La guía definitiva para asegurar los sitios de los clientes

KINSTA

Para tener la versión siempre actualizada,
escanea el código QR de arriba o visita:
https://kinsta.com/es/ebooks/

Publicado por KINSTA

La guía definitiva para asegurar los sitios de los clientes

La guía definitiva para asegurar los sitios de los clientes

Índice

La guía definitiva para asegurar los sitios de los clientes

Según las estadísticas en vivo de Internet, más de 100.000 sitios web son hackeados cada día. 😮 Por eso es tan importante tomarse un tiempo y repasar las siguientes recomendaciones sobre cómo endurecer mejor la seguridad de WordPress.

Cuando se trata de la seguridad de WordPress, hay mucho más que solo bloquear tu sitio, aunque a continuación te daremos las mejores recomendaciones sobre cómo hacerlo.

Invertir en un alojamiento seguro de WordPress

Comencemos con la seguridad a nivel de servidor web de la que es responsable tu proveedor de alojamiento especializado en WordPress. Es muy importante que elijas un proveedor de alojamiento al que puedas confiar tu negocio cuando migres los sitios de tus clientes.

Si estás alojando WordPress en tu propio VPS, entonces necesitas tener el conocimiento técnico para hacer estas cosas por ti mismo. Pero para ser honestos, tratar de ser un administrador de sistemas para ahorrar 20 euros al mes no es una forma efectiva de manejar un negocio.

El fortalecimiento del servidor es la clave para mantener un entorno de WordPress completamente seguro. Requiere múltiples capas de medidas de seguridad a nivel de hardware y software para asegurar que la infraestructura de TI que alberga los sitios de WordPress sea capaz de defenderse contra amenazas sofisticadas, tanto físicas como virtuales.

Por este motivo, los servidores que alojan WordPress deben actualizarse con el sistema operativo y el software (de seguridad) más recientes, así como probarse y escanearse a fondo para detectar vulnerabilidades y malware.

Los cortafuegos a nivel de servidor y los sistemas de detección de intrusos también deben estar en su lugar para mantener los sitios de tus clientes bien protegidos, incluso durante las fases de instalación de WordPress y construcción del sitio web. Además, todo el software instalado en la máquina destinado a proteger el contenido de WordPress debe ser compatible con los sistemas de gestión de bases de datos más recientes para mantener un rendimiento óptimo. El servidor también debería estar configurado para utilizar protocolos de cifrado seguro de redes y de transferencia de archivos (como SFTP en lugar de FTP) para ocultar el contenido sensible a intrusos malintencionados.

En Kinsta garantizamos un alojamiento de WordPress seguro para todos nuestros clientes. La seguridad está integrada en nuestra arquitectura desde el principio y es un método mucho más seguro que otros que están disponibles hoy en día.

Usar la última versión de PHP

PHP es la columna vertebral de cualquier sitio de WordPress, por lo que es muy importante que te asegures de que los sitios de tus clientes están usando la última versión en su servidor. Cada versión principal de PHP es típicamente soportada durante dos años después de su lanzamiento.

Durante ese tiempo, se arreglan y parchean regularmente los errores y los problemas de seguridad. A partir de hoy, cualquiera que ejecute en la versión PHP 7.1 o inferior ya no tiene soporte de seguridad y está expuesto a vulnerabilidades de seguridad sin parches.

Currently Supported Versions

Branch	Initial Release		Active Support Until		Security Support Until	
7.2	30 Nov 2017	*2 years, 2 months ago*	30 Nov 2019	*2 months ago*	30 Nov 2020	*in 9 months*
7.3	6 Dec 2018	*1 year, 2 months ago*	6 Dec 2020	*in 9 months*	6 Dec 2021	*in 1 year, 9 months*
7.4	28 Nov 2019	*2 months ago*	28 Nov 2021	*in 1 year, 9 months*	28 Nov 2022	*in 2 years, 9 months*

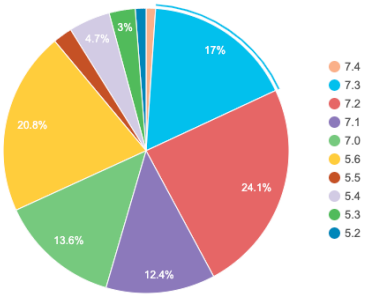
Or, visualised as a calendar:

Key

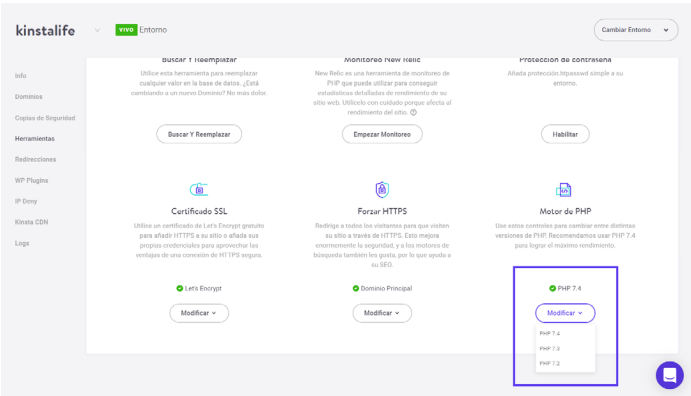
Active support	A release that is being actively supported. Reported bugs and security issues are fixed and regular point releases are made.
Security fixes only	A release that is supported for critical security issues only. Releases are only made on an as-needed basis.
End of life	A release that is no longer supported. Users of this release should upgrade as soon as possible, as they may be exposed to unpatched security vulnerabilities.

