

## Mantenimiento del espacio web

### • Actualizaciones de Joomla!

La actualización a las nuevas versiones de Joomla! es siempre necesaria si queremos que nuestro espacio web no tenga vulnerabilidades peligrosas, y mantenga depuradas sus funcionalidades. Aunque el proceso que se describe es sencillo, es conveniente realizar copias de seguridad antes de toda actualización, tal y como se describe en el apartado siguiente de este capítulo.

**Para las versiones 1.0.X**, la actualización se realizaba de forma sencilla y requería dos pasos:

- Descargar la actualización de la versión que tenemos a la nueva. La comunidad Joomla!, cada vez que aparecía una nueva versión 1.0.X ofrecía dos distribuciones, una completa para realizar instalaciones nuevas, y una de actualización.
- Una vez descargada la actualización, se descomprime el paquete en nuestro equipo, y utilizando un programa cliente de FTP se realiza una sobrescritura de las carpetas y archivos en el servidor donde tenemos instalado Joomla!

**Cuando aparece la versión 1.5** el proceso de actualización de las versiones anteriores 1.0.X no se puede realizar de esta forma, y es necesario realizar una migración, cuyos detalles se encuentran en el servicio de ayuda de Joomla! Spanish:

[http://ayuda.joomlaspanish.org/index.php?option=com\\_content&task=view&id=184&Itemid=66](http://ayuda.joomlaspanish.org/index.php?option=com_content&task=view&id=184&Itemid=66)

**Para las versiones 1.5.X** el proceso de actualización es análogo al de las versiones 1.0.X. En el espacio de descarga del proyecto Joomla!, cuando aparece una nueva versión, se disponen la nueva versión completa y la versión que es actualización de la anterior, y de todas las anteriores.

Nombre de la Publicación	Fecha de Publicación	Tamaño del Fichero	Contador de Descargas
<b>Joomla1.5.5</b>	2008-07-26 23:00:00		
<a href="#">Joomla_1.5.5-Stable-Full_Package.zip</a>		6 MB	25234
<a href="#">Joomla_1.5.5-Stable-Full_Package.tar.gz</a>		4 MB	4833
<a href="#">Joomla_1.5.5-Stable-Full_Package.tar.bz2</a>		3 MB	3162
<b>Joomla1.5.5updates</b>	2008-07-26 23:00:00		
<a href="#">Joomla_1.5.4_to_1.5.5-Stable-Patch_Package.tar.bz2</a>		101 KB	597

Si queremos, como es nuestro caso, realizar una actualización de la instalación de la

versión 1.5.4, tenemos que realizar los dos pasos mencionados anteriormente:

- Descargar la actualización.

### Observación: Localización del archivo de actualización.

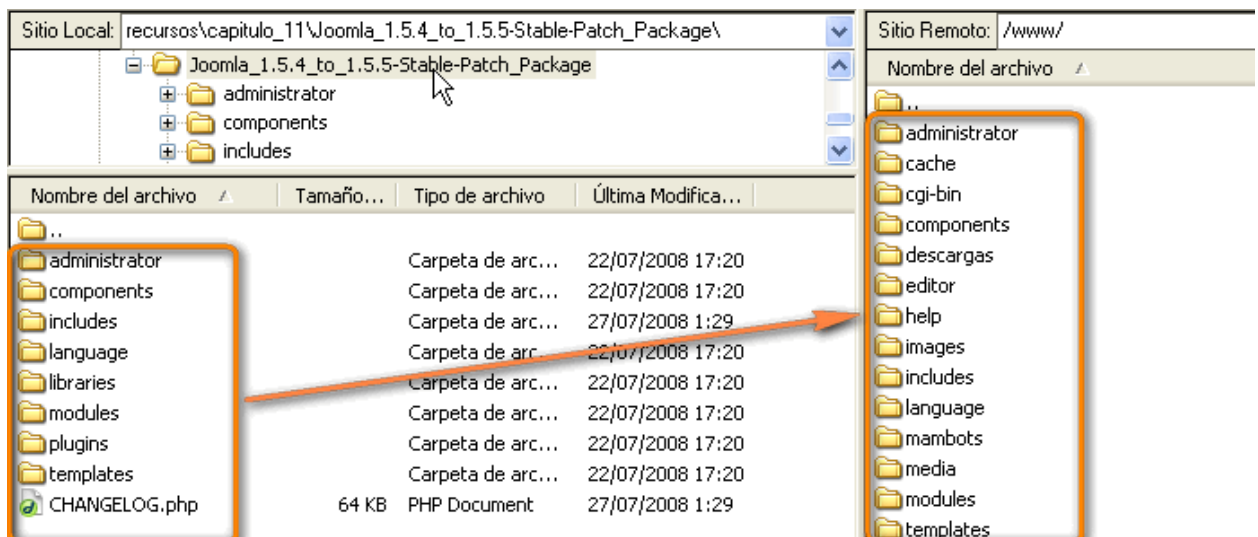
El archivo comprimido que utilizaremos para actualizar la versión 1.5.4 a 1.5.5 se encuentra localizado en **Recursos**:

