GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Guía básica para la securización de Wordpress

INTECO-CERT

Septiembre 2012

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

1. SOBRE LA GUÍA

Esta guía está estructurada para seguir el proceso de instalación y configuración de un sitio de *Wordpress* convencional, de forma que cada uno de los pasos o fases principales en el proceso es un apartado de la guía. Teniendo en cuenta lo anterior, la guía se estructura de la siguiente forma:

2. **Introducción** – Donde se realiza un breve recorrido por los orígenes de *Wordpress* a través de la evolución de la *Web 2.0* hasta llegar a las plataformas de publicación de bitácoras (*blogs*).

3. **Alojamiento** – Para esta guía se considera que la instalación se va realizar en un servicio de alojamiento externo, aunque la guía es perfectamente válida para un alojamiento propio, por ejemplo, un servidor personal o que se encuentra en las propias instalaciones de la organización. En este apartado se dan un conjunto de recomendaciones para llevar a cabo una selección apropiada del servicio de hosting, de forma que ofrezca las garantías de seguridad adecuadas.

4. **Instalación y primeros pasos** – A continuación se inicia el proceso de instalación de *Wordpress*, durante el cual será necesario tener en cuenta algunos aspectos de seguridad muy importantes.

5. **Seguridad de directorios y archivos** – Una vez concluida la instalación, comienza el proceso de securización de los archivos y directorios de **Wordpress**.

6. **Uso y configuración de *.htaccess*** – En relación con el anterior apartado y como complemento al mismo, se explica el uso de los ficheros de configuración distribuida, *.htaccess*, como medio de aplicar reglas y restricciones de seguridad.

7. **Copias de seguridad** – El siguiente punto aborda la creación de copias de seguridad, proporcionando una visión general del proceso, además de una descripción tanto del proceso manual como automatizado de copias de seguridad.

8. **Características adicionales de seguridad** – Para finalizar la configuración, en este apartado se describen algunas características adicionales de seguridad que es posible incorporar a *Wordpress*.

9. **Fuentes de información** – Proporciona un conjunto de enlaces con las fuentes de información utilizadas y otras fuentes de interés en relación con el contenido de la guía.

2. INTRODUCCIÓN

Desde el año 2000 se han producido varias revoluciones tecnológicas que han tenido enorme importancia en la evolución de las tecnologías de la información y de Internet. La última revolución la estamos viviendo ahora, en el momento de la publicación de esta guía, de la mano de los dispositivos y las tecnologías móviles. Pero en el año 2004 tomo forma una revolución que había comenzado a gestarse varios años antes, y que finalmente fue conocida como la revolución de la *Web 2.0*, un concepto que fue creado en 2004 por *Dale Dougherty* de *O'Reilly Media*, en referencia a los tremendos cambios que se estaban produciendo en Internet y en el *World Wide Web*.

Históricamente, la mayoría del contenido web de Internet ha provenido de compañías y organizaciones que mantenían diversos sitios web, y de forma mucho más minoritaria, de usuarios entusiastas de Internet, que poseían los conocimientos necesarios y utilizaban la web como un medio de compartir información. Pero la generación de contenido o su publicación de Internet seguía siendo complicada y la mayoría de los usuarios sencillamente utilizaba Internet y la web para consultar y buscar información.

Aproximadamente a principios de la década de 2000, comenzaron a aparecer compañías que desarrollaron servicios web con una filosofía distinta, basada en la participación y la capacidad de compartir información que creaban los propios usuarios. El máximo exponente de este fenómeno lo podemos encontrar en los servicios de creación de blogs o bitácoras, que tuvieron un crecimiento explosivo. El éxito fue tremendo y cualquier usuario podía crear su propio sitio web en minutos y comenzar a publicar contenido que estaba disponible para otros usuarios de Internet. Uno de los servicios más exitosos relacionado con la creación de *Blogs* fue *Blogger*, creado por Pyra Labs, y adquirido por Google en el año 2003.

En aquella época y de forma paralela a la creación de múltiples servicios y plataformas, comenzó el desarrollo de una aplicación web que tuvo un éxito increíble desde el lanzamiento de la primera versión, en mayo de 2003, hablamos de *Wordpress*. En la actualidad, *Wordpress* se ha convertido en una de las plataformas de más éxito, para creación de blogs y sitios de Internet para todo tipo de organizaciones y para millones de usuarios.

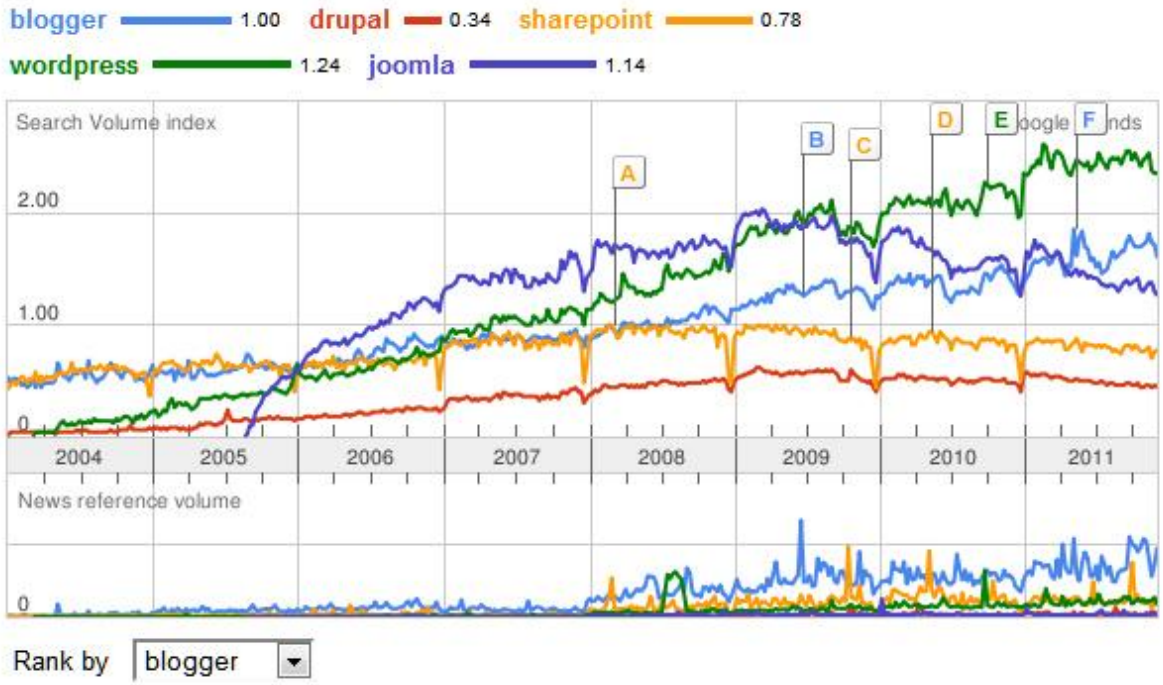
Wordpress basa su éxito en una aplicación desarrollada desde la usabilidad, el diseño y una funcionalidad que puede extenderse completamente a través de sus más de 20.000 *plugins* gratuitos y cientos de *plugins* comerciales.

En la actualidad *Wordpress* posee dos formatos o líneas de actividad. Por un lado, se ofrece como un servicio a través del sitio Wordpress.org, en el que cualquier usuario puede crear su propia bitácora en minutos. Por otro lado, Wordpress se ofrece como aplicación web que se puede descargar e instalar en un servidor web propio o en cualquier servicio de hosting.

La sencillez de *Wordpress*, su capacidad para crecer y aumentar su funcionalidad fácilmente, así como otras funcionalidades como su sistema de plantillas, su robustez, el uso de estándares y su mejora constante, con versiones que son publicadas regularmente,

además de una comunidad de desarrolladores y una compañía que lo apoya y es la responsable de su mantenimiento, han impulsado el crecimiento de *Wordpress*.

En la imagen podemos ver un gráfico de distintos gestores de contenido, como *Joomla* o *Drupal*, junto con *Wordpress*.



Como se aprecia en el gráfico, mientras *Drupal*, *Joomla* o *Blogger* han dejado de crecer desde finales de 2009, *Wordpress* (línea verde) ha seguido aumentando.

