

Noticias Internacionales

**SEGURIDAD DEL SITIO DE INTERNET**http://diplomaticweek.org/

**INTRODUCCIÓN.**

**ANÁLISIS WEB.**

**MEJORA DE LA EXPERIENCIA DEL USUARIO.**

**GENERACIÓN DE CONVERSIONES.**

**MEJORAR EL POSICIONAMIENTO EN BUSCADORES.**

**MEJORAR EL RENDIMIENTO DE LOS ANUNCIOS.**

**VELOCIDAD DEL SITIO.**

**COMPATIBILIDAD CON DISPOSITIVOS MÓVILES.**

**SEGURIDAD DE LA WEB.**

**PROBLEMAS SEO.**

**CONTENIDOS.**

**PROCEDIMIENTO DE ANÁLISIS.**



Noticias Internacionales

**ANÁLISIS TÉCNICO Y RESULTADOS**http://diplomaticweek.org/

**MEJORA DE LA EXPERIENCIA DEL USUARIO.**

**GENERACIÓN DE CONVERSIONES (VISITAS).**

**PLUGIN OFICIAL DE WORDPRESS | GENERADOR DE PALABRAS CLAVE.**

**PLUGIN DE STATCOUNTER.**

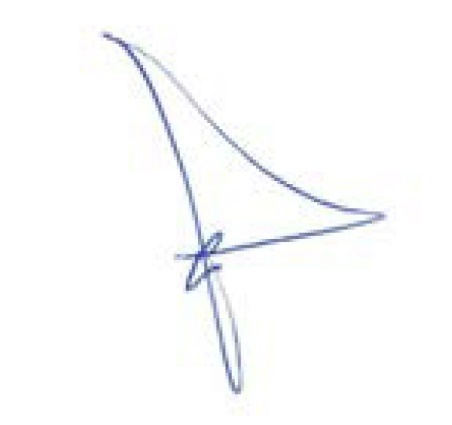
**MEJORAR EL RENDIMIENTO DE LOS ANUNCIOS. No disponible / no aplica.**

**COMPATIBILIDAD CON DISPOSITIVOS MÓVILES.**

**SEGURIDAD DE LA WEB.**

**PROBLEMAS SEO.**

**CONTENIDOS.**



Julián Marcelo Zappia  
Técnico Superior en Análisis de Sistemas  
Colaborador de Diplomatic Week



Noticias Internacionales

**DOCUMENTACIÓN DE AUDITORÍA**http://diplomaticweek.org/

Hemos hecho una recopilación de recomendaciones para proteger al máximo tu WordPress. Al ser el gestor de contenidos más utilizado en el mundo es bastante común que recibas ataques de hackers, fuerza bruta y robots. Si tienes todas las opciones marcadas por defecto podrías tener algún problema de seguridad que te deje sin página web o que incluya código malicioso. Mira a ver cuáles de estas acciones puedes hacer para estar mucho más protegido.

22 pasos para Proteger WordPress: Seguridad anti-hackers1. No utilices el prefijo wp\_ para la base de datos

Desde el primer momento de la instalación de WordPress tienes que especificar una serie de información que tienes que introducir para que WordPress se comunique con la base de datos.

La mayoría de esa información te la facilita tu proveedor de alojamiento, como el nombre de la base de datos, el usuario y contraseña de la misma. Pero sí hay una decisión que tomar: decidir el prefijo de las tablas que se crearán para WordPress.

Por defecto, en esta pantalla el prefijo ofrecido es wp\_, de manera que tus tablas quedarán tal que wp\_options, wp\_comments, wp\_posts, etc.

Y, por supuesto, esto es algo que todo hacker sabe, y es información gratuita que damos a cualquier posible atacante, que sabe que si no haces una instalación segura las tablas de WordPress – que son estándar – tendrán esos nombres completos si no cambias el prefijo.

