GUÍA PRÁCTICA

SEGURIDAD EN TU WORDPRESS

Una cuarta parte de webs publicadas en Internet a nivel mundial están realizadas con WordPress.

Esta popularidad tiene aspectos positivos como, por ejemplo, tener a tu disposición una comunidad enorme de desarrolladores, programadores y diseñadores a los que recurrir en caso de necesitar ayuda.

Pero a su vez, la existencia de ese gran volumen de instalaciones hace que sea muy goloso para usuarios maliciosos crear herramientas (robots) que husmean por internet buscando WordPress vulnerables.

¡No dejes que metan las narices en el tuyo!

Si tu WordPress es hackeado, los costes pueden ser importantes. No solo por tener que contratar a un técnico para que limpie la web, también tienes que considerar la pérdida de ventas y clientes potenciales y una pérdida de reputación.

Sigue nuestra guía de seguridad y actúa ahora para reducir los riesgos de sufrir un hackeo WordPress.

En Webempresa llevamos 19 años trabajando en el sector del hosting. Nuestro objetivo es conseguir clientes contentos y felices con su alojamiento para WordPress.

NUESTRA OBSESIÓN

SEGURIDAD + VELOCIDAD + SOPORTE

Todo el equipo ha participado en la creación de esta guía de seguridad con la que queremos ayudarte a conocer los riesgos a los que estás expuesto y enseñarte cómo levantar diferentes barreras de seguridad alrededor de tu WordPress.

¡Nos entusiasma WordPress!

Índice de contenidos

- **Más madera para usuario medio o avanzado**
    1. Activa la actualización automática en tu WordPress
    2. Modifica la url de login de tu WordPress
    3. Protege los archivos que pueden comprometer la seguridad de tu web
    4. Protege tu base de datos cambiando el prefijo de las tablas por defecto
    5. Protege el archivo wp-login.php
    6. Agrega una cabecera X-Content-Type
    7. Instala algún plugin de seguridad para WordPress
    8. Agrega una cabecera X-Frame-Options
    9. Agrega una cabecera X-XSS-Protection
    10. Protección extra mediante el fichero .htaccess
        - Impedir la ejecución de ficheros .php en el directorio uploads
        - Redirigir siempre los errores
        - Denegar el acceso a determinadas herramientas como wget, curl y perl
        - Evitar ataques de inyección SQL
    11. Protección adicional mediante el wp-config.php
    12. Deshabilitar XMLRPC para evitar ataques de DoS
    13. Bloqueos por user-agent
    14. Bloqueos por referer
    15. Crypto.php
        - ¿Cómo evitarla?

- **Recursos**

Lo más importante de todo

Siempre hay un riesgo

Sentimos decirte esto: tu WordPress nunca será 100% seguro. Los usuarios maliciosos están en constante innovación y se descubren fallos en plugins con frecuencia; sin embargo puedes hacer muchas cosas para minimizar el riesgo.

Aquí estamos nosotros para ayudarte, pero ten en cuenta que la seguridad requiere un trabajo constante y no puedes bajar la guardia.

¿WordPress es inseguro?

Esta es una pregunta que recibimos de forma habitual en nuestro servicio de soporte. La respuesta es que WordPress no es menos seguro que cualquier otro gestor de contenidos.

Dependiendo de cómo mimemos y usemos nuestro WordPress, lo mantendremos más o menos alejado de los malos.

Si nunca actualizas tu WordPress, tu tema es pirata, tu contraseña es 1234 y no tienes antivirus en tu ordenador... suponemos que también debes dejar tu coche con las llaves puestas y el motor en marcha un sábado por la tarde en un centro comercial, ¿verdad? ;)

wpdoctor.es después de analizar 20.000 WordPress se encontró con este dato:

Preocupante, ¿verdad? ¡Pues manos a la obra!

El eslabón más débil eres tú

1. Cuidado con tu conexión a Internet

¿Cómo te conectas a internet? Es mejor que trabajes conectado por cable ethernet en lugar de wifi.

Si te conectas por wifi, comprueba que utilizas seguridad WPA-2 y que has cambiado la contraseña de acceso a la administración del router que viene por defecto. ¡Utiliza una contraseña segura!

Si estás usando WPS en tu conexión wifi, desactívalo, ya que teniéndolo activo es muy fácil que te roben la contraseña de tu conexión.

Evita conectarte a tu WordPress desde equipos externos poco fiables como, por ejemplo, el ordenador de la recepción de un hotel.

Wifi gratis: alto precio en seguridad

Todos hemos caído en la tentación de usar las redes wifi abiertas que están disponibles por ejemplo en hoteles y cafeterías. ¡Wifi gratis! Pero usar una wifi de este tipo supone pagar un alto precio en cuestión de seguridad.

Desaconsejamos la conexión desde wifis abiertas o públicas, ya que no son seguras. En el caso de que sea imprescindible usarlas, comprueba que tienes tu equipo protegido con un antivirus y firewall actualizados, o conéctate a través de una VPN de confianza.

Hoy en día muchas soluciones de seguridad antivirus incluyen una VPN privada, esta sería una buena opción. También puedes contratar un servicio específico de VPN para que todas tus conexiones estén encriptadas. Si te conectas habitualmente desde redes no seguras (viajes, fuera de casa o de la oficina, etc.) con la VPN aumentarás mucho tu seguridad.

En todo caso, cuando estés fuera de casa o de la oficina, siempre es preferible que te conectes desde la conexión 3G de tu teléfono móvil que usar una conexión wifi cuya seguridad desconoces.

¿Proxy? No, gracias.