En la propia web de *Wordpress.com* se pueden ver las estadísticas del servicio de *Wordpress*, donde se indica que en la actualidad hay más de **58 millones** de sitios web funcionando con esta aplicación en su modalidad de servicio, a lo que había que sumar los sitios que funcionan con la aplicación web de *Wordpress*, que se estima en **14 millones**, lo que supone un total de **72 millones.**

A continuación se proporcionan algunos datos más que dan una idea del uso actual de *Wordpress* y de su velocidad de evolución (fuente http://lorelle.wordpress.com).

- Del total de sitios web que había en Internet en 2011, se estima que el 25% funciona con *Wordpress*.
- Ha habido un total de 98 versiones desde su lanzamiento en 2003.
- La versión 3.0 de *Wordpress* desde su lanzamiento se ha descargado más de 65 millones de veces.
- En el servicio de *Wordpress.com* se publican medio millón de artículos al día.

- Está disponible en más de 40 idiomas.

En la actualidad *Wordpress* se han convertido en una de las plataformas de gestión de contenidos más importantes, utilizada por todo tipo de organizaciones y compañías, grandes y pequeñas, pero también por multitud de pequeñas empresas y usuarios.

Lógicamente, el gran nivel de difusión y uso de *Wordpress* lo convierten en el posible blanco de ciber-ataques, que podrían tener importantes consecuencias para las organizaciones y usuarios utilizan esta herramienta para la gestión de sus sitios web. Esta es una de las razones por la cual INTECO-CERT ha elaborado esta guía básica, que proporciona un conjunto recomendaciones de seguridad y los pasos a seguir para aumentar la seguridad de *Wordpress*.

Por otro lado, la guía está pensada para usuarios con un nivel de conocimiento medio o alto, aunque su contenido se ha elaborado de forma que cualquier usuario pueda comprenderlo fácilmente. Aún así, se recomienda tener conocimientos técnicos suficientes como para llevar a cabo con éxito las configuraciones y los pasos que se describen en el documento.

Finalmente, desde INTECO-CERT esperamos que esta guía ayude a mejorar la seguridad de *Wordpress*, ayudando a conseguir un Internet más seguro para todos.

3. SERVICIO DE HOSTING

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 *Wordpress*, *Joomla!* o *Drupal*. Se tratan de CMS (*Content Management System*) o gestores de contenidos de código abierto, bajo *licencia GPL*, que ofrecen multitud de opciones gracias a su versatilidad y la posibilidad de añadirles complementos de terceros que les aportarán mucha más funcionalidad de la que poseen nativamente.

Los gestores de contenido en los que se centra este artículo están desarrollados bajo *PHP* y *HTML* y necesitan de una base de datos del tipo *MySQL* (se abre en nueva ventana)y de un servidor web, generalmente *Apache* aunque también se puede instalar sobre otros.

3.1. ESCENARIO

Imaginemos un usuario que decide crear su propio sitio web, de empresa o para un blog personal y decide contratar su propio servicio de alojamiento web a un proveedor e instalando desde cero su plataforma para la gestión de contenidos.

Para instalarlos 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!*, *WordPress* o *Drupal.*

3.2. CRITERIOS DE SELECCIÓN

- **Reputación del proveedor**: Es un parámetro ciertamente subjetivo, pero es importante que busquemos proveedores que ofrezcan garantías y cuya reputación sea razonablemente buena. Consultar en foros, buscadores y preguntar a otras empresas que ya dispongan de un servicio de hosting puede ser una buena forma de conocer su reputación o confiabilidad.

- **Tipo de alojamiento (arquitectura de servicio)**: la mayor parte de proveedores ofrecen dos tipo de alojamiento: *Windows* o *Linux*. Por razones de compatibilidad, *Joomla!*, *WordPress* y *Drupal* se comportan 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 el idioma para ayudar al usuario 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*, *phpMyAdmin*), etc.) puede facilitar enormemente la tarea a la hora de implementar un gestor de contenidos.

- **Seguridad**: conocer qué política aplica ante posibles problemas de seguridad del servidor o la frecuencia en 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.

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.

4. INSTALACIÓN

4.1. PRIMEROS PASOS

Como vimos en el apartado anterior, el primer paso es seleccionar un proveedor del servicio de *hosting* adecuado, a continuación se procederá a la contratación del servicio, lo cual puede realizarse a través de Internet, incluido el pago, para lo cual será necesario tomar precauciones, como en cualquier transacción u operación comercial que se realice a través de la red.

Una vez formalizado el contrato, el proveedor proporcionará una cuenta de acceso al panel de gestión del servicio de *hosting*. A través de esta cuenta se gestionan todos los aspectos relativos al servicio, por lo que es muy importante usar una contraseña que cumpla con los requisitos básicos de seguridad y sea guardada adecuadamente. Como vamos a ver a lo largo de esta entrega, será necesario disponer de varias cuentas, por lo que es recomendable utilizar alguna herramienta para la gestión de contraseñas.

Llegados a este punto vamos a suponer que se ha configurado un dominio, el espacio web correspondiente y se dispone de acceso FTP al espacio del *hosting*. Al igual que antes, en el caso de la contraseña de acceso por FTP (*File Transfer Protocol*), es conveniente usar una contraseña robusta y deshabilitar el servicio de FTP cuando no se use, para evitar posibles intentos de acceso a través de este servicio.

Otro aspecto más a la hora de configurar el CMS *Wordpress*, será crear una nueva base de datos, en este caso, sobre *MySQL*, que es el motor de base de datos que usa. Para ello, al igual que antes, será necesario crear una cuenta de acceso a la base de datos, por lo que es fundamental usar una contraseña robusta para dicha cuenta.

4.2. INSTALACIÓN

Al realizar la instalación es importante descargar la última versión estable de Wordpress. Hay que evitar instalar versiones RC (*Release Candidate*) o no estables, salvo que se lleven a cabo actividades relacionadas con el desarrollo de aplicaciones o funcionalidades para *Wordpress*.

Una vez descargada la última versión estable del código, se copia al espacio de hosting, en el raíz de la carpeta que alojará el sitio, por ejemplo, mediante el servicio FTP. Para iniciar la instalación únicamente hay que ir al navegador y escribir el dominio, previamente contratado, desde el cual se va a realizar la instalación (*Imagen 1*).

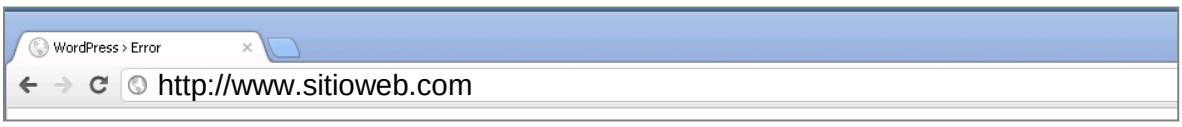


Imagen 1. Acceso al sitio web a través del navegador.

Al introducir la dirección en el navegador, aparecerá un mensaje de error indicando que aún no se ha realizado la instalación y nos informa que va a comenzar el proceso, y para ello es necesario crear un fichero denominado *wp-config.php (Imagen 2)*.

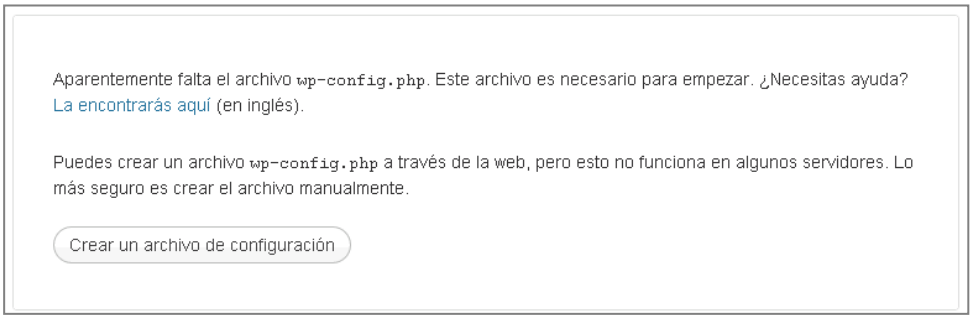


Imagen 2. Pantalla de inicio de la instalación, creación de fichero wp-config.php.

Al pulsar sobre crear el archivo de configuración se nos piden una serie de datos que serán incluidos en dicho fichero y que son necesarios para que *Wordpress* pueda funcionar. Los mostramos a continuación (*imagen 3*):

Imagen 3. Datos necesarios para realizar la instalación.

