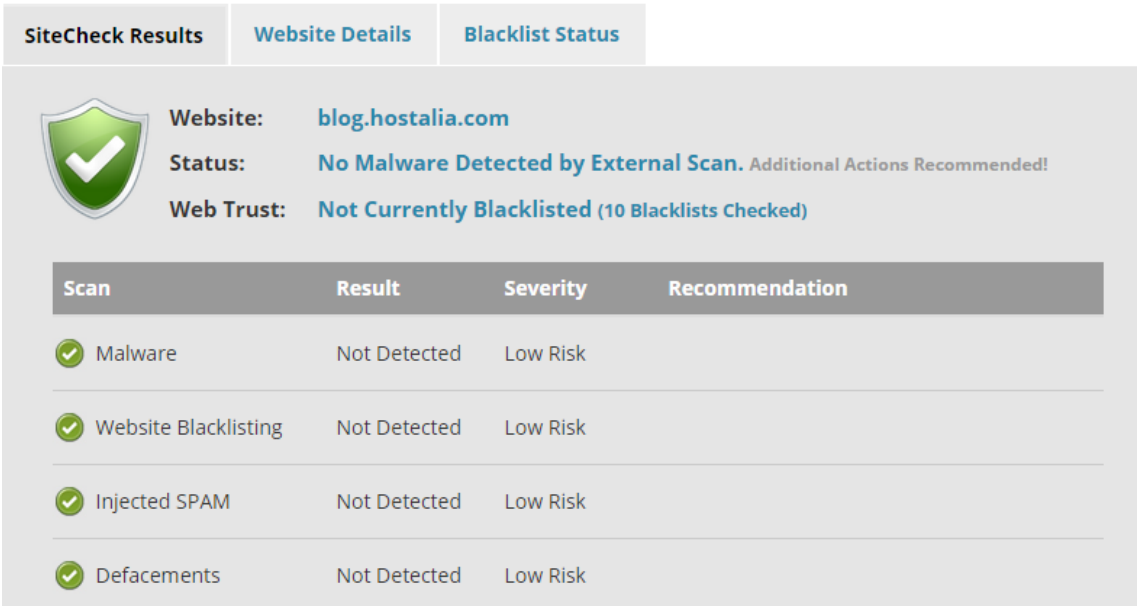
Consejos para mejorar la seguridad de nuestro WordPress

Cardenal Gardoki, 1
48008 BILBAO (Vizcaya)
Teléfono: 902 012 199
www.hostalia.com

La seguridad es un requisito imprescindible en cualquier página web, y los portales basados en WordPress tampoco son ajenos a recibir ataques. Por ello siempre es recomendable tener en cuenta unos consejos para mejorar la seguridad de nuestros sitios e impedir ataques que puedan poner en peligro la información que tengamos almacenada.

¿Cómo sabemos si nuestro WordPress ha sido infectado?

Lo primero que todos deberíamos hacer de forma periódica es revisar si nuestro sitio ha sufrido algún tipo de ataque, y para ello la forma más rápida es hacer uso de algunas de las herramientas de seguridad web que nos podemos encontrar en la red. Con sólo poner el nombre de nuestro dominio nos indicarán si hemos sido objeto de algún tipo de ataque.



Otra opción más tediosa es revisar la fecha de modificación de los archivos y carpetas que forman parte de nuestro portal, ya que por medio de este dato podremos contemplar si alguno de estos archivos ha sido modificado recientemente. Esto puede ser síntoma de que hayan añadido en él algún tipo de código malicioso.

Tampoco debemos olvidarnos de la herramienta de diagnóstico que nos ofrece Google, para ello sólo es necesario acceder a esta url cambiando "tu-sitio" por la URL de tu web.

http://www.google.com/safebrowsing/diagnostic?site=http://tu-sitio

Navegación segura
Página de diagnóstico de blog.hostalia.com

Nota informativa proporcionada por Google

¿Cuál es la clasificación actual de blog.hostalia.com?
Actualmente, este sitio no está clasificado como sospechoso.

¿Qué sucedió cuando Google visitó este sitio?
De las 13 páginas que hemos comprobado en el sitio durante los últimos 90 días, 0 páginas han provocado la descarga e instalación de software malicioso sin el consentimiento del usuario. La última vez que Google visitó el sitio fue el 2015-03-25 y no se ha encontrado contenido sospechoso en él en los últimos 90 días.