No navegues nunca a través de un proxy, y menos si se trata de un proxy gratuito. En internet hay muchos sitios donde aconsejan un proxy para navegar de forma anónima. No debes confundir anónimo con seguro.

Si navegas a través de un proxy todo tu tráfico pasa por un servidor de alguien a quien no conoces. Muchos de esos proxy se anuncian precisamente para espiar el tráfico que pasa por ellos y poder robar datos privados.

SSL para encriptar datos

Es muy aconsejable instalar un certificado SSL en tu web y acceder vía HTTPS porque así los datos viajarán encriptados por la red.

Cuando navegas con HTTPS toda la información se envía de forma cifrada al servidor, de modo que si hay un usuario conectado a la misma red que tú que esté intentando robar tus credenciales de acceso, solo verá una serie de caracteres sin ningún sentido.

Tienes más información al respecto en el artículo Qué es un certificado SSL y cómo protege mis datos.

No es necesario que compres el certificado más caro del mercado, con un certificado estándar de RapidSSL te puede servir.

También puedes probar la opción gratuita que te ofrece Let's Encrypt.

2. Usa contraseñas seguras

Nada de utilizar contraseñas como "12345", "password", "Juan", "nombredemiweb" o Qwerty". Si tienes una contraseña de este tipo, es mejor que la cambies antes de continuar leyendo.

Una buena contraseña debe contener mayúsculas, minúsculas, números y caracteres especiales (como una coma, una arroba o un guión).

EJEMPLO DE BUENA CONTRASEÑA: **7sP3@$zjT1b3**

La longitud de la contraseña también es un factor importante a tener en cuenta. Lo recomendable es que tenga una longitud de 12 caracteres o mayor.

Si te cuesta recordar una contraseña de este tipo puedes optar por construirte una que te resulte más fácil de recordar, como "25beatriz--Seguro++35".

No almacenes nunca contraseñas en tu navegador, usa un gestor de contraseñas cifrado como lastpass.com o 1Password.

Las contraseñas cortas o largas por si solas pueden ser vulneradas. ¡Utiliza siempre un segundo factor de autenticación!

Dobla la seguridad usando la doble autenticación

Utiliza un doble factor de autenticación siempre que puedas. Google te lo pone muy fácil con **Google Authenticator**, verás que configurarlo y empezar a usarlo es muy sencillo: https://support.google.com/accounts/answer/1066447?hl=es

Puedes habilitarlo para usarlo con los gestores de contraseña y con tu email. Tener el email protegido es importante, ya que muchas contraseñas o recordatorios se envían por correo electrónico. ¡No te dejes vencer por la pereza y habilítalo!

3. Tu equipo

Tienes que mantener limpios y protegidos los equipos y dispositivos desde donde accedes a la administración de tu WordPress.

Muchos usuarios maliciosos encuentran una puerta de entrada cuando los usuarios se conectan a la administración de WordPress desde un equipo hackeado. Cuando el usuario introduce las claves de acceso los atacantes capturan esos datos y entonces ya no habrá medida de seguridad posible que evite un desastre.

Sistema Operativo y navegador actualizados

Mantén actualizado el sistema operativo y también tu navegador, puedes elegir el navegador que más te guste pero asegúrate de que estás utilizando la última versión (por favor, no uses Internet Explorer 6 o navegadores obsoletos).

Lo ideal es que configures las actualizaciones automáticas, de este modo te aseguras de estar al día evitando la tarea de actualizar manualmente.

En la medida de lo posible, evita navegar por webs “sospechosas”, ya que algunas de ellas tratarán de instalar programas no deseados en tu equipo.

No utilices sistemas operativos “piratas” o instales programas procedentes de aplicaciones P2P o de páginas de descargas, porque es posible que incluyan un “regalo” en forma de troyano.

Descarga siempre los programas que vayas a instalar desde la web de los desarrolladores.

Antivirus y firewall

Debes contar con un buen antivirus y un firewall actualizados, ya que tener un antivirus con una base de datos de virus antigua es casi lo mismo que no tener ninguno.

Mantén activadas las opciones de firewall y análisis de seguridad por defecto del antivirus y ejecuta semanalmente una exploración completa de tu equipo.

Si el antivirus que estás utilizando no cuenta con un firewall, evalúa la posibilidad de agregar uno.

Si usas Windows puedes usar **Windows Defender** y utilizar el firewall de Windows que viene incorporado.

En este enlace puedes ver cómo usar **Windows Defender** para escanear malware: Uso de Windows Defender.

También puedes ver como habilitar o deshabilitar el firewall de Windows en este enlace: Activar y desactivar firewall de Windows.

Control de usuarios

Accede a tu equipo con un usuario con privilegios de usuario, no de administrador. De esta forma, será más difícil que se instalen aplicaciones no deseadas en tu máquina.

Si otra persona tiene que usar tu equipo, crea usuarios invitados o con permisos restringidos.

Control de accesos

Utiliza una contraseña segura y diferente para cada uno de los accesos: administración de WordPress, Webmail, FTP y para el acceso al panel de control del hosting.

Te recomendamos no usar FTP. Es habitual que los atacantes infecten equipos para obtener datos guardados de acceso FTP y así poder acceder al panel de control del hosting. En el caso de que no tengas alternativa y necesites usar FTP para conectar con tu hosting, utiliza SFTP o FTPS de forma que tu tráfico cliente/servidor quede cifrado.

