

Checklist 2026

de mantenimiento WordPress profesional para agencias

Organizado por frecuencia de ejecución: semanal, mensual, trimestral y anual. Cubre seguridad, actualizaciones, backups, rendimiento y documentación. Para uso interno de agencia o como base para definir el alcance de un plan externalizado.

4 frecuencias · 30+ tareas · El 90% de los hackeos en WordPress son prevenibles con estas tareas

WordPress alimenta el 43% de los sitios web activos a nivel global (W3Techs, 2025). Esa cuota lo convierte en el objetivo más frecuente de ataques automatizados. Un sitio sin mantenimiento activo tiene vulnerabilidades conocidas que los atacantes escanean de forma sistemática.

Para una agencia que gestiona los sitios de sus clientes, el riesgo no es solo técnico. Un hackeo o una caída daña la relación con el cliente independientemente de quién sea el responsable técnico. El cliente no distingue entre un fallo del hosting y un fallo de mantenimiento.

El 90% de los hackeos en sitios WordPress tienen como causa raíz plugins desactualizados, versiones de PHP sin soporte o contraseñas débiles. Los tres son prevenibles con mantenimiento activo.

01

Tareas semanales

Mayor impacto en seguridad y disponibilidad

Son las que detectan problemas antes de que se conviertan en incidencias.

☐

Verificación de disponibilidad

Confirmar que el sitio responde en su URL principal. Un monitor de uptime automatizado (UptimeRobot, Freshping) envía alertas en menos de 5 minutos desde que el sitio cae.

☐

Revisión de alertas de seguridad

Si el sitio tiene un plugin de seguridad activo (Wordfence, MalCare, Solid Security), revisar el panel de alertas. Los intentos de fuerza bruta y los accesos sospechosos aparecen ahí antes de convertirse en un problema real.



Revisión de formularios

Verificar que los formularios de contacto y suscripción envían correctamente y que los mensajes llegan al destino acordado. Los formularios dejan de funcionar por cambios en el servidor de correo, actualizaciones del plugin o filtros de spam que bloquean el dominio.



Revisión de errores en consola

Revisar los errores de JavaScript en el navegador y los errores PHP en el log del servidor. Detecta problemas que no son visibles para el usuario pero degradan el rendimiento o rompen funcionalidades secundarias.

02

Tareas mensuales

Núcleo del mantenimiento — entorno actualizado y rendimiento estable

Son las que mantienen el entorno actualizado y el rendimiento estable.



Actualización de WordPress core

Actualizar a la versión estable más reciente. Las actualizaciones de seguridad (minor updates) se aplican de forma inmediata. Las de versión mayor se aplican tras verificar compatibilidad con los plugins activos en un entorno de staging.



Actualización de plugins

Actualizar todos los plugins activos. Antes de actualizar en producción, revisar si alguna actualización tiene notas de cambios que puedan afectar al funcionamiento del sitio. WooCommerce, Elementor Pro y plugins de seguridad son los que más frecuentemente generan conflictos tras una actualización mayor.



Actualización de temas

Actualizar el tema activo y los temas inactivos instalados. Los temas inactivos con versiones antiguas son un vector de ataque habitual porque muchas agencias los olvidan al actualizar el resto del entorno.



Revisión de usuarios administradores

Verificar que solo tienen acceso de administrador las cuentas autorizadas. Eliminar usuarios inactivos o con permisos que ya no corresponden. Verificar que las contraseñas cumplen los criterios de complejidad mínima.



Backup verificado

Confirmar que el sistema de backup está funcionando y que el backup más reciente es restaurable. Un backup que existe pero no es restaurable no protege de nada. La verificación implica descargar el backup más reciente y comprobar que los archivos están completos y no están corruptos.



Revisión de PageSpeed

Medir el score con Google Lighthouse en móvil y compararlo con el mes anterior. Una degradación progresiva indica plugins, scripts de terceros o imágenes no optimizadas añadidos durante el mes. Umbral mínimo recomendado: 85/100 en móvil.



Revisión de espacio en disco

Verificar que el hosting no está cerca del límite de espacio asignado. Los logs de error que crecen de forma descontrolada o las librerías de medios sin limpiar pueden llegar al límite sin que nadie lo detecte hasta que el sitio deja de funcionar.

03

Tareas trimestrales

Salud técnica a medio plazo — base para el informe al cliente

Son las que mantienen el entorno técnico saludable a medio plazo y generan el informe que la agencia puede entregar al cliente como prueba del trabajo realizado.



Revisión de la versión de PHP

Verificar que el servidor ejecuta una versión con soporte oficial activo. En 2026, las versiones soportadas son PHP 8.1, 8.2 y 8.3. Las versiones sin soporte (PHP 7.4 y anteriores) no reciben parches de seguridad. Si el hosting ejecuta una versión sin soporte, coordinar con el cliente la actualización.