El sitio estaba alojado en 1 redes, incluidas AS16371 (ACENS_AS).

¿Este sitio ha actuado de intermediario en la distribución de software malicioso?
Parece que en los últimos 90 días, blog.hostalia.com no ha funcionado como intermediario en la infección de ningún sitio.

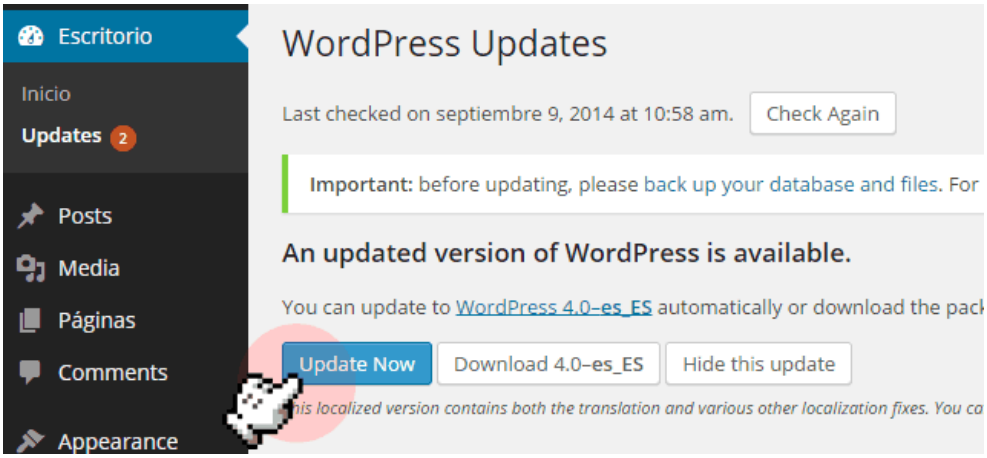
¿Este sitio ha alojado software malicioso?
No, este sitio no ha alojado software malicioso en los últimos 90 días.

Pasos siguientes:
- Volver a la página anterior.
- Si es el propietario de este sitio web, puede solicitar su revisión con Herramientas para webmasters de Google. En el Centro de asistencia para webmasters de

Si tuviéramos la mala suerte de que nuestro sitio hubiera sido infectado podemos hacer uso de la herramienta Google Webmaster Tools, desde donde podremos encontrar información muy valiosa sobre el tipo de ataque que hemos sufrido.

Actualizaciones, primera acción que nunca puede faltar

Una de las principales ventajas que nos ofrece WordPress es la gran comunidad de usuarios y desarrolladores que tiene detrás de sí, que continuamente va lanzando actualizaciones de la herramienta, no sólo el core de la aplicación, sino que también actualiza plugins y themes que están a nuestra disposición.



En cada una de estas actualizaciones se corrigen varios agujeros de seguridad que han sido detectados y que podrían ser utilizados por los atacantes para infectar nuestro sitio. Ya que nos ofrecen esta opción de actualizaciones periódicas, lo suyo es que lo aprovechemos. Aquí no vale decir "mientras que funcione, mejor no tocar", ya que esto conlleva un gran riesgo.

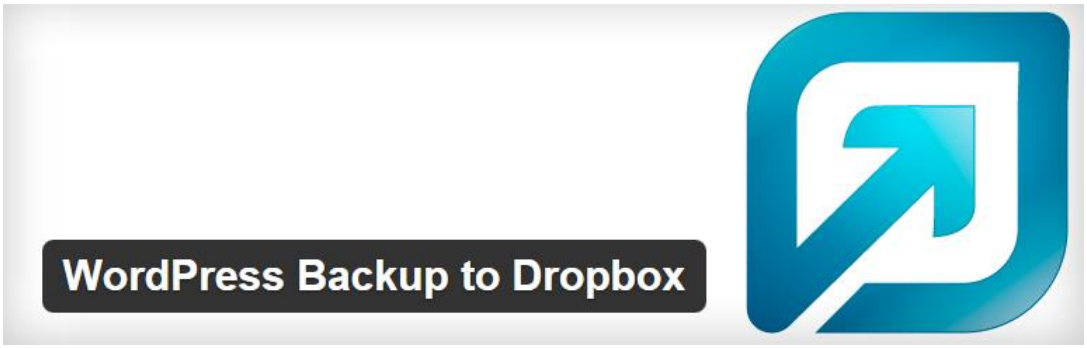
Desde hace algunas versiones WordPress ofrece la posibilidad de ser actualizado automáticamente cada vez que es lanzada una nueva versión. El propio escritorio de la administración nos indica si hay actualizaciones pendientes de plugins y themes.