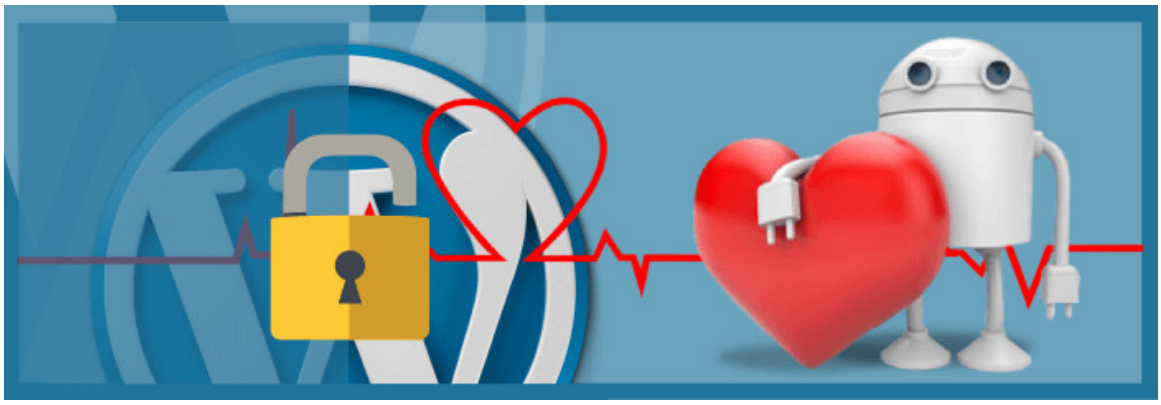
Aísla tu entorno de trabajo

Si solo dispones de un equipo físico de trabajo (computador), valora la posibilidad de trabajar con una máquina virtual.

Además de lo práctico que puede resultar para trasladar tu estación de trabajo de un equipo físico a otro y de facilitarte la vida con backups, etc., te permite aislar tu entorno de trabajo.

Así no mezclas tus cosas personales con las profesionales y hay menos posibilidades de que un desliz de tu vida personal afecte a tu vida profesional.

Cuidando de tu WordPress



1. ¡Mantén siempre a la última tu WordPress!

Cuando se lanza una nueva versión de WordPress no es solo para arreglar errores o añadir nuevas funcionalidades, también se hace para corregir los problemas de seguridad que se han ido detectando.

Tener una versión antigua de esta herramienta es como abrir una puerta a los usuarios maliciosos, ya que precisamente se aprovecharán de los fallos de seguridad conocidos para atacarnos.

Actualiza tu WordPress cada vez que veas una notificación de actualización en la administración; es muy sencillo y solo te llevará un minuto.

Si por algún motivo no puedes actualizar la versión de WordPress desde la administración de la web, también se puede actualizar manualmente. Consulta el artículo Actualizar WordPress manualmente para ver cómo puedes hacerlo.

Como siempre recomendamos, para evitar disgustos, realiza una copia de seguridad antes de actualizar.

2. Los plugins son maravillosos, ¡cuídalos!

La mayor parte de los ataques que recibe WordPress se realizan a través de los plugins.

Al igual que sucede con el propio WordPress, las actualizaciones suelen corregir problemas de seguridad, por lo que debes mantener tus plugins actualizados.

Puedes hacer las actualizaciones desde la administración de WordPress de forma automática y, al igual que en el anterior punto, es muy recomendable realizar una copia de seguridad antes de actualizar.

Limita el uso de plugins

Utiliza solo los plugins que vayas a necesitar: no es una buena idea instalar plugins en grandes cantidades ya que cada uno podría ser una puerta de entrada para hackear tu WordPress.

Quédate solo con los plugins imprescindibles y si has instalado un plugin que ya no utilizas... **¡desinstálalo!**.

También es importante que utilices plugins fiables. Lo ideal es que utilices el propio buscador de plugins que tienes en la administración de WordPress o que los descargues de la página oficial de plugins.

Si se trata de un plugin de pago asegúrate de que lo descargas desde la página de sus desarrolladores.

Nunca (repetimos, **NUNCA**) instales un plugin que hayas obtenido desde un torrent (red P2P), un gestor de descargas o una página sospechosa tipo "super-plugins-depago-gratis" ya que es muy posible que con el plugin venga un "regalo" en forma de código malicioso.

Es preferible pagar por la licencia de un plugin que quedarnos sin web.

Fíjate en el número de descargas del plugin (cuantas más mejor) y en la última fecha de actualización (si es de hace 2 años sospecha).

Si quieres probar un plugin haz un clon de tu web y pruébalo en ese clon, nunca en la web real que tienes publicada.

Puedes instalar el plugin Security Scanner que te avisará de las nuevas vulnerabilidades que aparezcan en los plugins de tu instalación de WordPress.

3. Cuida el tema que estés utilizando

Puedes utilizar tanto temas gratuitos como temas de pago, pero asegúrate siempre de utilizar la última versión disponible.

Si el tema que estás utilizando está en el directorio de wordpress.org, las actualizaciones se mostrarán de forma automática en la administración de WordPress. Para los temas de pago o temas gratuitos descargados desde otras webs, normalmente tendrás que comprobar de forma periódica si han publicado nuevas versiones que corrigen problemas de seguridad.

De nuevo, NUNCA utilices temas que hayas obtenidos desde gestores de descarga o páginas sospechosas: pueden venir hackeados de serie.

Instala solo temas procedentes de wordpress.org o de la web de sus desarrolladores.

4. Usuario admin, NO gracias.

No utilices el usuario admin para acceder a la administración de tu WordPress: si un hacker quiere entrar en la administración de tu web lo primero que hará será probar a utilizar el usuario "admin".

Lo mejor es que crees un nuevo usuario con privilegios de administrador (recuerda usar una contraseña segura).

Una vez hecho esto, cierra la sesión y vuelve a conectarte con el nuevo usuario que has creado.

