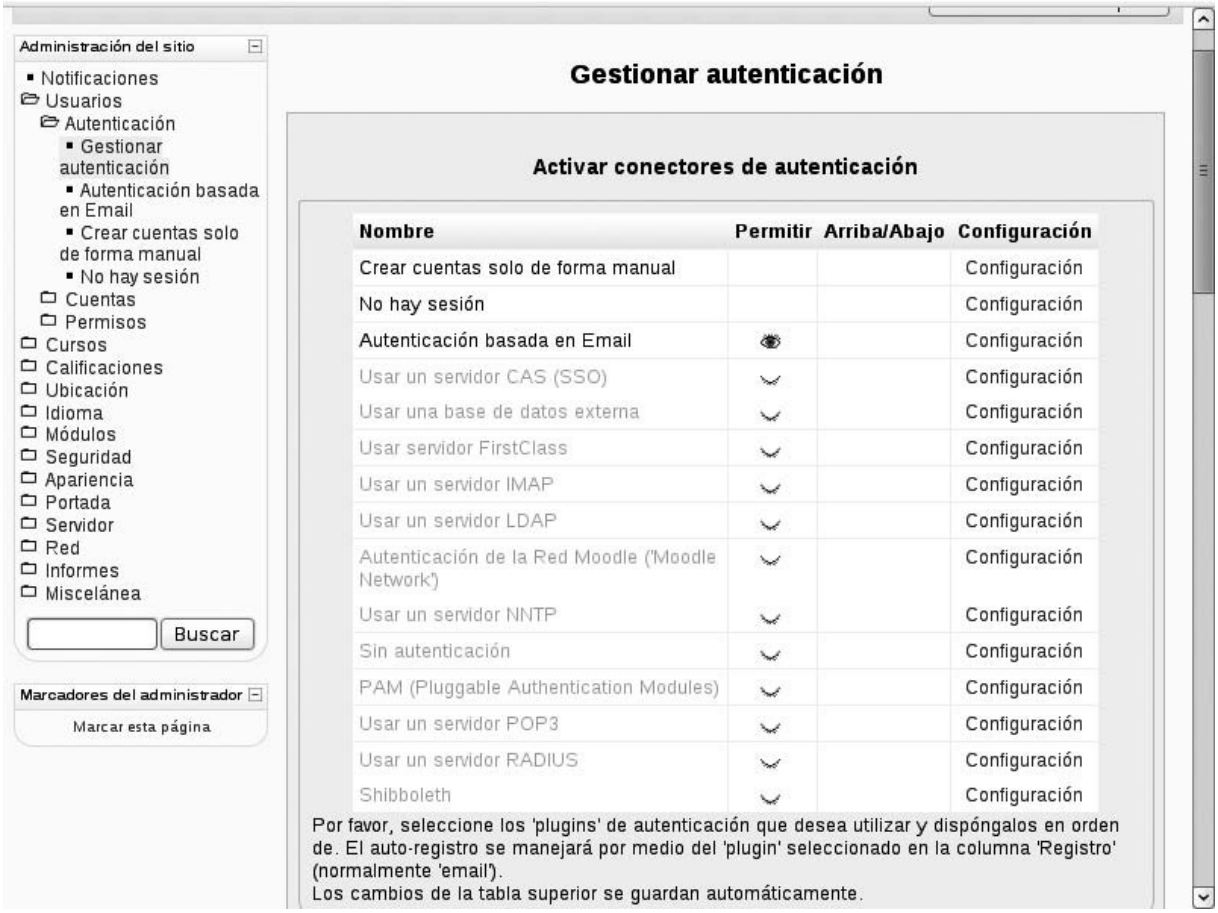
- Dejar bien claro en el campo instrucciones los pasos necesarios para una buena autenticación del usuario, así como la construcción de una buena contraseña de usuario

- Bloquear dominios de correo de tipo sospechoso. Esto hará que los que quieran autenticarse usando un determinado tipo de dominio de correo (ejemplo: *@yahoo.com*, *@hotmail.com*) sean automáticamente rechazados. Con esto no se es muy selectivo pero es bastante útil para evitar cuentas fraudulentas o gobernadas por *bots*. Al igual que se puede bloquear dominios se pueden permitir dominios de *email*

- Bloquear campos de usuario que considere importantes, como por ejemplo la dirección de correo y el nombre. Así se evita la suplantación de identidad del usuario. Si se bloquean campos requeridos por *Moodle*, se debe asegurar que se proporcionan esos datos de forma manual al crear las cuentas de usuario, si no estas cuentas no podrán ser usadas. Para ello existe la opción de 'Desbloqueado si está vacío' que evita este problema

- Regular los invitados no autenticados, determinando bien su rol y sus permisos asignados. En caso de inseguridad se debería desactivar el acceso de invitados, evitando que alguien anónimo acceda a la plataforma

Para insertar *reCAPTCHA* en la plataforma es necesario registrarse en la página oficial, una vez registrados nos darán dos claves: una pública para generar el *plugin* en el formulario de acceso y otra privada para la comunicación entre *Moodle* y el servidor *reCAPTCHA*. No hay que olvidar activarlo en las opciones de autenticación basada en email. Esto obliga a que sólo los usuarios autenticados puedan ver los perfiles del resto de usuarios para mantener a los visitantes anónimos y motores de búsqueda lejos de los perfiles de usuario.



Fg 1. Pantalla de gestión de autenticación

Fg 2 Pantalla de ejemplo de uso de reCHAPTCHA

2.3. Seguridad con las contraseñas

Uno de los cometidos del administrador podría ser forzar a los usuarios autenticados de la plataforma a que usen una contraseña segura para su inicio de sesión, para evitar el robo de contraseñas. No hay un estándar para la configuración de las contraseñas aunque se recomiendan las normas:

- Una longitud mínima de 8 caracteres
- Incluir letras, números y caracteres especiales (ejemplo: $,%,&)
- Debe incluir mayúsculas y minúsculas