22 pasos para Proteger WordPress: Seguridad anti-hackers

Así que el primer lugar donde debes empezar a asegurar WordPress es antes incluso de instalarlo, en este paso: cambia el prefijo para las tablas por defecto (wp\_) por otro a tu elección, por ejemplo wptabla\_ o X1jM\_ o lo que quieras. Lo importante no es lo largo o complicado que sea sino que, al menos, no dejes el prefijo por defecto.

22 pasos para Proteger WordPress: Seguridad anti-hackers2. No utilices el usuario admin para acceder a WordPress

Otra de las decisiones que tenemos que tomar durante la instalación de WordPress es el nombre del primer usuario para acceder a la administración de nuestra web, usuario que por defecto tendrá permisos totales de gestión de la misma.

Durante años WordPress ha ofrecido un nombre de usuario por defecto que, por supuesto, no debes utilizar. Así que en el momento de elegir el nombre de tu primer usuario para acceder a WordPress no elijas aquellos nombres comunes para esta tarea, como admin, Admin, root, etc., ya que son los primeros que comprobará un hacker que quiera tomar posesión de tu web.

22 pasos para Proteger WordPress: Seguridad anti-hackers

22 pasos para Proteger WordPress: Seguridad anti-hackers3. Utiliza una contraseña fuerte

Sé que es difícil de conseguir que me hagas caso con este truco tan básico, pero es fundamental que seas consciente de que cuanto más fácil de recordar (para ti) sea una contraseña, también será más fácil que los sistemas automáticos de acceso por fuerza bruta de los atacantes la consigan.

WordPress, en sus últimas versiones, incorpora un generador de contraseñas seguras y te «sugiere» utilizarlas. Ésta será siempre la mejor opción. Puedes, no obstante, saltarte esa recomendación y poner una contraseña sencilla, e insegura, pero estarías cometiendo el principal y más importante error de seguridad de todos los posibles.

Actualmente es innecesario utilizar contraseñas fáciles, pues todos los navegadores ofrecen la posibilidad de recordarlas por ti en tu ordenador. Así que usa siempre contraseñas seguras, que contengan letras en minúsculas, mayúsculas, números y caracteres especiales.

En caso de tener muchos usuarios registrados puedes incluso forzar el cambio de contraseñas para que sean todas seguras, incluida la de los administradores. Por ejemplo:

Forzando el cambio de contraseñas cada 30 días

Reiniciando todas las contraseñas

22 pasos para Proteger WordPress: Seguridad anti-hackers4. Usa siempre la última versión de WordPress

Si hay algo peligroso es trabajar en red con software obsoleto o no suficientemente actualizado. Los hackers suelen atacar principalmente sitios con versiones antiguas, no actualizadas, pues suelen ser más vulnerables al no incorporar la suficiente protección a tipos de ataque conocidos.

Afortunadamente, WordPress ofrece un sistema de actualizaciones automáticas, tanto para el mismo núcleo de WordPress como para plugins y temas.

22 pasos para Proteger WordPress: Seguridad anti-hackers

Por defecto, no deberás preocuparte de las actualizaciones de mantenimiento y seguridad de WordPress, pues las hace sin tu intervención. Simplemente te avisará cuando se haya actualizado. Pero sí deberás realizar, aunque sea con un simple clic, las actualizaciones a las versiones denominadas «mayores».

Por ejemplo, no hace falta tu intervención para actualizar de la versión 4.3.1 a la 4.3.2, WordPress las actualiza por ti. Pero sí desde la 4.3.x a la 4.4, aunque el proceso sea tan rápido y tan sencillo como pulsar un botón.

[Tweet «Los hackers atacan, sobre todo, webs con versiones no actualizadas porque son más vulnerables»]

22 pasos para Proteger WordPress: Seguridad anti-hackers5. Actualiza los plugins instalados

WordPress es seguro, y es normal que así sea porque hay una gran comunidad que se ocupa de su mantenimiento, desarrollo y crecimiento, pero no pasa lo mismo con los plugins.

Por muy utilizado que sea un plugin, muchas veces detrás hay un único programador que, por razones obvias, no dispone de los recursos ni el tiempo necesarios para tener siempre su plugin al día.