De los datos que se solicitan, los más importantes desde el punto de vista de la seguridad son la contraseña de la base de datos de *MySQL*, que habremos configurado previamente y como se ha indicado debe de cumplir los criterios mínimos de seguridad. Por otro lado, el parámetro que establece el «Prefijo de tabla» también es muy importante. Este parámetro establece el prefijo con el cual serán creadas todas las tablas de la base de datos de

Wordpress. Por defecto es "WP_" y si no se cambia, se corre el riesgo de ser vulnerable a ataques de inyección de código o consultas que explotan algún tipo de vulnerabilidad. Para evitarlo, se pone un prefijo aleatorio, por ejemplo, con tres o cuatro letras, un número o una combinación. A continuación (*Imagen 4*) se puede ver un ejemplo de cómo quedaría el formulario con los datos indicados.

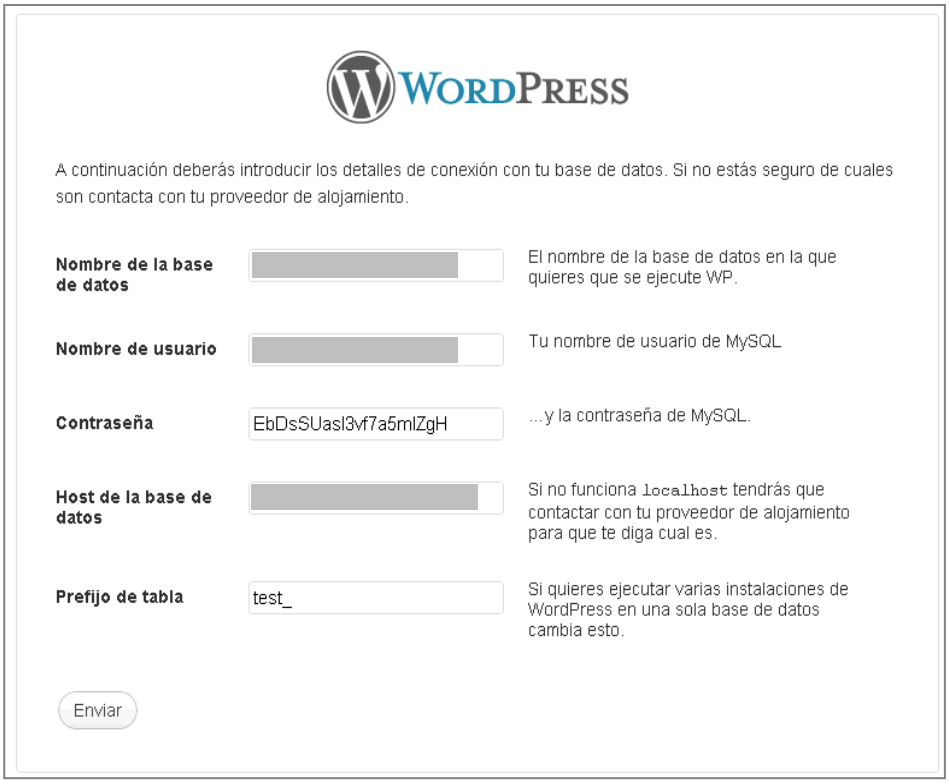


Imagen 4. Datos de configuración completos.

Una vez es enviado el formulario con los datos, se realiza la comprobación de los mismos y a continuación, si todo es correcto se nos muestra un mensaje indicando que no ha habido ningún problema y se puede iniciar la instalación *(imagen 5)*.

Imagen 5. Imagen que muestra que los datos son correctos y puede comenzar la instalación.

En la siguiente pantalla se solicitan más datos, algunos de ellos fundamentales desde el punto de vista de la seguridad, los vemos a continuación (*imagen 6*):

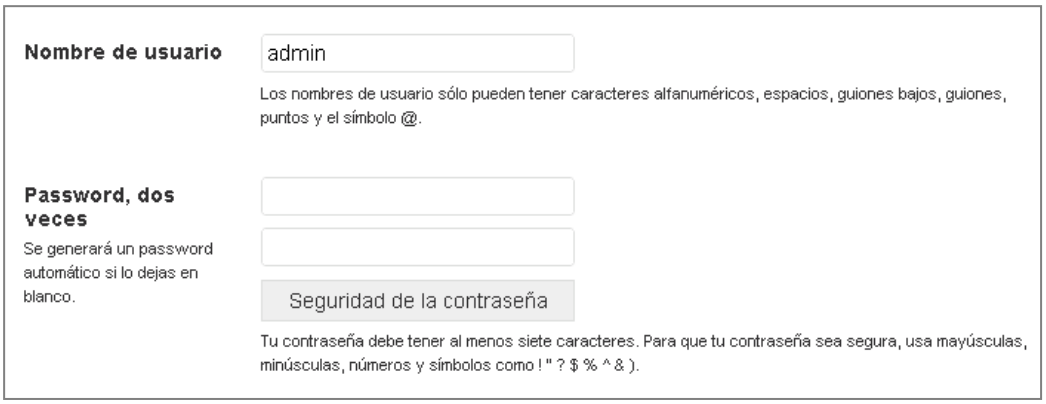


Imagen 6. Introducción de los datos correspondientes a la cuenta de administrador del sitio.

Se solicita el nombre de usuario de administrador de *Wordpress* y la contraseña. Al igual que ocurría antes con el parámetro de prefijo, usar el nombre de usuario por defecto supone un riesgo, para evitarlo, se recomienda usar un nombre de usuario aleatorio, o construido con alguna regla.

En cualquier caso, nunca se debe de usar el nombre por defecto. En cuanto a la contraseña, es fundamental utilizar una contraseña robusta y distinta de las anteriores. Una vez introducidos todos los datos que se solicitan en la pantalla anterior, procedemos a finalizar la instalación (*imagen 7*).

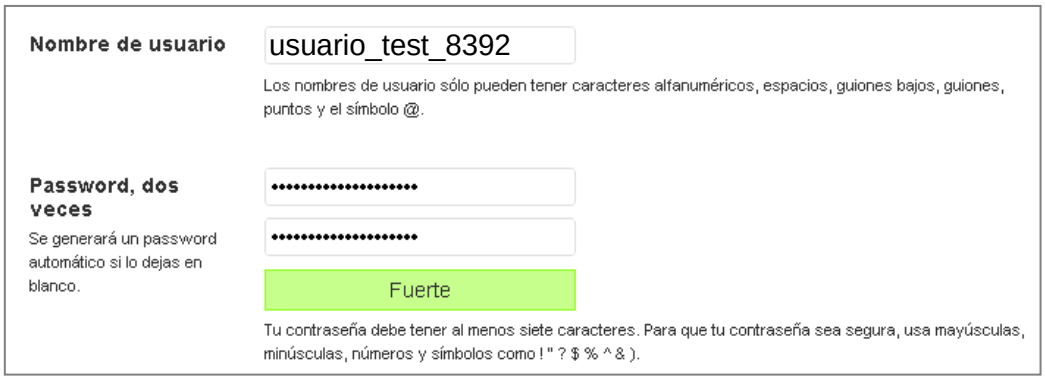


Imagen 7. Datos de la cuenta de administrador completados.

Una vez finalizada la instalación, nos mostrará un mensaje como el que se ve a continuación, y el formulario de acceso, para poder comenzar a trabajar con el *CMS*, con lo que la instalación está realizada (*imagen 8*).

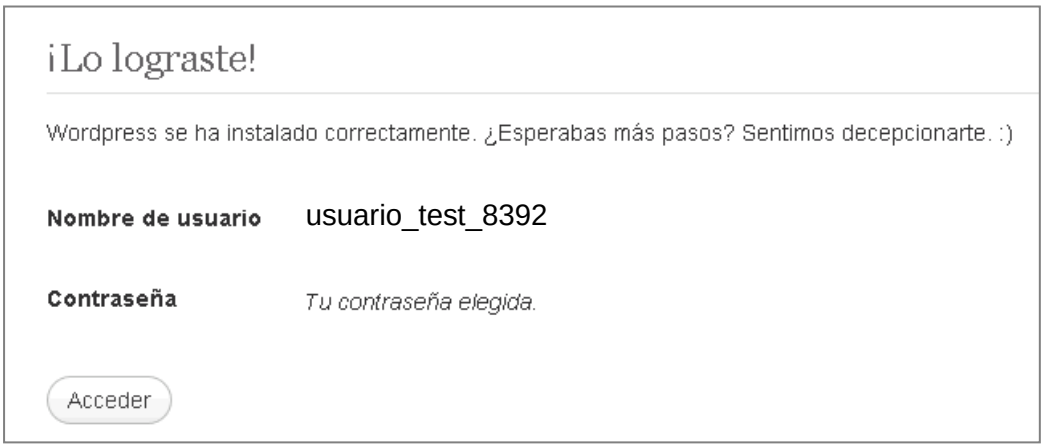


Imagen 8. Pantalla que muestra que la instalación ha finalizado y muestra el formulario de acceso al sitio.

