

# SECURIZACIÓN DEL CMS Joomla!



Joomla!™

inteco  
(cert)

El presente documento cumple con las condiciones de accesibilidad del formato PDF (Portable Document Format).

Se trata de un documento estructurado y etiquetado, provisto de alternativas a todo elemento no textual, marcado de idioma y orden de lectura adecuado.

Para ampliar información sobre la construcción de documentos PDF accesibles puede consultar la guía disponible en la sección [Accesibilidad > Formación > Manuales y Guías](#) de la página <http://www.inteco.es>.

## ÍNDICE

---

<b>1.</b>	<b>SOBRE LA GUÍA</b>	<b>4</b>
<b>2.</b>	<b>INTRODUCCIÓN</b>	<b>5</b>
<b>3.</b>	<b>SELECCIÓN DEL HOSTING</b>	<b>7</b>
<b>4.</b>	<b>INSTALACIÓN</b>	<b>9</b>
4.1.	Prefijo de la base de datos	11
4.2.	Usuario y contraseña de administrador	12
<b>5.</b>	<b>PERMISOS DE DIRECTORIOS Y ARCHIVOS</b>	<b>14</b>
5.1.	Área de administración (carpeta administrator)	16
<b>6.</b>	<b>HTACCESS Y ROBOTS.TXT</b>	<b>18</b>
6.1.	Htaccess	18
6.1.1.	Denegar el acceso a los archivos .htaccess e impedir mostrar el contenido de directorios	19
6.1.2.	Impedir el acceso a la página de administración de Joomla!	19
6.1.3.	Restringir el acceso a dominios e IPs	20
6.2.	Robots.txt	20
<b>7.</b>	<b>COPIAS DE SEGURIDAD</b>	<b>22</b>
7.1.	Copia de seguridad del directorio de instalación	22
7.2.	Base de datos	24
7.3.	Otras alternativas	25
<b>8.</b>	<b>EXTENSIONES DE TERCEROS</b>	<b>27</b>
8.1.	Extensiones que ayudan a proteger el sitio	28
<b>9.</b>	<b>ACTUALIZACIONES Y SERVICIOS DE INFORMACIÓN</b>	<b>30</b>
9.1.	Actualizaciones	30
9.2.	Foros y boletines de seguridad	30

## 1. SOBRE LA GUÍA

---

La presente guía tiene como objetivo introducir a los usuarios a las diferentes técnicas o mecanismos existentes para llevar a cabo una instalación segura de un gestor de contenidos basado en Joomla!<sup>1</sup>.

Los conocimientos técnicos del público al que está dirigido requiere nociones básicas-medias acerca de diferentes tecnologías como son los servidores web y las bases de datos. Esto les permitirá avanzar más rápidamente sobre los contenidos, pero en cualquier caso, cualquier usuario con conocimientos básicos podrá seguir sin demasiados problemas la información que se presenta en esta guía.

A lo largo del documento se describirán las pautas esenciales que un usuario debe seguir para llevar a cabo una instalación del gestor de contenidos que pasan desde la importante elección de un proveedor de alojamiento web (*hosting*) hasta la configuración básica de los archivos necesarios que garanticen un nivel adecuado de seguridad. También se hará referencia a la importancia de mantener un sistema de copias de seguridad que permitan la restauración del sistema ante un desastre así como las precauciones que se deben seguir a la hora de instalar módulos o extensiones de terceros.

---

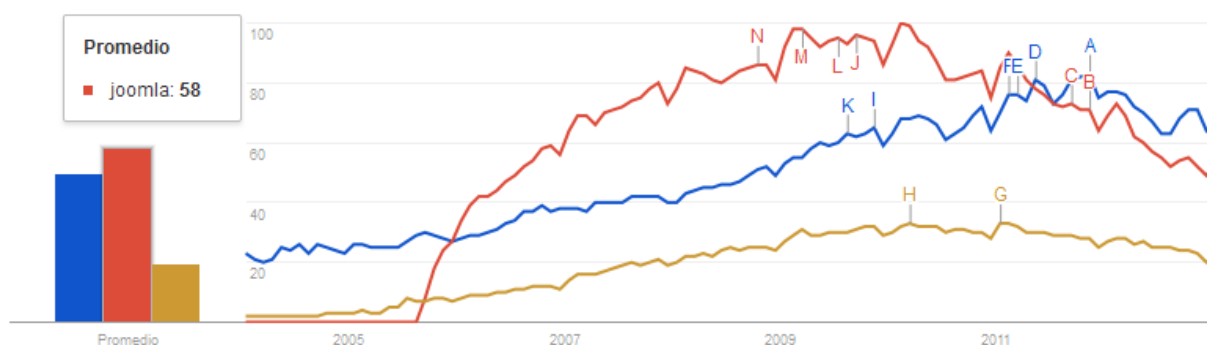
<sup>1</sup> Para la elaboración de esta guía se empleó la última versión de Joomla! estable que se correspondía con la 2.5. Actualmente ya está publicada la versión 3.0 y la mayoría de cuestiones que se indican en este documento son aplicables a la última versión.

## 2. INTRODUCCIÓN

En los orígenes de la WWW o *World Wide Web*, las páginas que se diseñaban eran de carácter estático y realmente simples, el lenguaje sobre el que se apoyaban, el HTML<sup>2</sup>, no permitía mucho más. Si había que realizar alguna modificación, se debía editar el código de cada página individualmente. Teniendo en cuenta esto, es posible hacerse una idea del trabajo que supondría el modificar por ejemplo sesenta páginas. Muchos desarrolladores y fabricantes identificaron esta problemática y en los años 90 se crean los lenguajes de programación “del lado del servidor” como ASP<sup>3</sup> ó PHP<sup>4</sup>, que junto con el uso de base/s de datos permitirían la generación dinámica de páginas web. Se abre así el camino para el desarrollo de los primeros gestores de contenido o CMS (*del inglés Content Management System*).

La utilización de un CMS por entonces, estaría demandada por empresas u organizaciones que necesitaran de un volumen elevado de publicaciones y actualizaciones de contenidos web como revistas, periódicos, etc. por lo que a mediados de los 90 comienzan a aparecer los primeros gestores de contenido de carácter comercial y en algunos casos, diseñados a medida para cada organización y que, debido a su coste, eran sólo accesibles por grandes compañías o empresas.

A partir del año 2000, con la evolución de la WWW hacia portales con más información y más necesidad de interacción de los usuarios, la proliferación de los gestores de contenidos se hace más notable y además de las soluciones comerciales existentes comienzan a aparecer los primeros gestores de contenidos de código abierto (*Open Source*) bajo licencia GPL<sup>5</sup> como PHP-Nuke<sup>6</sup> o Mambo<sup>7</sup> y otros muchos. Será de este último del que a partir de 2005 dé lugar un nuevo CMS denominado Joomla! a causa de un conflicto de intereses relacionados con el tipo de licencia de Mambo. A partir de entonces Joomla! fue cobrando popularidad hasta convertirse en uno de los CMS bajo GPL más utilizados:



<sup>2</sup> <http://www.w3.org/html/>

<sup>3</sup> [https://en.wikipedia.org/wiki/Active\\_Server\\_Pages](https://en.wikipedia.org/wiki/Active_Server_Pages)

<sup>4</sup> <https://es.wikipedia.org/wiki/PHP>

<sup>5</sup> <https://www.gnu.org/licenses/gpl.html>

<sup>6</sup> [http://www.dmoz.org/Computers/Programming/Languages/PHP/Scripts/Content\\_Management/PHP-Nuke/](http://www.dmoz.org/Computers/Programming/Languages/PHP/Scripts/Content_Management/PHP-Nuke/)

<sup>7</sup> <http://mambo-code.org/gf/project/mambo/>

Como se aprecia en el gráfico, Joomla! es uno de los CMS más utilizados junto con Drupal (marrón) o Blogger (Azul).

La sencillez de uso, tanto en la instalación como en la gestión, de Joomla! ha sido uno de los factores clave para su importante difusión a la hora de implementar portales tanto para grandes compañías como para usuarios.

Este nivel de difusión tan elevado, lo convierte en un posible objetivo para perpetrar ciberataques que podrían tener importantes consecuencias para los usuarios y empresas que utilizan este gestor de contenido como plataforma web. Sin duda, se trata de la razón más importante por la que el CERT de INTECO ha elaborado esta guía básica para la implementación de un portal web con el gestor de contenidos Joomla!, esperando que las recomendaciones y pautas que aquí se reflejan, ayuden a mejorar la seguridad.

### 3. SELECCIÓN DEL HOSTING

---

En muchas ocasiones los aspectos más importantes son considerados como detalles insignificantes y las razones de no detenerse para su análisis tienen consecuencias que podrían repercutir de manera negativa en el futuro. Esto se puede trasladar, en un ejemplo del mundo de las tecnologías, a la hora de escoger un proveedor que ofrece alojamiento para webs o “hosting”.

En multitud de situaciones de la vida cotidiana se suelen analizar cuestiones que se consideran importantes porque se conocen las consecuencias. Sirva el ejemplo a la hora de adquirir un coche y en el concesionario siempre se pregunta acerca de las opciones de seguridad de las que dispone el vehículo: dispositivos de seguridad activa como “cambio involuntario de carril”, etc. o de seguridad pasiva como el “número de airbags disponibles”. De este modo el conductor, una vez que conoce las características y cumplen con sus necesidades, adquirirá el coche. Si se tiene la intención de crear un portal web lógicamente, habrá que analizar sobre qué tipo de plataforma y características se quiere implantar.