- ☐ **Revisión de plugins desactualizados o abandonados**
Identificar los plugins que no han recibido actualizaciones en más de 12 meses. Un plugin abandonado por su desarrollador es un riesgo de seguridad que no va a corregirse. Si no existe una alternativa mantenida, documentarlo y planificar la sustitución.
- ☐ **Revisión de Core Web Vitals en Search Console**
Revisar el informe de Core Web Vitals en Google Search Console. Los errores de LCP, INP o CLS afectan directamente al posicionamiento orgánico del sitio. Documentarlos y planificar las correcciones en el siguiente ciclo.
- ☐ **Revisión de errores de indexación**
Revisar el informe de cobertura en Search Console para detectar páginas con errores de indexación: 404, redirección incorrecta, páginas bloqueadas por robots.txt o noindex involuntario.
- ☐ **Prueba de restauración del backup**
Restaurar el backup completo en un entorno de staging para verificar que el proceso de recuperación funciona correctamente. Registrar cuánto tiempo tarda la restauración. No es suficiente con que el backup exista.
- ☐ **Informe trimestral para el cliente**
Documentar las tareas realizadas, las actualizaciones aplicadas, el score de PageSpeed del mes más reciente y cualquier incidencia resuelta. Este informe es el argumento más efectivo para retener al cliente en la renovación.

04

Tareas anuales

Mayor alcance — requieren coordinación con el cliente

Son las de mayor alcance y las que requieren más coordinación con el cliente.

- ☐ **Renovación de dominio y SSL**
Verificar las fechas de expiración del dominio y del certificado SSL. Un dominio caducado o un SSL expirado tumban el sitio de forma inmediata. Configurar la renovación automática o establecer alertas con 60 días de antelación.
- ☐ **Auditoría técnica completa**
Revisión profunda del entorno: stack de plugins, estructura de archivos, configuración del servidor, logs de error acumulados y comparación del rendimiento actual con el del año anterior. Identifica la deuda técnica acumulada y las mejoras a planificar.
- ☐ **Revisión del plan de copias de seguridad**
Verificar que la política de backups sigue siendo adecuada para el volumen de contenido y la frecuencia de actualizaciones. Un sitio que se actualiza diariamente necesita backups diarios. Un sitio con actualizaciones mensuales puede funcionar con backups semanales.
- ☐ **Actualización de la documentación del proyecto**
Actualizar el documento interno de la agencia con los accesos actuales al sitio, los plugins instalados con sus versiones, las configuraciones específicas del proyecto y cualquier decisión técnica tomada durante el año. Crítico si el proyecto cambia de manos o se traspasa a otro partner.

Cómo estructurar el mantenimiento como servicio recurrente

01

Alcance claro

Qué tareas están incluidas y cuáles no. Los cambios de diseño, el desarrollo de nuevas funcionalidades y la creación de contenido no son mantenimiento técnico y deben facturarse por separado.

02

SLA de respuesta definido

Cuánto tiempo tarda la agencia en responder a una incidencia. La diferencia entre un SLA de 24 horas y uno de 72 horas es relevante para los clientes con sitios de alta visibilidad.

03**Informe periódico**

Un documento que el cliente recibe de forma regular con las tareas realizadas y el estado técnico del sitio. Es el argumento más efectivo para justificar el precio del plan en cada renovación.

04**Precio por sitio o por bolsa de sitios**

El modelo más habitual es un precio mensual fijo por sitio. Para agencias con muchos clientes, un modelo de bolsa (precio por bloque de 5 o 10 sitios) tiene mejor margen.

Preguntas frecuentes**¿Con qué frecuencia hay que actualizar los plugins de WordPress?**

Las actualizaciones de seguridad deben aplicarse en menos de 48 horas desde su publicación. Las actualizaciones de versión mayor se prueban primero en staging y se aplican en producción tras confirmar que no generan conflictos. Dejar plugins sin actualizar más de 30 días es el principal vector de entrada en los hackeos documentados.

¿Qué versión de PHP deben tener los sitios WordPress en 2026?

Las versiones con soporte oficial activo en 2026 son PHP 8.1, 8.2 y 8.3. PHP 7.4 llegó al fin de vida en noviembre de 2022 y no recibe parches de seguridad desde entonces. Un sitio que ejecuta PHP 7.4 tiene vulnerabilidades conocidas sin corrección disponible.

¿El mantenimiento WordPress incluye cambios de diseño o contenido?

No. El mantenimiento técnico cubre actualizaciones, seguridad, backups, rendimiento y monitoreo. Los cambios de diseño, el desarrollo de nuevas funcionalidades y la creación de contenido son tareas fuera del alcance del mantenimiento y se facturan por separado, habitualmente como bolsa de horas o proyecto independiente.

¿Qué diferencia hay entre un backup que existe y un backup verificado?

Un backup que existe es un archivo generado automáticamente por un plugin o el hosting. Un backup verificado es un backup que ha sido restaurado en un entorno de prueba y ha producido un sitio funcional. La diferencia es que el primero puede estar corrupto, incompleto o ser incompatible con la versión actual de WordPress sin que nadie lo sepa hasta el momento en que se necesita restaurar.

¿Qué herramientas se usan para el monitoreo de uptime?

UptimeRobot y Freshping son las más habituales para monitoreo de disponibilidad. Ambas tienen planes gratuitos con comprobaciones cada 5 minutos y notificaciones por email o SMS. Para sitios con SLA estrictos, los planes de pago comprueban cada 1 minuto.