Después accede al gestor de usuarios, edita el usuario "admin" y cambia sus privilegios de administrador por suscriptor o elimina directamente el usuario "admin".

Si lo eliminas, asegúrate de reasignar las entradas y páginas que estaban asignadas al usuario “admin” a otro usuario existente.

Con este cambio, un usuario malicioso no solo tendrá que saber la contraseña de un usuario administrador, sino también su nombre.

Si eres un usuario avanzado y prefieres realizar el cambio de cuenta directamente, puedes hacerlo siguiendo los pasos de nuestro artículo Cambiar el usuario de WordPress desde phpMyAdmin

5. Realiza backups periódicos y automatizados

Algunos proveedores de hosting ya realizan copias de seguridad automáticas pero, por si las moscas, es una buena idea que hagamos copias periódicas de nuestra web.

Tendrás que hacer las copias con más o menos frecuencia en función de la cantidad de información que vayas añadiendo.

Es importante realizar copias de seguridad antes de realizar acciones como la actualización de plugins o WordPress, la instalación de nuevos plugins, cambios en la base de datos, etc...

A veces se producen resultados no deseados y si la última copia es reciente no perderás trabajo previo.

Existen plugins para Wordpress que nos permitirán hacer esta tarea de forma automática como XCloner, del que hablamos en nuestro blog.

Es importante que realicemos las copias de seguridad en un almacenamiento externo como Dropbox, cuentas FTP externas o Amazon S3, o bien que nos descarguemos las copias que realizamos, ya que si alguien nos borra todos los datos de la web también perderemos la propia copia de seguridad.

Para evitar problemas de espacio en tu cuenta de hosting elimina las copias de seguridad tras descargarlas.

6. Limita los intentos de acceso fallidos

Una de las formas más habituales que usan los usuarios maliciosos para acceder a la administración de WordPress son los ataque por por fuerza bruta.

Esto consiste en probar el acceso al administrador con todas las combinaciones posibles de usuario y contraseña. Habitualmente estos ataques están basados en diccionarios de contraseñas, por eso es importante utilizar contraseñas complejas o robustas.

Limitar el número de intentos de conexión fallidos desde una única dirección IP puede reducir el riesgo de sufrir un acceso ilícito.

La mayoría de plugins de seguridad ya permiten configurar este límite, pero si prefieres no usarlos, hay plugins con esta finalidad específica como BruteProtect de Automattic. Tienes más información en nuestro blog: Limita los intentos de conexión fallidos al dashboard.

En nuestro hosting, bloqueamos IP's automáticamente cuando detectamos varios intentos de acceso fallidos a la administración o al panel de control cPanel.

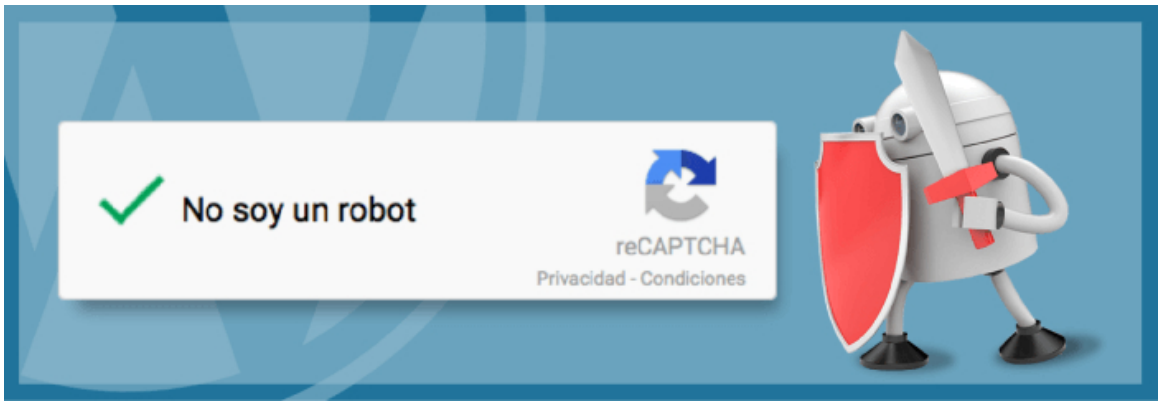
7. Protección adicional con Captcha y doble autenticación

El uso de opciones adicionales de autenticación añadirá una capa más de seguridad a tu WordPress.

Administración de WordPress

Te recomendamos proteger el acceso a la administración de tu WordPress con un formulario de autenticación con Captcha o un doble factor de autenticación como por ejemplo Latch.

En nuestro blog te hablamos de las dos opciones en los artículos Aumenta la seguridad de WordPress autenticando en dos pasos y Protege y bloquea el dashboard de WordPress con Latch.



Formularios

Es habitual que se utilicen los formularios de la web para hacer SPAM usando bots. Para prevenirlo debes proteger la creación de comentarios con un Captcha.

Para protegerte contra el spam puedes utilizar el plugin Akismet, que está instalado por defecto en WordPress.

También tenemos un artículo sobre esto, no te pierdas Pon a raya el spam en WordPress con Akismet.

8. Asegúrate de mantener los usuarios imprescindibles y con privilegios mínimos.

Es muy probable que los usuarios creados en tu sitio web con privilegios de administrador tengan una contraseña débil, comprometiendo así la seguridad de tu WordPress. Concediendo a los usuarios únicamente los privilegios indispensables se reducen las posibilidades de que la seguridad se vea comprometida.

Ante la duda, puedes resetear todas las contraseñas de usuarios de tu WordPress fácilmente. Solo tienes que seguir los pasos del artículo Seguridad en WordPress ¿cómo resetear todas las contraseñas?.