En la actualidad cualquier persona con unos conocimientos informáticos a nivel de usuario puede ser capaz de crear una página web para diversos fines: promocionar su negocio, crear un blog personal, etc. Para esta labor existen multitud de aplicaciones web como es el caso de Joomla!. Se trata de un gestor de contenido de código abierto (bajo licencia GPL) que ofrece multitud de opciones gracias a su versatilidad y la posibilidad de añadirle complementos de terceros que le aportarán mucha más funcionalidad de la que posee nativamente. Joomla! está desarrollado bajo PHP y HTML que necesita de una base de datos del tipo MySQL<sup>8</sup> y de un servidor web, generalmente Apache<sup>9</sup> aunque también se puede instalar sobre otros.

Para instalar Joomla! el primer punto que se ha de tener en cuenta es la selección de un proveedor de alojamiento web que cumpla con las necesidades que el gestor de contenido requiere. Sin duda este es uno de los puntos esenciales que se debe considerar ya que una mala elección, puede repercutir en la calidad de servicio, seguridad del sitio web, etc. Puesto que en la actualidad existen multitud de empresas que ofrecen este servicio, puede resultar una tarea poco transparente de cara al usuario. Para facilitar esta labor, a continuación se listan las premisas que se deben seguir para seleccionar un proveedor de hosting adecuado para Joomla!:

- **Reputación del proveedor:** aspecto clave. Es muy importante el tener en consideración a empresas de alojamiento que tengan bastante experiencia en el sector.
- **Tipo de alojamiento (arquitectura de servicio):** la mayor parte de proveedores ofrecen dos tipo de alojamiento: Windows o Linux. Por razones de compatibilidad,

---

<sup>8</sup> <https://www.mysql.com/>

<sup>9</sup> <https://www.apache.org/>

**Joomla! se comporta mejor sobre servidores Linux** y aunque un alojamiento basado en Windows también puede ser válido, es posible que en el futuro se puedan presentar inconvenientes relacionados con actualizaciones, funcionalidades, etc. En general, para poder instalar Joomla! será necesario que el proveedor disponga de los componentes: PHP, MySQL y Apache. En definitiva, para este tipo de gestores de contenidos se recomienda utilizar servidores basados en Linux. Mencionar que los proveedores de hosting gratuito pueden ser una alternativa para realizar pruebas, pero no se recomiendan como posibilidad ya que en muchas ocasiones las condiciones del servicio no suelen cubrir aspectos esenciales como las garantías de “tiempo en línea” (Uptime) o recuperación ante desastres (copias de seguridad).

- **Espacio y transferencia:** aunque no es un tema relacionado con la seguridad, hay que seleccionar un proveedor que satisfaga las necesidades en relación a estos temas y que garanticen la disponibilidad del servicio. Hay que poner especial atención sobre aquellos hosting que ofrecen espacio web y transferencia ilimitada. En estos casos se recomienda leer con atención las condiciones del servicio puesto que en ocasiones la oferta puede que no sea tal.
- **Soporte:** hay que conocer claramente qué servicios ofrecen en relación a posibles problemas que pudieran surgir como las caídas del servidor o que el idioma para ayudar al usuario sea el castellano así como los tiempos de respuesta.
- **Elementos técnicos:** la mayoría de proveedores de alojamiento suelen ofrecer las mismas herramientas o parecidas, para facilitar la gestión del sitio al usuario. Saber cuáles están disponibles (cPanel<sup>10</sup>, phpMyAdmin<sup>11</sup>, etc.) puede facilitar enormemente la tarea a la hora de implementar un gestor de contenidos como Joomla!. Un buen proveedor de alojamiento debe permitir los ajustes PHP de manera local.
- **Seguridad:** conocer qué política aplica ante posibles pirateos del servidor o la generación de copias de seguridad del mismo, es esencial a la hora de hacer frente a estos incidentes, de ahí la importancia de este aspecto del proveedor. Si no lo deja claro en las condiciones es recomendable informarse.
- **Política de uso y condiciones del servicio:** hay que poner especial atención en este punto y detenerse sobre cuáles son las condiciones de contratación y otros aspectos a tener en cuenta como la situación del *datacenter* o las leyes que aplican al país donde está alojado, entre otros.

Una vez valorados los aspectos anteriores ya sería cuestión de elegir el proveedor de alojamiento en función de otros elementos de carácter más secundario como sería el precio, descuentos o algún tipo de paquete u oferta de la que poder beneficiarse. Una vez contratado el servicio solo restaría comenzar con la instalación.

---

<sup>10</sup> <https://cpanel.net/>

<sup>11</sup> [http://www.phpmyadmin.net/home\\_page/index.php](http://www.phpmyadmin.net/home_page/index.php)

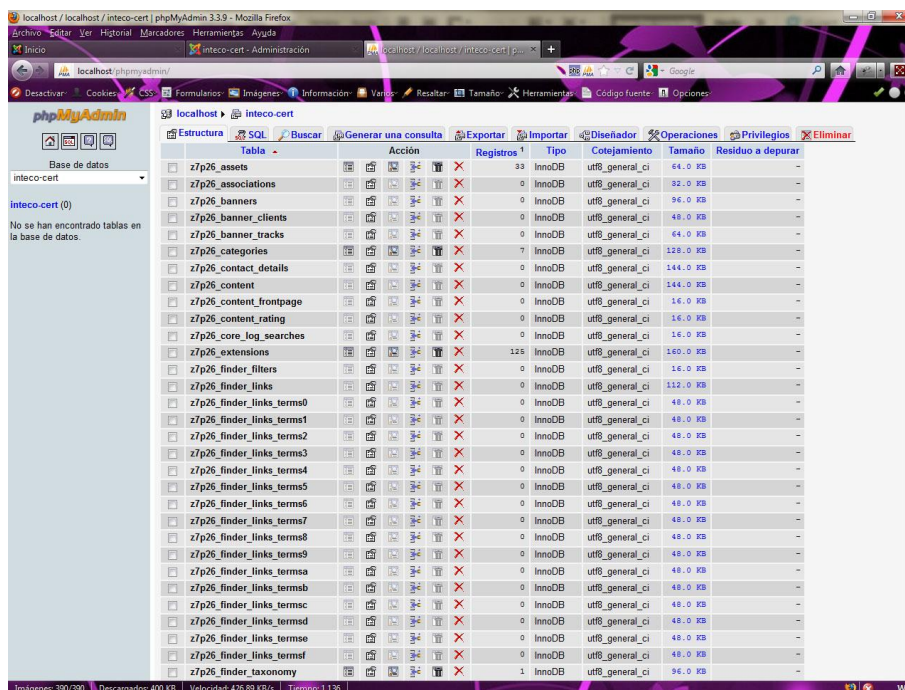


## 4. INSTALACIÓN

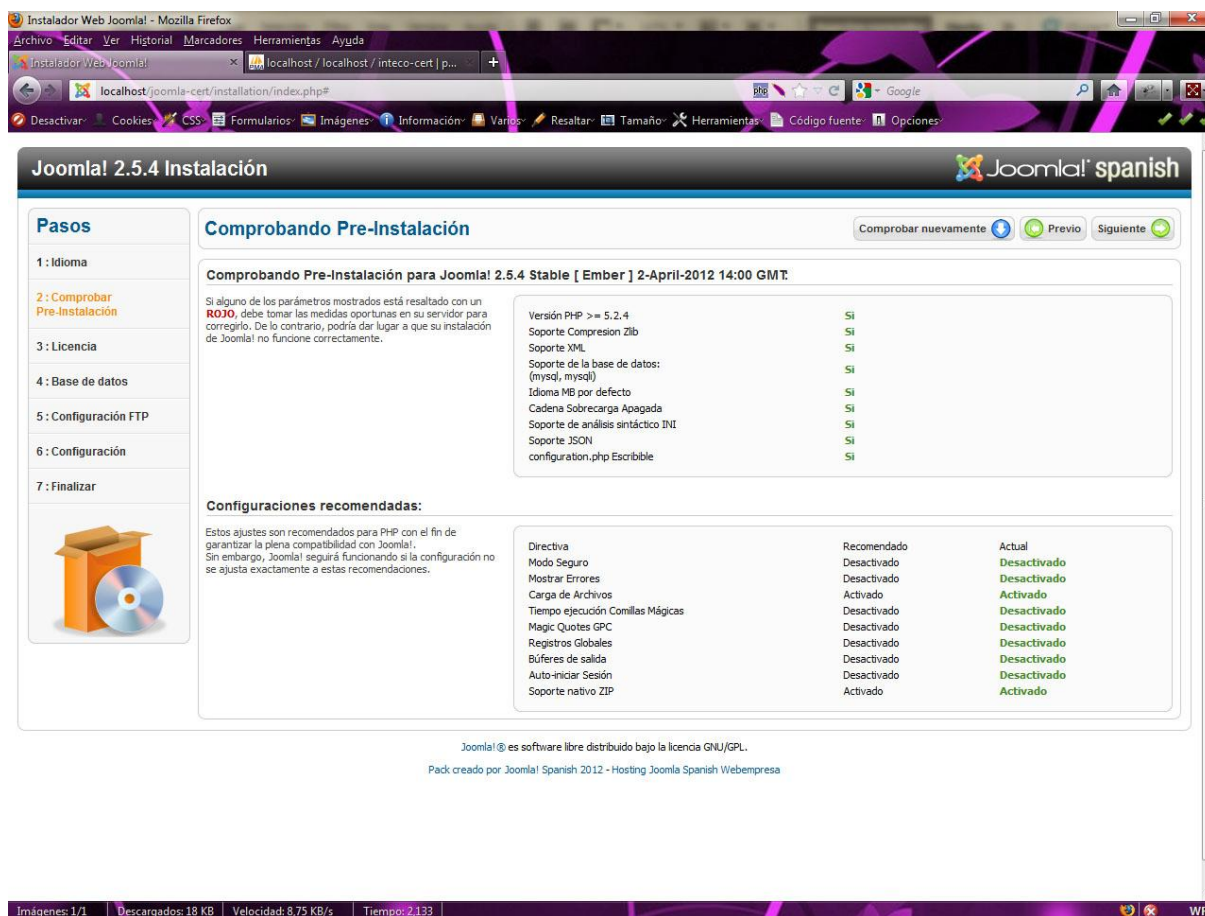
Tras seleccionar un proveedor de alojamiento adecuado para Joomla!, el siguiente paso será descargar la última versión del CMS. Para ello, es posible descargar la versión en inglés desde el sitio oficial <http://www.joomla.org/download.html> ó la versión en español desde <http://www.joomlaspanish.org>. Una vez descargada, descomprimos el archivo para a continuación, subirlo al servidor. Para realizar esta tarea, generalmente, al contratar el hosting el proveedor nos facilitará una cuenta de FTP (File Transfer Protocol) con la que a través de un cliente para la transferencia de archivos, una extensión en un navegador o a través del panel de control del hosting será posible subirlos al directorio público.