¿Y sabes qué? De acuerdo con la página oficial de estadísticas de WordPress alrededor del 34% de los usuarios de WordPress todavía están en PHP 5.6 o inferior, lo que significa que más de un tercio de los usuarios están usando actualmente versiones de PHP que ya no están soportadas. ¡Eso da miedo!

Versiones de PHP



Aquí en Kinsta solo recomendamos el uso de versiones estables y soportadas de PHP, incluyendo 7.2, 7.3 y 7.4. Las versiones de PHP 5.6, 7.0, y 7.1 han sido eliminadas. Incluso puedes cambiar entre las versiones de PHP con un solo clic desde el tablero de MyKinsta.



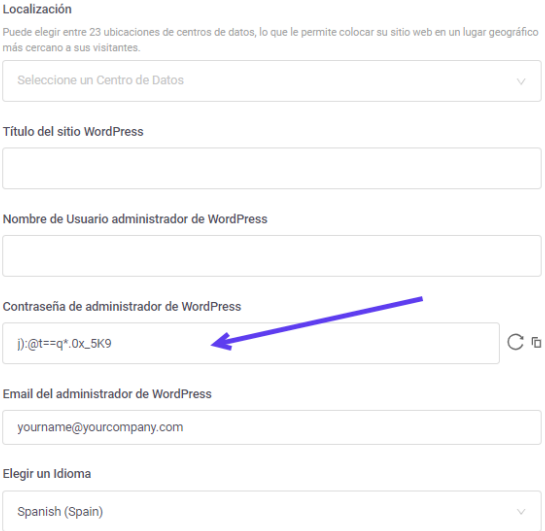
¡Si quieres pruébalo tú mismo, solo tienes que ir a demo.kinsta.com y verificarlo!

Usar nombres de usuario y contraseñas inteligentes

Sorprendentemente, una de las mejores maneras de reforzar la seguridad de WordPress es simplemente usar nombres de usuario y contraseñas inteligentes. Suena bastante fácil, ¿verdad? Bueno, echa un vistazo a la lista anual de SplashData 2019 de las contraseñas más populares robadas durante el año (ordenadas por orden de popularidad).

- 123456
- 123456789
- qwerty
- Contraseña
- 1234567
- 12345678
- 12345
- iloveyou
- 111111
- 123123

La contraseña más popular es «123456». Esa es una de las razones por las que aquí en Kinsta en las nuevas instalaciones de WordPress forzamos a que se utilice una contraseña compleja para cualquiera de los clientes de acceso al wp-admin (como se ve abajo en nuestro proceso de instalación de un solo clic). Esto no es opcional.



Mira esta función con la demo de MyKinsta.

La función central de WordPress wp_hash_password utiliza el marco de hashing de contraseñas phpass y ocho pasadas de hashing basado en MD5. Y en lo que respecta a la instalación de WordPress, nunca debes usar el nombre de usuario “admin” predeterminado en los sitios de tus clientes, sino crear nombres de usuario únicos de WordPress para sus cuentas de administrador.

También es importante usar diferentes contraseñas para cada sitio del cliente. La mejor manera es almacenarlas localmente, en una base de datos encriptada en tu ordenador.

Una buena herramienta gratuita para esto es KeePass. Si no quieres ir por este camino también hay administradores de contraseñas en línea como 1Password o LastPass.

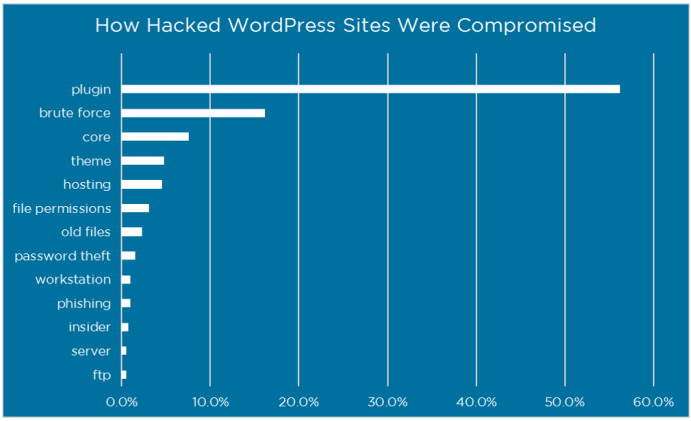
Utiliza siempre la última versión de WordPress, plugins y temas

Otra forma muy importante de reforzar la seguridad de los sitios de tus clientes es mantenerlos siempre actualizados. Esto incluye el núcleo de WordPress, los plugins y los temas. Estos se actualizan por una razón, y muchas veces incluyen mejoras de seguridad y correcciones de errores.

Desafortunadamente, millones de empresas que utilizan versiones anticuadas del software y de los plugins de WordPress siguen creyendo que van por el buen camino del éxito empresarial. Citan razones para no actualizar, como «tu sitio se romperá» o «las modificaciones del núcleo desaparecerán» o «el plugin X no funcionará» o «simplemente no necesitan la nueva funcionalidad».