Como recordatorio a lo que se ha explicado en los anteriores apartados, INTECO-CERT recomienda no utilizar parámetros de configuración por defecto, salvo si estos pudieran afectar al funcionamiento de la aplicación.

5. CONFIGURACIÓN DE SEGURIDAD BÁSICA

En el apartado anterior se describió el proceso de instalación básica de *Wordpress*. Durante dicho proceso era necesario tener en cuenta algunos aspectos de seguridad relacionados con cuentas de acceso o datos de configuración iniciales.

Una vez realizada la instalación básica será necesario limitar el acceso a ciertos ficheros y directorios. A continuación vamos a describir el proceso seguido para protegerlos. El orden no es realmente importante, lo fundamental es aplicar la protección a todos ellos.

Para comprender como se aplican los permisos a directorios y archivos, vamos mostrar el contenido del directorio donde está alojado *Wordpress*. El contenido se puede ver a continuación (*imagen 9*).

Nombre de archivo	Tamaño d...	Tipo de arc...	Última modificac...	Permisos	Propietario/...
..					
wp-admin		File Folder	28/05/2012 12:...	flcdmpe (07...	7249046 600
wp-content		File Folder	04/06/2012 11:...	flcdmpe (07...	7249046 600
wp-includes		File Folder	28/05/2012 12:...	flcdmpe (07...	7249046 600
.htaccess	4	HTACCESS ...	04/06/2012 11:...	adfrw (0644)	7249046 600
index.php	397	PHP File	28/05/2012 12:...	adfrw (0644)	7249046 600
licencia.txt	17.935	Text Docu...	28/05/2012 12:...	adfrw (0644)	7249046 600
license.txt	16.572	Text Docu...	28/05/2012 12:...	adfrw (0644)	7249046 600
readme.html	9.735	Firefox HT...	28/05/2012 12:...	adfrw (0644)	7249046 600
wp-activate.php	4.268	PHP File	28/05/2012 12:...	adfrw (0644)	7249046 600
wp-app.php	40.272	PHP File	28/05/2012 12:...	adfrw (0644)	7249046 600
wp-blog-header.php	274	PHP File	28/05/2012 12:...	adfrw (0644)	7249046 600
wp-comments-post.php	3.989	PHP File	28/05/2012 12:...	adfrw (0644)	7249046 600
wp-config-sample.php	3.590	PHP File	28/05/2012 12:...	adfrw (0644)	7249046 600
wp-config.php	3.852	PHP File	04/06/2012 11:...	adfrw (0666)	7249046 600
wp-cron.php	2.684	PHP File	28/05/2012 12:...	adfrw (0644)	7249046 600
wp-links-opml.php	1.997	PHP File	28/05/2012 12:...	adfrw (0644)	7249046 600
wp-load.php	2.578	PHP File	28/05/2012 12:...	adfrw (0644)	7249046 600
wp-login.php	27.695	PHP File	28/05/2012 12:...	adfrw (0644)	7249046 600
wp-mail.php	7.777	PHP File	28/05/2012 12:...	adfrw (0644)	7249046 600
wp-pass.php	413	PHP File	28/05/2012 12:...	adfrw (0644)	7249046 600
wp-register.php	334	PHP File	28/05/2012 12:...	adfrw (0644)	7249046 600
wp-settings.php	9.913	PHP File	28/05/2012 12:...	adfrw (0644)	7249046 600
wp-signup.php	18.545	PHP File	28/05/2012 12:...	adfrw (0644)	7249046 600
wp-trackback.php	3.702	PHP File	28/05/2012 12:...	adfrw (0644)	7249046 600
xmlrpc.php	3.266	PHP File	28/05/2012 12:...	adfrw (0644)	7249046 600

Imagen 9. Imagen del directorio principal de Wordpres y de la columna que muestra los permisos de directorios y archivos.

Como vemos en la imagen, hay una columna que muestra los permisos (dentro del recuadro rojo), tanto de los directorios como de los archivos.

Antes de comenzar con las operaciones de configuración, hay que indicar que se da por supuesto que **el usuario sabe establecer permisos tanto a archivos como a directorios y comprende su funcionamiento**, además de disponer de acceso al servidor que aloja el sitio web, con privilegios suficientes.

5.1. DIRECTORIO RAÍZ Y ARCHIVOS

A continuación se realiza una breve descripción de los archivos a proteger y de los permisos a aplicar al directorio raíz de Wordpress y su contenido.

- **/directorio_raiz/** – El directorio raíz de *Wordpress* es aquel que contiene lo que aparece en la imagen anterior. Los permisos del directorio deberán de ser 0755.

- **.htaccess** – Este fichero, está directamente relacionado con la seguridad y el acceso a los directorios y ficheros. Será explicado en la próxima entrega. De momento, lo importante es que donde se instale *Wordpress* deberá de existir uno y sus permisos serán 0644.

- **readme.html** – A pesar de que se trata de un archivo *html* con información general relativa a *Wordpress*, conviene protegerlo de forma que no sea posible acceder a él de forma que un atacante pueda ver la versión de *Wordpress* instalada a través de este fichero. Para ello, establecemos sus permisos a 0440.

- **wp-config.php** – Se trata de uno de los ficheros más importantes de *Wordpress* ya que en él se almacenan los parámetros básicos de funcionamiento de Wordpress. Una vez configurado *Wordpress*, conviene protegerlo. Para ello establecemos los permisos a 0644.

5.2. DIRECTORIOS PRINCIPALES

A continuación se realiza una breve descripción de los principales directorios a proteger.

- **wp-admin** – contiene el conjunto de código relacionado con la administración del sitio Web. Es un directorio que debe de ser protegido. Los permisos de este directorio serán los mismos que el directorio raíz, es decir, 0755.

- **wp-content** – es el directorio en el cual se almacena todo lo que el usuario incorpore a la instalación básica de *Wordpress* para dotarla de mayor funcionalidad, así como diversos contenidos, como imágenes, etc. Sus permisos serán 0755.

- **Wp-includes** – contiene el grueso del código que hace funcionar *Wordpress*. Sus permisos serán 0755.

5.3. LISTADO DE DIRECTORIOS

Para evitar el listado de directorios se usan, entre otras técnicas, el uso de ficheros *index.php*. Estos ficheros contienen un código muy simple, que no lleva a cabo ninguna acción, pero que al ser ejecutados impiden (a priori) que se pueda ver el contenido de los directorios.

El código es el siguiente y como se puede observar únicamente contiene un comentario, que además no se muestra en la ejecución, por lo que la ejecución del fichero mostrará una página *html* en blanco.

```
<?php
//Silence is golden
?>
```

Deberemos de disponer un fichero *index.php* con el código anterior en los directorios que se muestran a continuación y todos ellos tendrán los permisos **0644.**

```
wp-admin/index.php
wp-content/index.php
wp-content/plugins/index.php
wp-content/uploads/indexp.php
?>
```

6. CONFIGURACIÓN DE HTACCESS

En la anterior entrega de esta serie de notas, se describió el proceso de configuración básica de seguridad para la protección de directorios de *Wordpress*. Además de establecer los permisos adecuados a ciertos directorios y ficheros, es posible realizar una configuración más avanzada y completa mediante el uso del fichero htaccess.

El fichero *htaccess* es un fichero del Servidor Web Apache, denominado también fichero de configuración distribuida, mediante el cual es posible definir distintas directivas que permiten modificar el comportamiento del servidor web, pudiendo distribuirlas en varios ficheros sin necesidad de usar la configuración global de servidor web, posibilitando distintos comportamientos del servidor.

Las directivas que se pueden incluir en *htaccess* son muy variadas y permiten realizar todo tipo de acciones. En el caso que se menciona, únicamente interesan aquellas destinadas a la seguridad y en concreto a proteger ciertos directorios y comportamientos en *Wordpress*.

El fichero *htaccess* se puede crear de forma automática en el directorio donde es instalado *Wordpress*. Si el directorio raíz donde se va a instalar *Wordpress* se crea a través de herramientas del servicio de *hosting*, entonces, se suele generar de forma automática un fichero vacio o con alguna configuración por defecto. Si el directorio es creado manualmente, entonces, por lo general, hay que crear el fichero también manualmente, por ejemplo, a través de una consola.