Generalmente la instalación de Joomla! se realiza en el directorio que el proveedor crea para las páginas web (suele ser *public\_html*) aunque en muchas ocasiones es posible encontrarse un directorio *root* o *raíz*, en el que no aparece ninguna carpeta, donde se podrá iniciar la instalación del gestor de contenidos. Tras conectarse con el servidor, se procederá a la subida de archivos en el directorio que el proveedor haya dispuesto (también sería posible crear subdirectorios donde poder instalar Joomla!).

Paralelamente se debe configurar el acceso a la base de datos necesaria para la instalación y funcionamiento de Joomla!. Para ello hay que crear una nueva base de datos con un usuario y una contraseña robusta para el acceso. En ocasiones el proveedor puede facilitar una base de datos cuando se contrata el paquete de alojamiento web. Esta tarea es necesaria realizarla a través del panel de control del *hosting* sobre el que, en algunos casos, es posible tener acceso a la aplicación phpMyAdmin para configurar la base de datos.



Una vez que tengamos todos los datos iniciaremos el proceso para la instalación de Joomla!. Para ello simplemente hay que acceder al dominio a través de un navegador web y teclear [www.midominio.com](http://www.midominio.com) donde midominio.com será el nombre de dominio que hayamos adquirido con el pack del proveedor de alojamiento. Arrancará de manera automática el instalador de Joomla!. El aspecto de la página que se abre tras seleccionar el idioma de instalación y pulsar “Siguiente”, debe ser similar al de la imagen siguiente:



En ella se puede ver un resumen de las comprobaciones que el instalador realizará para verificar que la instalación se puede llevar a cabo. Si apareciera alguna en color rojo habría que tomar las medidas adecuadas para corregir la configuración. La mayor parte de inconvenientes en relación a las configuraciones recomendadas son configurables a través del panel de gestión del proveedor de alojamiento. Generalmente se encuentran bajo un literal similar a “Ajustes de PHP local”. En esa sección se podrán activar y desactivar opciones como el registro global, mostrar errores, etc.

Tras verificar que todo está correcto y aceptar la “Licencia Pública General GNU”, pulsando “siguiente” avanzaríamos al siguiente paso:

**Joomla! 2.5.4 Instalación**

**Pasos**

- Idioma
- Comprobar Pre-Instalación
- Licencia
- Base de datos**
- Configuración FTP
- Configuración
- Finalizar

**Configurando la base de datos**

**Configurando la conexión**

Para configurar Joomla! y ejecutarlo en el servidor son 4 simples pasos:

- Debe especificar el nombre del servidor donde Joomla! ha de ser instalado.
- Introducir el nombre de usuario de MySQL, contraseña y nombre de la base de datos que desea utilizar con Joomla!.
- Introducir un prefijo a ser utilizado por las tablas de esta instalación de Joomla!.
- Seleccionar la forma de utilizar las tablas existentes de una instalación anterior.

**Configuración Básica**

Tipo Base de Datos \*  
Mysql *Esto es por lo general "mysql"*

Nombre del Host \*  
localhost *Esto es por lo general "localhost"*

Usuario \*  
root *O algo como "root" o un nombre de usuario dado por el host*

Contraseña \*  
..... *Para la seguridad del sitio es obligatorio el uso de una contraseña para la cuenta de mysql.*

Nombre de la base de datos \*  
inteco-cert *Algunos hosts permiten sólo un determinado nombre de DB para el sitio. Utilice el prefijo de tabla si desea instalar varios sitios con Joomla!.*

Prefijo de la tabla \*  
z7p26\_ *No utilizar "bak\_" ya que este se utiliza para tablas destinadas a copias de seguridad.*

Procesar base de datos antigua \*  
☒ Respalidar  
☐ Eliminar *Cualquier copia de seguridad de las tablas existentes de su anterior instalación de Joomla! será reemplazada.*

Joomla!® es software libre distribuido bajo la licencia GNU/GPL.  
Pack creado por Joomla! Spanish 2012 - Hosting Joomla Spanish Webempresa

Imágenes: 1/1 Descargados: 2 KB Velocidad: 22,22 KB/s Tiempo: 0,259

En este paso debemos introducir los siguientes datos:

- Tipo de base de datos: MySQL
- Nombre del host: el servidor de base de datos que nos ha facilitado el proveedor
- Usuario, contraseña y nombre de base de datos: los que haya facilitado el proveedor o los que haya creado el usuario.

#### 4.1. PREFIJO DE LA BASE DE DATOS

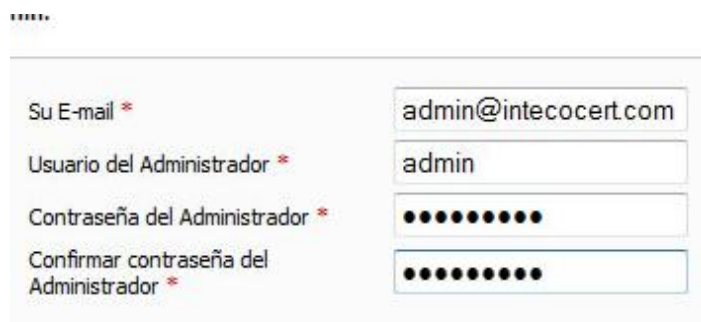
Este es un aspecto de seguridad importante a la hora de crear la estructura de tablas ya que Joomla!, hasta la versión 2.X por defecto creaba el prefijo “jos\_” en el nombre de las tablas por lo que un posible atacante lo tenía muy fácil para conocer el nombre de las mismas ya que el resto del nombre es común para todas las instalaciones (ejemplo: *jos\_users*). Con la última versión de Joomla! se genera un prefijo aleatorio, pero es recomendable modificarlo por uno que el usuario considere y que preferiblemente, no tenga relación con el nombre del sitio. Por ejemplo:



Una vez rellenado el formulario se continúa con la instalación pulsando el botón siguiente. En caso de existir algún inconveniente con la información proporcionada, el instalador nos mostrará un mensaje indicando dónde se encuentra el problema. El siguiente paso será configurar un FTP si fuera necesario aunque en la mayoría de los proveedores no lo es y **tampoco se recomienda activarlo**. Avanzamos en la instalación pulsando “Siguiente” omitiendo este paso.

## 4.2. USUARIO Y CONTRASEÑA DE ADMINISTRADOR

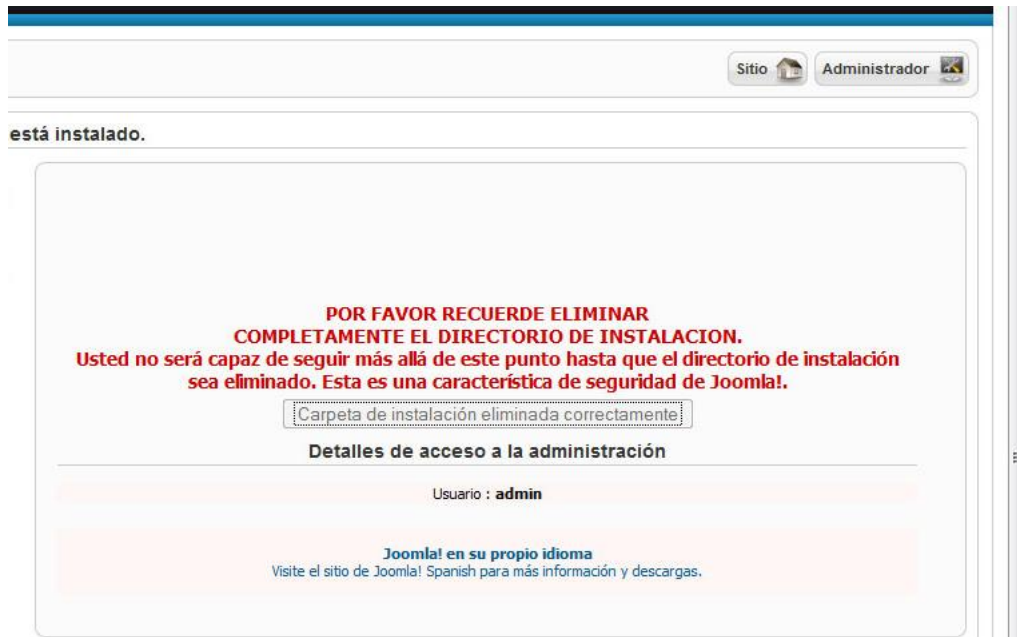
En este punto de la instalación se solicita el nombre del sitio web, y lo que es más importante, las credenciales del usuario. Tras introducir la dirección de correo electrónico asociada a la instalación (importante que esté activa para poder recuperar la contraseña en caso de olvido), se procede a introducir el nombre de usuario y la contraseña del mismo. Joomla! por defecto rellena el formulario correspondiente al “Usuario del Administrador” con el nombre “admin”.



