wp-config.php seguro

Las llaves del sitio: configúralas bien

Por Fabini | @fabinidc — Guía gratuita disponible en fabini.one

Esta guía te ofrece snippets prudentes y un checklist completo para endurecer WordPress sin romper nada. Enfoque conservador: siempre con backup.

Antes de tocar nada: seguridad primero

Precauciones obligatorias

Antes de modificar wp-config.php, debes tomar estas medidas de seguridad esenciales. Un error en este archivo puede tumbar completamente tu sitio web.

- Realiza backup completo de archivos y base de datos
- Verifica que tienes acceso a FTP o panel de control
- Descarga una copia local de wp-config.php actual
- Anota la versión de WordPress que usas
- Ten a mano los datos de acceso a tu hosting

¿Por qué es crítico?

El archivo wp-config.php es el corazón de tu instalación WordPress. Contiene las credenciales de base de datos y configuraciones sensibles.

Una coma mal puesta, una comilla sin cerrar o un paréntesis de más pueden causar pantalla blanca completa. No hay margen de error.

Si algo sale mal, necesitarás restaurar desde el backup. Por eso insistimos: **siempre backup antes de modificar**.

Recordatorio crítico: Guarda una copia de seguridad antes de cada cambio. Si usas un plugin de backup automático, actívalo manualmente antes de continuar.

Qué es wp-config.php: visión rápida

El archivo wp-config.php es el archivo de configuración principal de WordPress. Se encuentra en la raíz de tu instalación y actúa como puente entre WordPress y tu base de datos MySQL.

Conexión a base de datos

Define el host, nombre de base de datos, usuario y contraseña. Sin estos datos correctos, WordPress no puede arrancar.

Seguridad y claves

Contiene las sales y claves de cifrado que protegen las sesiones de usuario y cookies. Fundamentales para la seguridad.

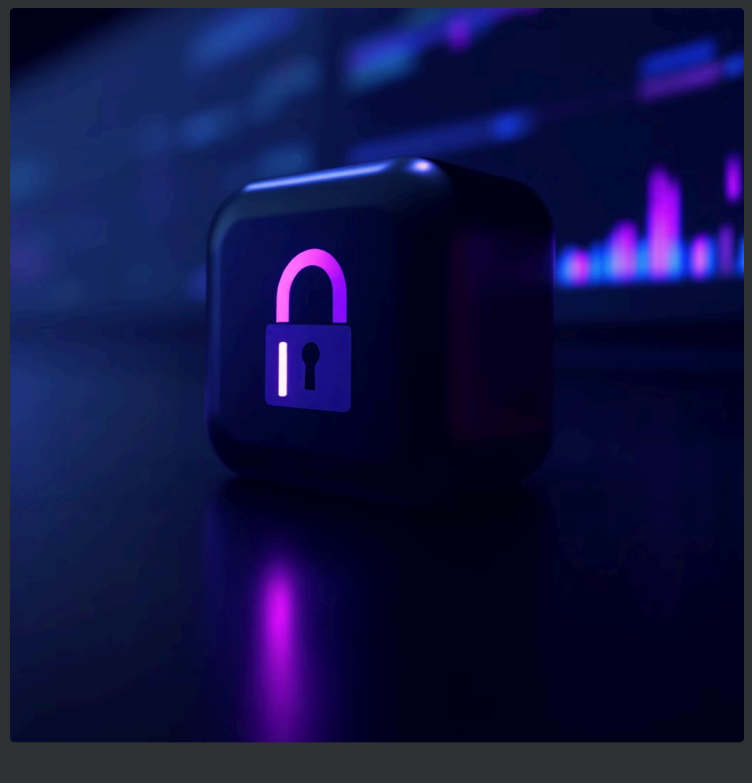
Ajustes avanzados

Controla debug, límites de memoria, idioma, URLs del sitio, permisos de edición y muchas otras configuraciones críticas.

Este archivo se lee en cada petición que hace WordPress. Por eso debe estar optimizado, protegido y libre de errores. Cualquier directiva define() que añadas aquí tiene efecto inmediato en todo el sitio.

A diferencia de otros archivos de WordPress, wp-config.php no se sobrescribe en las actualizaciones automáticas. Tus cambios permanecen, pero esto también significa que eres responsable de mantenerlo actualizado y seguro.

Snippet 1: Desactivar editor de archivos



¿Por qué hacerlo?