En nuestro caso, el fichero se ha creado automáticamente al crear el directorio que va a contener *Wordpress* mediante las herramientas del servicio de alojamiento. Lo podemos ver en la imagen que se muestra a continuación.

Nombre de archivo	Tamaño d...	Tipo de arc...	Última modificac...	Permisos	Propietario/...
..					
wp-admin		File Folder	28/05/2012 12:...	flcdmpe (07...	7249046 600
wp-content		File Folder	04/06/2012 11:...	flcdmpe (07...	7249046 600
wp-includes		File Folder	28/05/2012 12:...	flcdmpe (07...	7249046 600
.htaccess	4	HTACCESS ...	04/06/2012 11:...	adfrw (0644)	7249046 600
index.php	397	PHP File	28/05/2012 12:...	adfrw (0644)	7249046 600
licencia.txt	17.935	Text Docu...	28/05/2012 12:...	adfrw (0644)	7249046 600
license.txt	16.572	Text Docu...	28/05/2012 12:...	adfrw (0644)	7249046 600
readme.html	9.735	Firefox HT...	28/05/2012 12:...	adfrw (0644)	7249046 600
wp-activate.php	4.268	PHP File	28/05/2012 12:...	adfrw (0644)	7249046 600

Imagen 10. Imagen que muestra el fichero htaccess que se encuentra en el directorio raíz de Wordpress.

6.1. NO PERMITIR MOSTRAR EL CONTENIDO DE DIRECTORIOS

Debido a que *Wordpress* es muy conocido, su estructura de directorios también lo es, lo que supone un riesgo debido a que es posible que un atacante aprovechando ese conocimiento para intentar listar el contenido de los directorios y obtener información sobre plugins, temas, etc.

Para evitarlo, utilizamos la siguiente directiva.

```
#no permitir mostrar el contenido de directorios
Options All -Indexes
```

6.2. PROTEGER WP-CONFIG.PHP

La primera directiva que vamos a indicar se refiere a la protección del fichero *wp-config.php*, donde se almacena la configuración de *Wordpress*. Para evitar su modificación o el acceso desde el exterior para ver su contenido, incorporamos el código que vemos a continuación.

```
#proteger el archivo wp-config.php
<Files wp-config.php>
Order allow, deny
Deny from all
</Files>
```

6.3. PROTEGER EL ACCESO AL DIRECTORIO WP-CONTENT

El directorio *wp-content* aglutina todos aquellos ficheros y contenidos que sirven para personalizar un sitio, desde temas gráficos, plugins y otros ficheros. Para protegerlo de accesos no autorizados utilizamos la siguiente directiva.

```
#proteger el acceso al directorio wp-content
Order allow, deny
Deny from all
<Files ~".(xml|css|jpe?g|png|gif|js)$">
Allow from all
</Files>
```

6.4. LIMITAR EL ACCESO POR IP COMO ADMINISTRADOR

Por lo general los administradores de sitios web suelen acceder a la gestión de un sitio web desde varias *IP's* más o menos habituales, aunque hoy día, los dispositivos móviles suponen que está premisa no se cumpla, pero limitar el acceso como administrador a una o varias *IP's* es una técnica muy efectiva para proteger la gestión de un sitio web.

Para aplicar esta característica de seguridad, incorporamos el código que se muestra a continuación.

```
#limitar el acceso como administrador por IP
Order allow, deny
Allow from XXX.XXX.XXX.XXX (reemplazar con la dirección ip que
se desea permitir)
Deny from all (denegamos el acceso a todas, excepto la ip de la
línea superior)
```

6.5. LIMITAR EL ACCESO POR IP A DIRECCIONES MALICIOSAS (BANEO)

En ocasiones se producen intentos de intrusión de determinadas *IP's* desde las cuales se lanzan ataques reiterados en forma de intentos de acceso, ataques de fuerza bruta contra formularios de acceso, etc. Cuando esto ocurre, es posible limitar estas direcciones *IP* mediante una directiva similar a la que hemos visto en el apartado anterior.

```
# limitar el acceso por IP a direcciones maliciosas (baneo)
<Limit GET POST>
Order allow, deny
Deny from XXX.XXX.XXX.XXX (ip maliciosa bloqueada)
Allow from all (permitimos al resto de IP's)
</Limit>
```

6.6. LIMITAR EL ACCESO POR DOMINIO A DIRECCIONES MALICIOSAS (BANEO)

Al igual que en el apartado anterior, es posible limitar el acceso no solo por *IP* sino también por dominio, tal y como se muestra a continuación:

```
# limitar el acceso por dominio (baneo)
RewriteEngine On
Options +FollowSymlinks
RewriteCond %{HTTP_REFERER} dominio_a_banear\.com [NC]
RewriteRule .* - [F]
```

6.7. PROTEGER EL FICHERO .HTACCESS

Finalmente, podemos incluir una directiva para proteger el propio fichero *.htaccess*, tal y como se ve a continuación, de forma que se previene el acceso a cualquier fichero cuyo nombre comience con la cadena de texto "hta".

```
# proteger el archivo htaccess
<Files ~"^.*\.([Hh][Tt][Aa])">
Order allow, deny
Deny from all
Satisfy all
</Files>
```

Además de estas directivas, es posible incluir otras, pero **la inclusión de directivas deberá de ser cuidadosa**. En el siguiente apartado conoceremos algunos plugins que permiten incorporar características de seguridad adicionales.

7. COPIAS DE SEGURIDAD

7.1. MÉTODO MANUAL

En las anteriores entregas de esta serie hemos visto como la seguridad debe de estar presente desde los primeros pasos de la instalación, en este caso, de *Wordpress*. Si llevamos a cabo todos los pasos indicados hasta ahora en las anteriores entregas, llegaremos a un punto en el cual tendremos una instalación "limpia" de *Wordpress*, es decir, una instalación con las opciones y complementos básicos incluidos en *Wordpress*, y sin ningún tipo de personalización o añadido que modifique la configuración básica, salvo aquellos aspectos que se han visto en anteriores entregas y que están relacionados exclusivamente con la seguridad.

Llegados a esta fase, es muy interesante y recomendable realizar la primera copia de seguridad de la instalación de *Wordpress*, de forma que sea posible volver a este punto si se produce algún problema durante la instalación de añadidos, complementos, temas o personalizaciones en el sitio.

7.2. CONTENIDO DE LA COPIA DE SEGURIDAD

La copia de seguridad de *Wordpress*, para que sea completa debe de incorporar dos elementos que indicamos a continuación:

- Copia de seguridad de la base de datos, **incluyendo todas las tablas con los datos, sean o no propias de *Wordpress***, como ocurre en el caso de los plugins de Wordpress, que en ocasiones necesitan crear tablas adicionales.

- Copia de seguridad del directorio de Wordpress, donde se ha realizado la instalación del sitio. La copia de seguridad deberá de incluir el núcleo (*core*) de *Wordpress*, temas, código adicional, plugins, etc, en definitiva, todo el directorio de la instalación completo.

Para la realización de la copia de seguridad se puede usar un método manual o más o menos automatizado. Para esta entrega, vamos a explicar el proceso de copia de seguridad a través de un método clásico y más manual. En una entrega posterior de esta serie, aprenderemos a realizar las copias de seguridad mediante plugins o complementos de terceros que facilitan esta labor.

7.3. COPIAS DE SEGURIDAD MEDIANTE CONSOLA DE COMANDOS

Para la realización de las copias de seguridad manuales de Wordpress necesitamos abrir una consola (*Shell*) para conectarlos al servidor mediante *Telnet* o *Ssh*.

En caso que el servidor no permita la conexión a través de *Ssh*, realizaremos la conexión mediante Telnet y además necesitaremos acceder mediante *FTP* para la descarga de los ficheros generados durante la copia de seguridad.

Para la copia de seguridad de la base de datos, seguimos los siguientes pasos:

Paso 1. Abrimos una consola (Shell) y accedemos por telnet o ssh al servidor donde se encuentra el gestor de base de datos.