Por razones de seguridad es altamente recomendable modificar este nombre por otro diferente. En caso de mantener “admin” hay que considerar que si un usuario malintencionado quisiera acceder a la zona de administración, ya conoce la mitad de la barrera existente. Si además no se crea una contraseña robusta, es relativamente fácil que por medio de un ataque de fuerza bruta se acceda a la zona de administración. (Para instalaciones finalizadas que mantengan este usuario, se recomienda modificarlo a través de la gestión de usuarios de la administración de Joomla!)

En capítulos posteriores, veremos cómo añadir medidas adicionales de seguridad para el acceso a la administración del gestor de contenidos.

Para finalizar la instalación se avanzará pulsando “Siguiente” y el instalador indicará que se debe borrar la carpeta de instalación “*installation*”. En la última versión de Joomla! se ha incluido un botón que automatiza el proceso y no es necesario eliminarla de modo manual.



Tras finalizar la instalación, el instalador ha creado el archivo *configuration.php* con los parámetros que se han introducido durante el proceso. En caso de ser necesaria alguna modificación relacionada con la base de datos, nombre del sitio, etc. será posible editar este archivo manualmente para aplicar los cambios.



## 5. PERMISOS DE DIRECTORIOS Y ARCHIVOS

Tras la instalación exitosa del gestor de contenidos es muy importante proteger con los permisos adecuados todo el árbol de directorios y archivos que componen la estructura de Joomla!. Puesto que la aplicación web se encuentra en un directorio con acceso de lectura para todo el mundo (*public\_html*, *raíz* o similar), como mínimo se ha de verificar que los permisos se han establecido adecuadamente.

Es cierto que la mayoría de proveedores de alojamiento web reconocidos, suelen aplicar los permisos sobre archivos y carpetas de manera adecuada, pero para poder comprobarlo y puesto que el *hosting* debería estar basado en Linux, antes es necesario explicar brevemente, sin entrar en detalle, cómo se gestionan los permisos en este sistema operativo.

Para Linux existen tres tipo de usuarios/propietarios: Owner o propietario, Group o grupo y Other/Public u otros. Y existen tres tipo de permiso: de lectura (r), escritura (w) y ejecución (x), y a cada permiso, los sistemas Linux los asignan a través de un valor numérico, así para lectura sería un “4”, para escritura un “2” y para ejecución un “1”.

Propietario (Owner)			Grupo (Group)			Other (Otros)/Public		
r (leer)	w (escribir)	x (ejecutar)	r (leer)	w (escribir)	x (ejecutar)	r (leer)	w (escribir)	x (ejecutar)
4	2	1	4	2	1	4	2	1

En relación a los tipos de usuario y el tipo de permisos, Linux los representa de izquierda a derecha y realizando una suma numérica.

Teniendo en cuenta lo anterior y como medida general, para toda la estructura de carpetas (no archivos) donde está instalado Joomla! serían aplicables los permisos **755** que se traducen como:

- Los propietarios, es decir el usuario que ha facilitado el *hosting* al contratar el servicio, tendrán control total (lectura, escritura y ejecución) sobre las carpetas del servidor (**7**).
- Los miembros del grupo tendrán permisos de lectura y ejecución (**5**). En el caso de alojamiento web, el grupo (Group) en el caso de un alojamiento web pertenece al propietario (Owner).
- El resto de usuarios, los que acceder a la página web y sus servicios, tendrán permisos de lectura y ejecución (**5**).

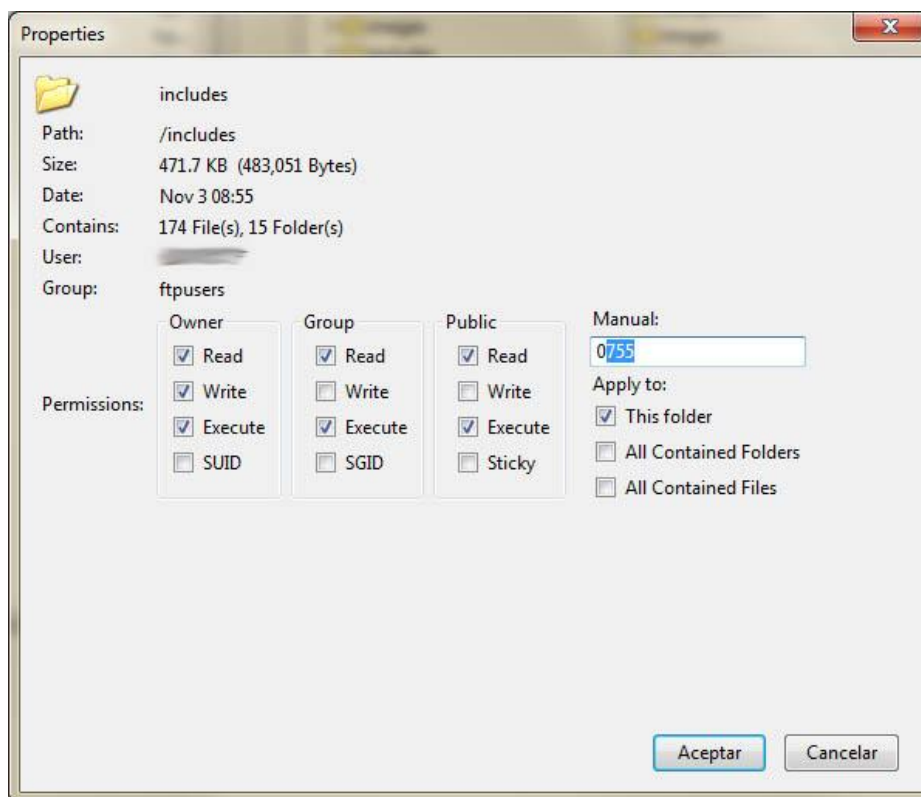
Para los archivos la configuración será distinta. Hay que aplicar permisos **644** que se traducirían, siguiendo la información de la tabla, como:

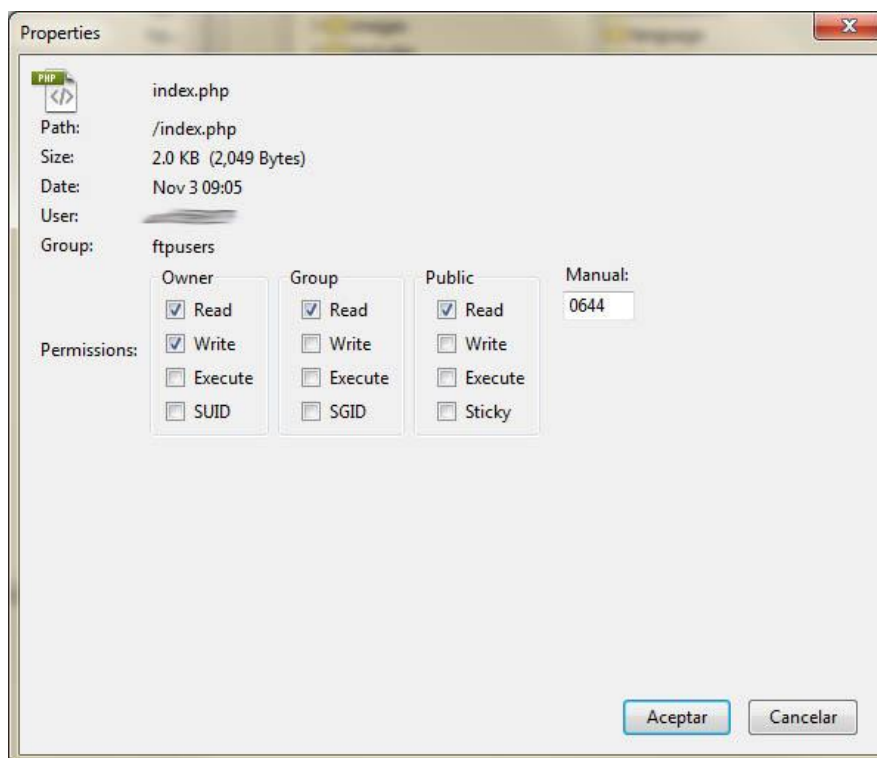
- Los propietarios tendrán permiso de lectura y escritura sobre los archivos del servidor (**6**).
- Los miembros del grupo tendrán permisos de lectura (**4**).
- El resto de usuarios, los que acceden a la página web y sus servicios, tendrán permisos de lectura (**4**).