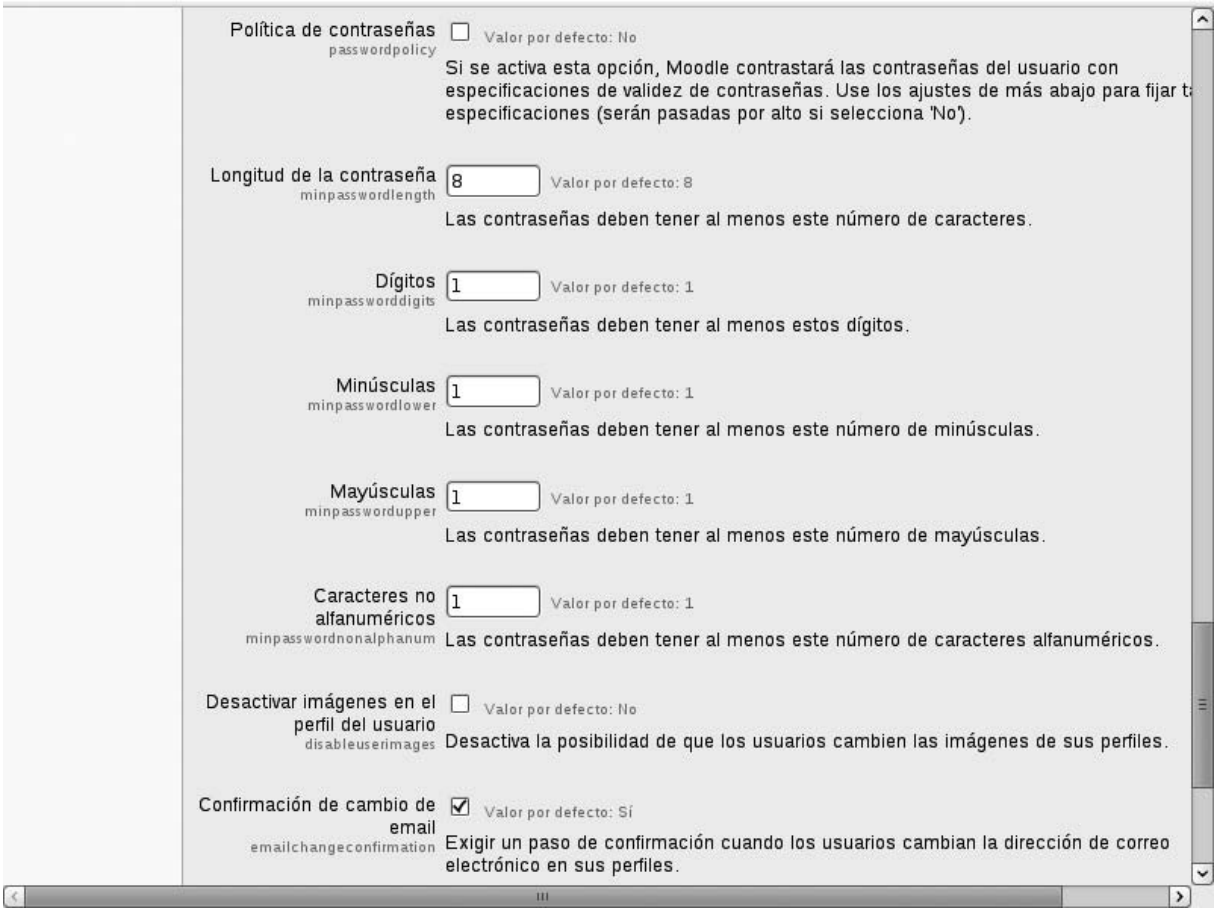
Desde *Moodle* se puede configurar los patrones que debe tener la contraseña de los usuarios. Estos se configuran desde Administración -> Seguridad -> Políticas del sitio. Desde allí se puede definir la longitud de caracteres, los caracteres mínimos no alfanuméricos, cantidad de mayúsculas y minúsculas, dígitos, etc.

Como ejemplo, una contraseña del tipo: "*GT65*&es*", podemos decir que no es una segura porque, aunque cumpla con los requisitos de 8 caracteres incluyendo mayúsculas, números y especiales, no es fácil de recordar con que casi siempre habrá que restaurarla o escribirla en un lugar para recordarla. Es conveniente que sea una contraseña fácil de recordar pero siguiendo las normas comentadas.

Seguridad en definición de Roles

Los roles, bien definidos, pueden ser una herramienta magnífica para la gestión de los permisos de los usuarios autenticados y de la seguridad general de la plataforma a la hora de definir perfectamente qué es lo que puede hacer un usuario o qué es lo que no puede hacer. Mal gestionado puede provocar ataques internos, pudiendo incluso provocar que usuarios no autorizados tengan permisos administrativos poniendo en peligro toda la gestión del sistema.

Moodle tiene configurado por defecto siete roles básicos que son de mayor nivel de permiso a menor: *Administrador*, *Creador de cursos*, *Profesor*, *Profesor no editor*, *Estudiante*, *Invitado* y *Usuario autenticado*. Cada grupo es englobado en un tipo de rol y estos a su vez tienen una serie de permisos definidos. Cada rol se puede asignar de forma global y también de forma específica para cada curso, los permisos de los roles son heredados. Por ejemplo, si tenemos permisos de Creador de cursos de rol global podemos tener también el rol de Estudiante en un curso determinado, teniendo los permisos de Estudiante en el curso y los permisos heredados de Creador de Cursos que no sean incompatibles entre ellos.



Fg 3. Pantalla para política de contraseñas

En cuestión de permisos dentro de los roles hay cuatro, del más bajo al más alto nivel: No ajustado, Permitir, Prevenir y Prohibir. En cuanto a heredar, si no se define un permiso, entonces el permiso de la habilidad recoge el de un rol general que tenga. Permitir y Prevenir se cancelaran uno con el otro si se fija la misma habilidad en el mismo nivel de contexto. Si esto ocurre, nos referimos al nivel de contexto previo para determinar el permiso de la habilidad. Prohibir: Si fijamos prohibir en una habilidad, significa que la habilidad no podrá ser anulada. Prohibir siempre tiene prioridad y crea un alto permanente. Establezcamos un par de ejemplos de usos de rol.

Ejemplo 1. Un usuario tiene rol de *Estudiante* en un curso que permite a todos los estudiantes escribir en los wikis de "Todos" y "Tareas". Pero este usuario también se le asignó un rol de *Invitado* en el nivel contexto de módulo (para el wiki "Bucles") y a los invitados se les prohíbe escribir en el wiki de "Bucles". Por lo que este estudiante puede escribir en los wikis de "Todos" y "Tarea" pero no en el de "Bucles".

Ejemplo 2. Otro usuario se le ha asignado un rol ficticio de *Estudiante Travieso* que prohíbe colocar mensajes en cualquier foro para todo el sitio. Sin embargo su profesor le asigno un rol de *Estudiante* en el "Foro de la Ciencia" en un curso determinado. Debido a que un permiso de prohibir en un contexto más alto siempre gana, este usuario es incapaz de colocar mensajes en el "Foro de Ciencia".