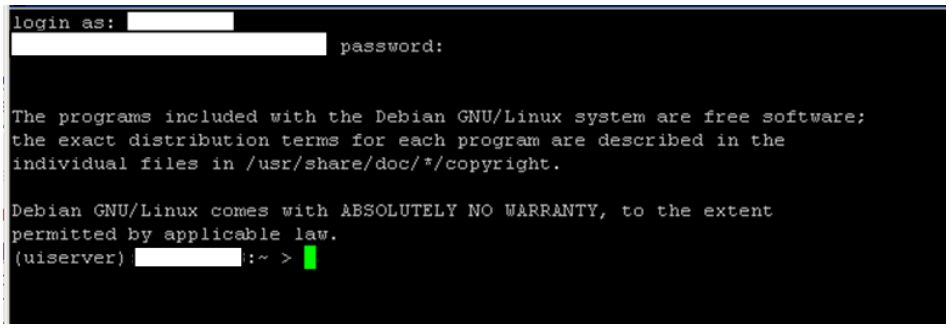


Imagen 11. Imagen de la consola de Linux en el servidor que aloja el sitio web de Wordpress.

Paso 2. Lanzamos el comando que nos permite realizar la copia de seguridad de la base de datos seleccionada, mediante el comando mysqldump, perteneciente a MySQL.

```
mysqldump -h [servidor] -u [usuario] -p [base de datos] >
fichero.sql
```

El resultado será un fichero *SQL* que contendrá las sentencias necesarias para llevar a cabo una restauración de la base de datos. **Para la copia de seguridad del directorio de Wordpress, seguimos los siguientes pasos, continuando los puntos anteriores**.

Paso 3. Localizamos el directorio donde se encuentra la instalación de *Wordpress* en el servidor.

Paso 4. A continuación realizamos un comando para comprimir el directorio y todo su contenido en un único fichero, tal y como se muestra a continuación:

```
tar -zcvf nombre-archivo.tar.gz nombre-directorio
```

El resultado será un fichero empaquetado que contendrá todo el sitio de Wordpress.

Paso 5. Finalmente, el último paso consistirá en la descarga de ambos ficheros, el fichero *SQL* de la base de datos y el fichero comprimido de *Wordpress* mediante *FTP* o *FTP* sobre *SSH*, al ordenador. El conjunto de estos dos ficheros constituirá la copia de seguridad de Wordpress. Para la descarga por *ftp*, usamos los siguientes comandos:

```
Conexión al servidor ftp: ftp servidor.com
Para descarga de ficheros: get nombre-archivo.tar.gz
```

Para la descarga por FTP sobre SSH (SFTP), usamos los siguientes comandos:

```
Conexión al servidor ssh: sftp USC username@usc-host
Para descarga de ficheros: get nombre-archivo.tar.gz
```

En relación con el proceso de copia de seguridad, se **recomienda realizar la copia de seguridad de forma regular** o si se van a añadir nuevos complementos o funcionalidades. Por otro lado, es muy recomendable, **mantener una copia de seguridad fuera del servidor**, de forma que en caso de fallo del servicio de hosting, sea posible replicar el sitio en otro proveedor.

7.4. MÉTODO AUTOMÁTIZADO Y PLUGINS

Como hemos visto en la anterior entrega, la realización de copias de seguridad en *Wordpress* no es un proceso complicado, por otro lado, las copias de seguridad mediante consola o scripts permiten realizar todo tipo de automatizaciones, pero cuando se trata de facilitar el proceso y la gestión de las copias de seguridad, es conveniente utilizar los complementos y plugins, puesto que facilitan la tarea de forma considerable y ofrecen opciones muy interesantes.

En la actualidad, *Wordpress* cuenta con más de **20.000 plugins gratuitos**, entre los cuales se encuentran diversos plugins para copias de seguridad.

Algunos de los plugins son mixtos en relación con su licencia de uso, ya que se pueden utilizar gratuitamente, pero si se desean más funcionalidades es necesario contratar un servicio o adquirir una versión de pago**.**

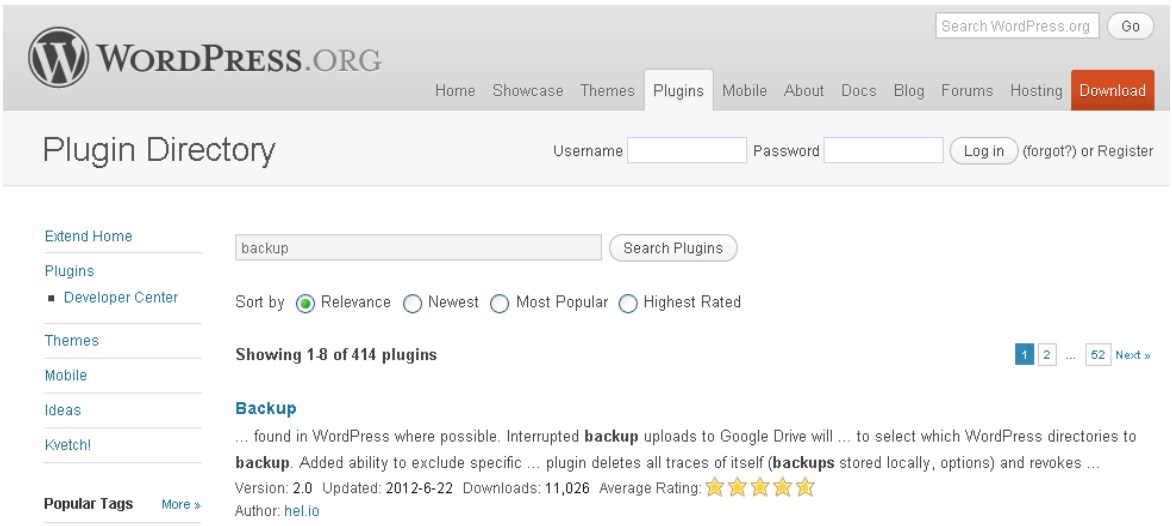


Imagen 12. Imagen del buscador de plugins de Wordpress.

En la imagen (*figura 12*) que se muestra a continuación puede verse el buscador de plugins de *Wordpress.org*. Si introducimos el término *backup* en el buscador, el resultado arroja más de 400 plugins relacionados con el término.

7.4.1. Consideraciones iniciales

Como se indicó en la anterior entrega, la copia de seguridad de *Wordpress* requiere dos procesos diferenciados:

- Copia de seguridad de la base de datos
- Copia de seguridad del directorio de Wordpress

En relación con esto, podemos clasificar los plugins de *Wordpress* enfocados a la realización de copias de seguridad en dos grupos bien diferenciados:

- **Plugins de copia de seguridad parcial**. Son plugins que solo permiten realizar la copia de seguridad de la base de datos.

- **Plugins que permiten realizar copias de seguridad completas**. Por otro lado tenemos los plugins que permiten realizar una copia de seguridad completa, de forma que guardan la base de datos y los ficheros.

A la hora de realizar una copia de seguridad, **se recomienda utilizar plugins que permiten realizar la copia completa**. Además, es muy importante comprobar que la versión del plugin de copias de seguridad que hayamos elegido sea compatible con la versión de *Wordpress*.

7.4.2. Copia de seguridad completa con plugin

Para el ejemplo que se va a describir a continuación utilizaremos *Online Backup for WordPress*, un plugin gratuito con opción de pago, que puede ser descargado desde la web del fabricante o directamente desde el panel de gestión de *Wordpress*. En nuestro caso, vamos a usar el panel de gestión de *Wordpress*. A continuación se describen los pasos a seguir:

Paso 1. Acceder como Administrador a *Wordpress,* acceder a la sección de plugins, tal y como se muestra en la imagen (*imagen 13*). A continuación pulsamos en «añadir nuevo» (recuadro rojo).

Imagen 13. Imagen de la pantalla de gestión de plugins de Wordpress.

Paso 2. En el campo de búsqueda introducir el término, en este caso, usamos la palabra *backup*, cuyo resultado es el que se muestra a continuación. Como se puede observar en la imagen, aparecen varios resultados, entre ellos el plugin que nos interesa, ***Online Backup for Wordpress***. Debajo del nombre del plugin pulsamos en «instalar ahora».

Imagen 14. Imagen del listado de plugins instalados, entre ellos el plugin de copias de seguridad.

Paso 3. Una vez finalizado el proceso de instalación, se activa el plugin y accedemos a su pantalla de configuración.