Copias de seguridad: prevenir antes que lamentar

Las copias de seguridad nos dan plenas garantías de poder volver a un estado anterior en caso de sufrir cualquier tipo de ataque o pérdida de información, y en el caso de un portal con WordPress no iba a ser menos.

Hoy en día, si contamos con un servicio de hospedaje web de garantías, el proceso de backup suele estar automatizado o bien el proveedor ofrecer alguna opción en su panel de control que nos permita realizarlo de forma automática. Además, también nos podemos encontrar con plugins desarrollados para WordPress que nos permite poder realizar el backup de nuestro portal para poder restaurarlo en caso de ser necesario. Veamos a continuación algunos de estos plugins.

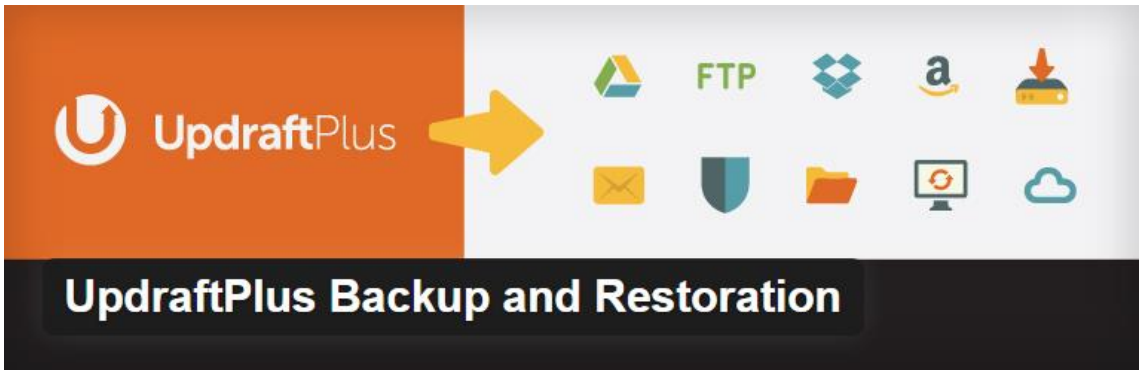
WordPress Backup to Dropbox



WordPress Backup to Dropbox es un plugin que permite programar el día, la hora y la frecuencia con la que realizar la copia de seguridad de nuestro sitio, tanto de los ficheros como de la base de datos. También ofrece la posibilidad de excluir aquellos directorios o archivos que no queremos que formen parte de la copia de seguridad.

Una vez realizada la copia, podemos indicarle si queremos que esta se almacene en el propio servidor o bien que utilice nuestro espacio en Dropbox para ello.

UpdraftPlus Backup and Restoration



UpdraftPlus Backup and Restoration es otro de los muchos plugins desarrollados para WordPress que podemos utilizar para realizar las copias de nuestro sitio. Este plugin, a diferencia del anterior, no sólo permite realizar la copia, sino que además ofrece el servicio de restauración.

También ofrece la posibilidad de enviar la copia por correo electrónico, FTP, Google Drive y unos cuantos métodos más.

Backup WordPress

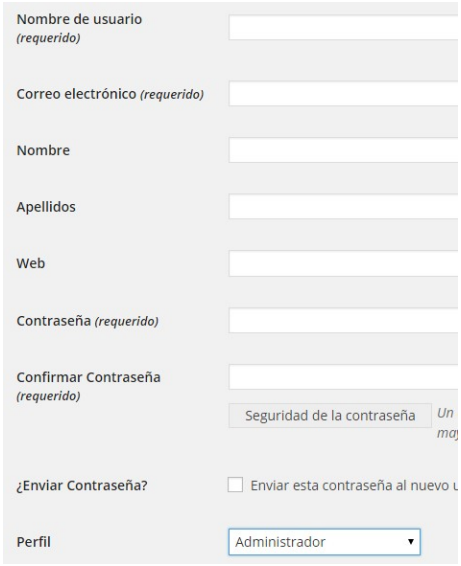
BackUp WordPress se caracteriza por la sencillez de su uso además de realizar copias de seguridad utilizando muy pocos recursos de memoria. Permite la gestión de múltiples programaciones de fechas para realizar el backup, y si lo deseamos puede enviar vía correo electrónico la copia que acaba de realizar.