Con cada permiso que queramos modificar nos aparecerá una serie de indicaciones que indican los riesgos que asumimos al permitir dicho permiso. Estos peligros son: inyección de código *XSS* (crear vulnerabilidades de distintos orígenes), puede ver información confidencial, puede tener permisos administrativos y puede *hacer spam*.

La definición de los roles, permisos y peligros están definidos en el párrafo *5.1.2.3 de la carpeta Permisos* de la plataforma.

Generalizando, lo que se debe tener en cuenta a la hora de la seguridad en los roles es:

- Sólo debe haber un usuario con permisos de *administrador*, normalmente el creador de la plataforma. Si se necesita ayuda se puede crear un rol nuevo como administrador secundario que sea heredado de administrador y gestionar los permisos correctamente

- Sólo el administrador debe tener este permiso de *moodle/site:doanything* (Permiso para todo)

- Sólo se debe dar roles globales al administrador y al creador de cursos. El resto se deja con el rol por defecto *usuario* autenticado. Una vez que estén los cursos creados, se pueden asignar roles a los *usuarios*

- No dar privilegios al rol de *invitado*

- No modificar los roles predefinidos de la plataforma *Moodle*, estos roles están bien gestionados y cada rol tiene bien definidos los tipos de permisos. Si se necesita modificar un rol para que se ajuste a lo deseado es mejor crear un nuevo rol que herede del rol que se desea modificar

- Evitar en lo posible asignar roles a los usuarios

3. COPIAS Y RESTAURACIÓN DE SEGURIDAD

Las copias de seguridad son archivos comprimidos en zip que se crean para tener un respaldo si es necesario ir a una versión anterior, como por ejemplo, cuando se actualiza la plataforma. Las copias de seguridad son costosas en CPU por lo que no hay que realizar varias copias al día, es mejor programarlas para una hora donde no haya muchos usuarios. Veremos las copias de seguridad tanto de la plataforma como de los cursos.

Copias y restauración de la plataforma Moodle

Lo siguiente es la creación y restauración de copias de seguridad de una plataforma *Moodle* incrustada en un servidor GNU/Linux. Para WinNT es igual pero cambiando las instrucciones. Los datos que hay que salvar son los de la base de datos, los archivos de datos y el código fuente.

Para la seguridad en lo que respecta a las bases de datos recomendamos el siguiente *script* que puede ejecutarse en Unix para hacer una copia de la base de datos (es buena idea ejecutar dicho script a diario mediante un cron programado):

```
cd /my/ backup/directory
mv moodle-database.sql.gz moodle-database-old.sql.gz
mysqldump-h example.com -u nombredeusuario –password=micontraseña -C -Q -e –create-
options nombredemibasededatos > moodle-database.sql
gzip moodle-database.sql
```

Se puede crear copias de seguridad de la base de datos usando el gestor de base de datos. Cuando se realicen copias de la base de datos completa de un sitio *Moodle*, los administradores deben tener cuidado y vigilar que no se produzcan problemas con la codificación de caracteres. En algunos casos, las copias de seguridad creadas con *mysqldump* o con *phpmyadmin* puede que no codifiquen adecuadamente todos los datos, dando como resultado la inclusión de caracteres a bastardos. Una solución es usar MySQL Administrator http://dev.mysql.com/downloads/gui-tools/5.0.html [44] u otra herramienta que fuerce una codificación de los datos UTF-8 (8-bit Unicode Transformation Format).

En cuanto a la seguridad con los archivos de datos, estos archivos se almacenan en una carpeta definida a la hora de instalar la plataforma *Moodle*. Normalmente, si no se ha cambiado la configuración por defecto debe estar en la siguiente ruta: /var/moodledata/

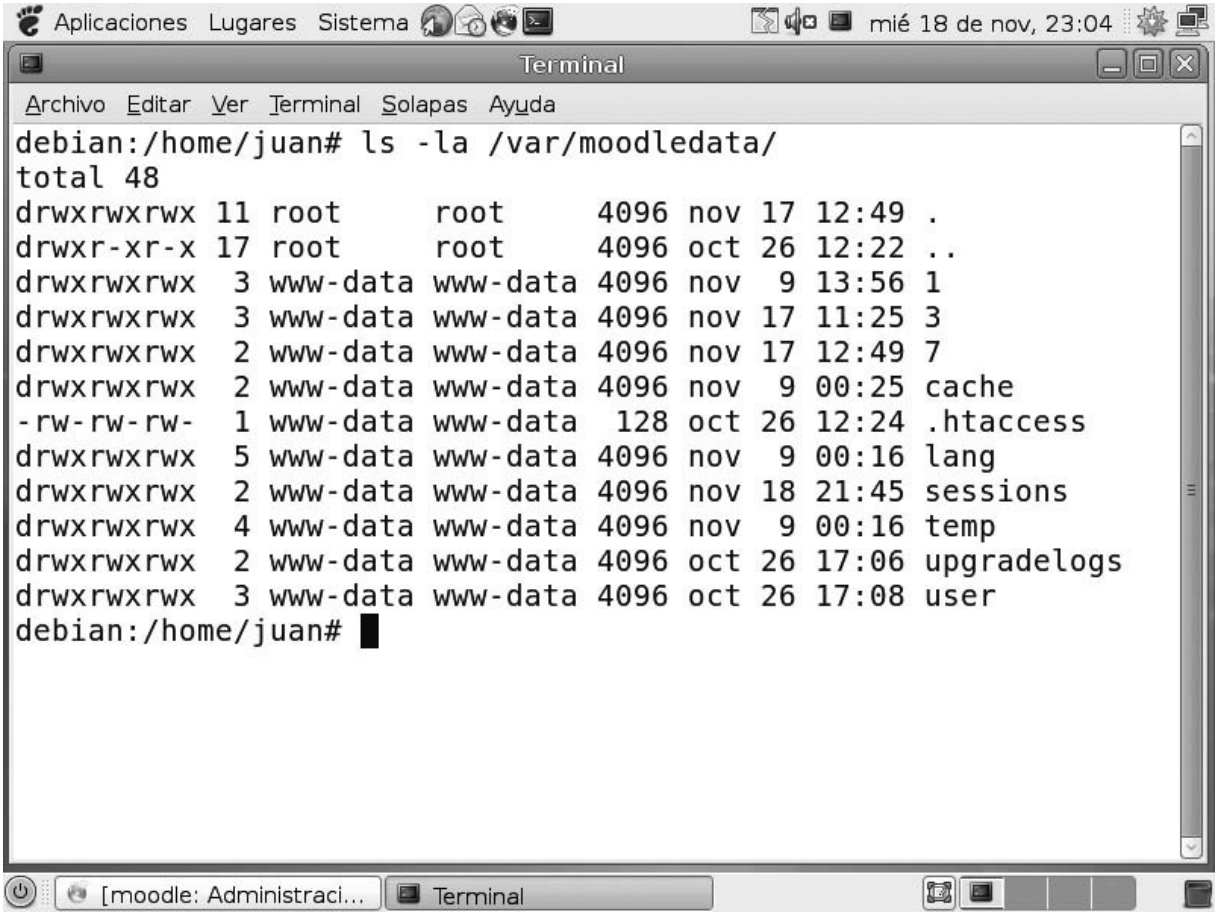
Para crear una copia de seguridad de los archivos simplemente se ejecuta una instrucción que almacene dichos archivos en un *zip*.

```
# tar czvf moodledata.tgz /var/moodledata
```