Revisa periódicamente qué usuarios existen y elimina los que no se usen o no deban tener acceso a tu WordPress.

9. Ocultar la versión de WordPress

Cada versión de WordPress tiene una serie de vulnerabilidades conocidas que los usuarios maliciosos intentan aprovechar. Ocultar la versión de WordPress que estás utilizando hará que no sea tan fácil identificar esas vulnerabilidades.

La encargada de mostrar la versión de tu WordPress en tu web es la función wp_head(), que incluye una llamada a la función **wp_generator()**.

Para ocultar esa información, tienes que incluir la siguiente línea en el archivo functions.php de tu WordPress:

```
remove_action('wp_head', 'wp_generator');
```

10. Audita tu WordPress

Utiliza herramientas para verificar distintos apartados importantes de la seguridad de tu WordPress.

Webempresa ofrece de forma gratuita un análisis de seguridad para WordPress desde wpdoctor.es.

Con **wpdoctor** podrás comprobar de forma automática si estás al día en muchos de los puntos tratados en esta guía:

- Te avisa si no estás utilizando la última versión de WordPress y de sus plugins más importantes.
- Comprueba si el acceso al administrador está protegido contra ataques de fuerza bruta.
- Te muestra la información que se puede recolectar de tu instalación y te indica cómo ocultarla.

Puedes comprobar la salud de tu WordPress con Google Safe Browsing: https://www.google.com/transparencyreport/safebrowsing/diagnostic/?hl=es

O también directamente en Google Console (antes Webmaster Tools): https://www.google.com/webmasters/tools/security-issues

La primera línea de defensa: El Hosting

Ahora que estás al tanto de los peligros que acechan y de las medidas de seguridad que debes aplicar para minimizar el riesgo, llega el momento de hablar del hosting.

De poco te servirá tener un WordPress a prueba de balas si el servidor donde lo has alojado es un coladero. Un servicio de hosting debe proporcionar elementos de seguridad a nivel de servidor; **debe ser la primera línea de defensa**.

1. Usa un proveedor de hosting profesional

Verifica las características del servicio de hosting que vayas a contratar para tu web y asegúrate que la seguridad es una de sus prioridades.

Sistema Operativo

Te recomendamos apostar por Linux frente a Windows. Ambas plataformas presentan problemas de seguridad y suelen ser objeto de ataques de usuarios maliciosos; sin embargo Linux continúa llevando cierta ventaja gracias a la comunidad de desarrolladores con la que cuenta.

Linux no está libre de riesgos pero, hasta el momento, es capaz de solucionar los problemas de seguridad de forma mucho más rápida y eficiente que Windows.

2. ¿Tu hosting está al día en seguridad?

A continuación te indicamos algunas de las medidas que deberías valorar en un servicio de hosting compartido.

Los permisos correctos de tu Hosting deben ser:

- 644 para archivos.
- 755 para carpetas.

Si no los tienes así por defecto ya puedes ir pensando en cambiar de Hosting.

Uso de un sistema de aislamiento por cuenta de alojamiento, de forma que un mal comportamiento o el hackeo de una web alojada en el servidor no afecte al resto.

Uso de aplicaciones de monitorización en tiempo real que analicen todos los ficheros que se leen o se graban en disco, para asegurar que no tienen malware ni código sospechoso.

Uso de sistemas para evitar Ataques de Denegación de Servicio (DDoS).

Medidas preventivas para evitar ataques de fuerza bruta a WordPress.

Uso de un WAF (Web Application Firewall). Gracias a él se pueden establecer reglas de seguridad, que pararán la mayor parte de los ataques que se realicen a un WordPress.

De esta forma, aunque algún plugin de tu web tenga una vulnerabilidad en el código, es probable que el WAF evite este ataque.

Configuración a nivel de servidor que evite que se pueda hacer un listado de directorios (que un usuario pueda ver los archivos de una determinada carpeta de la web) o averiguar la versión de PHP que se está ejecutando, ya que esto compromete gravemente la seguridad.

Protección de las bases de datos. Entre otras medidas, lo correcto sería que sólo se permitiera el acceso a la mismas desde el propio servidor, y no desde equipos remotos.

Puerto MySQL cerrado: lo ideal es que el puerto de MySQL esté cerrado, y si necesitas acceder desde tu casa, que te habiliten el acceso solamente a tu IP.

Para esto necesitarás una IP fija o una cuenta de DynDNS.

Software actualizado: al igual que ocurre con tu WordPress y sus plugins, es importante que el software que utilice el servidor se encuentre actualizado, ya que las versiones antiguas del mismo también pueden ser vulnerables.

Un valor añadido que puede ofrecer un servicio de hosting es la realización de copias de seguridad automáticas de nuestros datos de forma que, si tenemos que volver a un estado anterior de nuestra web, siempre dispongamos de alguna copia de seguridad.

Pero recuerda que el hecho de que tu servicio de hosting ya haga copias de seguridad automáticas no es excusa para que hagas tus propias copias.

La copia disponible en tu servicio de hosting no tiene por qué corresponder con la fecha exacta del estado de la web que quieres recuperar.

Estas son solo algunas de las medidas que aplicamos en Webempresa y que nos permiten a nosotros y a nuestros clientes dormir más tranquilos.

Monitorizamos 24 horas todos nuestros servicios y nuestro equipo técnico recibe alertas cuando se detectan actividades sospechosas para poder actuar de inmediato y de forma coordinada con el cliente.

Nuestros administradores de sistemas actualizan periódicamente las reglas que protegen los WordPress alojados en nuestros servidores ante vulnerabilidades o fallos de seguridad.