En resumen y como recomendación, se deben aplicar los permisos:

- **755** para directorios o carpetas.
- **644** para archivos.

Para comprobar los permisos o modificarlos, es posible hacerlo mediante un cliente FTP o a través de alguna aplicación de gestión de archivos que nos facilite el proveedor de *hosting* accediendo a las propiedades de la carpeta o archivo en cuestión. En la imagen siguiente se muestra una captura del componente FireFTP para Firefox tras acceder a las propiedades de la carpeta “includes” (755) y al archivo “index.php” (644).





En este caso el cliente FTP facilita la aplicación de permisos mediante una serie de “checks” que contienen los textuales de los mismos: lectura (Read), escritura (Write) y ejecución (Execute), agrupados en columnas para cada tipo propietario (Owner, Group y Public). Además también es posible aplicar permisos de manera recursiva para facilitar la tarea y evitar ir archivo por archivo o carpeta por carpeta.

Hay que mencionar que es posible que determinadas extensiones o módulos requieran la modificación de ciertos permisos para poder instalarlo. Tras añadirlo a Joomla! hay que volver a aplicar los permisos recomendados en los archivos o carpetas que se han modificado, además, es posible que algunos componentes requieran determinados permisos que es posible que pongan en riesgo la seguridad del sitio, en este caso, es recomendable optar por otra solución.

## 5.1. ÁREA DE ADMINISTRACIÓN (CARPETA ADMINISTRATOR)

Joomla! como la mayoría de gestores de contenidos, cuenta con dos partes diferentes en su sistema. Por un lado encontramos la parte pública o “*Front-end*” y por otro, la parte privada/de administración o “*Back-end*”.

La primera sería la parte que está accesible para todo el mundo y que es visible a través de la navegación web, la “página web en sí”. En cambio la parte de administración está reservada para aquellos usuarios que gestionan la plataforma como son los administradores o los usuarios que van a publicar contenidos o realizar tareas de mantenimiento. Mencionar que la parte de administración de Joomla! tiene su propio directorio en el árbol de carpetas donde se ubican todos los archivos necesarios para la presentación web, gestión, etc.



Puesto que la zona de administración debe ser considerada un punto clave a proteger con el objetivo de impedir lo máximo posible accesos no autorizados, es necesario implementar los mecanismos adecuados que aporten seguridad en este aspecto. Como se comentó en el punto de la instalación, la primera acción a tomar sería modificar el nombre de usuario “administrador” por defecto (admin) y utilizar una contraseña robusta.

Otra medida que se puede implementar es modificar el ID por defecto del usuario Super Administrador (42 en Joomla! 2.X). Es posible realizar el cambio a través de la base de datos, pero lo más sencillo sería crear un nuevo usuario con privilegios de Super Administrador, cerrar la sesión y tras conectarse con las credenciales del nuevo usuario, eliminar el original.

+ Opciones

			id	name	username	email	
<input type="checkbox"/>			42	Super User	s00cc3r	admin@intecocert.com	bd6cf58d262c74ff958788
<input type="checkbox"/>			43	usuario2	usuario2	user@intecocert.com	ac5a61d6d5c38b7397e8

↑ [Marcar todos/as](#) / [Desmarcar todos](#) Para los elementos que están marcados:

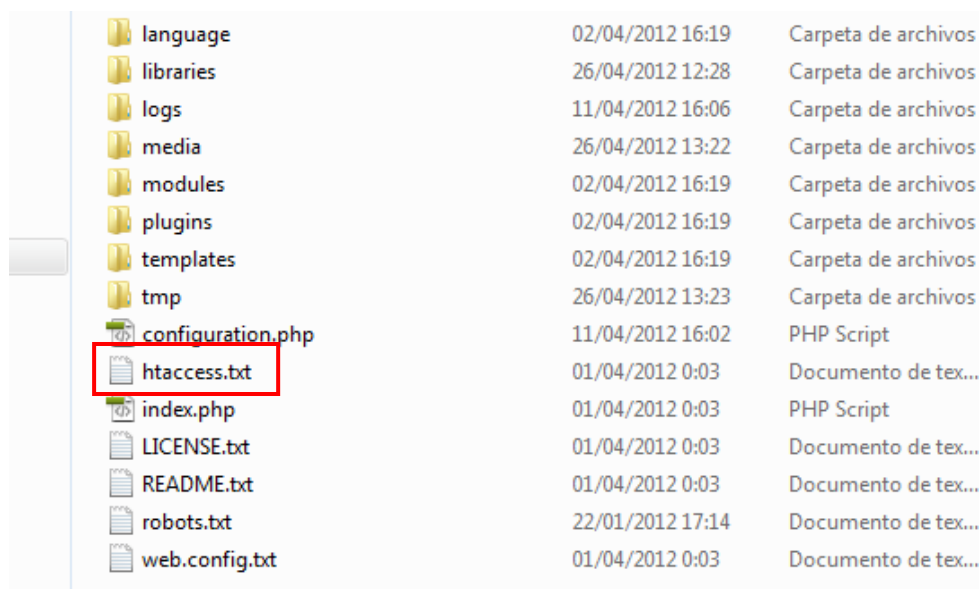
## 6. HTACCESS Y ROBOTS.TXT

En el punto anterior se ha comentado cómo asignar adecuadamente los permisos tanto a los directorios como a los archivos para mantener un mínimo de seguridad. En este punto se tratará cómo restringir el acceso a determinados directorios y archivos mediante la configuración de .htaccess y cómo evitar que los buscadores indexen archivos o rutas del sitio web que no queremos que sean visibles a través de las búsquedas como por ejemplo URLs de administración, de configuración, etc.

### 6.1. HTACCESS

Aunque la mayoría de opciones de configuración de un servidor web dentro de un alojamiento basado en Apache están solo accesibles para el administrador del del servidor en el ISP, es posible aplicar determinadas configuraciones editando el archivo .htaccess. Estas configuraciones, denominadas “directivas”, permiten aportar funcionalidades que variarán el comportamiento de sitio web pudiendo implementar varios archivos .htaccess sobre distintos directorios y archivos en base a las necesidades. En este caso concreto nos centraremos sobre las que aportan seguridad sobre Joomla!, aunque son aplicables al resto de gestores de contenidos u otros sitios web basados en Apache.

Cuando se finaliza la instalación de Joomla! el CMS crea por defecto el archivo “htaccess.txt” que no tendrá efecto hasta que se modifique su nombre, de htaccess.txt a .htaccess.



language	02/04/2012 16:19	Carpeta de archivos
libraries	26/04/2012 12:28	Carpeta de archivos
logs	11/04/2012 16:06	Carpeta de archivos
media	26/04/2012 13:22	Carpeta de archivos
modules	02/04/2012 16:19	Carpeta de archivos
plugins	02/04/2012 16:19	Carpeta de archivos
templates	02/04/2012 16:19	Carpeta de archivos
tmp	26/04/2012 13:23	Carpeta de archivos
configuration.php	11/04/2012 16:02	PHP Script
htaccess.txt	01/04/2012 0:03	Documento de tex...
index.php	01/04/2012 0:03	PHP Script
LICENSE.txt	01/04/2012 0:03	Documento de tex...
README.txt	01/04/2012 0:03	Documento de tex...
robots.txt	22/01/2012 17:14	Documento de tex...
web.config.txt	01/04/2012 0:03	Documento de tex...

Inicialmente en Joomla!, este archivo está configurado para facilitar la reescritura de las URL y optimizar el sitio en los motores de búsqueda, pero a través de ciertos parámetros, será posible aplicar diferentes configuraciones que aportarán mayor seguridad al sitio web. Hay que indicar que el archivo .htaccess únicamente afecta al directorio, subdirectorios y archivos en los que está incluido. Además hay que tener en cuenta que algunos ISPs

pueden restringir el uso de este tipo de archivos, por lo que se debe verificar antes de contratar el hosting la posibilidad de utilizar este tipo de medidas.

### 6.1.1. Denegar el acceso a los archivos .htaccess e impedir mostrar el contenido de directorios

Para evitar que estos archivos y la información de configuración sean visibles por terceros, en cada archivo .htaccess que creemos se debe añadir:

```
<Files .htaccess>
order allow,deny
deny from all
</Files>
```

En algunas ocasiones también interesará que la estructura de directorios de Joomla!, a pesar de ser bastante conocida, no sea mostrada y ocultar así los archivos y carpetas que componen el sitio. Para ello basta con añadir al archivo .htaccess la siguiente línea:

Options All -Indexes

### 6.1.2. Impedir el acceso a la página de administración de Joomla!

Puesto que la URL que da acceso a la zona de administración de Joomla! es ampliamente conocida (misitio.com/administrator) y para evitar ataques de fuerza bruta sobre el formulario, es necesario implementar alguna medida que restrinja su acceso como la necesidad de un usuario y contraseña adicional (autenticación HTTP). Para ello es posible ayudarse del .htaccess indicando la configuración siguiente:

```
AuthType Basic
AuthName "Área de administración"
AuthUserFile /.htpasswd/users.pwd
require valid-user
```

Hay que indicar que esta configuración se debe aplicar en un archivo .htaccess en el directorio /administrator. Para que la configuración funcione correctamente adicionalmente, hay que crear un archivo de texto con los usuarios y contraseñas que podrán acceder al directorio (en el ejemplo *users.pwd*) y ubicarlo en un directorio, a ser posible oculto y fuera de la carpeta pública (en el ejemplo */.htpasswd*). Puesto que el formato de la contraseña para apache se ha de cifrar con MD5, el archivo *users.pwd* que contiene el usuario “*usuario*” y contraseña “*contraseña*”, tendría el siguiente formato:

usuario:\$apr1\$M7NxvAOW\$7zz4QH.lopT1dpOkrEII\$0

Para ayudarnos a generar las listas de usuarios podemos utilizar servicios como <http://www.htaccesstools.com/htpasswd-generator/> que convierten la contraseña al formato adecuado.

