WordPress: Checklist de Seguridad Rápida

Una guía práctica para administradores de WordPress que necesitan fortalecer la seguridad de su sitio web en 15-20 minutos. Este checklist está diseñado para reducir los riesgos más comunes de forma inmediata, sin necesidad de conocimientos técnicos avanzados.

Cómo Usar Esta Checklist

Objetivo Claro

Reducir riesgos comunes de seguridad hoy mismo. No se trata de una auditoría completa, sino de cerrar las puertas más importantes de entrada a posibles ataques.

Qué Necesitas

Acceso de administrador a tu WordPress y al panel de control de tu hosting o CDN. Tener estos accesos a mano acelerará significativamente el proceso.

Método de Trabajo

Marca cada punto completado. Si no puedes realizar alguna acción ahora mismo, agenda una fecha específica para hacerlo. La clave está en la acción inmediata.

> 💡 **Microcopy**: "Primero cierra puertas, luego ventanas." La seguridad se construye paso a paso, empezando por lo más crítico.

Copia de Seguridad AHORA

Backup Completo Inmediato

Antes de realizar cualquier cambio en tu sitio web, es fundamental tener una copia de seguridad completa. Un backup incluye tanto la base de datos (con todo el contenido, usuarios y configuraciones) como todos los archivos del sitio web.

La mayoría de plugins de backup ofrecen opciones "one-click" que simplifican enormemente este proceso. Si tu hosting incluye backups automáticos, también puedes generar uno manualmente desde el panel de control.

- Ejecutar backup completo (base de datos + archivos)
- Descargar o guardar copia fuera del servidor
- Verificar que el archivo se ha generado correctamente

🔎 **Comprueba:** Recibes el archivo ZIP del backup o tienes disponible la opción de restauración desde tu panel de control. Un backup que no se puede restaurar no sirve de nada.

Autenticación de Dos Factores (2FA)

El 2FA es una de las medidas de seguridad más efectivas y fáciles de implementar. Añade una capa adicional de protección que hace extremadamente difícil que alguien acceda a tu sitio web, incluso si conoce tu contraseña.

01

Instalar Aplicación TOTP

Descarga una aplicación como Authy, Google Authenticator o 1Password en tu móvil. Estas aplicaciones generan códigos temporales que cambian cada 30 segundos.

02

Configurar en WordPress

Usa un plugin como "Two Factor" o "Wordfence" para configurar el 2FA. Escanea el código QR con tu aplicación móvil para vincular tu cuenta.

03

Guardar Códigos de Recuperación

Descarga y guarda los códigos de backup en un lugar seguro, fuera del servidor. Te permitirán acceder si pierdes tu teléfono.

04

Probar el Sistema

Cierra sesión e inicia sesión de nuevo para verificar que el 2FA funciona correctamente. Este paso es crucial para evitar quedarte bloqueado.

Actualizaciones y Limpieza

WordPress Core Actualizado

Mantén WordPress siempre en su última versión estable. Las actualizaciones de seguridad suelen ser críticas y deben aplicarse tan pronto como estén disponibles. WordPress suele actualizarse automáticamente para parches de seguridad menores.

Plugins y Temas al Día

Los plugins y temas desactualizados son una de las principales puertas de entrada para los atacantes. Revisa regularmente la sección de actualizaciones en tu escritorio de WordPress y aplica todas las disponibles.

Eliminar lo Innecesario

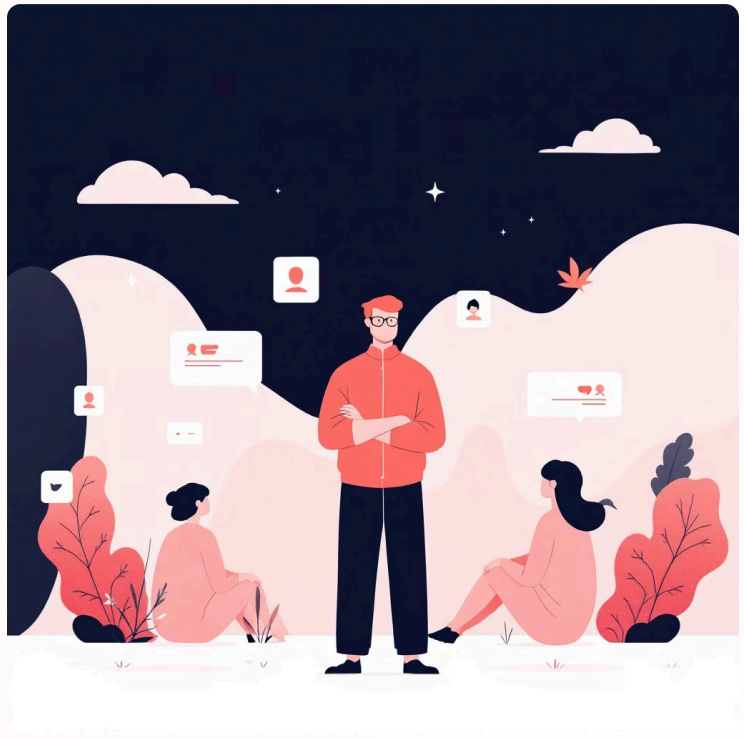
Desinstala completamente todos los plugins y temas que no estés utilizando. Un plugin inactivo puede seguir siendo vulnerable y proporcionar una vía de acceso no autorizado a tu sitio web.

🔎 **Comprueba:** No hay avisos rojos en tu Escritorio de WordPress. Una instalación segura no debería mostrar alertas de seguridad o actualizaciones pendientes.

Gestión de Usuarios y Roles

Principio del Menor Privilegio

Solo debe haber 1-2 usuarios con rol de **Administrador** real. El resto de usuarios deben tener el mínimo nivel de permisos necesario para realizar su trabajo: Editor, Autor, Colaborador o Suscriptor según corresponda.