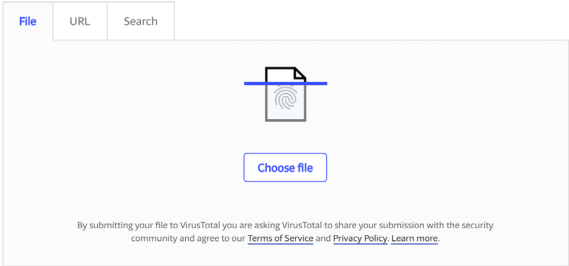
De hecho, los sitios web se rompen mayormente debido a errores en versiones antiguas de WordPress. Las modificaciones básicas nunca son recomendadas por el equipo de WordPress ni por los desarrolladores expertos que entienden los riesgos que implican. Y las actualizaciones de WordPress incluyen principalmente parches de seguridad indispensables junto con la funcionalidad adicional necesaria para ejecutar los últimos plugins.

¿Sabías que se ha informado de que las vulnerabilidades de los plugins representan el 55,9% de los puntos de entrada conocidos por los ciberdelincuentes? Eso es lo que WordFence encontró en un estudio donde entrevistaron a más de 1000 propietarios de sitios WordPress que habían sido víctimas de ataques. Actualizando tus plugins puedes asegurarte mejor de no ser una de estas víctimas.



También te recomendamos que solo instales plugins de confianza para tus clientes. Las categorías «destacados» y «populares» del repositorio de WordPress pueden ser un buen lugar para empezar. O descárgalos directamente del sitio web del desarrollador. Desaconsejamos encarecidamente el uso de plugins y temas de WordPress anulados.

Puedes usar una herramienta online como VirusTotal para escanear un plugin o los archivos de un tema para ver si detecta algún tipo de malware.



También hay muchos recursos que te ayudarán a estar al tanto de las últimas actualizaciones de seguridad y vulnerabilidades de WordPress. Mira algunos de ellos incluidos a continuación:

- Bloggers de Seguridad WP: Un impresionante recurso agregado de más de 20 fuentes de seguridad.
- Base de datos de vulnerabilidad de WPScan: Cataloga más de 10.000 vulnerabilidades del núcleo de WordPress, plugins y temas.
- ThreatPress: Base de datos actualizada diariamente de plugins, temas y vulnerabilidades principales de WordPress.
- Archivo oficial de seguridad de WordPress

Bloquea tu administrador de WordPress

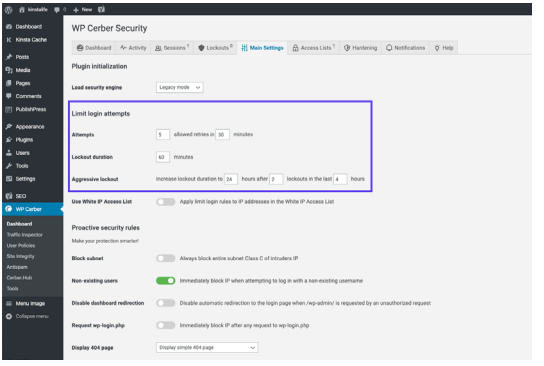
A veces la popular estrategia de seguridad por oscuridad de WordPress es apropiadamente efectiva para un negocio en línea y un sitio de WordPress promedio. Si haces más difícil a los ciberdelincuentes encontrar ciertas puertas traseras, entonces es menos probable que te ataquen. Bloquear el área de administración de WordPress de tus clientes y el inicio de sesión es una buena manera de reforzar tu seguridad. Dos buenas maneras de hacerlo es primero cambiar la URL de inicio de sesión predeterminada de wp-admin y también limitando los intentos de inicio de sesión.

¿Cómo cambiar la URL de inicio de sesión de WordPress?
De forma predeterminada, la URL de inicio de sesión de tu sitio de WordPress es domain.com/wp-admin. Uno de los problemas de esto es que todos los bots, hackers y scripts de ahí fuera también lo saben. Cambiando la URL puedes hacerte menos blanco y protegerte mejor contra los ataques de fuerza bruta. Esta no es una solución para todo, es simplemente un pequeño truco que definitivamente puede ayudar a protegerte

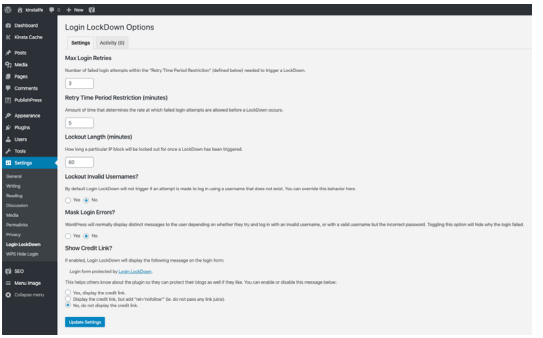
Para cambiar la URL de inicio de sesión de WordPress recomendamos utilizar el complemento de inicio de sesión gratuito de WPS Hide. Solo recuerda elegir algo único que no esté ya en una lista que un bot o script pueda intentar escanear.

¿Cómo limitar los intentos de acceso?

Aunque la solución anterior de cambiar la URL de inicio de sesión del administrador puede ayudar a disminuir la mayoría de los intentos de login malintencionados, poner un límite también puede ser muy eficaz. El plugin gratuito Cerber Limit Login Attempts es una gran manera de configurar fácilmente la duración de los bloqueos, los intentos de acceso y las listas blancas y negras de IP.