Este método puede ser lento ya que se vuelven a comprimir archivos ya comprimidos y salvados. Para una mejor gestión se puede usar *rsync* para comprimir sólo los archivos modificados o nuevos.

Para la seguridad con *el código fuente* se siguen los mismos pasos para comprimir el código fuente, pero en vez de comprimir la carpeta de datos se comprime la carpeta donde está alojada la plataforma.

```
# tar czvf moodle.tgz /var/www/moodle/
```



Fg 4. Pantalla con las copias de archivos para la copia de restauración de un curso

Y por último, para restaurar copias de seguridad los archivos comprimidos se descomprimen en las respectivas carpetas. Se pueden seguir algunos pasos de seguridad:

- Cambiar el nombre del directorio original de *Moodl*e a otro diferente (así lo conservará con otro nombre) y colocar la copia de seguridad de *Moodle* en su lugar

- Hacer una nueva base de datos, restaurar la copia de seguridad de base de datos en ella, y cambiar en *Moodle* el archivo config.php para conectarse a esta nueva base de datos. Después se importa la copia de seguridad a dicha nueva base de datos

Copias y restauración de un curso

Como administrador o profesor se pueden hacer regularmente copias de seguridad de un curso, esto es bastante útil para restaurar un estado anterior, recuperar datos perdidos e incluso migrar el curso a otra plataforma. Para ello deben seguirse los siguientes pasos (Caeiro-Rodriguez, *et al.,* 2005: 333).

- Como profesor o administrador, ir a la página principal del curso

- Hacer clic en enlace de "Copia de seguridad..." desde el bloque de administración
- Desde la pantalla de configuración es posible seleccionar los contenidos (actividades y usuarios) a incluir en la copia de seguridad mediante los desplegables
- Pulsar en Continuar
- Después, es posible editar el nombre de la copia de seguridad y ver el listado de los contenidos (actividades y usuarios)
- Pulsar en continuar, al final de la página
- En la siguiente ventana se nos da un listado de las acciones realizadas y, al final, se nos indica el resultado de la copia. Pulsar en continuar
- Finalmente, se nos muestra el archivo que contiene la copia de seguridad

Si se desea se puede hacer una copia en un ordenador local, para aumentar la seguridad, este proceso requiere bastante ancho de banda si el curso tiene mucho contenido. Para hacer una copia local simplemente hay que seleccionar el archivo de copia de seguridad con el botón derecho del ratón y seleccionar "guardar destino como…"

Para restaurar luego una copia de seguridad de un curso se siguen los siguientes pasos:

- Con el rol de profesor o administrador, ir a la página principal
- Hacer clic en el enlace de Archivos del bloque de Administración
- Subir la copia respaldo del curso
- Hacer clic en enlace de "Restaurar..." desde el menú de Administración
- Hacer clic en el botón "Subir un archivo" y elegir el archivo (*zip*) que contiene la copia de seguridad a restaurar. Si ya se hizo se debe pasar al siguiente apartado
- Hacer clic en el enlace Restaurar y seguir las instrucciones del procedimiento

Para restaurar luego el curso se permite elegir entre tres opciones de restauración:

- Nuevo curso: restaurar en un nuevo curso, no sin afectar al resto
- Curso existente, borrando el primero: Al restaurar el curso debemos seleccionar un curso de los ya existentes para sobrescribir este, es decir, restaura el curso pero sobrescribe el curso anterior

- Curso existente, agregando información: Al restaurar el curso existente, agregando información, debemos seleccionar un curso de los ya existentes para añadir el curso sobre este todo el contenido del curso que se pretende restaurar al curso seleccionado. En caso de que se tengan actividades y recursos en el curso elegido, se añaden justo debajo de estas actividades y mantiene los nombres de los temas

Después de restaurarlo se debe borrar la copia de seguridad para ahorrar espacio en el servidor.

4. EL ANTIVIRUS

Como hemos comentado en la administración de la plataforma *Moodle,* se puede descargar e instalar el antivirus *ClamAV®* que es *GPL*. Una vez instalado y configurado el antivirus se conecta automáticamente con *Moodle* si activamos las opciones. El antivirus es muy útil si queremos que se analicen los archivos que se suben al servidor, evitando así la inserción de virus o cualquier otro archivo nocivo para el sistema.

Para configurar el antivirus es necesario especificar la ruta donde está instalado el programa. La ruta debe ser: */usr/bin/clamscan* o*/usr/bin/clamdscan*.