Nombre del archivo: **Joomla\_1.5.4\_to\_1.5.5-Stable-Patch\_Package.zip**

Si se ha decidido utilizar desde el principio la versión distribuida en español, el archivo de actualización se llama:

**Joomla\_1.5.4\_a\_1.5.5-Spanish-Parche\_Pack.zip**

- Una vez descargada la actualización, se descomprime el paquete en nuestro equipo, y utilizando un programa cliente de FTP se realiza una sobrescritura de las carpetas y archivos en el servidor donde tenemos instalado Joomla! Si estuviéramos trabajando con una instalación en un servidor local, está claro que lo que debemos hacer es una copia del contenido del archivo de actualización sobre las carpetas y archivos de la instalación, sobrescribiendo todo el contenido.



### • Copias de seguridad del espacio web.

Es conveniente realizar copias de seguridad con cierta frecuencia. En caso de que el sitio web deje de estar operativo, por el motivo que sea, siempre podremos recuperar la última copia de seguridad realizada.

El proceso es sencillo, se necesita hacer una copia de seguridad de la estructura completa de carpetas y archivos; y una copia de seguridad de la base de datos.

- Utilizando un programa cliente de FTP, la copia de todas las carpetas y archivos de nuestro sitio Joomla! es sencilla, no hay que hacer nada más que descargarlos en nuestro equipo, y con un poco de paciencia, la tendremos

reproducida y a buen recaudo.

- Para realizar la copia de seguridad de la base de datos, es necesario actuar sobre ella, y si disponemos de alguna aplicación gestora de bases de datos, phpMyAdmin, por ejemplo, el proceso es sencillo. Los paneles de control de servidores contratados pueden permitir, en algunos casos, realizar directamente copias de seguridad.

Accedemos a phpMyAdmin, tal y como se explicó en el capítulo 2, y seleccionamos nuestra base de datos.

The screenshot shows the phpMyAdmin interface for a MySQL server at localhost, connected to the 'joomla' database. The 'Estructura' (Structure) tab is active, displaying a table list with columns: Tabla, Acción, Registros, and Tipo. The tables listed are:

Tabla	Acción	Registros	Ti
<input type="checkbox"/> jos_banner	[Icons]	8	Myl
<input type="checkbox"/> jos_bannerclient	[Icons]	1	Myl
<input type="checkbox"/> jos_bannertrack	[Icons]	0	Myl
<input type="checkbox"/> jos_categories	[Icons]	22	Myl
<input type="checkbox"/> jos_components	[Icons]	33	Myl
<input type="checkbox"/> jos_contact_details	[Icons]	1	Myl
<input type="checkbox"/> ios_content	[Icons]	43	Myl

Aparece la página que muestra todas las tablas de la base de datos con información de los parámetros que la definen. En la parte superior observamos unas pestañas que permiten acceder a diversas acciones que se pueden hacer con la base de datos. Elegimos “Exportar”, y entramos en la página que define la exportación de la base de datos completa.