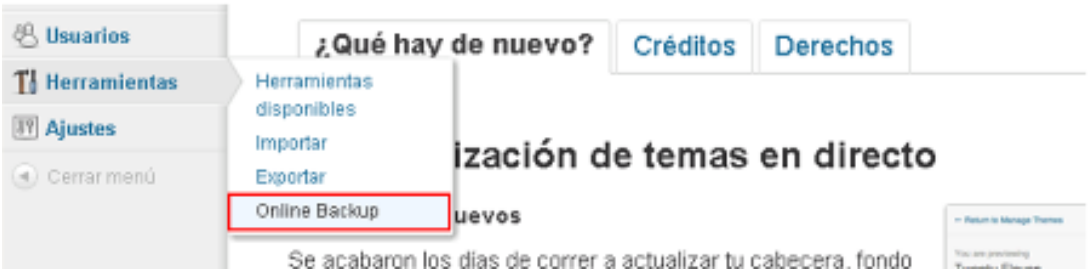


Imagen 15. Imagen de las herramientas instaladas en Wordpress.

Paso 4. Una vez en la pantalla de configuración, podemos ver las distintas opciones que ofrece. En la pantalla de bienvenida (*imagen 16*) se muestra información general de estado sobre su configuración y las características activas.

Imagen 16. Imagen de la pantalla de bienvenida del plugin.

Paso 5. A continuación pulsamos en la opción del menú «*backup*» y llegamos a la pantalla desde la cual podemos realizar la copia de seguridad. En la pantalla se muestran dos apartados, en el primero de ellos, permite seleccionar que elementos queremos incluir en la copia de seguridad. Como se ve puede ver, es posible seleccionar entre «*Database*» y «*Filesystem*», es decir, la base de datos y los ficheros de *Wordpress* respectivamente. Marcamos las dos opciones.

Además, permite seleccionar el tipo de copia de seguridad. Hay tres opciones:

1. ***ONLINE***. La primera de ellas es online, es decir, que se realiza sobre un servicio externo de almacenamiento, concretamente sobre el que ofrece la compañía que desarrolla el plugin.

2. ***DONWLOAD***. La segunda opción realiza la copia de seguridad y permite su descarga al ordenador.

3. ***EMAIL***. La tercera opción es idéntica a la anterior, pero enviar la copia de seguridad por correo electrónico a la dirección que se solicita al pulsar esa opción.

Para este ejemplo elegimos la segunda opción (**DOWNLOAD**).

Además hay que indicar que el plugin no permite realizar copias incrementales o mantener varias copias al mismo tiempo, salvo que se use la primera opción.

Finalmente, pulsamos en el botón «*Start Manual Backup*» y realizamos la copia de seguridad (*imagen 17*).

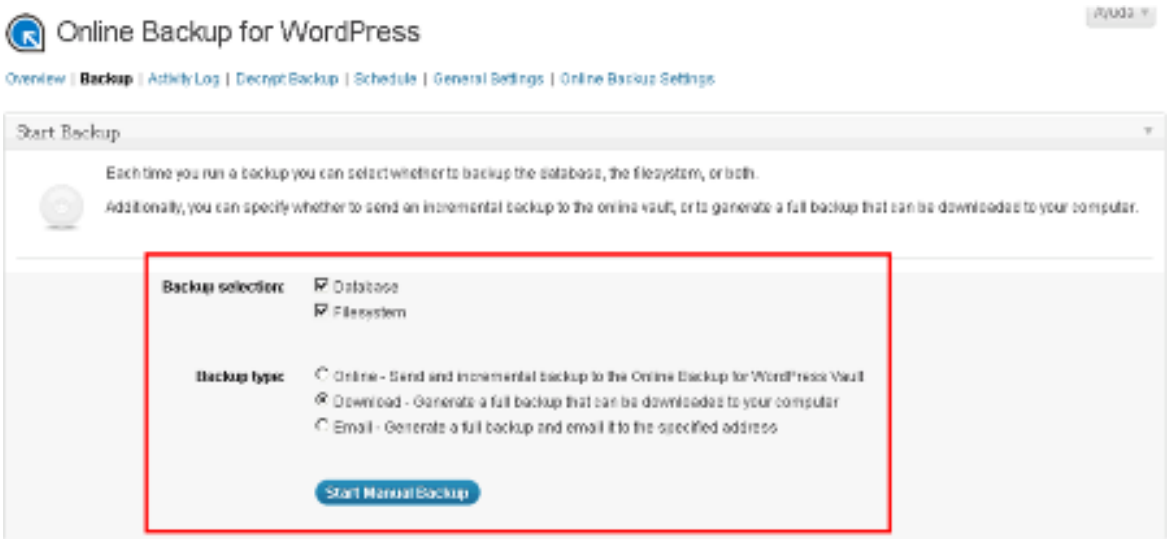


Imagen 17. Imagen de las opciones de la copia de seguridad.

Paso 6. Durante el proceso de copia de seguridad se muestra una barra de progreso, tal y

como se ve a continuación (*imagen 18*):

Imagen 18. Imagen del progreso de la copia de seguridad.

Una vez finalizado el proceso, el archivo de copia de seguridad queda almacenado en el propio servidor y tenemos la opción de descargarlo. Si no hacemos nada más, el fichero permanecerá en el servidor hasta la próxima copia de seguridad, que eliminará la copia anterior y creará una nueva.

Imagen 19. Imagen que muestra que la copia de seguridad ha finalizado y ya es posible descargarla o borrarla.

Paso 7. Además de realizar la copia de seguridad de forma manual, es decir, que es el usuario el que inicia el proceso, es posible programar su realización, además de otras opciones.

Tal y como se ve, en la imagen a continación (*imagen 20*), en el caso de la programación de la copia de seguridad, es posible programarla en los intervalos que se muestran en la imagen (cada hora, cada 6 horas, cada 12 horas, diariamente y semanalmente), pudiendo incluso fijar la hora y el minuto a la que se tiene que realizar y seleccionar donde se va a realizar, en este caso, únicamente permite dos opciones, por correo electrónico o a través del servicio de copia de seguridad on-line que proporciona el fabricante del plugin.

El uso del correo electrónico para el envío de los ficheros de copia de seguridad no se recomienda, puesto que los archivos fácilmente pueden superar los 10 megas y habría que asegurarse de que el servicio de correo electrónico permita el envío de ficheros tan grandes.

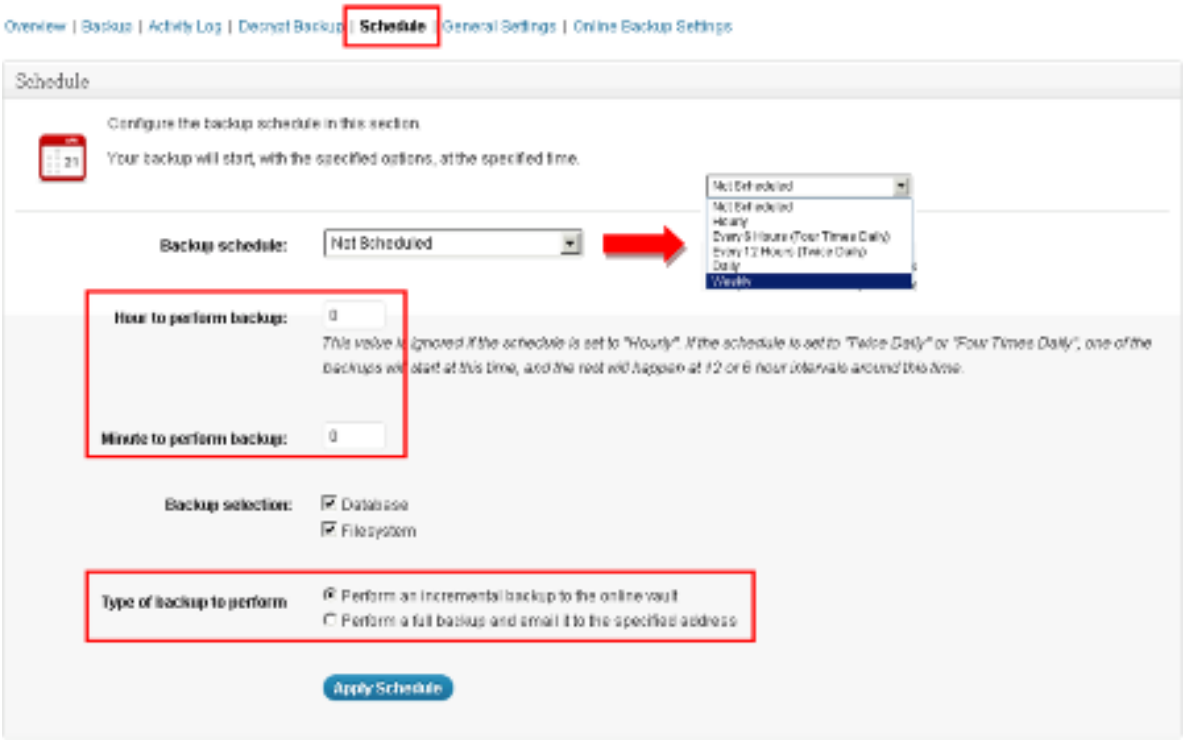


Imagen 20. Imagen que muestra la programación de la copia de seguridad para que se realice de forma automática periódicamente.