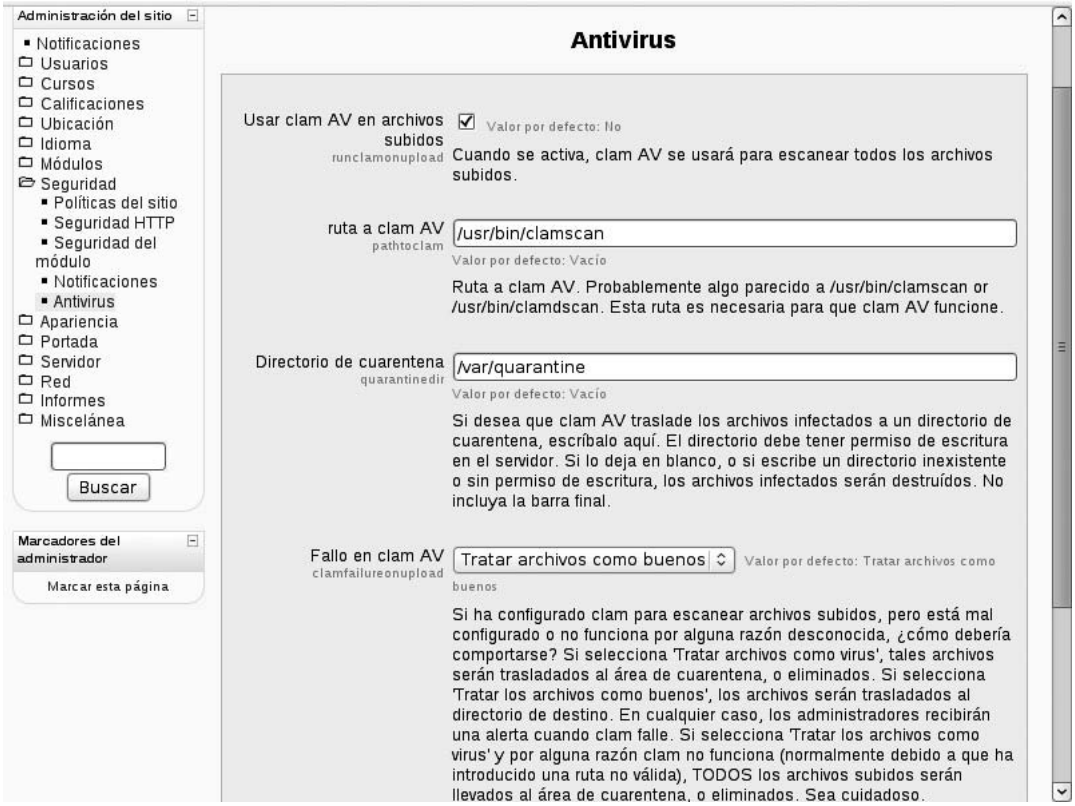
5. EL VISOR DE SUCESOS DE ***MOODLE***

Desde *Moodle* se puede configurar el visor de sucesos de la plataforma. Toda actividad de cualquier usuario se guarda en los registros del sistema. Se pueden visualizar los ficheros *logs* desde dentro de la plataforma en la carpeta Informes y luego Registros desde el bloque de administración. Nos saldrá una pantalla que nos indicará el día que queremos ver los registros, si queremos ver un curso en concreto o toda la plataforma, los participantes y las acciones a ver.

Estos registros se pueden descargar en formato ODT, en formato de texto plano o en formato Excel para almacenarlos.

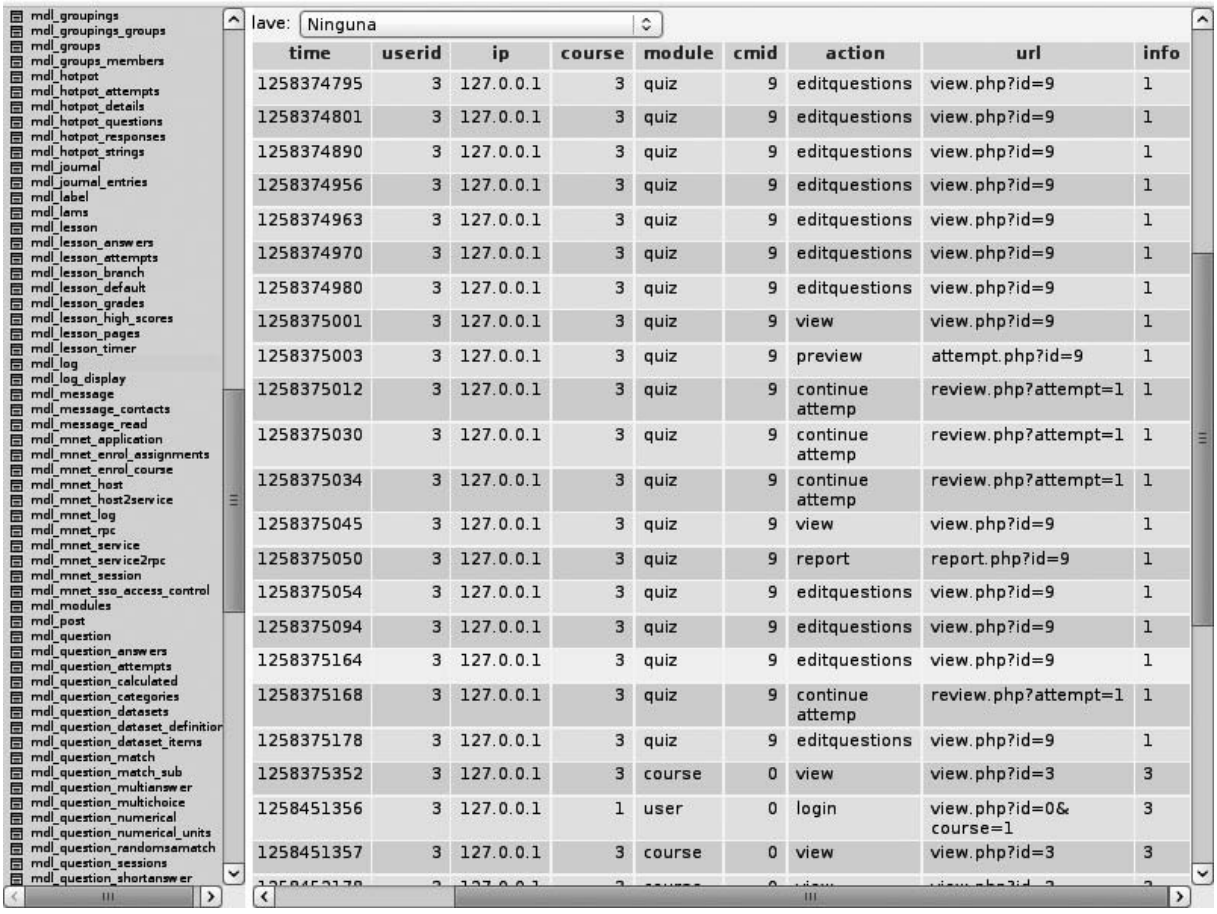
Los ficheros *logs* no es necesario almacenarlos, ya se almacenan directamente cuando se hace una copia de seguridad de la base de datos. Si queremos tener copias de seguridad específicas de los *logs*, se tiene que salvar la tabla *mdl_log* de la base de datos *Moodle*. Esto se puede hacer con el *phpmyadmin* u otro programa de gestión de *MySQL*

Si se tiene activada las estadísticas se pueden ver un informe con las estadísticas generales del sitio *Moodle*. Este informe estadístico se puede enviar por correo a los usuarios elegidos. Desde estos informes se puede acceder con facilidad a los registros que deseemos. Cada vez que se genera un informe estadístico se consumen muchos recursos del sistema, así que es conveniente que se automatice a unas horas donde no haya tráfico de usuarios.