The screenshot shows the 'Export' configuration page in phpMyAdmin. The title is 'Ver el volcado esquema de la base de datos'. The page is divided into several sections:

- Exportar:** A list of tables to export: jos\_banner, jos\_bannerclient, jos\_bannertrack, jos\_categories, jos\_components, jos\_contact\_details. Below this are options for file format: Datos CSV, CSV para datos de MS Excel, Microsoft Excel 2000, Microsoft Word 2000, LaTeX, Hoja de cálculo Open Document, Texto Open Document, PDF, SQL (selected), and XML.
- Opciones SQL:**
  - añadir su propio comentario en el encabezado (In segmenta las oraciones)
  - Incluir lo exportado en una transacción
  - Deshabilitar la revisión de las llaves extranjeras (foreign keys)
  - Modalidad compatible con SQL: MYSQL323
  - Estructura:
    - Añada DROP TABLE / DROP VIEW
    - Añada IF NOT EXISTS
    - Añadir el valor AUTO\_INCREMENT
    - Usar "backquotes" con tablas y nombres de campo
  - Añadir en los comentarios:
    - Fechas de creación/actualización/revisión
  - Datos:
    - Completar los INSERTS
    - INSERTs extendidos
    - Longitud máxima de la consulta creada: 50000
    - Usar "inserts" con retraso
    - Usar la opción ignore inserts
    - Usar hexadecimal para campos binarios
    - Tipo de exportación: INSERT
- Enviar (genera un archivo descargable):**
  - Plantilla del nombre del archivo (1): \_DB\_ (  recordar la plantilla )
  - Compresión:  Ninguna  "comprimido con zip"  "Comprimido con gzip"

A 'Continuar' button is located at the bottom right.

En principio, podemos dejar todo como se ve en la imagen, incluyendo las opciones “Añada DROP TABLE” y “Añada IF NOT EXISTS”, la indicación de que se genere un archivo descargable y eligiendo, si lo deseamos, algún tipo de compresión.

Es adecuado tener en cuenta la modalidad compatible con SQL, porque a la hora de recuperar la base de datos será importante. Elegimos “MYSQL323”.

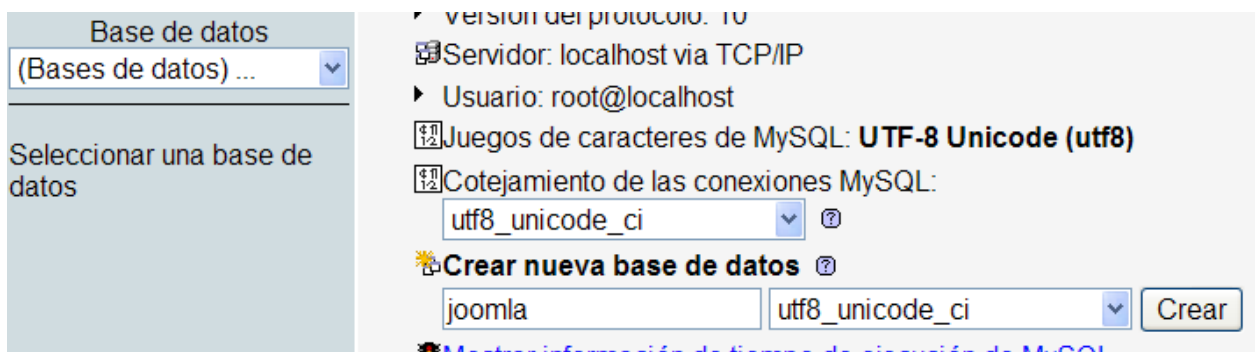
Sólo queda decidir que “*Continúe*” con la operación y ya podemos descargar el archivo en nuestro equipo. Tendrá un nombre del tipo “joomla.sql”, “joomla.sql.zip” o “joomla.sql.gz”, si la base de datos que estamos exportando se llamaba “joomla”, claro.