Implementando esta medida, cuando un usuario trate de acceder a la URL `misitio.com/administrator`, previa a la aparición del formulario de acceso a la administración del portal, se mostrará otro solicitando las credenciales del archivo `users.pwd`.

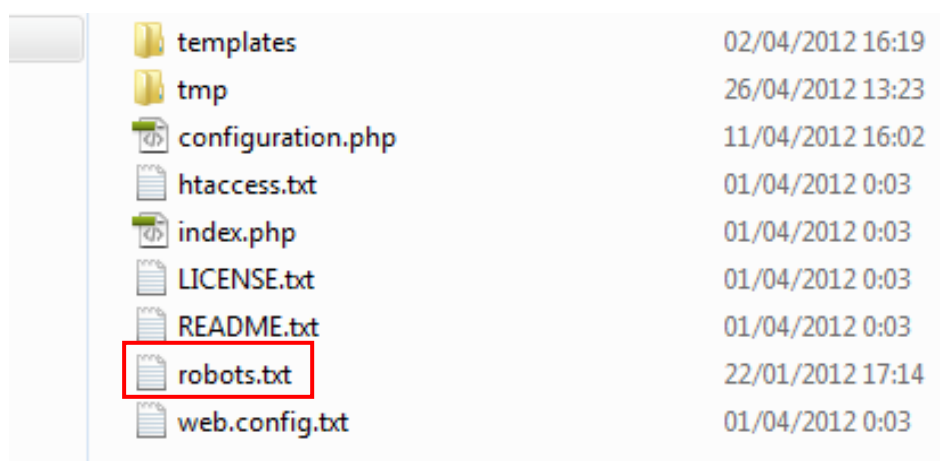
### 6.1.3. Restringir el acceso a dominios e IPs

En determinadas circunstancias como ataques reiterados (fuerza bruta en formularios, intentos de acceso a zonas restringidas, etc.) desde una IP o dominio concreto, mediante `.htaccess` es posible denegar el acceso al sitio web. Para ello, debemos añadir el siguiente código en el archivo:

```
order deny,allow
deny from xxx.xxx.xxx.xxx #xxx son los números correspondientes a la IP
deny from .dominio.es #sustituir .dominio.es por el nombre de dominio que se quiere restringir
allow from all
```

## 6.2. ROBOTS.TXT

Generalmente, una vez que se implementa un sitio web y se pone en producción, el siguiente paso es la promoción. Ésta generalmente se realiza añadiendo el dominio en los buscadores más populares y aplicando ciertas técnicas (SEO y SEM) para hacer que nuestra página sea mostrada en los primeros puestos de las búsquedas. Para facilitar el rastreo e indexación por los “*crawlers*” (arañas o robots de los motores de búsqueda) se debe configurar adecuadamente el archivo `robots.txt`. A través de este fichero, mediante una serie de directivas, le indicaremos al crawler qué páginas puede indexar el buscador y cuáles no. Por lo general no nos interesa que el buscador añada las páginas de administración, configuración, etc. La última versión de Joomla! por defecto genera en el raíz (*root*) del sitio web un archivo `robots.txt`:



templates	02/04/2012 16:19
tmp	26/04/2012 13:23
configuration.php	11/04/2012 16:02
htaccess.txt	01/04/2012 0:03
index.php	01/04/2012 0:03
LICENSE.txt	01/04/2012 0:03
README.txt	01/04/2012 0:03
robots.txt	22/01/2012 17:14
web.config.txt	01/04/2012 0:03

Que tiene la siguiente configuración:

User-agent: \*

Disallow: /administrator/  
Disallow: /cache/  
Disallow: /cli/  
Disallow: /components/  
Disallow: /images/  
Disallow: /includes/  
Disallow: /installation/  
Disallow: /language/  
Disallow: /libraries/  
Disallow: /logs/  
Disallow: /media/  
Disallow: /modules/  
Disallow: /plugins/  
Disallow: /templates/  
Disallow: /tmp/

Inicialmente es una configuración válida siempre que se cumplan nuestras necesidades. Si queremos añadir un nuevo directorio o ruta a proteger contra la indexación de los buscadores, la incluiremos en la lista. Para más información acerca de todas las configuraciones posibles de robots.txt se puede visitar <http://www.robotstxt.org/>.

## 7. COPIAS DE SEGURIDAD

---

En los puntos anteriores hemos visto cómo ir configurando de manera segura la instalación de Joomla! desde los primeros pasos hasta añadir opciones de seguridad adicionales mediante la configuración de determinados archivos. Llegados a este punto ya tenemos disponible una instancia del gestor de contenido completamente funcional y de la que deberíamos realizar una copia de seguridad previa a la instalación de plantillas, *plugins* o complementos adicionales que aportarán mayor funcionalidad al CMS.

El objetivo de la copia de seguridad, como en cualquier aplicación o sistema, es el poder restaurar la plataforma lo más rápido posible al estado previo a un incidente, fallo o cualquier otra situación que afecte a la correcta funcionalidad de Joomla!.

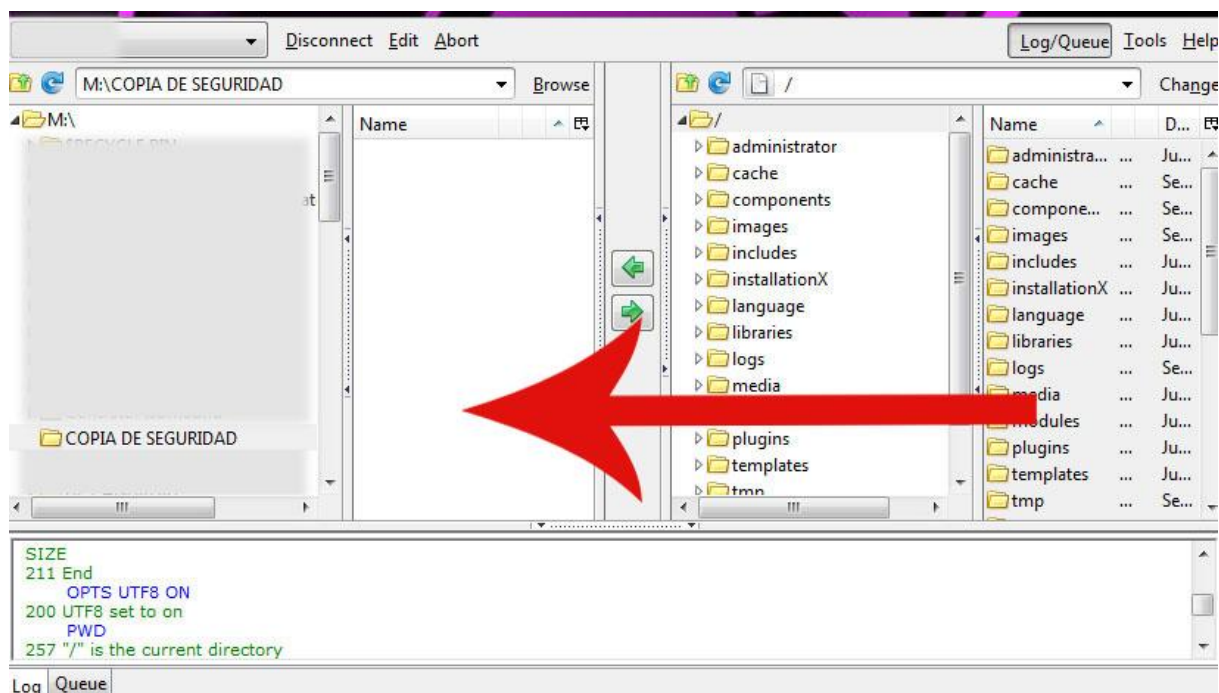
Una copia de seguridad de Joomla! y prácticamente de cualquier gestor de contenidos, consta de dos elementos:

- **Directorio de instalación de Joomla!:** también denominado “*document root*” (o directorio raíz) es la carpeta o directorio en el que se almacenan los archivos que componen el gestor de contenidos, sus archivos de configuración y complementos o *plugins*. Generalmente se ubican en la parte pública del hosting que hayamos contratado (*public\_html*, *www/public*, etc.)
- **Base de datos:** el lugar donde se almacena toda la información correspondiente a la instalación, contenidos, configuración del propio Joomla! así como de la configuración y contenidos de los distintos *plugins* o complementos. Mencionar que inicialmente tiene un número de tablas que se puede ir incrementando en la medida que se vayan instalando extensiones, complementos, etc.