El seguimiento de las nuevas formas de atacar WordPress debe ser una tarea diaria y constante, ¡no se puede bajar la guardia!.

Más madera para usuario medio y avanzado

Las medidas de seguridad que se pueden aplicar para proteger tu WordPress son muchas, y no queremos abrumarte con cambios complicados.

Sin embargo si eres un usuario avanzado y quieres seguir trabajando en la seguridad de tu WordPress, aquí tienes algunas mejoras adicionales que puedes aplicar.

1. Activa la actualización automática en tu WordPress

En la versión 3.7 de WordPress se hizo una gran mejora añadiendo la actualización automática de WordPress.

Manteniendo esta opción activada, nos aseguraremos de que las actualizaciones de seguridad se instalarán tan pronto como estén disponibles.

Puedes configurar las actualizaciones automáticas del núcleo de WordPress desde el fichero wp-config.php. Tan solo debes añadir las siguientes líneas para cada una de las configuraciones:

```
//Todas las actualizaciones del núcleo desactivadas define( 'WP_AUTO_UPDATE_CORE', false ); //Todas las actualizaciones del núcleo activadas define( 'WP_AUTO_UPDATE_CORE', true ); //Sólo actualizaciones menores del núcleo activadas define( 'WP_AUTO_UPDATE_CORE', 'minor' );
```

Las actualizaciones de plugins y plantillas es mejor hacerlas de forma manual, ya que pueden ser más sensibles y podrían provocar errores en la web si no se verifica bien la compatibilidad con la versión de WordPress.

2. Modifica la url de login de tu WordPress

En webs realizadas con WordPress el acceso a la administración se realiza por defecto en la url:

*http://midominio.com/wp-admin*o *http://midominio.com/wp-login.php*

Los atacantes son conscientes de este acceso y tratan de explotar el acceso mediante lanzar ataques de fuerza bruta.

Modificando esta url de acceso a la administración evitarás esos intentos de acceso por fuerza bruta.

Aprende cómo hacerlo consultando el artículo Modifica el login de WordPress para evitar ataques de fuerza bruta.

En Webempresa, para nuestros clientes, ya incorporamos medidas de seguridad encaminadas a proteger los accesos a /wp-admin y /wp-login.php contra este tipo de ataques por lo que no es necesario que implementes este tipo de medidas de seguridad..

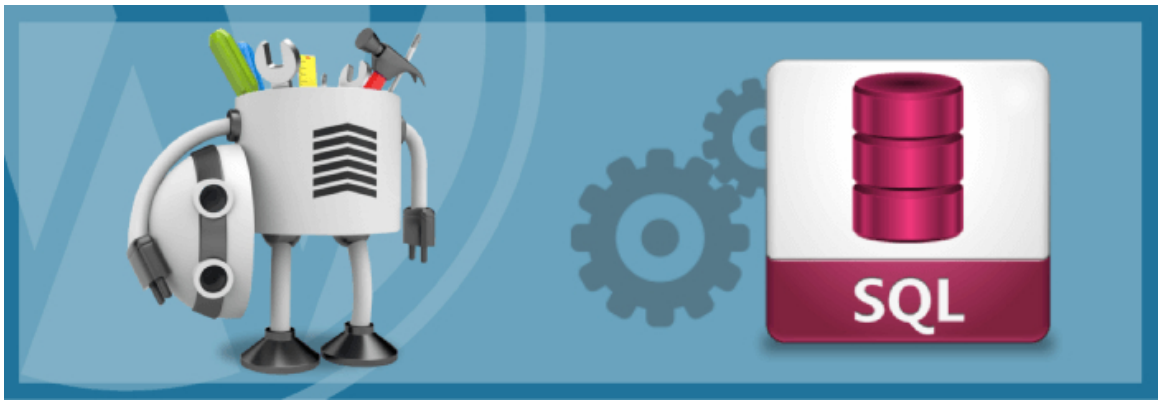
3. Protege los archivos que pueden comprometer la seguridad de tu web.

Existen diversos archivos que pueden comprometer la seguridad de WordPress.

Hay algunos archivos que se añaden con la instalación de WordPress, que son meramente informativos, pero cuya información puede ser útil para los atacantes.

Puedes ver en nuestro blog cómo protegerlos: Archivos que comprometen la seguridad de WordPress.

4. Protege tu base de datos cambiando el prefijo de las tablas por defecto



La base de datos es donde guardas toda la información de tu instalación de WordPress.

Como imaginarás es muy goloso para los crackers y spammers, que intentan enviar códigos automatizados para acceder a tus datos.

Muchos usuarios se olvidan de cambiar el **prefijo de base de datos** al instalar WordPress.

Esto hace que sea más fácil para los usuarios maliciosos planificar un ataque masivo al dirigirse al prefijo por defecto de las tablas de la base de datos que es: wp_ .

Lo recomendable es que cambies el prefijo por defecto al instalar el WordPress.

Si ya lo tienes instalado, puedes cambiar el prefijo fácilmente con el plugin Change DB Prefix.

Recuerda hacer una copia de seguridad de la base de datos antes de realizar ningún cambio.

5. Protege el archivo wp-login.php

Si no permites registro y acceso de usuarios en el frontal del WordPress es recomendable que protejas el acceso al wp-login.php o permitas únicamente el acceso desde IPs autorizadas (si te conectas con IPs fijas).

¿Quieres aprender cómo protegerlo? En este artículo te lo enseñamos: Cómo proteger el archivo wp-login.php.

¡Ojo! Esto solo debes hacerlo si los visitantes de tu web no necesitan identificarse como usuario.

Por ejemplo, en una tienda online no deberás proteger el archivo wp-login.php.