Si buscas una solución de seguridad más simple para WordPress, otra gran alternativa es el plugin gratuito Login Lockdown.

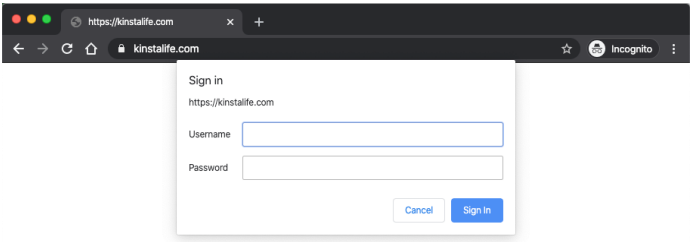


Login LockDown registra la dirección IP y la hora de cada intento de acceso fallido. Si se detecta más de cierto número de intentos en un corto período de tiempo desde el mismo rango de IP, entonces la función de inicio de sesión se desactiva para todas las solicitudes de ese rango. Y es completamente compatible con el plugin de acceso WPS Hide que mencionamos anteriormente.

Si trasladas el sitio de tus clientes a Kinsta, no necesitas instalar ningún plugin adicional. Nuestra plataforma bloquea los intentos maliciosos automáticamente.

¿Cómo añadir la autenticación básica de HTTP (protección htpasswd)?

Otra forma de bloquear el acceso al administrador es añadir la autenticación HTTP. Esto requiere un nombre de usuario y una contraseña antes de poder acceder a la página de inicio de sesión de WordPress.

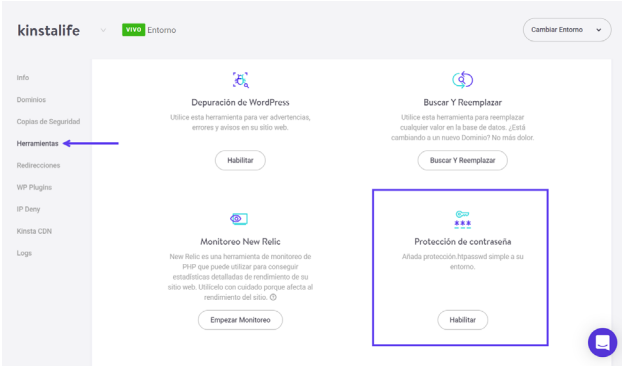


Revisa esta función con la demo de MyKinsta.

Importante: Esto generalmente no se debe usar en sitios de comercio electrónico o sitios de membresía. Pero puede ser una forma muy efectiva de evitar que los bots lleguen a tu sitio.

Si alojas los sitios de tus clientes en Kinsta, puedes utilizar nuestra sencilla herramienta de protección con contraseña (htpasswd) en el tablero de mandos de MyKinsta (lo puedes ver en acción en la cuenta gratuita de demostración de MyKinsta).

Puedes encontrarla en la sección «Herramientas» de tu sitio. Simplemente haz clic en «Activar», elige un nombre de usuario y una contraseña, ¡y listo!



Mira esta función con la demo de MyKinsta.

Después de que se habilite, cada sitio de WordPress requerirá una autenticación para acceder a él. Puedes cambiar las credenciales en cualquier momento o desactivarlo cuando ya no lo necesites.

Aprovechar la autenticación de dos factores (2FA)

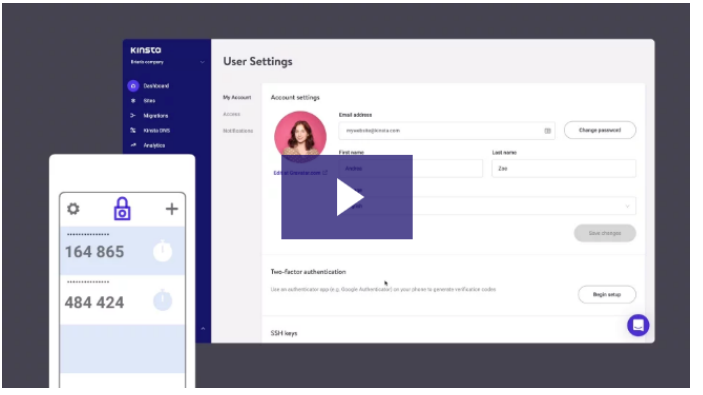
La autenticación de dos factores implica un proceso de dos pasos en el que se necesita la contraseña y un segundo método para iniciar la sesión. En la mayoría de los casos, esto es 100% efectivo en la prevención de ataques de fuerza bruta a los sitios de WordPress de tus clientes.

Respecto a la autenticación de dos factores hay dos aspectos a tener en cuenta:

El primero es tu cuenta y/o el panel de control que tienes con tu proveedor de alojamiento web. Si alguien tiene acceso a él, podría cambiar las contraseñas de todos tus clientes, borrar sus sitios web, cambiar los registros DNS y todo tipo de cosas horribles. Nosotros aquí en Kinsta usamos 2FA basado en el autenticador para tu panel de control de MyKinsta porque:

- El 2FA basado en el autenticador es más seguro que el 2FA basado en SMS porque no está ligado a tu número de teléfono móvil y no depende de la tecnología SMS heredada. Esto hace que la 2FA basada en el autenticador sea resistente a las técnicas de intercambio de SIM.
- El 2FA basado en el autenticador se puede usar con aplicaciones de gestión de contraseñas como 1Password para mayor comodidad. Al agregar tus detalles de 2FA a un administrador de contraseñas, no tendrás que depender de un dispositivo externo para acceder a MyKinsta.