### 7.1. COPIA DE SEGURIDAD DEL DIRECTORIO DE INSTALACIÓN

El modo más sencillo para realizar la copia de seguridad del directorio de instalación de Joomla! es a través de un cliente FTP o mediante alguna aplicación de gestión que puede proporcionar el proveedor de alojamiento web.

Mediante el primer método, tras conectarnos al proveedor, únicamente tenemos que seleccionar todos los archivos y directorios en la parte del servidor, y arrastrarlos hacia alguna carpeta que hayamos seleccionado en nuestro ordenador para realizar la copia desde el cliente ftp:



La otra opción es a través de alguna aplicación para la gestión de archivos que nos ofrezca el proveedor en el panel de control del dominio. El sistema es similar, seleccionamos todos los archivos y los descargamos a una carpeta en nuestro equipo.

Datos    Modificar    Transferencia    Archivo ZIP					
Path /					
Carpeta	Nombre	Tam...	Tipo	Modificado	Per...
/	administrator	-	Carpeta	05.06.2012 10:47	755
/	cache	-	Carpeta	18.09.2012 15:38	755
/	components	-	Carpeta	17.09.2012 16:49	755
/	images	-	Carpeta	17.09.2012 16:09	755
/	includes	-	Carpeta	05.06.2012 10:49	755
/	installationX	-	Carpeta	05.06.2012 10:50	755
/	language	-	Carpeta	05.06.2012 10:50	755
/	libraries	-	Carpeta	05.06.2012 10:52	755
/	logs	-	Carpeta	25.09.2012 11:38	755
/	media	-	Carpeta	05.06.2012 10:52	755
/	modules	-	Carpeta	05.06.2012 12:04	755
/	plugins	-	Carpeta	05.06.2012 12:04	755
/	templates	-	Carpeta	05.06.2012 12:03	755
/	tmp	-	Carpeta	18.09.2012 15:38	755
/	xmlrpc	-	Carpeta	05.06.2012 10:58	755
	.htaccess	3722	-	05.06.2012 17:59	644
	CHANGELOG.php	78097	PHP-Datos	05.06.2012 10:58	644
	COPYRIGHT.php	1172	PHP-Datos	05.06.2012 10:58	644
	CREDITS.php	14955	PHP-Datos	05.06.2012 10:58	644
	INSTALL.php	4344	PHP-Datos	05.06.2012 10:58	644
	LICENSE.php	17816	PHP-Datos	05.06.2012 10:58	644

## 7.2. BASE DE DATOS

Existen diversos métodos para realizar un respaldo de la base de datos de Joomla!, pero la más sencilla es a través del administrador de base de datos phpMyAdmin. Esta aplicación se encuentra disponible en los proveedores de alojamiento más populares y facilita enormemente las operaciones con las bases de datos MySQL.

Para realizar la copia de seguridad simplemente tenemos que acceder a phpMyAdmin a través del panel de control del *hosting* y realizar los siguientes pasos:

- Seleccionar la base de datos en la columna de la izquierda y hacer clic en la pestaña exportar
- Seleccionar todas las tablas en el formulario “Exportar” y verificar que está marcado “SQL”
- Dejar las “opciones SQL” por defecto (como se muestra en la imagen)
- Marcar “Enviar” para que phpMyAdmin genere un archivo descargable
- Dar un nombre al archivo o plantilla
- Pulsar sobre “continuar” para descargar el archivo al ordenador



The screenshot shows the Joomla! database export tool interface. The left sidebar lists database tables, with 'db' selected (1). The main area shows the 'Exportar' (Export) tab, where 'SQL' is selected (3). The 'Opciones SQL' (SQL Options) section is visible, including checkboxes for 'Estructura' (Structure) and 'Datos' (Data). The 'Enviar (genera un archivo descargable)' button is highlighted (4). The 'Plantilla del nombre del archivo' (File name template) field is set to '\_\_\_DB\_\_\_' (5). The 'Continuar' (Continue) button is highlighted (6).

### 7.3. OTRAS ALTERNATIVAS

En algunos casos los servicios de *hosting* proveen de herramientas para realizar copias de seguridad de manera automática que pueden facilitar sobremanera todo el proceso de respaldo. Además en muchas ocasiones no sólo permiten realizar una copia del sitio web y la base de datos, sino que también se ofrece la posibilidad de realizar un back-up de las cuentas de correo y de ftp entre otros

Seleccione Items a incluir a la copia de seguridad	
<b>Datos del Website</b>	
Carpetas del Dominio: Resguarda todos los archivos del usuario de todos los dominios	<input checked="" type="checkbox"/>
Listas de Subdominios: Resguarda la lista de subdominios de cada dominio	<input checked="" type="checkbox"/>
<b>E-Mail</b>	
Cuentas de Email de todos los dominios	<input checked="" type="checkbox"/>
Redirecciones: Incluye todas las direcciones redirigidas.	<input checked="" type="checkbox"/>
Autorespondedores: Incluye todos los autorespondedores y mensajes.	<input checked="" type="checkbox"/>
Mensajes de Vacaciones: Incluye todos los mensajes de vacaciones y horarios.	<input checked="" type="checkbox"/>
Listas de Correo: Incluye la lista, digest-list y archivos.	<input checked="" type="checkbox"/>
Configuraciones de E-mail: Incluye los filtros y la direccion de catchall.	<input checked="" type="checkbox"/>
<b>Ftp</b>	
Cuentas Ftp	<input checked="" type="checkbox"/>
Configuraciones de Ftp	<input checked="" type="checkbox"/>
<b>Bases de datos</b>	
Bases de Datos: Resguarda todas las Bases de Datos del usuario	<input checked="" type="checkbox"/>
Database data	<input checked="" type="checkbox"/>
<input type="button" value="Crear Backup"/>	

El único inconveniente es que el formato de archivo de copia de seguridad puede que únicamente sea válido para el proveedor de alojamiento sobre el que se ejecuta, por lo que se recomienda realizar un respaldo manual para garantizar la restauración con independencia del servicio de *hosting* que contratemos.

Adicionalmente, las operaciones de respaldo es posible realizarlas a través de una interfaz de comandos (*Shell*) o con un cliente SSH. Para más información acerca de este método puede consultar la entrada: [Asegurando Wordpress V: copias de seguridad](#).

Desde el CERT de INTECO se recomienda realizar copias de seguridad periódicas de manera regular y siempre que se realice algún tipo de cambio con el objetivo de poder restaurar la instancia del gestor de contenidos y mantener su funcionalidad.

## 8. EXTENSIONES DE TERCEROS

---

Uno de los aspectos más atractivos de los gestores de contenidos y por lo tanto de Joomla! es que mediante extensiones, plugins o módulos es posible ampliar las funcionalidades del sitio web que se implemente sobre esta plataforma. En la actualidad existen extensiones para casi cualquier cosa que esté relacionada con el Web 2.0 así como para otro tipo de funcionalidades como el comercio electrónico, galerías de imágenes, formación y un larguísimo etcétera.

Aunque este tipo de aplicaciones pueden en muchos casos dar solución a algún tipo de desarrollo sin necesidad de “picar” ni una línea de código, se debe ser consciente de que las extensiones han sido programadas por personas que quizás no hayan puesto el interés adecuado a la hora de desarrollarlo, en lo que al aspecto de la seguridad se refiere. Por esta razón nos podemos encontrar aplicaciones que cumplen la funcionalidad para la que han sido diseñadas pero en cambio no implementan las medidas de seguridad necesarias para ser instaladas en Joomla!. También es posible que se dé el caso de que la aplicación se haya desarrollado con las medidas de seguridad adecuadas para un determinado momento pero que con la combinación de más vectores de ataque pueda suponer un riesgo para el portal.

Por ello se debe poner especial cuidado a la hora de escoger las extensiones, módulos o plugins a instalar en la instancia de Joomla!. Además, en la actualidad es posible escoger entre multitud de extensiones que realizan la misma función.

Las premisas esenciales para instalar este tipo de aplicaciones serían:

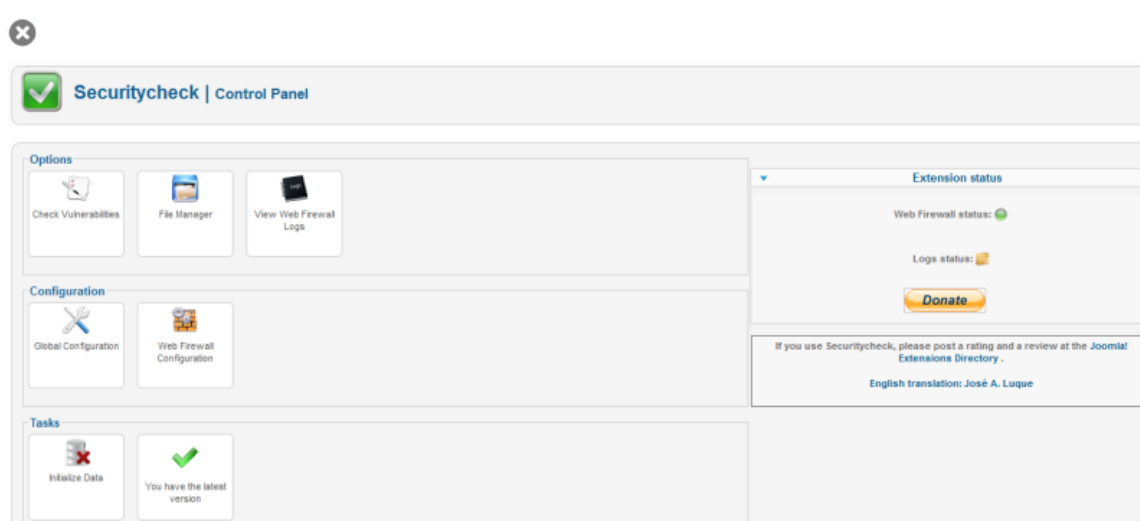
- **Verificar el historial de vulnerabilidades.** Evidentemente lo más recomendable es utilizar aplicaciones que no se encuentren en la lista de extensiones vulnerables (para más antiguas consultar esta otra lista). En caso contrario se está asumiendo un riesgo elevado del compromiso de la seguridad de la web.
- **Comprobar si está incluida en el Directorio de Extensiones de Joomla!** (JED Joomla! Extensions Directory). En este portal se realiza un primer filtrado comprobando que la aplicación cumple unos estándares mínimos (tanto de usabilidad como de seguridad).
- **Página del desarrollador y comunidad de soporte.** Este es un punto a tener en cuenta ya que aportará información acerca de cuánto tiempo lleva desarrollándose y el tipo de soporte con el que cuenta (foros, etc.). Adicionalmente en las web de los desarrolladores es posible comprobar el funcionamiento a través de una “*Demo*” antes de su instalación.
- **Versión nativa.** Siempre se debe verificar que la extensión esté disponible para la versión de Joomla! que se ha instalado. Esto evita tener que activar el “modo herencia” (*Legacy mode* –solo para Joomla! 1.5.X) que permite la instalación de