WordPress incluye un editor de temas y plugins en el panel de administración. Si un atacante consigue acceso a tu admin, puede modificar código PHP directamente desde el navegador.

Desactivar este editor cierra una puerta de entrada común para inyecciones de código malicioso.

Código a añadir

```
// Desactivar editor de archivos
define('DISALLOW_FILE_EDIT', true);
```

Ubicación: Añade esta línea antes de `/* ¡Eso es todo, deja de editar! */` en tu wp-config.php.

Efecto: Las opciones "Editor de temas" y "Editor de plugins" desaparecen del menú de administración.

Reversión: Cambia `true` por `false` o elimina la línea para restaurar el editor.

Nota importante: Si necesitas editar archivos, usa FTP o el administrador de archivos de tu hosting. Es más seguro que hacerlo desde el navegador.

Snippet 2 y 3: SSL y claves de seguridad

1

Forzar HTTPS en administración

```
// Forzar SSL en admin
define('FORCE_SSL_ADMIN', true);
```

Requisito previo: Tu sitio debe tener un certificado SSL correctamente instalado y activo. Si no tienes HTTPS funcionando, este cambio causará redirecciones infinitas.

Beneficio: Todas las sesiones de administración viajan cifradas. Protege credenciales y cookies de intercepción en redes públicas.

2

Rotar claves y sales únicas

```
/* Sales únicas de autenticación */
define('AUTH_KEY',         '[[copia aquí]]');
define('SECURE_AUTH_KEY',  '[[copia aquí]]');
define('LOGGED_IN_KEY',    '[[copia aquí]]');
define('NONCE_KEY',        '[[copia aquí]]');
define('AUTH_SALT',        '[[copia aquí]]');
define('SECURE_AUTH_SALT', '[[copia aquí]]');
define('LOGGED_IN_SALT',   '[[copia aquí]]');
define('NONCE_SALT',       '[[copia aquí]]');
```

Generador oficial: Visita https://api.wordpress.org/secret-key/1.1/salt/ — Copia todo el bloque y pega en wp-config.php, reemplazando las líneas existentes.

Efecto de rotación: Invalida todas las sesiones activas. Todos los usuarios (incluido tú) deberán volver a iniciar sesión. Útil si sospechas intrusión.

Estas dos configuraciones son fundamentales para la seguridad básica. El SSL protege la transmisión; las sales protegen el almacenamiento de sesiones. Rotar las sales cada 3-6 meses es una buena práctica preventiva.

Snippet 4 y 5: Debug y prefijo de tablas

01

Debug correcto en producción

```
// Producción: errores ocultos al público
define('WP_DEBUG', false);

// Si necesitas depurar sin mostrar:
define('WP_DEBUG_LOG', true);
define('WP_DEBUG_DISPLAY', false);
@ini_set('display_errors', 0);
```

En producción, `WP_DEBUG` debe estar en `false`. Si activas el modo log, los errores se guardan en `/wp-content/debug.log`. Revísalo periódicamente y apaga el log cuando termines de depurar.

02

Cambiar prefijo de tablas

```
// Evita el prefijo predecible 'wp_'
$table_prefix = '[[wp_x3_]]';
```

Advertencia crítica: Cambiar esto en sitios existentes requiere renombrar tablas en la base de datos manualmente. No lo hagas a ciegas. En instalaciones nuevas, usa un prefijo personalizado desde el inicio.

El modo debug es tu aliado al desarrollar, pero tu enemigo en producción. Nunca dejes errores visibles al público: revelan rutas del servidor, versiones de plugins y otros datos sensibles que facilitan ataques.

El prefijo de tablas personalizado dificulta ataques SQL injection automatizados que asumen el prefijo estándar `wp_`. Es una capa extra de ofuscación, no una defensa completa.

Snippets opcionales: rendimiento y control

Limitar revisiones y autosave

```
// Control de revisiones
define('WP_POST_REVISIONS', 10);
define('AUTOSAVE_INTERVAL', 120);
```

Reduce el tamaño de la base de datos limitando revisiones a 10 y autoguardado cada 2 minutos (120 segundos). Ajusta según tus necesidades.

Método de sistema de archivos

```
// Solo si hay problemas de permisos
define('FS_METHOD', 'direct');
```

Usar con cautela: Depende del hosting. Preferible solucionar permisos de usuario en el servidor que forzar este método.

Definir URLs del sitio

```
// Útil al migrar o cambiar dominio
define('WP_HOME', 'https://[[tudominio.com]]');
define('WP_SITEURL', 'https://[[tudominio.com]]');
```

Fija las URLs para evitar problemas tras migraciones. Recuerda actualizar estos valores si cambias de dominio.