## • Restauración de una copia de seguridad del espacio web.

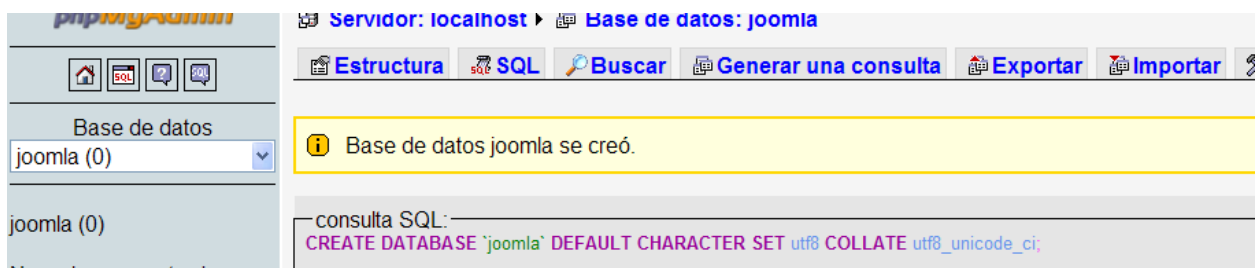
Si tenemos recuperada la copia de seguridad, la restauración del espacio web requiere dos pasos.

- Restaurar la estructura de archivos y carpetas en el servidor, para lo que utilizaremos un programa cliente de FTP.
- Restaurar la base de datos. Si tenemos la opción de utilizar un gestor de bases de datos tipo PhpMyAdmin el proceso es sencillo.

### 1. Creamos una base de datos vacía.



### 2. Observamos la indicación de que la base de datos se ha creado, pero todavía no tiene tablas,



### 3. Y unas pestañas en la parte superior con las operaciones que podemos hacer con la base de datos. Elegimos “Importar”.

4. Localizamos el archivo que descargamos cuando hicimos la restauración de la base de datos, “joomla.sql.gz”, por ejemplo, y elegimos la modalidad compatible con SQL “MYSQL323”. Decidimos “Continuar”.

**Importar**

Archivo a importar

Localización del archivo de texto:   (Tamaño máximo: 2,048KB)

Juego de caracteres del archivo:

La compresión escogida para el archivo a importar se detectará automáticamente de: Ninguna, gzip, zip

---

Importación parcial

Permita la interrupción de la importación en el caso de que el script detecte que se ha acercado a su límite de tiempo. Esto podría ser un buen método para importar archivos grandes; sin embargo, puede dañar las transacciones.

Número de registros (consultas) a saltarse desde el inicio

---

Formato del archivo importado

SQL

Opciones SQL

Modalidad compatible con SQL

5. Y ya hemos realizado la importación de la base de datos.

The screenshot shows a database management interface with a top navigation bar containing icons for home, SQL, search, and generate query. Below the navigation bar, there is a sidebar on the left with a 'Base de datos' dropdown menu set to 'joomla (36)'. The main area displays a yellow message box with an information icon and the text: 'La importación se ejecutó exitosamente, se ejecutaron 99 consultas.' Below the message, the 'Importar' section is visible, showing the 'Archivo a importar' field.

Dominar la restauración del sistema Joomla! al completo permite un trabajo más que interesante: **preparar el sitio web en local para más tarde reproducirlo en un servidor remoto.**

6. Es importante tener claro que aunque hayamos realizado correctamente estos pasos en la restauración de un sistema, si se realiza reponiendo una copia de seguridad, nada cambia con respecto a la configuración básica del sistema, pero si lo hacemos en un servidor distinto y/o en una localización relativa distinta, tenemos que realizar alguna modificación en el archivo de configuración, “configuration.php”
7. El proceso es sencillo, con un cliente de FTP descargamos el archivo de configuración en nuestro equipo para editarlo, abriéndolo con una aplicación de edición de código.

## 8. Debemos modificar la información de:

- La base de datos. Localizamos las líneas que definen el “host”: usuario, contraseña, nombre de la base de datos, y corregimos la información detallada entre comillas (‘localhost’, por ejemplo) con la información real que debemos conocer del servidor en el que estamos restaurando la copia de seguridad de Joomla!

```
var $dbtype = 'mysql';
var $host = 'localhost';
var $user = 'usuario';
var $password = 'contrasena';
var $db = 'joomla';
var $dbprefix = 'jos_';
```

- La posición absoluta de las carpetas “logs” y “tmp” en el servidor.

```
var $log_path = 'C:\\wamp\\www\\joomla\\logs';
var $tmp_path = 'C:\\wamp\\www\\joomla\\tmp';
```

