

PHP sin soporte y PHP2Shell: checklist para dueños de sitios WordPress

La corrección oficial de PHP2Shell (21 oct 2026) solo cubre PHP 8.2 a 8.5. Si tu sitio usa PHP 7.4, 8.0 u 8.1, recorre esta lista en orden.

CORRECCIÓN OFICIAL
PHP 8.2 – 8.5

7.4 / 8.0 / 8.1
Sin soporte

ACTUALIZAR A
PHP 8.3 u 8.4

FIN DE SOPORTE 8.2
31 dic 2026

A Saber dónde estás

- ☐ **Tu versión de PHP:** _____ Salud del sitio → Información → Servidor.
- ☐ **¿Estás en 7.4, 8.0 u 8.1? Pregúntale a tu hosting** si tu PHP incluye las correcciones del 21 de octubre. Algunos hostings corrigen sin cambiar el número de versión.
- ☐ **Confirma que esta configuración esté desactivada** (php.ini o PHP-FPM; en hosting compartido, pregunta):
`session.upload_progress.enabled = 0` Cubre el CVE-2026-115560, aún sin corrección.
- ☐ **Haz la lista de tu tema y tus plugins** con la fecha de su última actualización. Lo que lleva años sin actualizarse es el mayor riesgo.

B Elegir el camino

☐ Parche del hosting

Tu hosting o proveedor de Linux recompiló el PHP viejo con la corrección. Cobertura desigual; solo gana tiempo.

☐ Soporte extendido pagado

Parches comerciales (p. ej. Ubuntu Pro, Freexian ELTS, TuxCare). Un costo anual por seguir en código viejo.

☐ Actualizar a PHP 8.3 / 8.4

El único camino que recibe todas las correcciones futuras del propio PHP. Requiere pruebas; ver sección C.

No elijas PHP 8.2 como destino: su soporte de seguridad termina el 31 dic 2026. WordPress 7.1 funciona con PHP 7.4 a 8.5 y recomienda 8.3 o superior.

C Actualizar sin romper el sitio

- ☐ **01 Respaldo completo y restauración probada**
Archivos + base de datos, fuera del servidor.
- ☐ **02 Crear una copia de pruebas (staging)**
Todos los cambios van ahí primero.
- ☐ **03 Actualizar WordPress, tema y plugins**
En staging, antes de tocar PHP.
- ☐ **04 Reemplazar plugins abandonados**
Años sin actualizar = planear un cambio.
- ☐ **05 Pasar staging a 8.3 / 8.4**
Registro de errores activo, sin mostrarlos.
- ☐ **06 Probar lo que te da ingresos**
Formularios, pagos, accesos, búsqueda, correo.
- ☐ **07 Cambiar producción en hora tranquila**
Respaldo nuevo y reversión lista.
- ☐ **08 Vigilarlo durante 48 horas**
Registro de errores, pedidos y formularios.

D Revisar si alguien entró antes

Se reportaron intentos de explotación desde el **17 oct 2026**, cuatro días antes de la corrección. Si el sitio tuvo PHP sin corregir después de esa fecha, revisa:

- ☐ **Cuentas de administrador.** Usuarios → Administradores: ¿hay alguien que no reconozcas?
- ☐ **Archivos PHP en uploads.** Cualquier archivo .php dentro de wp-content/uploads es una señal de alerta.
- ☐ **Archivos modificados hace poco** que no tocaste, sobre todo en la raíz del sitio y en las carpetas del tema.
- ☐ **Tareas programadas.** Cron jobs desconocidos en el panel del hosting o eventos programados de WordPress que no reconoces.
- ☐ **Registros de errores.** Ráfagas de errores "Allowed memory size", o procesos de PHP que fallan y se reinician sin causa clara.

Un resultado limpio no prueba que el sitio esté limpio, pero sí hace mucho menos probable una intrusión silenciosa.

E Si encuentras algo

- ☐ **Saca el sitio de línea sin borrarlo.** Muestra una página de mantenimiento o detén el servidor web. No desactives solo PHP: el servidor podría mostrar tu código como texto.
- ☐ **Guarda los registros** (servidor web, PHP, panel del hosting) antes de que se borren.
- ☐ **Cambia todas las claves que usa el sitio:** contraseña de la base de datos, claves y salts de WordPress, contraseñas de administrador, claves de API.
- ☐ **Restaura un respaldo anterior al 17 de octubre** si no puedes asegurar que el sitio está limpio, y corrige o actualiza PHP antes de volver a publicarlo.
- ☐ **Revisa tus obligaciones de notificación** si pudieron quedar expuestos datos personales (clientes, pedidos, cuentas).

F Que la próxima alerta no te tome por sorpresa

- ☐ **Actualizaciones mensuales** de WordPress, tema y plugins; las grandes, primero en staging.
- ☐ **Respaldos automáticos fuera del servidor**, con una restauración de prueba al menos cada trimestre.
- ☐ **Un recordatorio con las fechas de fin de soporte de PHP.** Están en php.net/supported-versions. Planea las actualizaciones con meses de anticipación.
- ☐ **Alguien que siga los avisos de seguridad** de tu stack, para que te enteres de la próxima alerta antes que tus clientes.

¿Quieres una segunda opinión o prefieres delegarlo?

Empieza con una revisión de exposición gratis: qué PHP usa tu sitio y qué implicaría actualizarlo, y luego una cotización fija antes de cualquier trabajo. Lo hacemos con respaldo previo, en staging y con un reporte escrito. Tú conservas todos los accesos y archivos.

wordpress.com
hola@wordpress.com