Es por ese motivo que la principal vía de entrada de ataques a una instalación WordPress es en su mayoría a través de plugins sin actualizar.

WordPress nos ofrece un sistema de aviso y actualizaciones automáticas de los plugins instalados, así que cuando veas que alguno necesita actualizarse no te lo pienses.

En caso de no utilizar plugins del directorio oficial es posible que WordPress no identifique automáticamente si hay actualizaciones disponibles. En ese caso deberás estar pendiente de la web del desarrollador.

22 pasos para Proteger WordPress: Seguridad anti-hackers6. Actualiza el tema activo

Igualmente importante es usar siempre una versión actualizada del tema activo, pues los hackers saben que no se suelen cambiar muy a menudo, lo que les da tiempo para aprender de su código e inventarse modos de hacerte la vida más complicada e incluso meterte en problemas.

Si usas un tema del directorio oficial, de nuevo, WordPress te avisará de las actualizaciones. Y si utilizas un plugin que hayas adquirido en otro sitio deberás estar pendiente de las noticias de su creador para actualizarlo cuando haya novedades.

22 pasos para Proteger WordPress: Seguridad anti-hackers7. No utilices plugins o temas obsoletos

Una de las más importantes fuentes de vulnerabilidad son los plugins y temas obsoletos o abandonados por sus desarrolladores. Revisa frecuentemente la página del programador de tu tema y plugins para comprobar si ha actualizado recientemente su producto y, en caso contrario, busca una alternativa que te ofrezca las mismas prestaciones.

Si utilizas temas y plugins del directorio oficial de WordPress encontrarás toda la información disponible, como la fecha de la última actualización y la compatibilidad con las últimas versiones de WordPress.

Además, el directorio oficial de WordPress retira automáticamente plugins y temas que no se hayan actualizado durante más de dos años, lo que supone una garantía adicional.

En caso de utilizar temas y plugins descargados de otros sitios deberás comprobarlo en su propia web e instalar manualmente cualquier actualización.

22 pasos para Proteger WordPress: Seguridad anti-hackers8. Borra los plugins y temas que no utilices

En línea con la acción anterior, es un peligro tener instalados plugins y temas inactivos, por la sencilla razón de que les prestaremos menos atención al no estar activos. No solo ocupan espacio en tu alojamiento sino que suponen una vía de entrada a posibles vulnerabilidades en tu web.

El único tema activo que deberías dejar instalado es el último tema por defecto de WordPress disponible (ahora mismo Twenty Fifteen), que supone una regla de protección adicional para tu web, ya que si WordPress detecta un problema en tu tema activo y no puede cargarlo intentará activar automáticamente el tema por defecto si lo encuentra instalado.

22 pasos para Proteger WordPress: Seguridad anti-hackers9. Descarga plugins y temas de sitios seguros

El sitio más seguro para descargar plugins y temas es el directorio oficial, en cuyas direcciones tienes versiones actualizadas, comprobadas y seguras de los últimos desarrollos. Son los temas y plugins que puedes instalar desde el instalador incluido en tu WordPress, y que también puedes visitar en las siguientes direcciones:

https://es.wordpress.org/plugins/

https://es.wordpress.org/themes/

Además, hay mercados de temas y plugins como Envato, Woothemes o Elegant Themes, de gran calidad y cuidado por sus productos.

Por supuesto, nunca descargues plugins y temas de las redes P2P como Torrent o eMule, suelen estar todos infectados de virus y malware.

22 pasos para Proteger WordPress: Seguridad anti-hackers10. Protege el archivo de configuración de WordPress

El archivo de configuración de WordPress, el fichero wp-config.php, contiene información muy sensible sobre tu servidor:

Nombre de la base de datos

Usuario de la base de datos

Contraseña de la base de datos

Prefijo de las tablas de la base de datos.

Por este motivo es vital protegerlo de miradas ajenas y, por supuesto, de modificaciones no deseadas.

Para ello puedes realizar las siguientes acciones:

Moverlo a una carpeta superior, de manera que si está situado en la ruta …/public\_html/midominio.es/ lo muevas a la carpeta …/public\_html/.