módulos y plugins desarrollados para Joomla! 1.0.X que, presumiblemente, se pueden haber dejado de soportar y pueden tener algún tipo de vulnerabilidad.

## 8.1. EXTENSIONES QUE AYUDAN A PROTEGER EL SITIO

Por otro lado, tenemos la posibilidad de instalar complementos o plugins que pueden facilitar en gran medida las tareas de administración como pueden ser las copias de seguridad, control de logs de acceso, etc. A continuación listamos algunas de ellas que nos han parecido interesantes pero como hemos indicado anteriormente, hay cientos de aplicaciones que se pueden utilizar:

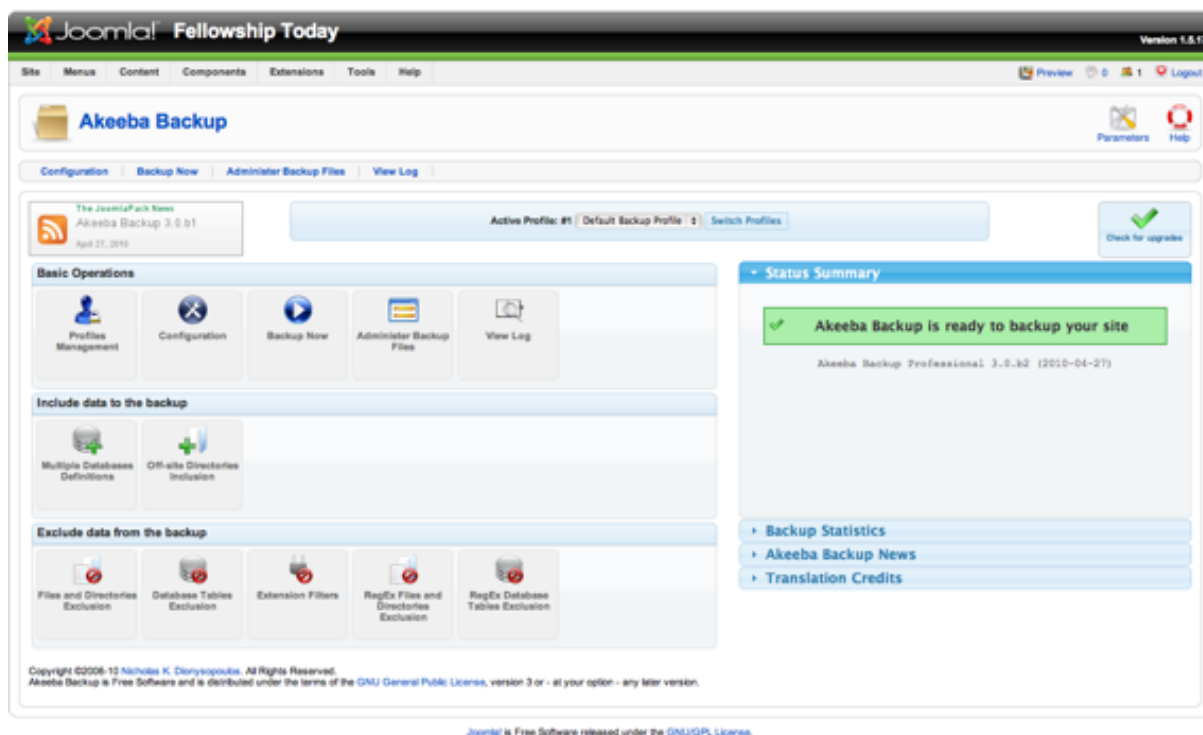
- **Securitycheck:** comprueba las versiones de todos los componentes instalados evitando que el usuario tenga que hacerlo manualmente. Además esta aplicación tiene funcionalidad de cortafuegos de aplicación para Joomla!. Está compuesta de dos elementos, el plugin, que permite configurar el firewall para proteger el sitio y el componente que muestra los registros. Adicionalmente esta aplicación puede proteger contra multitud de ataques web (XSS, SQLi, etc.)



### Securitycheck

Control Panel

- **Akeeba BackUp:** una excelente aplicación para realizar copias de seguridad automatizadas (Base de datos y directorio de instalación) y restaurarlas rápidamente en un servidor adecuado para alojar gestores de contenido tipo Joomla!. Actualizado tanto para las versiones 2.X como 3.X



Como resumen indicar que se debe controlar qué extensiones se instalan en la instancia del gestor de contenidos y obviamente, **siempre** debemos instalar las últimas versiones además de realizar comprobaciones periódicas del desarrollo y continuidad de las aplicaciones.

## 9. ACTUALIZACIONES Y SERVICIOS DE INFORMACIÓN

---

### 9.1. ACTUALIZACIONES

Como en cualquier aplicación o software que se precie, el mantener una política de actualizaciones es esencial con el objetivo de cubrir los agujeros de seguridad que se vayan descubriendo. En el caso del gestor de contenidos Joomla! se debe proceder del mismo modo previa evaluación del impacto que una actualización pueda provocar como la incompatibilidad entre complementos, plugins, etc. No obstante se debe considerar adecuadamente estos aspectos primando sobre todos los relacionados con la seguridad.

Generalmente, los procedimientos para actualizar el CMS Joomla! suelen ser sencillos y varían ligeramente en función de si se trata de actualizaciones dentro de la misma rama (por ejemplo de la v1.5.19 a la v1.5.23), o si es un cambio de versión (de la v1.5.x a la 2.5.x). Los primeros únicamente requieren la sustitución de los archivos antiguos por los de la nueva versión. En el caso de la segunda opción, en ocasiones es posible hacerlos directamente pero por lo general requieren de una instalación limpia de la versión de Joomla! que se quiere instalar y realizar una migración de datos.

En el sitio oficial <http://docs.joomla.org> se puede encontrar información útil acerca de cómo actualizar entre las distintas versiones del gestor de contenidos.

### 9.2. FOROS Y BOLETINES DE SEGURIDAD

Relacionado con el punto anterior, es sumamente recomendable suscribirse a servicios de información que nos permitan estar al día en relación a la aparición de nuevas versiones de Joomla! o el descubrimiento de agujeros de seguridad, que nos permitan actualizar o corregir los problemas lo más rápido posible.

Algunos recursos útiles:

- [Servicios de alerta temprana del CERT de INTECO](#): cuenta por un lado con una base de datos de vulnerabilidades en las que se publican las vulnerabilidades que se van descubriendo además de la posibilidad de suscribirse a un boletín en el que personalizar las alertas en base a un producto como por ejemplo Joomla!. Por otro lado cuenta con un servicio de “Avisos de seguridad” a través del que se notifican las actualizaciones y nuevas versiones de los productos más populares.
- [La comunidad de Joomla!](#): portal oficial de la comunidad de Joomla! en el que se pueden encontrar listas de correo, foros, nuevos desarrollos, etc.



**Puedes seguirnos desde:**

**WWW**     [\*\*http://cert.inteco.es\*\*](http://cert.inteco.es)



**Perfil Twitter INTECO-CERT:**  
[\*\*https://twitter.com/intecocert\*\*](https://twitter.com/intecocert)



**Perfil Scribd INTECO-CERT:**  
[\*\*http://es.scribd.com/intecocert\*\*](http://es.scribd.com/intecocert)



**Perfil Youtube INTECO-CERT:**  
[\*\*http://www.youtube.com/intecocert\*\*](http://www.youtube.com/intecocert)



**Perfil LinkedIn INTECO-CERT:**  
[\*\*http://www.linkedin.com/groups/INTECOCE-RT-Centro-respuesta-incidentes-seguridad-4362386L\*\*](http://www.linkedin.com/groups/INTECOCE-RT-Centro-respuesta-incidentes-seguridad-4362386L)

**Puedes enviarnos tus comentarios o consultas a:**



[\*\*consultas@cert.inteco.es\*\*](mailto:consultas@cert.inteco.es)