Aquí está lo fácil que es habilitarlo:



El segundo aspecto de la autenticación de dos factores se refiere a las instalaciones reales de WordPress de tus clientes. Para esto hay algunos plugins que tal vez quieras probar y recomendar:

- Duo Two-Factor Authentication
- Google Authenticator – WordPress Two Factor Authentication (2FA)
- Two Factor Authentication

Después de instalar y configurar uno de los plugins anteriores en el sitio web de un cliente, normalmente tendrán un campo adicional en su página de inicio de sesión de WordPress para introducir su código de seguridad. O, con el plugin Duo, primero iniciarán la sesión con sus credenciales y luego se les pedirá que elijan un método de autenticación, como Duo Push, llamada o código de acceso.

Usar HTTPS para conexiones cifradas - Certificado SSL

Una de las formas más olvidadas de reforzar la seguridad de WordPress es instalar un certificado SSL y ejecutar los sitios a través de HTTPS. HTTPS (Hypertext Transfer Protocol Secure) es un mecanismo que permite que cualquier navegador o aplicación web se conecte de forma segura con un sitio web. Un grave error es pensar que si los sitios de tus clientes no aceptan tarjetas de crédito no necesitan SSL.

Bueno, vamos a explicar algunas razones por las que HTTPS es importante más allá del comercio electrónico. Muchos proveedores de alojamiento, incluyendo Kinsta, ofrecen certificados SSL gratuitos con Let's Encrypt.

6 razones clave por las que HTTPS es importante más allá del comercio electrónico

1. Seguridad añadida
¿Qué tan importante es la información de acceso de tus clientes? Bueno, deberías saber que cada vez que un usuario se conecta, esa información se pasa al servidor en texto plano. HTTPS es absolutamente vital para mantener una conexión segura entre un sitio web y un navegador. De esta manera puedes evitar que los ciberdelincuentes o un intermediario accedan a los sitios de tus clientes.

2. SEO
Google ha dicho oficialmente que el HTTPS es un factor de posicionamiento. Como la mayoría de tus clientes probablemente aprovecharían cualquier posible ventaja de SEO y SERP para vencer a sus competidores, esto es algo obvio.

3. Confianza y credibilidad
Según una encuesta de GlobalSign, el 28,9% de los visitantes buscan la barra de direcciones verde en su navegador. Y el 77% de ellos están preocupados de que sus datos sean interceptados o mal utilizados en línea. Al ver ese candado verde, los clientes tendrán instantáneamente más tranquilidad al saber que sus datos están más seguros.

4. Datos de referencia
Mucha gente no se da cuenta de que los datos de referencia HTTPS a HTTP están bloqueados en Google Analytics. Entonces, ¿qué pasa con los datos? Bueno, la mayoría de ellos se agrupan con la sección de «tráfico directo». Si alguien va de HTTP a HTTPS, el remitente sigue pasando.

5. Advertencias Chrome
A partir del 24 de julio de 2018, las versiones de Chrome 68 y superiores comenzaron a marcar todos los sitios no HTTPS como "No seguros" y, a partir de 2020, el popular navegador comenzó a desaprobar el soporte para las versiones TLS heredadas. Google está dejando mucho más claro a los visitantes que un sitio web de WordPress podría no estar funcionando con una conexión segura. Por eso HTTPS es más importante que nunca.

6. Rendimiento
Debido a un protocolo llamado HTTP/2, muchas veces, aquellos que ejecutan sitios optimizados correctamente sobre HTTPS pueden incluso ver mejoras en la velocidad. HTTP/2 requiere HTTPS debido al soporte de los navegadores. La mejora en el rendimiento se debe a una variedad de razones como el hecho de que HTTP/2 puede soportar mejor multiplexación, paralelismo, compresión HPACK con codificación Huffman, la extensión ALPN y el empuje del servidor.

Y con TLS 1.3, las conexiones HTTPS son aún más rápidas. Kinsta soporta TLS 1.3 en todos nuestros servidores y en nuestro CDN de Kinsta.

Consulta nuestra guía detallada de migración HTTPS de WordPress para ponerte en marcha y aprender más en nuestra comparación de TLS vs SSL.

Desactivar XML-RPC

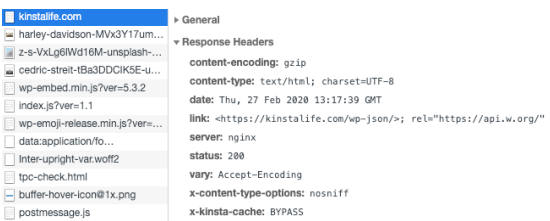
En los últimos años, el XML-RPC se ha convertido en un objetivo cada vez más grande para los ataques de fuerza bruta. Hay algunos plugins de WordPress como Jetpack que dependen de XML-RPC, pero la mayoría de la gente no lo necesita y puede ser beneficioso simplemente deshabilitar el acceso a él.

Si eres cliente de Kinsta, no tienes que preocuparte por esto ya que hemos implementado medidas activas y pasivas para detener los ataques y las intenciones maliciosas en su camino. Específicamente, cuando se detecta un ataque a través de XML-RPC se añade un pequeño fragmento de código en el archivo de configuración de Nginx para evitar que se produzca un error 403.