El plugin que se ha descrito es uno de muchos, cada uno de los cuales ofrecen distintas opciones, muchas veces limitadas, de forma que si se quieren opciones más potentes o completas hay que contratar el servicio adicional o adquirir la versión de pago.

De cualquier forma y dependiendo del escenario, buscaremos la opción y el plugin que mejor se adapte a las necesidades del sitio web, que en cada caso serán distintas.

En relación con el proceso de copia de seguridad, se recomienda realizar la copia de seguridad de forma regular o si se van a añadir nuevos complementos o funcionalidades.

Por otro lado, es muy recomendable, **mantener una copia de seguridad fuera del servidor**, de forma que en caso de fallo del servicio de hosting, sea posible replicar el sitio en otro proveedor.

8. OTRAS FUNCIONALIDADES DE SEGURIDAD

Como se ha visto a lo largo de las entregas anteriores, mejorar la seguridad en *Wordpress* es un proceso relativamente sencillo. Hasta ahora, la mejora de la seguridad se ha centrado en el proceso de instalación y la configuración inicial, como parte del proceso de securización básica.

Una vez que se ha finalizado la instalación y configuración general de *Wordpress* comienza la creación del sitio web, incorporando contenidos y funcionalidades que podemos encontrar en otros lugares, como son los formularios de contacto, el registro de usuarios o el envío de boletines. A medida que se añadan nuevas funcionalidades también será necesario incorporar medidas de seguridad adicionales.

En los apartados siguientes, vamos a ver un conjunto de plugins y aplicaciones que permiten configurar características existentes en *Wordpress*, añadir otras nuevas y que complementan aquellas que se han visto en los apartados anteriores o realizar comprobaciones en relación con la seguridad de nuestro sitio web.

8.1. AKISMET

Akismet es un servicio de protección Anti-Spam que se utiliza en combinación con un *pluging* que viene incorporado por defecto en la instalación de Wordpress.

El funcionamiento es sencillo, basta con crear una cuenta gratuita en el servicio web para conseguir un código denominado *Key API*. Una vez que se dispone de ese código, se procede a activar el plugin en el sitio de *Wordpress* y a continuación solicitará dicho código (*imagen 21*). Una vez introducido, la protección Anti-Spam comienza a trabajar por sí sola.

Imagen 21. Imagen de la pantalla de configuración de Akismet.

8.2. WEBSITEDEFENDER

Otro plugin muy interesante para conocer el estado de la seguridad de *Wordpress* y realizar algunas tareas relacionadas con la seguridad es *WebSiteDefender*. Al igual que *Akismet*, se trata también de un servicio combinado con un plugin gratuito y que se puede descargar desde la gestión de *plugins* de *Wordpress*.

Con este plugin, se puede obtener un resumen general del nivel de seguridad del sitio, además proporciona información sobre el servidor web, un resumen de los permisos de los directorios, información y recomendaciones relativos a la seguridad de la base de datos.

Además, una vez configurado el servicio asociado al *plugin*, basta con crear una cuenta gratuita y configurar el *plugin* para que mensualmente recibamos un informe de estado del sitio y de posibles alertas o incidencias.

Imagen 22. Imagen de la pantalla de información del plugin WebsiteDefender.

8.3. SECURE WORDPRESS

Secure Wordpress es un plugin de la misma compañía que desarrolla el plugin *WebSiteDefender* , pero a diferencia del anterior, está pensado para configurar ciertas características de *Worpdress* que mejoran la seguridad general del sitio. Por ejemplo, ocultar la versión del *Wordpress*, desactivar algunos mensajes de error, eliminar la opción de actualización de *Wordpress* para usuarios que no sea administradores, etc.

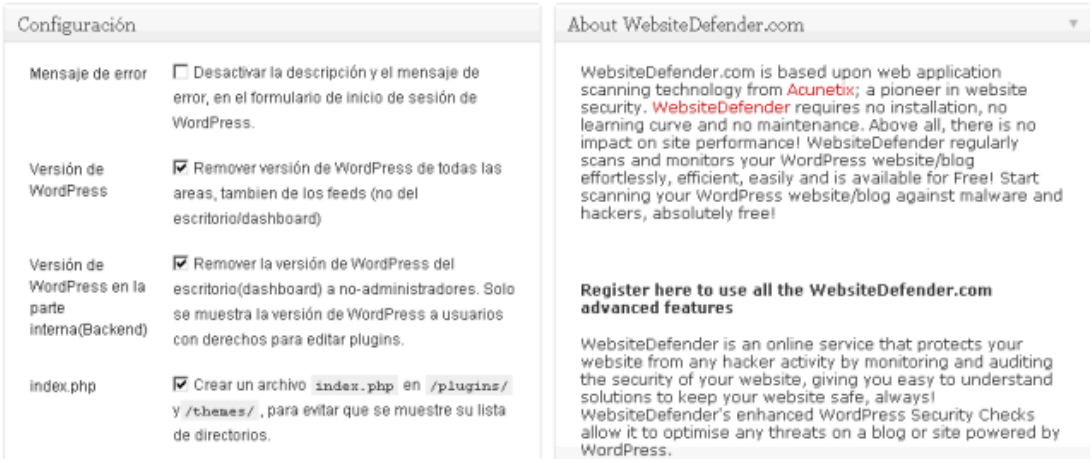


Imagen 23. Imagen de la pantalla de configuración del plugin Secure Wordpress.

8.4. 6SCAN SECURITY

6Scan Security es un plugin similar a los anteriores, pero enfocado a la detección de vulnerabilidades y agujeros de seguridad. Funciona en combinación con un servicio que se ofrece en modalidad gratuita y de pago. En la versión de pago, permite acceder a un nivel de protección que va más allá de la detección de vulnerabilidades, ofreciendo protección activa contra ataques externos, backup automático, etc. Este plugin es un ejemplo del tipo de plugin hacía el que están evolucionando muchos complementos de seguridad para *Wordpress*.

Imagen 24. Imagen de la pantalla de información del plugin 6Scan.

8.5. OTROS PLUGINS

Además de los plugins comentados hay muchos otros para tareas tan diversas como:

- Incorporar códigos de seguridad (captchas) en formularios mediante Re-Captcha de Google.
- Proteger el acceso a *Wordpress*, limitando el número de intentos de acceso o bloquear determinadas Ip's, mediante plugins como WP-Ban o IP Filter.
- Gestionar los ficheros *.htaccess* de forma centralizada con BulletProofSecurity.
- Proteger contenido en función de distintos roles o usuarios mediante Page Security by Contexture.
- Comprobar los enlaces incluidos en el contenido de Wordpress mediante F-Secure Safe Links.

Los plugins que se han descrito no son más que un ejemplo de la gran cantidad de posibilidades que ofrece *Wordpress* a través de estos complementos.

Es importante recordar que a la hora de incorporar plugins a *Wordpress* es fundamental asegurarse que funciona con la versión de *Wordpress* que está instalada y es recomendable verificar la última actualización del plugin.

Además, en relación con lo anterior, **se recomienda realizar la copia de seguridad previa** si se van a añadir nuevos complementos o funcionalidades.

9. FUENTES DE INFORMACIÓN

Wordpres.org

http://wordpress.org

Wordrpess.org – Plugins

http://wordpress.org/extend/plugins/

Wordpress.org – Stats

http://en.wordpress.com/stats/

Lorelle on Wordpress

http://lorelle.wordpress.com/2012/03/29/wordpress-stats-and-numbers-breaking-their-own-records/

INTECO (cert)

Puedes seguirnos desde:

WWW **http://cert.inteco.es**

Perfil Twitter INTECO-CERT:

https://twitter.com/intecocert

Perfil Scribd INTECO-CERT:

http://es.scribd.com/intecocert

Perfil Youtube INTECO-CERT:

http://www.youtube.com/intecocert

Perfil Linkedin INTECO-CERT:

http://www.linkedin.com/groups/INTECOCERT-Centro-respuesta-incidentes-seguridad-4362386L

Puedes enviarnos tus comentarios o consultas a:

consultas@cert.inteco.es