6. Agrega una cabecera X-Content-Type

Con esta cabecera evitarás que haya usuarios que intenten suplantar archivos css o js por ejecutables.

Se puede evitar con el sencillo cambio que te explicamos en el artículo : Cabecera X-Content-Type-Options para evitar problemas de Seguridad.

7. Instala algún plugin de seguridad para WordPress

Este tipo de plugins te ayudarán a aumentar la seguridad de distintas formas. te permiten desde proteger el acceso a la administración hasta revisar los archivos de tu WordPress en busca de código malicioso.

Existen multitud de opciones, como por ejemplo:

- Wordfence
- Ithemes Security (antes conocido como Better WP Security)

Si quieres conocer todas las características de Wordfence, te las mostramos en este artículo: Como mejorar la seguridad de WordPress con Wordfence Security.

Recuerda deshabilitar las estadísticas (tabla wfhits) para no sobrecargar tu WordPress.

Una opción interesante de Wordfence es la verificación de ficheros básicos de WordPress para comprobar si han sido modificados.

Ten precaución a la hora de configurar este tipo de plugins, ya que podrías bloquear tu propio acceso con estas herramientas.

Antes de instalar algún plugin de este tipo, haz una copia de seguridad. Así podrás volver al estado anterior en caso de problemas.

¡No te vuelvas loco con la instalación de plugins!

Ten presente que instalar todos los plugins de seguridad que encuentres no va a hacer que tu WordPress sea más seguro y es posible que tenga comportamientos inesperados provocados por haber varios plugins modificando archivos claves para el funcionamiento de tu WordPress, como puede ser el archivo .htaccess.

8. Agrega una cabecera X-Frame-Options

Añadiendo esta cabecera evitaremos que nuestra web cargue en un frame o iframe (marcos).

Con ello, evitaremos también ataques de tipo clickjacking y no podrán suplantar nuestra web cargándola desde una ubicación externa.

Si permites esto, podría estar tu contenido en otro dominio y tener problemas con Google si lo considera contenido duplicado.

Tienes todos los detalles en el artículo Cabecera X-Frame-Options para mejorar la seguridad de tu web

9. Agrega una cabecera X-XSS-Protection

Añadiendo esta cabecera puedes aumentar la seguridad frente ataques de tipo XSS. Te lo contamos todo sobre esta cabecera en Cabecera X-XSS-Protection para evitar ataques XSS en IE y Chrome.

Tras añadir la cabecera, tanto si lo haces en el archivo .htaccess como si lo haces en el functions.php, asegúrate de revisar que tu web funciona según lo esperado.

Si ves que afecta de algún modo al funcionamiento de tu web, elimina el código añadido para revertir el cambio.

Recuerda hacer siempre una copia de seguridad de los archivos que vayas a editar.

10. Protección extra mediante el fichero .htaccess

Hay varias fórmulas con las que puedes añadir protecciones extra mediante **.htaccess**

Impedir la ejecución de ficheros .php en el directorio uploads

El directorio /uploads normalmente se utiliza para almacenar imágenes o vídeos y a veces puede ser explotado por usuarios maliciosos que suben código PHP infectado aprovechando los scripts para subir imágenes de WordPress.

Una buena solución es añadir un fichero .htaccess en el directorio uploads impidiendo el acceso a ficheros php:

```
<Files *.php>  Deny from all  </Files>
```

También se puede limitar el acceso exclusivo a documentos de imagen en directorios como el uploads:

```
Order Allow,Deny  Deny from all  <FilesMatch "^[^.]+\.(?i:jpe?g|png|gif)$">  Al
low from all  </FilesMatch>
```

Para evitar que algunos códigos maliciosos se intenten esconder bajo nombres como *xxxxxx.php.jpg*, también se puede bloquear por estructura:

```
<FilesMatch "\.(php|php\.)(.+)(\w|\d)$">  Order Allow,Deny  Deny from all  </F
ilesMatch>
```

Redirigir siempre los errores

Redirigir los errores es una buena práctica para evitar que se muestre información que pueda dar pistas a algún individuo malintencionado:

```
ErrorDocument 404  http://www.misitio.com ErrorDocument 403  http://www
.misitio.com
```

Denegar el acceso a determinadas herramientas como wget, curl, perl, etc.

Aunque muestres contenido públicamente en tu web, es posible que te interese evitar que puedan copiarlo.

No hay forma de protegerlo del todo, pero para dificultar la tarea podemos denegar el acceso a ciertas herramientas de modo que no puedan escanear la web y descargar contenido:

```
RewriteCond %{HTTP_USER_AGENT} ^$ [OR] RewriteCond %{HTTP_USER_AGENT} ^(java|curl|wget) [NC,OR] RewriteCond %{HTTP_USER_AGENT} (winhttp|HTTrack|clshttp|archiver|loader|email|harvest|extract|grab|miner) [NC,OR] RewriteCond %{HTTP_USER_AGENT} (libwww-perl|curl|wget|python|nikto|scan) [NC,OR] RewriteCond %{HTTP_USER_AGENT} (<|>|'|%0A|%0D|%27|%3C|%3E|%00) [NC] RewriteRule .* - [F]
```

Evitar ataques de inyección SQL

WordPress por defecto tiene medidas para evitar este tipo de ataques, pero ¿quién sabe si alguno de tus plugins puede tener algún agujero en este aspecto?