Añadir los últimos encabezados de seguridad HTTP

Otro paso que puedes dar para fortalecer la seguridad del sitio web WordPress de tu cliente es aprovechar los encabezados de seguridad de HTTP. Estos se configuran normalmente a nivel de servidor web y le dicen al navegador cómo comportarse cuando se maneja el contenido. Hay muchos encabezados de seguridad HTTP diferentes, pero a continuación se detallan los más importantes.

- Política de seguridad de contenidos
- Protección de X-XSS
- Strict-Transport-Security
- X-Frame-Options
- Llaveros públicos
- Tipo de contenido X



Puedes comprobar qué encabezados se están ejecutando actualmente en cada instalación de WordPress lanzando Chrome DevTools y mirando el encabezado en la respuesta inicial de tu sitio

Aquí hay un ejemplo en kinstalife.com (un sitio de demostración). Puedes ver que estamos utilizando el encabezado de opciones de tipo x-contenido.

Cuando se trata de sitios de clientes, como en el ejemplo que se muestra, siempre se añaden por defecto las opciones de tipo x-contenido, mientras que las opciones de tipo x-frame y la seguridad de transporte estricta se establecen solo si es necesario.

Si necesitas escanear los sitios de tus clientes, puedes hacerlo con la herramienta gratuita securityheaders.io de Scott Helme.

También es importante recordar que al implementar las cabeceras de seguridad de HTTP cómo puede afectar a los subdominios de WordPress. Por ejemplo, si añades la cabecera de la Política de seguridad de contenidos y restringes el acceso por parte de los dominios, también tendrás que añadir tus propios subdominios. Si no estás seguro de cómo implementarlos, siempre puedes preguntar a tu proveedor de hosting si puede ayudarte.

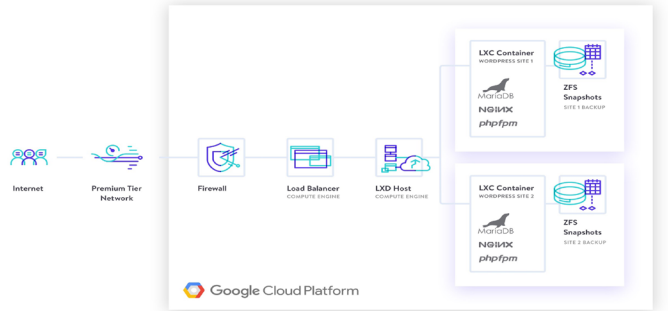
Usar los plugins de seguridad de WordPress

Hay un montón de grandes desarrolladores y empresas que ofrecen grandes soluciones para ayudar a proteger mejor tu sitio de WordPress. Los más importantes son:

- Seguridad de Sucuri
- iThemes Security
- Seguridad de Wordfence
- Registro de auditoría de seguridad de WP
- WP fail2ban
- Seguridad y cortafuegos All In One WP
- SecuPress
- Seguridad a prueba de balas
- VaultPress

- Google Authenticator - Autenticación de dos factores
- Ninja de seguridad
- Defender
- Seguridad de la web de Astra
- Seguridad del escudo
- Ocultar mi WP
- WebARX

Kinsta tiene cortafuegos de hardware, seguridad activa y pasiva, comprobaciones de tiempo de funcionamiento al minuto y muchas otras características avanzadas para evitar que los atacantes accedan a tus datos. Si, a pesar de nuestros esfuerzos, tu sitio está comprometido, lo arreglaremos gratuitamente.

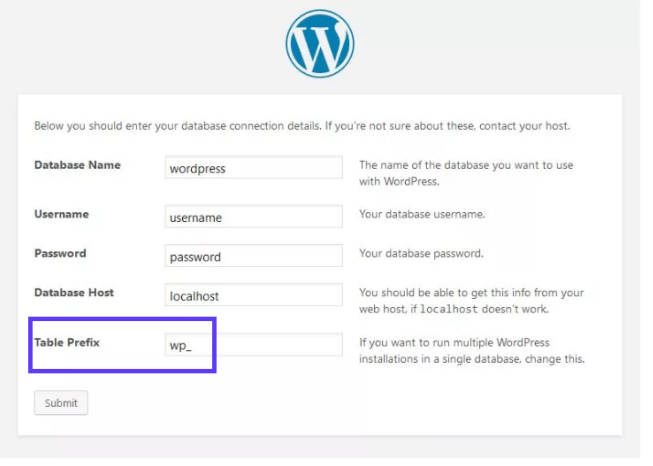


Una característica muy importante que muchos plugins de seguridad incluyen es una utilidad de suma de verificación. Esto significa que inspeccionan cada una de las instalaciones de WordPress de tu cliente y buscan modificaciones en los archivos centrales según lo dispuesto por WordPress.org (a través de la API). Cualquier cambio o modificación de estos archivos podría indicar un pirateo.

También puedes usar WP-CLI para ejecutar tu propia suma de comprobación. Echa un vistazo a estos plugins de seguridad adicionales de WordPress que pueden ayudar a bloquear a los malos.

Fortalecer la seguridad de la base de datos

Hay un par de maneras de mejorar la seguridad de tu base de datos de WordPress. La primera es usar un nombre de base de datos inteligente. Cambiar el nombre de la base de datos a uno más complejo ayuda a proteger tu sitio, haciendo más difícil que los hackers identifiquen y accedan a los detalles de la base de datos.