Eliminar el usuario admin

La mayoría de los ataques que sufre una instalación de WordPress para intentar conseguir el acceso a la administración es mediante el uso de la técnica de 'fuerza bruta', usando el nombre de usuario "admin" que se suele activar por defecto a la hora de poner en marcha la aplicación. Por este motivo, es más que aconsejable eliminar este usuario y utilizar otro como administrador.

Este proceso lo podemos hacer desde el panel de control de WordPress siempre y cuando tengamos acceso como administrador y teniendo en cuenta que siempre debe haber como mínimo un usuario de tipo administrador dado de alta. El proceso para llevar a cabo esta tarea sería el siguiente.

1.- Entramos en la administración de nuestro WordPress con nuestros datos de administrador.
2.- Nos vamos al apartado de "Usuarios" y creamos uno nuevo con privilegio administrador.



3.- Una vez que hayamos rellenado todos los datos y hayamos pulsado el botón de aceptar, tendremos que eliminar del sistema el viejo usuario "admin".

Refuerza la seguridad de la zona de login

Relacionado con lo hablado en el punto anterior sobre los ataques por fuerza bruta, podemos utilizar algún plugin que limite el número de intentos de login, bloqueando temporalmente el acceso cuando se falla un número determinado de ocasiones, como por ejemplo utilizando Orbisius Limit Logins, que bloquea las direcciones IP que están intentando acceder al sistema y que han introducido los datos de forma errónea un determinado número de veces.

Otra opción para mejorar la seguridad de esta zona es la de añadir el clásico Captcha a nuestro formulario de acceso. Con esto estaremos impidiendo que los robots puedan acceder de forma automática al no poder saltarse este campo extra añadido.

Consejos desde el .htaccess

Además de los plugins y las medidas de seguridad que ya ofrece el core de WordPress, también podemos aumentar la seguridad haciendo uso del archivo .htaccess que se instala en la raíz del sitio, haciendo uso de sencillas directivas. Veamos algunos ejemplos que pueden mejorar la seguridad de nuestro sitio.

Evitar la exploración de carpetas

Si queremos impedir que los usuarios puedan navegar y ver el contenido de las distintas carpetas que forman parte de nuestra instalación, lo podemos conseguir añadiendo la siguiente línea a nuestro archivo .htaccess.

Options All -Indexes

Proteger el archivo wp-config.php

Este archivo es probablemente el más importante de la instalación del WordPress ya que es ahí donde se incluye la información que necesita la herramienta para un perfecto funcionamiento, como es los datos de conexión a la base de datos o ciertas directivas de configuración. Si queremos impedir que se pueda acceder a él, se puede conseguir mediante el siguiente código.

<files wp-config.php> order allow,deny deny from all </files>

Bloquear el acceso al directorio wp-content

También es recomendable impedir el acceso a esas carpetas donde no nos interesa que los usuarios puedan entrar como es el directorio wp-content, donde se guarda todas las imágenes, themes o plugins utilizados en nuestra instalación. Para conseguir esto lo podemos hacer mediante el siguiente código.

Order deny, allow Deny from all <files ~".(xml|css|jpe?g|png|gif|js)$"> Allow from all </files>

Impedir el acceso de determinadas direcciones IP

Si detectamos que estamos sufriendo algún tipo de ataques desde determinadas direcciones IP, podemos impedir el acceso desde esas direcciones de forma sencilla mediante este código.

<Limit GET POST>

order allow,deny

deny from xx.xx.xxx.xxx /reemplazar la IP a banear

allow from all

</Limit>

En este caso podemos añadir tantas líneas "deny from" como sea necesario.

Proteger el archivo .htaccess de accesos indeseados

También es recomendable proteger el propio archivo .htaccess de esos accesos indeseados. Esto lo podemos conseguir utilizando lo siguiente.

<files .htaccess> order allow,deny deny from all </files>

A lo largo de este libro blanco hemos visto algunos consejos que podemos aplicar a nuestra instalación de WordPress para mejorar la seguridad, pero además de esto, siempre podemos acudir a expertos del sector o blogs especializados en este campo, como el que te ofrecemos en Hostalia, para buscar solución a esos problemas relacionados con esta aplicación de software libre.