Podemos conocer esta referencia absoluta localizando la información del “Directorio base de apertura” (*Open basedir*) desde la información que nos proporciona Joomla! sobre la configuración de PHP:

### Ayuda >> Información del sistema >> Configuraciones de PHP

Directorio base de apertura (Open basedir):	/tmp:/var/tmp:/var/www/errors/:usr/share/php:/home/vol1/260mb.com/pacus_1250728/cursojoomla.260mb.com/htdocs
---	--

Lo podemos ver en esta imagen, correspondiente a una restauración realizada en un alojamiento web gratuito. Teniendo presente que si la instalación se ha realizado sobre una carpeta creada en el nivel de “htdocs”, será incluida en la especificación de esta referencia absoluta.

En caso de que necesitemos conocer la ruta de un espacio en remoto, si el servidor web es Linux, podemos crear un archivo de texto con el siguiente contenido,

```
mylinux# cat getcwd.php
<?
echo getcwd();
?>
```

guardarlo, por ejemplo con el nombre “ruta.php”, subirlo por FTP a nuestro espacio web, y ejecutarlo, es decir, escribiendo una URL de este tipo en un navegador:

<http://www.midominio.com/ruta.php>

El único problema que podemos tener al realizar respaldos de copias de seguridad es que algunas extensiones utilizan rutas absolutas a carpetas y archivos y es probable que el sitio recuperado no funcione como se esperaba, habrá que comprobarlo.

### **Observación: Automatización de creación de copias de seguridad.**

Existen varias extensiones que permiten realizar copias de seguridad, desde aquellas que automatizan la copia de la base de datos, incluso para enviarla regularmente por correo electrónico, hasta aquellas que permiten operaciones más complejas. En este caso, se presenta una extensión que una vez instalada permite gestionar fácilmente copias de seguridad de las carpetas y archivos del servidor y de la base de datos. Es un componente y el archivo de instalación se encuentra en **Recursos**.

Nombre del archivo: **com\_joomlapack-1.2-j15.zip**

Se incluye un archivo de documentación distribuido por los desarrolladores:

**JoomlaPack\_User\_Manual\_1.2.pdf**

Aunque la restauración de una copia de seguridad es más complejo para este tipo de aplicaciones, y el componente no lo permite, se incluye una aplicación PHP que debe ser ejecutada desde el servidor una vez descomprimida y subida por FTP, y que permite la recuperación del espacio:

**kickstart\_1.2.zip**

- **La seguridad en nuestro espacio web<sup>1</sup>.**

El tema de la seguridad de un espacio web es realmente delicado y complejo, pero en estos momentos sólo nos podemos centrar en lo que podemos hacer, en primera instancia, para mantener nuestro espacio protegido en la red, y considerando que si tenemos nuestro sitio albergado en un servidor remoto, lo más probable es que no podamos modificar las configuraciones del servidor HTTP ni de PHP.

Joomla! ya es en sí un sistema muy seguro, pero es preciso actuar con cierta diligencia si no queremos tener sorpresas desagradables. Esta colección de primeras recomendaciones debe servir de inicio de un proceso complejo, pero necesario.

- Utiliza **versiones** de Joomla! descargadas de **sitio fiables**:

<http://joomla.org>,

<http://joomla.org>

<http://www.joomlaspanish.org>.

- **No instales extensiones sospechosas**, con poco soporte por parte de los desarrolladores. Hay que estar atento a las orientaciones que nos dan los espacios oficiales del proyecto Joomla! a este respecto, existe mucha documentación.
- Realiza **copias de seguridad** del sistema con frecuencia.
- **Actualiza** el sistema con la última versión. Cuando se descubre una vulnerabilidad, es muy corto el tiempo en el cual se desarrolla un parche o arreglo para la misma. Si tienes el sistema actualizado o parcheado con los últimos “patches” disminuyes notablemente la probabilidad de que te “hackeen” el sitio web.
- Utiliza **.htaccess** para controlar los accesos, y para proteger con contraseña el directorio **/administrator/** (HTTP Authentication<sup>2</sup>).