Protegerlo contra escritura cambiando los permisos a 444.

Añade las siguientes reglas al fichero de Apache .htaccess para evitar accesos no deseados:

<Files wp-config.php>

order allow,deny

deny from all

</Files>

22 pasos para Proteger WordPress: Seguridad anti-hackers11. Protege la carpeta de archivos subidos

La carpeta uploads, situada en la ruta tusitio.es/wp-content/uploads donde se suben las imágenes y documentos que adjuntas a tus publicaciones en WordPress, es la más susceptible de ataques. De modo que es importantísimo protegerla para evitar que se ejecuten desde la misma virus o scripts maliciosos.

WordPress no permite por defecto la subida de archivos ejecutables a esta carpeta pero hay técnicas que utilizan los hackers para saltarse esta regla. Así que debemos aplicar protección extra, definiendo expresamente qué extensiones de archivo se podrán subir a la misma.

Para ello, añadiremos las siguientes líneas de código al fichero oculto de configuración de Apache .htaccess, situado en la carpeta donde instalaste WordPress:

<Files ~ ".\*\..\*">

Order Allow,Deny

Deny from all

</Files>

<FilesMatch "\.(jpg|jpeg|jpe|gif|png|bmp|tif|tiff|doc|pdf|rtf|xls|numbers|odt|pages|key|zip|rar)$">

Order Deny,Allow

Allow from all

</FilesMatch>

22 pasos para Proteger WordPress: Seguridad anti-hackers12. Haz copias de seguridad

Si hay una regla fija en la seguridad es que da igual las medidas que apliques, siempre habrá alguna vulnerabilidad nueva para la que no estemos protegidos, siempre iremos un paso por detrás de los ataques malintencionados. Así que, en caso de desastre, lo único que nos puede salvar de una eventual pérdida de todo nuestro contenido es disponer de copias de seguridad.

Comprueba que tu proveedor de alojamiento web dispone de copias de seguridad automáticas completas. Y, además, instala un plugin de copias de seguridad como BackWPup, que te permite programar distintas tareas de copia de seguridad, pudiendo guardar tus copias en otro servidor, enviarlas por email, o incluso automatizar su guardado en servicios Cloud como DropBox, Amazon S3 o Google Drive, entre otros.

[Tweet «Para evitar ataques de extraños en tu Wordpress, la regla número 1 es tener copias de seguridad»]

22 pasos para Proteger WordPress: Seguridad anti-hackers13. Limita los intentos de acceso

La mayoría de los actuales ataques contra sitios WordPress se realizan mediante intentos masivos de acceso a través de la pantalla de login, así que es imprescindible proteger el acceso interno a tu WordPress.

Para ello, podemos aplicar distintas medidas de seguridad:

Inhabilitar el registro de usuarios, evitando de este modo que usuarios con malas intenciones aprovechen posibles vulnerabilidades para obtener permisos extra en tu instalación y la posibilidad de realizar cambios en la misma.

Añade un sistema de comprobación humana como reCaptcha, que evita accesos indeseados de máquinas automatizadas que intenten obtener acceso a tu sitio.

Instala algún plugin para evitar intentos de acceso masivos como Limit login attempts, el módulo Protect de JetPack o las utilidades de este tipo de la mayoría de los plugins de seguridad, para que bloqueen este tipo de ataques.

22 pasos para Proteger WordPress: Seguridad anti-hackers14. Instala un plugin de seguridad

Muchas de las medidas de protección que podemos aplicar a nuestra instalación de WordPress vienen incluidas en plugins especializados en asegurar WordPress.

La mayoría de ellos contienen ajustes para evitar ataques de fuerza bruta, inyecciones de código y modificaciones de archivos de sistema, incluyendo sistemas de aviso para que estés informado de cualquier posible ataque en curso.

Los más recomendables son los siguientes:

WordFence

iThemes Security

Bulletproof

22 pasos para Proteger WordPress: Seguridad anti-hackers15. Utiliza permisos de archivos y carpetas seguros

Por defecto, WordPress aplica permisos de lectura y escritura a archivos y carpetas que, en ocasiones, pueden modificarse, bien automáticamente por algunos plugins, bien manualmente al subir tú mismo archivos desde las utilidades de cPanel o, incluso, mediante clientes FTP.