Fg 5. Pantalla del antivirus recomendado

Fg 6. Pantalla del curso que muestra los Informes



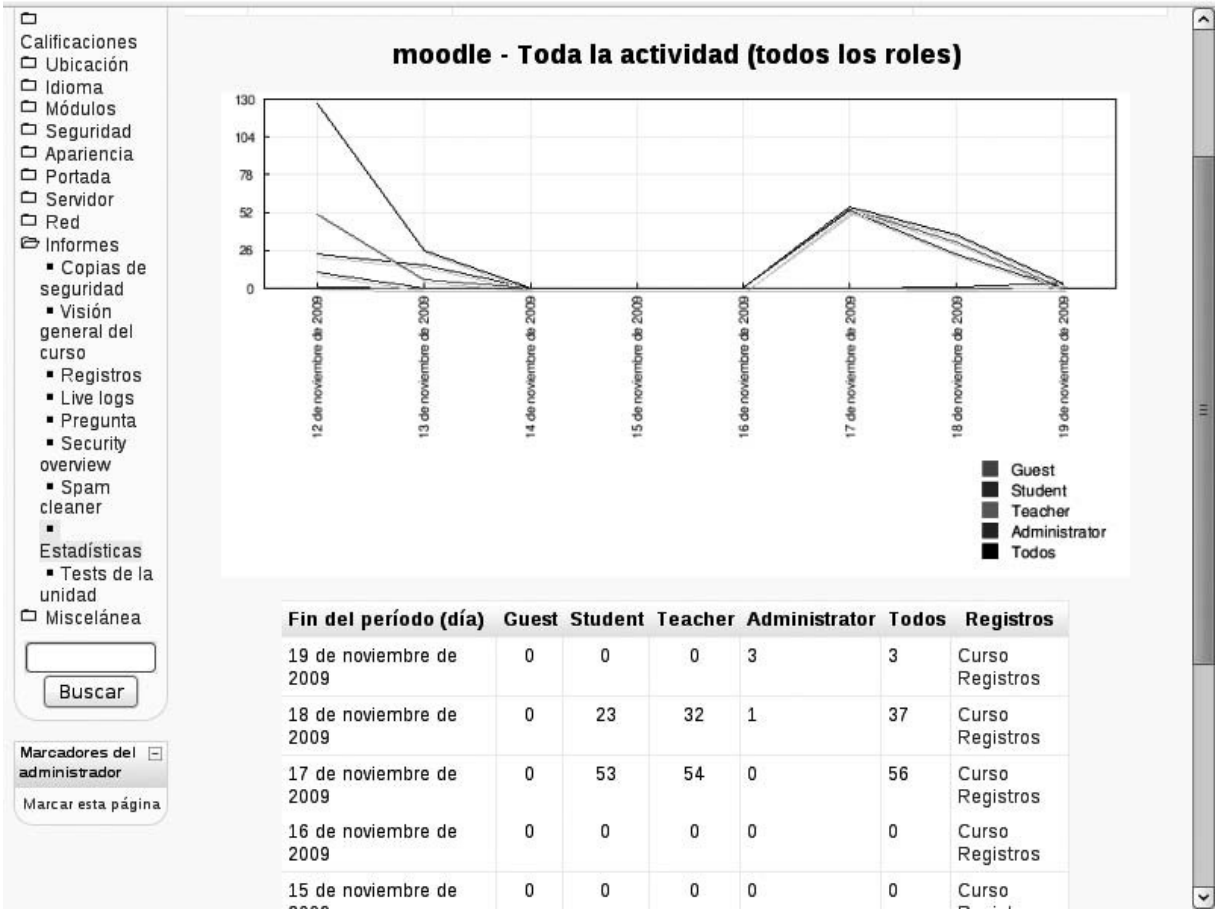
time	userid	ip	course	module	cmid	action	url	info
1258374795	3	127.0.0.1	3	quiz	9	editquestions	view.php?id=9	1
1258374801	3	127.0.0.1	3	quiz	9	editquestions	view.php?id=9	1
1258374890	3	127.0.0.1	3	quiz	9	editquestions	view.php?id=9	1
1258374956	3	127.0.0.1	3	quiz	9	editquestions	view.php?id=9	1
1258374963	3	127.0.0.1	3	quiz	9	editquestions	view.php?id=9	1
1258374970	3	127.0.0.1	3	quiz	9	editquestions	view.php?id=9	1
1258374980	3	127.0.0.1	3	quiz	9	editquestions	view.php?id=9	1
1258375001	3	127.0.0.1	3	quiz	9	view	view.php?id=9	1
1258375003	3	127.0.0.1	3	quiz	9	preview	attempt.php?id=9	1
1258375012	3	127.0.0.1	3	quiz	9	continue attemp	review.php?attempt=1	1
1258375030	3	127.0.0.1	3	quiz	9	continue attemp	review.php?attempt=1	1
1258375034	3	127.0.0.1	3	quiz	9	continue attemp	review.php?attempt=1	1
1258375045	3	127.0.0.1	3	quiz	9	view	view.php?id=9	1
1258375050	3	127.0.0.1	3	quiz	9	report	report.php?id=9	1
1258375054	3	127.0.0.1	3	quiz	9	editquestions	view.php?id=9	1
1258375094	3	127.0.0.1	3	quiz	9	editquestions	view.php?id=9	1
1258375164	3	127.0.0.1	3	quiz	9	editquestions	view.php?id=9	1
1258375168	3	127.0.0.1	3	quiz	9	continue attemp	review.php?attempt=1	1
1258375178	3	127.0.0.1	3	quiz	9	editquestions	view.php?id=9	1
1258375352	3	127.0.0.1	3	course	0	view	view.php?id=3	3
1258451356	3	127.0.0.1	1	user	0	login	view.php?id=0&course=1	3
1258451357	3	127.0.0.1	3	course	0	view	view.php?id=3	3

Fg 7. Pantalla de los informes

6. LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS EN ***MOODLE***

Aunque la plataforma *Moodle* tiene enteramente quién puede y quién no puede acceder a datos sensibles, normalmente es conveniente seguir varios pasos para adecuar la plataforma a la LOPD (Ley Orgánica de Protección de Datos).