Forzar idioma del sitio

```
define('WPLANG', 'es_ES');
```

Límites de memoria PHP

```
define('WP_MEMORY_LIMIT', '128M');
define('WP_MAX_MEMORY_LIMIT', '256M');
```

Aumenta con prudencia. Consulta los límites de tu plan de hosting.

Ubicación y permisos del archivo

Mover wp-config.php fuera del webroot

Si tu hosting lo permite, puedes mover wp-config.php un nivel por encima de la carpeta pública. WordPress lo detecta automáticamente.

Ruta típica:

```
/home/[[usuario]]/wp-config.php
/home/[[usuario]]/public_html/
```

Copia el archivo, prueba el sitio y, si funciona, elimina el original de la raíz pública. Si algo falla, revierte inmediatamente.

Permisos de archivo correctos

Los permisos controlan quién puede leer, escribir o ejecutar el archivo en el servidor.

- **Recomendado:** 400 o 440
- **Nunca:** 777 (escritura global es peligrosa)
- **Propietario:** Debe ser el usuario correcto del hosting

Verifica permisos desde FTP o panel de control. Un archivo legible por otros puede exponer credenciales de base de datos.

Consejo de hosting: Algunos hostings compartidos no permiten mover wp-config.php. Consulta con soporte antes de intentarlo.

Checklist de seguridad imprimible

Usa esta lista para auditar tu wp-config.php en menos de un minuto. Marca cada punto al completarlo.

- **Backup completo realizado**

  Archivos y base de datos respaldados antes de cualquier cambio

- **DISALLOW_FILE_EDIT activado**

  Editor de archivos deshabilitado en el panel de administración

- **FORCE_SSL_ADMIN activo**

  Administración forzada por HTTPS (solo si tienes certificado SSL)

- **Claves y sales rotadas**

  Fecha de última rotación: [[dd/mm/aaaa]] — Rotar cada 3-6 meses

- **WP_DEBUG configurado correctamente**

  False en producción; si usas log, no muestres errores al público

- **Prefijo de tablas personalizado**

  En instalaciones nuevas, evita usar 'wp_' como prefijo

- **wp-config.php movido fuera del webroot**

  Solo si tu hosting lo permite; prueba antes de eliminar el original

- **Permisos revisados**

  Archivo en 400 o 440; propietario correcto; nunca 777

Auditoría recomendada: Revisa este checklist trimestralmente o tras cualquier incidente de seguridad sospechoso.

Troubleshooting y control trimestral

Problemas comunes y soluciones rápidas

1

Pantalla blanca completa

Causa: Error de sintaxis en wp-config.php — falta una coma, punto y coma o comilla mal cerrada.

Solución: Restaura desde backup. Revisa línea por línea el código añadido.

2

Redirección HTTPS infinita

Causa: FORCE_SSL_ADMIN activo sin certificado SSL correcto, o reglas duplicadas en .htaccess/servidor.

Solución: Desactiva temporalmente FORCE_SSL_ADMIN. Verifica certificado y configuración de proxy/CDN.

3

Archivo debug.log gigante

Causa: WP_DEBUG_LOG activo durante mucho tiempo en producción.

Solución: Desactiva WP_DEBUG_LOG, elimina o vacía el archivo debug.log vía FTP.

Tabla de control trimestral

Fecha	Sales rotadas	SSL admin	File edit off	Debug ok	Permisos	Notas
[[dd/mm]]	✓ / ×	✓ / ×	✓ / ×	✓ / ×	400	[[libre]]
[[dd/mm]]	✓ / ×	✓ / ×	✓ / ×	✓ / ×	400	[[libre]]
[[dd/mm]]	✓ / ×	✓ / ×	✓ / ×	✓ / ×	400	[[libre]]

Cierre: configuración bien puesta = menos riesgo

Un wp-config.php correctamente configurado es tu primera línea de defensa. No es la única, pero es fundamental. Combínalo con plugins de seguridad, actualizaciones regulares y backups automáticos para proteger tu WordPress.

> Más plantillas y recursos en **fabini.one**
>
> Si esta guía te sirvió, etiqueta **@fabinidc** en redes sociales.

Nota legal: Esta guía se ofrece como recurso educativo. El autor no se responsabiliza por daños derivados de su aplicación. Siempre prueba en entorno de desarrollo primero.