Los permisos por defecto que deben tener archivos y carpetas en WordPress son los siguientes:

Archivos: 644

Carpetas: 755

Si algún archivo o carpeta tiene más permisos sería una posible fuente de vulnerabilidades. Deberás cambiarlos a los permisos por defecto desde el administrador de archivos de cPanel o tu cliente FTP favorito.

22 pasos para Proteger WordPress: Seguridad anti-hackers

22 pasos para Proteger WordPress: Seguridad anti-hackers

22 pasos para Proteger WordPress: Seguridad anti-hackers

22 pasos para Proteger WordPress: Seguridad anti-hackers16. Utiliza un proxy inverso como CloudFlare

Una medida que no solo mejorará la seguridad sino también la seguridad de WordPress es usar un servicio CDN, o red de entrega de contenidos remotos como CloudFlare, con un plan gratuito muy completo y plugins que facilitan su integración con WordPress.

Además de ofrecer un sistema de cache muy potente, también incorpora medidas de protección como las siguientes:

Ofuscación de emails, evitando la captura de direcciones de email mostradas en tu web

Bloqueo de IPs de visitantes con comportamientos sospechosos de ser atacantes

Siempre online, para mostrar una versión en cache de tu web incluso cuando estés siendo objeto de un ataque en curso

22 pasos para Proteger WordPress: Seguridad anti-hackers17. Crea una cuenta en Google Search Console

Las antiguas herramientas para webmasters de Google, ahora conocidas como Google Search Console, además de herramientas fundamentales de analítica y análisis de tu web, ofrece protección extra para tu WordPress.

En definitiva, que es imprescindible que des de alta tu sitio en la Search Console para que Google te informe de:

Actualizaciones de WordPress

Inyecciones de código

Avisos de problemas de usabilidad

Problemas de velocidad

Plugins como Yoast SEO o All in one SEO pack permiten la integración de WordPress con la Search Console de manera sencilla.

22 pasos para Proteger WordPress: Seguridad anti-hackers18. Impide el acceso de sploggers

Si por algún motivo permites los registros de usuarios en tu WordPress debes protegerte contra los conocidos como sploggers, usuarios que se registran masivamente en webs para intentar acceder a su configuración, añadir comentarios spam o incluso inyectar malware.

La solución definitiva para este tipo de usuarios es, por supuesto, no activar el registro de usuarios (comportamiento por defecto de WordPress). Pero si por motivos de fidelización o marketing tienes habilitado el registro deberás instalar el mejor plugin que existe para detectar y eliminar esta amenaza: WangGuard.

22 pasos para Proteger WordPress: Seguridad anti-hackers19. Protege el archivo .htaccess

22 pasos para Proteger WordPress: Seguridad anti-hackersHemos visto varias acciones que podemos realizar desde el archivo de Apache .htaccess, pero por el mismo motivo es igualmente importante proteger este mismo archivo.

El archivo .htaccess es un fichero del servidor Apache que aplica reglas a cualquier aplicación instalada en tu alojamiento, en nuestro caso WordPress, pudiendo aplicar medidas de seguridad y seguridad, entre otras.

Para proteger también el archivo .htaccess de accesos no deseados puedes incluir las siguientes líneas en el mismo archivo:

<files .htaccess>

order allow,deny

deny from all

</files>

22 pasos para Proteger WordPress: Seguridad anti-hackers20. Protégete del spam

Una de las tareas habituales de cualquier administrador de un gestor de contenidos, como WordPress, es controlar el spam en los comentarios. Primero, porque es fuente de distracciones y enlaces no deseados en los formularios de comentarios. Y segundo, porque algunos hackers utilizan estos formularios para inyectar código que podría comprometer la seguridad de tu instalación de WordPress.