Acciones Inmediatas:

- Revisar lista de usuarios administradores
- Eliminar cuentas de ex-colaboradores
- Verificar que no existe usuario "admin"
- Cambiar roles excesivos por otros más restrictivos

Si tienes un usuario llamado "admin", cámbialo inmediatamente. Es el primer nombre que prueban los atacantes. Usa nombres menos predecibles y siempre con contraseñas robustas.

1-2

Administradores

Número máximo recomendado para la mayoría de sitios web

30d

Revisión de Usuarios

Frecuencia recomendada para auditar cuentas activas

🔎 **Comprueba:** Ve a Usuarios → filtra por rol de Administrador. Deberías ver solo las cuentas estrictamente necesarias.

Protección del Login

La página de login de WordPress (wp-admin) es el objetivo principal de los ataques de fuerza bruta. Los atacantes utilizan bots para probar miles de combinaciones de usuario y contraseña hasta encontrar una que funcione.

Limitar Intentos de Login

Instala un plugin como "Limit Login Attempts Reloaded" que bloquee IP tras varios intentos fallidos. Configúralo para permitir máximo 3-5 intentos antes del bloqueo temporal.

CAPTCHA en el Login

Añade reCAPTCHA de Google al formulario de login para distinguir entre usuarios reales y bots automatizados. Esto reduce dramáticamente los ataques automatizados.

Desactivar Registro Público

Si no necesitas que los usuarios se registren por sí mismos, desactiva esta opción en Ajustes → Generales. Cada cuenta adicional es un riesgo potencial.

Una configuración adicional muy efectiva es cambiar la URL de login por defecto (wp-admin) por una personalizada. Plugins como "WPS Hide Login" permiten hacerlo fácilmente, ocultando completamente el formulario de login estándar.

HTTPS y Certificados SSL

Activar SSL

Configura tu hosting para que ofrezca certificado SSL automático. La mayoría incluyen Let's Encrypt gratuito.

Forzar Redirección

Configura WordPress para que todas las URLs HTTP se redirijan automáticamente a HTTPS.

Renovación Automática

Verifica que el certificado se renueva solo, sin intervención manual cada 90 días.

El HTTPS no solo protege la información que viaja entre tu sitio y los visitantes, sino que también es un factor de posicionamiento en Google. Los navegadores modernos marcan los sitios HTTP como "no seguros", lo que puede afectar la confianza de tus usuarios.

Para forzar HTTPS en WordPress, puedes añadir estas líneas en tu archivo wp-config.php:

```
define('FORCE_SSL_ADMIN', true);
define('WP_HOME','https://tudominio.com');
define('WP_SITEURL','https://tudominio.com');
```

🔎 **Comprueba:** El candado verde aparece en la barra de direcciones del navegador al visitar tu sitio. Prueba accediendo con HTTP para verificar que redirige a HTTPS.

Sistema de Backups Automatizado

La regla 3-2-1 es el estándar de la industria para backups seguros: **3 copias** de tus datos, en **2 tipos diferentes** de almacenamiento, con **1 copia off-site** (fuera de tu servidor principal).

1 Backup Diario de Base de Datos

Configura backups automáticos diarios de la base de datos, que contiene todo tu contenido, usuarios, comentarios y configuraciones. Son archivos pequeños pero críticos.

2 Backup Semanal Completo

Una vez por semana, realiza backup completo incluyendo archivos, themes, plugins y uploads. Estos archivos cambian menos frecuentemente.

3 Almacenamiento Off-Site

Envía automáticamente las copias a Google Drive, Dropbox, Amazon S3 o Backblaze. Si tu servidor falla, tendrás acceso a tus datos.

4 Retención y Limpieza

Mantén backups de 14-30 días y elimina automáticamente los más antiguos para optimizar el espacio de almacenamiento.

Plugins recomendados para esto incluyen UpdraftPlus, BackWPup o Jetpack Backup. Muchos hostings también ofrecen sistemas de backup integrados que puedes configurar desde el panel de control.

Monitorización y Siguientes Pasos

Firewall y Protección WAF

Activa el Web Application Firewall (WAF) de tu CDN o hosting. Cloudflare, por ejemplo, ofrece reglas básicas gratuitas que bloquean automáticamente muchos tipos de ataques comunes.

Permisos de Archivos

Configura los permisos correctos: archivos en 644 y directorios en 755. Añade `define('DISALLOW_FILE_EDIT', true);` en wp-config.php para desactivar el editor de archivos desde WordPress.

Alertas y Monitorización

Configura notificaciones por email para:

- Logins de administrador
- Cambios en usuarios
- Actualizaciones de plugins
- Intentos de login fallidos

Programa escaneos semanales o mensuales de malware e integridad de archivos usando plugins como Wordfence o Sucuri.

01

Hoy: Puntos 1-5

Backup, 2FA, actualizaciones, usuarios y protección de login. Son las medidas más críticas e inmediatas.

02

Esta Semana: Puntos 6-10

HTTPS, backups automáticos, WAF, permisos y monitorización. Completan tu estrategia de seguridad básica.

03

Cada Mes: Mantenimiento

Test de restauración de backup, revisión de usuarios activos y repaso general de la configuración de seguridad.

> 📝 **Tip final:** Documenta todos los cambios realizados y guarda evidencias (capturas, logs) en tu Drive o Notion. Un registro de cambios te ayudará en futuras auditorías y resolución de problemas.

Recuerda que esta checklist cubre la seguridad básica-intermedia. Para sitios web críticos o con alto tráfico, considera realizar una auditoría de seguridad profesional completa.