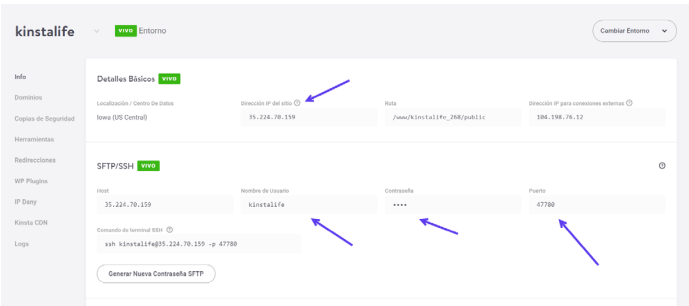


Una segunda recomendación es utilizar un prefijo diferente en la tabla de la base de datos. Cuando instalas WordPress, te pide un prefijo de tabla. De forma predeterminada, WordPress utiliza wp_. Cambiar esto a algo como 39xw_ puede ser mucho más seguro.

Si eres cliente de Kinsta y alojas todos los sitios de tus clientes con nosotros, esto no es necesario. ¡Tenemos el sitio y la base de datos bloqueados para ti!

Utiliza siempre conexiones seguras

¡No podemos insistir lo suficiente en lo importante que es usar conexiones seguras! Asegúrate de que tu proveedor de hosting especializado en WordPress toma precauciones como ofrecer SFTP o SSH. SFTP o Protocolo de Transferencia de Archivos Seguro (también conocido como protocolo de transferencia de archivos SSH) es un protocolo de red utilizado para la transferencia de archivos. Es un método más seguro que el FTP estándar.



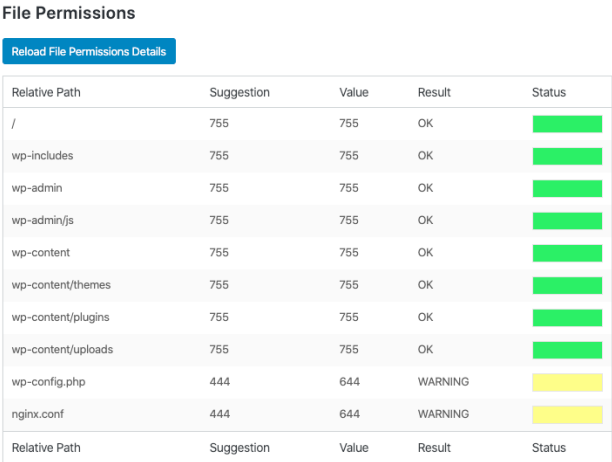
Revisa esta función con la demo de MyKinsta.

Solo apoyamos las conexiones SFTP en Kinsta para asegurar que tus datos permanezcan seguros y encriptados. La mayoría de los hosts de WordPress también suelen usar el puerto 22 para SFTP. Aquí en Kinsta llevamos esto un paso más allá y cada sitio tiene un puerto aleatorio que se puede encontrar en su tablero MyKinsta.

Comprobar los permisos de archivo y de servidor

Los permisos de archivo, tanto en las instalaciones de tus clientes como en los servidores web, son cruciales para reforzar la seguridad de estos entornos. Si los permisos son demasiado débiles, alguien podría acceder fácilmente a tu sitio y causar estragos. Por otro lado, si tus permisos son demasiado estrictos, esto podría romper la funcionalidad de tu sitio. Por lo tanto, es importante tener los permisos correctos establecidos en todos los ámbitos.

Puedes usar un plugin gratuito como iThemes Security para escanear los permisos de los sitios WordPress de tus clientes.



Aquí hay algunas recomendaciones típicas para los permisos de archivos y carpetas en WordPress:

- Todos los archivos deben ser 644 o 640 excepto wp-config.php, que debe ser 440 o 400, para evitar que otros usuarios del servidor lo lean.
- Todos los directorios deben ser 755 o 750.
- No se deben dar nunca permisos 777 a los directorios, ni siquiera a la carpeta Uploads.

Lee el artículo del Codex de WordPress sobre el cambio de los permisos de los archivos para una explicación más detallada.

Protección DDoS

DDoS es un tipo de ataque DOS en el que se utilizan múltiples sistemas para apuntar a un solo sistema causando un ataque de Denegación de Servicio (DoS). Los ataques DDoS no son nada nuevo: según Britannica el primer caso documentado data de principios de 2000. A diferencia de alguien que hackea tu sitio, este tipo de ataques normalmente no lo dañan sino que simplemente lo derriban por unas horas o días.

¿Qué puedes hacer para protegerte? Una de las mejores recomendaciones es usar un servicio de seguridad de terceros con buena reputación como Cloudflare o Sucuri.

Su avanzada protección DDoS puede utilizarse para mitigar los ataques DDoS de todas las formas y tamaños, incluidos los que tienen como objetivo los protocolos UDP e ICMP, así como los ataques SYN/ACK, de amplificación del DNS y de capa 7. Otros beneficios incluyen ponerte detrás de un proxy que ayuda a ocultar tu dirección IP de origen, aunque no es a prueba de balas.

No pases por alto el proveedor que utiliza tu proveedor de alojamiento porque eso también es muy importante.