**.htaccess** es un archivo de texto oculto que contiene una serie de directivas para el servidor Apache. Cuando un cliente solicita un archivo al servidor, éste busca desde el directorio raíz hasta el subdirectorio que contiene el archivo solicitado, el archivo **.htaccess**, y tiene en cuenta estas reglas antes de proceder con la petición, es decir, se aplican las normas especificadas al directorio en el que se encuentre **.htaccess** y los directorios por debajo de él.

Ejemplos de usos para **.htaccess** pueden ser restringir el acceso a determinados archivos, impedir el listado de los archivos de un directorio, redireccionar, personalizar las páginas de error o impedir el acceso a determinadas IP's o rangos de IP. Por ejemplo, aunque son muchas más las posibilidades que permite **.htaccess** para proteger nuestro sistema:

1 Los contenidos de este apartado se corresponden con las recomendaciones de seguridad que ofrece <http://www.joomlaos.net>, propiedad de Gonzalo Reynoso, y se introducen en este texto con autorización expresa del autor.

2 Utilizar HTTP Authentication supone manipular código en varios archivos, y excede del propósito de este texto. Si quieres tener una buena referencia para dominar el control de seguridad que se puede realizar con “.htaccess”, en “Joomlaos”, puedes encontrar una buena referencia para completar esta información (<http://www.joomlaos.net/seguridad-en-Joomla!-utilizando-.htaccess-en-servidores-linux-apache.php>).



➤ **Impedir el listado del contenido de un directorio.**

Cuando se intenta acceder a un directorio, en ausencia de un archivo de índice, Apache muestra por defecto el contenido del directorio. Si queremos impedir al usuario ver el contenido de un directorio, bastaría con crear un archivo de índice, por ejemplo `index.html`, pero existe una solución más elegante mediante la directiva "Options". Basta crear un archivo `.htaccess` que contenga la línea:

```
Options -Indexes
```

También podríamos utilizar la directiva `DirectoryIndex`, que especifica qué archivos actúan como índice por defecto, y qué archivo mostrar en el caso de que éstos no se encuentren. Por ejemplo la línea:

```
DirectoryIndex index.php index.html index.htm /prohibido.php
```

indicaría al servidor que debe buscar los archivos `index.php`, `index.html` o `index.htm`, en ese orden, y en el caso de no encontrar ninguno de ellos, cargar el archivo `prohibido.php`.

➤ **Controlar el acceso a carpetas o archivos.**

Podrías querer deshabilitar totalmente el acceso a una carpeta. En este caso sólo los archivos principales accederán a ellos mediante el sistema de archivos, pero no se podrán acceder vía web. Simplemente, crea un archivo `.htaccess` en esa carpeta que contenga:

```
#deny all access
deny from all
```

Si se quiere permitir el acceso desde una IP específica,

```
#deny all access
deny from all
allow from 10.0.0.1
```

o para un rango específico de IP's (forzado mediante la máscara de red).

```
allow from 192.168.0.0/24
```

También se puede bloquear el acceso a un archivo específico,

```
<files privado.html>
Order allow,deny
Deny from all
</files/>
```

- Utiliza servicios online de **detección y alertas contra hackers**.
- Investiga y conoce muy bien el funcionamiento de **usuarios y permisos** en sistemas Unix/Linux. No otorgues permisos innecesarios de escritura a cualquier archivo o directorio. Haz no escribible el archivo "configuration.php" después de hacer cambios.

- Utiliza **componentes SEFs** avanzados para enmascarar las verdaderas URLs de Joomla!
- **Evita** utilizar **nombres o contraseñas "fáciles"** de adivinar o de vulnerar mediante "fuerza bruta" (operaciones recursivas). Nunca utilices las mismas contraseñas y usuarios para FTP y para las bases de datos.
- Contrata **"hostings" profesionales**, donde conocen a fondo y dan mucha importancia al tema de la seguridad. La configuración de PHP es vital aquí: registros globales desactivados, modo seguro, activación de comillas mágicas GPC, ejecución de shell deshabilitado para PHP, etc.
- **Deshabilita** el **reporte de errores** de PHP, hasta el momento en que necesites identificar problemas.