Este marco general lo establece INTECO (Instituto Nacional de Tecnologías de Comunicación) y AEPD (Agencia Española de Protección de Datos). Se puede comparar la plataforma educativa como una pequeña red social de carácter formativo y para ello existe el "Estudio sobre la privacidad de los datos personales y la seguridad de la información en las Redes Sociales Online", que se puede visitar en la página web de AEPD https://www.agpd.es



Fin del período (día)	Guest	Student	Teacher	Administrator	Todos	Registros
19 de noviembre de 2009	0	0	0	3	3	Curso Registros
18 de noviembre de 2009	0	23	32	1	37	Curso Registros
17 de noviembre de 2009	0	53	54	0	56	Curso Registros
16 de noviembre de 2009	0	0	0	0	0	Curso Registros
15 de noviembre de	0	0	0	0	0	Curso

Fg 8. Pantalla de la estadística de los informes

Este estudio define, entre otras muchas cosas, las posibles situaciones de riesgo para la protección de la intimidad que pueden ser (Romero-Moreno *et al*,207: 2007).

- En el momento del registro de alta como usuario, si es que no está configurado correctamente la privacidad del perfil, también si se ha publicada información sensible desde el inicio de la actividad en la Red

- En el momento de participación en la red como usuario, en la medida en que el grado de información, datos e imágenes publicados pueden ser excesivos y afectar a la privacidad, tanto personal como de terceros

  - Por lo que respecta a la privacidad personal: a pesar de que sean los usuarios los que voluntariamente publican sus datos, los efectos sobre la privacidad pueden tener un alcance mayor al que consideran en un primer momento ya que estas plataformas disponen de potentes herramientas de intercambio de información, la capacidad de procesamiento y el análisis de la información facilitada por los usuarios

- Por lo que respecta a la privacidad de terceros: es esencial que los usuarios tengan en cuenta que la publicación de contenidos con información y datos respecto a terceros no puede ser realizada si éstos no han autorizado expresamente su publicación, pudiendo solicitar su retirada de forma inmediata

- En el momento de darse de baja de la plataforma en la medida en que el usuario solicite dar de baja su perfil, pero aún así continúen datos publicados por éste, o información personal e imágenes propias publicadas en los perfiles de otros usuarios

Además existe en España, desde el punto de vista normativo, una protección especial para el caso de menores, usuarios masivos de este tipo de servicios *online*, que les otorga un estatus de protección más elevado que al resto de usuarios, en la medida en que el consentimiento para la disposición de los derechos requiere de la intervención de sus padres o tutores legales.

Hay que tener en cuenta tres tipos de protecciones de información:

- Protección de datos de carácter personal

- Protección de la propiedad intelectual e industrial de los contenidos

- Protección de los consumidores y usuarios

De este estudio se obtiene algunas recomendaciones de seguridad:

- Transparencia y facilidad de acceso a la información

  - Resulta fundamental que este tipo de plataformas expongan toda la información relativa a sus servicios de forma clara y comprensible, de manera que el lenguaje empleado en sus condiciones de uso y políticas de privacidad sea absolutamente comprensible para cualquier tipo de usuario

  - Es esencial que las redes sociales destaquen dentro de sus páginas de inicio un apartado específico destinado a informar a los usuarios

  - Se recomienda la creación de pequeñas páginas web con contenido específico y con acceso directo desde la página principal de la red social, en los que se exponga información mediante “preguntas frecuentes” y contenidos multimedia

  - Es esencial que las redes sociales mantengan su política de privacidad y condiciones de uso sin cambios importantes y trascendentales para los usuarios

- Garantizar a los usuarios el control absoluto del tratamiento de sus datos e información publicada en la red poniendo a su disposición el mayor número de herramientas tecnológicas, encaminadas a hacer efectivos sus derechos de forma automática, sencilla y rápida

- Establecer, por defecto, estándares de seguridad y privacidad, referidos a la no indexación por defecto de los datos personales o a la especial protección de los datos sensibles

- Garantizar la seguridad tecnológica de la plataforma. En este sentido, es vital la correcta elección por parte de la plataforma, de un prestador de servicios de Internet (Internet Service Provider o ISP) que cuente con un elevado nivel de seguridad: servidores seguros, centros de respaldo y accesos seguros, entre otras medidas

- Eliminación de la información después de un tiempo prudencial sin que el usuario haya entrado en la plataforma

- Respetar los derechos de acceso y cancelación

Aplicación de la LOPD a la plataforma

En el ámbito de respeto a la LOPD de una plataforma *Moodle*, el sitio debería cumplir todo lo visto anteriormente en concepto de seguridad para cumplir las recomendaciones de seguridad del Estudio. Para establecer nuestra plataforma se debe seguir cuatro sencillos pasos (Romero-Moreno, 2008: 45):

- En el formulario de la solicitud de alta debe incluirse la llamada clausula LORTAD. Para establecer una página de términos y condiciones (LORTAD) de nuestro sitio web simplemente basta con seguir estos pasos:

  - Crea los términos y condiciones en una página Web (archivo HTML)

  - Subir a la raíz de *Moodle*. Si el archivo se llama “condiciones.html”, la ruta será algo como: ../moodle/condiciones.html

  - Entrar a: Administración del sitio -> Seguridad -> Políticas del sitio -> En “URL a la política del sitio” se escribe la dirección donde están las condiciones: http://localhost/moodle/condiciones.html

  - Se pincha en Aceptar *Moodle deslogueará* a todos los usuarios y cuando vuelvan a entrar deberán aceptar las condiciones del sitio

  - Todas las nuevas cuentas, sin importar cómo fueron creadas, deben aceptar las condiciones

- Comunicación a la Agencia de Protección de Datos de la Base de Datos de alumnos, profesores, etc.

- Definir en el Documento de Seguridad de la empresa las especificaciones del dominio de formación

- Establecer mecanismos de protección de los flujos de información (HTTPS, SSH, FTP)

Moodle tiene configurado por defecto siete roles básicos que son de mayor nivel de permiso a menor: *Administrador*, *Creador de cursos*, *Profesor*, *Profesor no editor*, *Estudiante*, *Invitado* y *Usuario autenticado*. Cada grupo es englobado en un tipo de rol y estos a su vez tienen una serie de permisos definidos. Cada rol se puede asignar de forma global y también de forma específica para cada curso, los permisos de los roles son heredados. Por ejemplo, si tenemos permisos de Creador de cursos de rol global podemos tener también el rol de Estudiante en un curso determinado, teniendo los permisos de Estudiante en el curso y los permisos heredados de Creador de Cursos que no sean incompatibles entre ellos.