Los cortafuegos de hardware, como el Google Cloud Platform Firewall que utilizamos en Kinsta, están instalados y tienen restricciones muy estrictas basadas en el software para proteger los sitios de sus clientes y también tienen software para detectar los ataques DDoS en el momento en que se producen.

Esto significa que tú y tus clientes os beneficiais de un modelo de seguridad que se ha ido construyendo a lo largo de 15 años y que actualmente asegura productos y servicios como Gmail, Search, etc.

Google emplea actualmente a más de 500 profesionales de seguridad a tiempo completo.

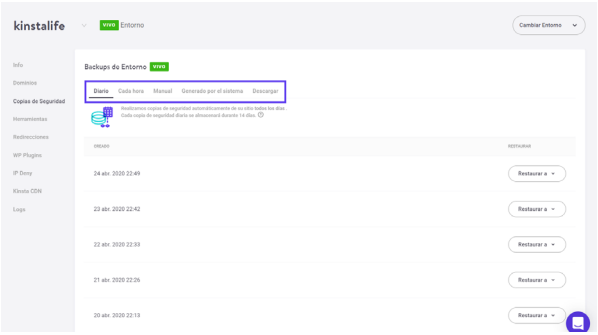
Además de Google Cloud Platform, también usamos contenedores Linux (LXC y LXD) para organizarlos, lo que nos permite aislar completamente no solo cada cuenta, sino cada sitio web WordPress por separado.

Si aún así tu sitio web se infecta, Kinsta proporciona reparación de sitios infectados y eliminación de malware de forma gratuita. Si uno de los sitios de tus clientes está infectado, nuestro equipo de soporte hará todo lo necesario para limpiarlo.

¡Obtén más detalles sobre la seriedad con la que nos tomamos la seguridad en Kinsta! 

Haz siempre copias de seguridad

No importa lo seguro sea tu sitio, nunca será 100% seguro. Por eso necesitas copias de seguridad en caso de que suceda lo peor. Las copias de seguridad son lo único que todo el mundo sabe que necesita, pero no siempre las hace. La mayoría de las recomendaciones que aquí se describen son medidas de seguridad que puedes tomar para proteger mejor los sitios de tus clientes y tu negocio.



Conoce esta función con la demo de MyKinsta.

La mayoría de los proveedores de alojamiento administrado de WordPress ahora proporcionan copias de seguridad. Kinsta tiene cinco tipos diferentes de copias de seguridad:

- A diario: Kinsta crea copias de seguridad automatizadas de todos los sitios de tus clientes cada 24 horas para que puedas descansar con tranquilidad por la noche.
- Cada hora: Si necesitas una programación de copias de seguridad más frecuente, puedes activar copias de seguridad automáticas de 6 horas o cada hora para cualquier sitio objetivo que lo requiera (esto se suma a tu plan mensual).
- Manual: si las copias de seguridad automatizadas no son suficientes, puedes crear copias de seguridad manuales

para cada sitio que estés administrando y tener esta copia adicional disponible durante 14 días o más, según tu plan actual.

- Generado por el sistema: antes de las tareas críticas como usar la herramienta de búsqueda-reemplazo en MyKinsta, pasar un entorno de staging en producción, y restaurar un backup en tu entorno en vivo, Kinsta activará las copias de seguridad generadas por el sistema.
- Archivo descargable: si todo esto no es suficiente, una vez por semana, se puede descargar un archivo zip de cada sitio web que contiene los archivos y un archivo SQL con el contenido de la base de datos del sitio.

Las opciones de backup no vienen solas, ya que Kinsta te permite restaurar fácilmente cualquier sitio con un solo clic. Esto es conveniente, ¿no?

¡Prueba gratis lo fácil que es crear copias de seguridad con MyKinsta!

Si tu proveedor de alojamiento no tiene copias de seguridad, hay algunos plugins populares de WordPress que puedes usar para automatizar el proceso.

Plugins de backup de WordPress

Los plugins de backup de WordPress te permiten obtener tus copias de seguridad a través de FTP o integrarse con una fuente de almacenamiento externo como Amazon S3, Google Cloud Storage, Google Drive o Dropbox. Recomendamos encarecidamente optar por una solución incremental para que use menos recursos:

- Duplicator
- WP Time Capsule
- BackupBuddy
- UpdraftPlus
- BackUpWordPress
- BackWPup
- WP BackItUp

Kinsta no permite plugins de backup no incrementales debido a problemas de rendimiento: manejamos todo esto por ti a nivel de servidor para que no ralentice los sitios de tus clientes.

Resumen

La seguridad es un juego de capas. Cuanto más éxito tengas apilando nuevas capas de seguridad una encima de la otra, más seguros serán los sitios de tus clientes. Todo comienza con el uso de contraseñas inteligentes, manteniendo el núcleo y los plugins y temas actualizados, y siguiendo otras mejores prácticas de seguridad que hemos cubierto aquí.

Pero eso no es todo lo que deberías hacer para reducir las posibilidades de tener que lidiar con sitios de clientes pirateados. Al elegir un proveedor de alojamiento administrado en WordPress como Kinsta, la mayoría de las medidas de seguridad las tomamos por ti, permitiéndote construir una base sólida, segura y escalable para asegurar el futuro de los sitios de tus clientes. Y el de tu negocio.

¿Quieres probar lo fácil que es administrar los sitios de tus clientes en Kinsta?

¡Visita demo.mykinsta.com!


KINSTA