Para ello podemos, y debemos, aplicar diferentes estrategias:

Añadir un sistema de comprobación humana Captcha mediante plugins Really Simple CAPTCHA o el anteriormente comentado WangGuard.

Activa un plugin de comprobación de spam como Akismet.

Proteger los formularios de la inyección de caracteres especiales.

Y, por supuesto, y sin necesidad de instalar nada, aplicar reglas de control de spam desde los Ajustes -> Comentarios de tu instalación de WordPress:

Aprobando manualmente todos los comentarios.

22 pasos para Proteger WordPress: Seguridad anti-hackers

Añadiendo reglas para marcar como spam automáticamente comentarios no deseados.

22 pasos para Proteger WordPress: Seguridad anti-hackers

22 pasos para Proteger WordPress: Seguridad anti-hackers21. Evita la vulnerabilidad pingback

Hay una vulnerabilidad concreta, denominada como vulnerabilidad pingback, que merece una mención especial porque, aunque de fácil solución, dejaría inactivas funciones importantes de WordPress como la gestión remota, el uso de aplicaciones móviles o incluso el sistema de pingbacks y trackbacks.

Está relacionada con el protocolo XML-RPC, que es el que permite que WordPress se conecte, por ejemplo, con la aplicación WordPress para iOS o Android, así como editores offline y algunos sistemas de sindicación de contenidos, por lo que en principio inactivar este protocolo no parece recomendable.

Lo malo es que es una vía abierta de posibles inyecciones de código por parte de atacantes.

No obstante, si tuvieses claro que nunca vas a utilizar este tipo de aplicaciones la solución es tan sencilla como borrar el archivo de la instalación de WordPress denominado xml-rpc.php.

El único problema es que cuando actualices WordPress se volverá a crear, así que una medida más precisa sería añadir estas líneas al ya conocido archivo .htaccess:

# proteger xmlrpc

<Files xmlrpc.php>

Order Deny,Allow

Deny from all

</Files>

22 pasos para Proteger WordPress: Seguridad anti-hackers22. Comprueba los cambios en los archivos de tu instalación de WordPress

Debes tener presente que la seguridad debe ser una preocupación permanente y activa. Pero, afortunadamente, WordPress nos ayuda a automatizar muchas de estas tareas y de manera totalmente gratuita casi siempre.

Y un modo estupendo de vigilar nuestra instalación de WordPress es utilizando plugins como iThemes Security o WordFence, vistos anteriormente. Estos plugins vigilarán por nosotros la integridad y posibles cambios de los archivos de nuestra instalación de WordPress, tratando de evitar modificaciones y, cuando no sea posible, avisándonos de estos cambios para que podamos revertirlos y así permanecer seguros.

22 pasos para Proteger WordPress: Seguridad anti-hackers

[Tweet «Aquí tienes 22 consejos para proteger la seguridad de tu WordPress y evitar posibles ataques»]

¿Sabes más trucos para mejorar la seguridad?

Espero que te sirvan todos estos trucos y acciones para proteger WordPress. No son todos los que existen pero sí los más importantes. No obstante, seguro que tú sabes algún truco más, así que no te cortes y cuéntamelo en los comentarios.

También, si tienes alguna duda, estoy deseando escucharla y contestarte.

PLUGINS OFICIALES DE WORDPRESS (GRATUITOS).

<https://es.wordpress.org/plugins/>

TEMAS OFICIALES DE WORDPRESS (GRATUITOS).

<https://es.wordpress.org/themes/>

<https://themeforest.net/>

<https://www.elegantthemes.com/gallery/>

WORDFENCE (CORTAFUEGOS, ANÁLISIS DE MALWARE Y SEGURIDAD DE INICIO DE SESIÓN).

<https://wordpress.org/plugins/wordfence/>

ITHEMES SECURITY.

<https://wordpress.org/plugins/better-wp-security/>

BULLETPROOF SECURITY PRO.

<https://wordpress.org/plugins/bulletproof-security/>

CLOUDFARE.

<https://www.cloudflare.com/es-es/>

CAPTCHA.

<https://wordpress.org/plugins/really-simple-captcha/>