7. CONCLUSIONES

El artículo que hemos presentado trata del tan actual tema de la seguridad informática y lo hace aplicado a una plataforma de formación virtual de software libre y por tanto de código abierto. Hemos presentado unas pautas para que todos aquellos que se decidan a usar la herramienta (una verdadera *gema* en el mundo de la formación virtual) puedan trabajar con la tranquilidad de que sus cursos no sufren ningún tipo de ataques informáticos.

Considerando que en toda formación (académica o en el ámbito de la formación continua de los profesionales) debe ir inexorablemente ligada a la evaluación, nos ha parecido muy importante tratar y publicar los aspectos de seguridad de la plataforma, aspectos que en el ámbito del *eLearning* no se encuentra suficientemente tratada y resuelta.

8. BIBLIOGRAFÍA

Britain, S. AA Review of Learning Design: Concept, Specifications and Tools. A report for the JISC ELearning Pedagogy Programme, 2004.

Caerio-Rodríguez, M., Llamas N., M. and Anido-Rifón, L. *An EMLmeta-model proposal for the modeling of Collaborative Educational.* SIIE 2005, Leiria , 2005, p. 333-338.

Romero-Moreno, L. M., Ortega, F. J. and Troyano, J.A. *Obtaining Adaptation* for Virtual Courses by Using a Collaborative Tool *and Learning Design,* Proceedings EATIS 2007, Faro, 2007, p. 207-219.

Romero-Moreno, L.M. Monografía *Sistemas Virtuales de Formación Colaborativos: Una Metodología de Análisis de sus Herramientas*. Dirección General de Universidades. Consejería de Innovación, Ciencia y Empresa, 2008.

9. REFERENCIAS

Advance Distributed Learning, 2010, < http://www.adlnet.org>

Aula Global, Elearning y PyMEs – El E-learning en las PyMES, 28 Febrero 2006, <http://www.aulaglobal.net.ve/observatorio/articles.php?lng=es&pg=152>

ARIADNE, 2010, < www.ariadne-eu.org/>

The Apache Software Foundation, Apache HTTP Server Project, 2010, <http://httpd.apache.org/>

Blackboard, Blackboard, 2010, <http://www.webct.com/>

CAMPUS EXTENDS, 2010, http://campusextends.uib.es/

CEN European Committee For Standard, 2010, <http://www.cen.eu>

García Peñalvo, Francisco José. Universidad de Salamanca, "Estado actual de los

sistemas e-learning", 2010, <http://campus.usal.es/~teoriaeducacion/rev_numero_06_2/n6_02_art_garcia_penalvo.htm>

Ochoa, Sergio, Historia de E-Learning, 31 Enero 2007,

http://ajincompu.blogspot.com/2007/01/historia-de-e-learning.html

Centro de Formación Permanente. Universidad de Sevilla, e-Learning. Definición

y características, 2010,< http://www.cfp.us.es>

IMS Global Learning Consortium Inc. http://www.imsproject.org

IMS Global Learning Consortium, IMS GLC, 2009, <http://www.imsglobal.org/>

IMS Global Learning Consortium Inc.http://www.imsglobal.org/specifications.html

LTSC (Learning Technology Standard Comittee) http://ltsc.ieee.org

Official documentation of LAMS http://www.lamsfoundation.org/

Official documentation of LAMS http://www.lamscommunity.org

Official documentation of LAMS http://www.lamsinternational.com/documentation/

Página Moodle http://moodle.org/

Moodle Docs, Moodle Docs en español, <http://docs.moodle.org/es/Página_Principal>

Wikipedia, Moodle, 19 Noviembre 2009, http://es.wikipedia.org/wiki/Moodle

González de Felipe, Ana Teresa, Guía de Apoyo para el uso de Moodle 1.9.4. Usuario Profesor, 2009,

*<http://es.cvs.moodle.org/moodle/*checkout*/contrib/docs/es/1.9.4_usuario_profeor.pdf>*

Castro López-Tarruella, Enrique; Pérez Oñate, Borja; Clerencia Pérez, Isaac,

Moodle: Manual del Profesor, 2004, <http://moodle.unizar.es/file.php/1/Manualprofesor-moodle.pdf>

De la Torre, Aníbal, Plataforma Moodle. Resolviendo actividades, 2006,

http://www.adelat.org/media/docum/moodle/docum/23_cap03.pdf

Comunidad Moodle, Security Announcements, 2009, http://moodle.org/security/ SpamSlayer, Backup of Moodle using Linux, 2008,

<http://www.moodletutorials.org/view_video.php?viewkey=e257e44aa9d5bade97ba>

Fundación Tripartita para la Formación en el Empleo, 2009, <http://www.fundaciontripartita.org>

OPEN UNIVERSITY http://www.open.ac.uk

OPEN UNIVERSITEIT NEDERLAND http://www.ou.nl/

The PHP Group, PHP, 2009, <http://www.php.net/>

Sun Microsystems, MySQL, 2009, <http://www.mysql.com/>

phpMyAdmin Devel Team, phpMyAdmin, 2009,

<http://www.phpmyadmin.net/home_page/index.php>

ErfurtWiki, EfurtWiki, 12 Mayo 2005, http://erfurtwiki.sorceforge.net

ClamAV, ClamAV, 2009, <http://www.clamav.net>

Google, API de Google Maps, 2009,

http://code.google.com/intl/es/apis/maps/

Glencoe, ExamView Pro user's guide, <http://www.ntcschool.com/sites/common_assets/health_fitness/exam_view_inst.pdf>

Half-Baked Software, Hot Potatoes, <http://hotpot.uvic.ca/>

Sun Microsystems, MySQL Administrator, 2009,

<http://dev.mysql.com/doc/administrator/en/index.html>

Agencia Española de Protección de Datos, Agencia Española de Protección de Datos, 2009, https://www.agpd.es/

ReCAPTCHA, ReCAPTCHA, <http://recaptcha.net>

Estudio de las redes sociales: Instituto Nacional de Tecnologías de Comunicación; Agencia Española de Protección de Datos, Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online, <https://212.170.242.196/portalweb/canaldocumentacion/publicaciones/common/studios/est_inteco_redesso_022009.pdf>

Página RDF http://www.w3.org/TR/rdf-schema

Página Reload http://www.reload.ac.uk/

South Cheshire College, Learnwise, 2009, <http://www.scheshire.ac.uk/new_scc/courses/learnwise/learn.asp>

UNED http://www.uned.es/

UOC http://www.uoc.edu