Por si fuese el caso, puedes servirte del siguiente código para prevenir algunos ataques de inyección SQL.

```
RewriteCond %{QUERY_STRING} (;|<|>|'|"|\)|%0A|%0D|%22|%27|%3C|%3E|%00).*(/\*|union|select|insert|cast|set|declare|drop|update|md5|benchmark) [NC,OR] RewriteCond %{QUERY_STRING} \.\./\.\. [OR] RewriteCond %{QUERY_STRING} (localhost|loopback|127\.0\.0\.1) [NC,OR] RewriteCond %{QUERY_STRING} \.[a-z0-9] [NC,OR] RewriteCond %{QUERY_STRING} (<|>|'|%0A|%0D|%27|%3C|%3E|%00) [NC] RewriteRule .* - [F]
```

11. Protección adicional mediante el wp-config.php

Si quieres evitar que desde la administración de WordPress se pueda modificar el código de ficheros, puedes añadir la siguiente línea al fichero wp-config.php

```
define('DISALLOW_FILE_EDIT', true);
```

Si la web ya está creada y no necesitas añadir nuevos plugins o plantillas, también puedes deshabilitar la instalación de temas y plantillas añadiendo:

```
define('DISALLOW_FILE_MODS',true)
```

12. Deshabilitar XMLRPC para evitar ataques de DoS

Esta funcionalidad se utiliza bastante para realizar ataques de denegación de servicios. Desde una localización oculta se lanzan muchas solicitudes pingback forjadas a mano a muchos WordPress, diciendo que en tu web han hablado sobre ellos.

Estos WordPress irán a comprobar si realmente les has enlazado descargando tu página, y al recibir tantas peticiones de descarga juntas desde tantos sitios web, tu web quedará bloqueada.

Puedes evitarlo de dos modos:

1. Cerrar por completo el comportamiento XMLRPC. El problema de deshabilitar XMLRPC es que pierdes alguna funcionalidades interesantes, como los pingback y los trackback.
2. Disponer de un Firewall Web (WAF) que te proteja mediante reglas avanzadas que realizan recuento de todas peticiones XMLRPC que recibes y, en caso de que este número se dispare demasiado, bloquean todo ese tráfico. Esta opción la tenemos implementada con éxito en Webempresa.

Si te decides a deshabilitar XMLRPC, puedes hacerlo manualmente o utilizando el plugin XMLRPC Disable.

Para hacerlo manualmente has de añadir esta línea en el fichero **functions.php**:

```
add_filter('xmlrpc_enabled', '__return_false');
```

13. Bloqueos por user-agent

En ocasiones puede ser necesario bloquear algunas aplicaciones, como por ejemplo a determinados robots, estableciendo bloqueos por user-agent en el fichero .htaccess.

De este modo evitarás el acceso de un user-agent determinado a tu web.

Algunos códigos de ejemplo para bloquear por user-agent pueden ser los siguientes:

```
RewriteEngine On RewriteCond %{HTTP_USER_AGENT} ^.*(Baiduspider|HTTrack|Yandex).*$ [NC] RewriteRule .* - [F,L] SetEnvIfNoCase user-Agent ^Baiduspider [NC,OR] SetEnvIfNoCase user-Agent ^Yandex [NC,OR] SetEnvIfNoCase user-Agent ^[Ww]eb[Bb]andit [NC,OR] SetEnvIfNoCase user-Agent ^HTTrack [NC]  <limit GET POST>  Order Allow,Deny  Allow from all  Deny from env=bad_bot  </limit>
```

14. Bloqueos por referer

También puedes ver necesario bloquear conexiones que vienen desde un determinado referer, para lo cual podrías utilizar cualquiera de los siguientes códigos:

```
RewriteEngine On RewriteCond %{HTTP_REFERER} example\.com [NC,OR] Re
writeCond %{HTTP_REFERER} example\.net RewriteRule .* - [F]

SetEnvIfNoCase Referer "example\.com" bad_referer SetEnvIfNoCase Referer
"example\.es" bad_referer   Order Allow,Deny Allow from ALL Deny from env
=bad_referer
```

Con este bloqueo conseguirías bloquear el acceso a tu web desde un enlace ubicado en un dominio determinado.

15. Crypto.php

Esta es una de las vulnerabilidades más importantes y conocidas de WordPress.

Afecta directamente a las plantillas y plugins no autenticados por el repositorio oficial de wordpress.org y normalmente viene integrado en plantillas o plugins pirateados u obtenidos de forma ilícita.

El propósito del malware es añadir a tu web enlaces a otros sitios web que normalmente vinculan a sitios con fines maliciosos.

También puede ser utilizada con otros fines ya que esta infección puede comunicarse con servidores de control para realizar otras tareas (envío de SPAM, alojar otro tipo de contenido, realizar ataques a otras webs, etc.)

La infección normalmente está en una pequeña línea de código como la siguiente:

```
<?php include('assets/images/social.png'); ?>
```

Como se puede ver, lo que hace es incluir un script llamando a un código que hay oculto en un fichero **.png**, que en teoría debería ser una simple imagen.

¿Cómo evitarla?

La principal medida para evitar esta vulnerabilidad es no descargar plugins ni plantillas de sitios no contrastados, nuestra recomendación es realizar siempre las descargas desde el repositorio oficial de WordPress.org

En el caso de que estés infectado, te recomendamos instalar el plugin de seguridad **Wordfence** que incluye una opción para analizar las imágenes como si de código php se tratara.

Desconfía si por ejemplo ves ficheros PHP en directorios donde solo debería haber imágenes, como el directorio /wp-content/uploads.

Más recursos

- Auditoría WordPress gratuita: wpdoctor.es
- Blog de Sucuri: https://blog.sucuri.net/espanol/
- Guía de herramientas: https://info.securityinabox.org/es
- Cómo resetear todas las contraseñas: http://goo.gl/d9tM4A
- Comprueba si tienes plugins vulnerables aquí.