Checklist: Seguridad y Backups WordPress

Una guía práctica en 3 pasos esenciales: autenticación de doble factor, actualizaciones seguras y backups 3-2-1. Diseñada para administradores WordPress con conocimientos básicos-medios que buscan proteger sus sitios web de forma eficiente.

Tiempo total: **≈15 minutos** | Nivel: **Básico-medio** | Por Fabini (@ilfabini)

Antes de empezar: Lo que necesitas saber

Requisitos técnicos

- Acceso administrador a WordPress
- Acceso al panel del hosting
- App de autenticación móvil
- Correo electrónico operativo

Duración estimada

≈15 minutos totales

Puedes completar cada paso por separado según tu disponibilidad. No es necesario hacerlo todo de una vez.

Objetivo principal

Reducir los riesgos de seguridad más comunes y garantizar que tengas una copia de seguridad restaurable de tu sitio web.

Esta guía no sustituye el servicio profesional de ciberseguridad.

Paso 1: Activar autenticación de doble factor (2FA)

La autenticación de doble factor añade una capa extra de seguridad a tu WordPress. Es el primer escudo contra accesos no autorizados.

1 Instalar plugin 2FA

Busca e instala un plugin TOTP compatible con apps como Google Authenticator o Authy.

2 Configurar tu usuario admin

Escanea el código QR con tu app de autenticación y guarda la clave de respaldo.

3 Guardar códigos de recuperación

Almacénalos en un lugar seguro, **fuera del servidor**.

4 Activar para roles críticos

Exige 2FA a perfiles Administrador y Editor con una política clara.

5 Probar el sistema

Cierra sesión e inicia sesión usando el 2FA para verificar que funciona correctamente.

Consejo clave: "La contraseña protege la puerta; el 2FA cierra el cerrojo."

Paso 2: Actualizaciones seguras del sistema

Las actualizaciones parchan vulnerabilidades conocidas. Actualizar pronto evita agujeros de seguridad que los atacantes pueden explotar.

01

Hacer copia previa

Siempre realiza un backup completo (base de datos + archivos) antes de cualquier actualización importante.

02

Actualizar WordPress core

Instala la versión estable más reciente del núcleo de WordPress desde el panel de administración.

03

Actualizar plugins y temas

Revisa y actualiza todos los plugins activos. **Elimina los plugins y temas inactivos** para reducir superficie de ataque.

04

Configurar auto-updates

Activa las actualizaciones automáticas para plugins esenciales y actualizaciones menores de core, si tu hosting lo recomienda.

05

Verificar funcionamiento

Revisa que la web funciona correctamente: página de inicio, login y páginas clave del sitio.

Paso 3: Sistema de backups 3-2-1

3	2	1
Copias	Medios diferentes	Copia off-site
Mantén siempre **3 copias** de tus datos importantes	Usa **2 tipos de almacenamiento** distintos (servidor + externo)	Al menos **1 copia fuera** del hosting principal

Configuración recomendada

- **Backup diario** de base de datos
- **Backup semanal** de archivos completos
- Envío automático a almacenamiento externo
- Retención de 14-30 días según actividad
- Cifrado de backups cuando sea posible

Importante: Documenta dónde están las copias y quién tiene acceso. Una copia no probada no es una copia real.

Test de restauración: Verificar que funciona

Probar la restauración es tan importante como hacer el backup. Este paso opcional te ahorrará problemas cuando realmente lo necesites.

1

Crear entorno de prueba

Utiliza el staging de tu hosting o monta un entorno local para las pruebas de restauración.

2

Restaurar parcialmente

Prueba restaurando solo la base de datos o una carpeta específica como /uploads para verificar el proceso.

3

Verificar funcionamiento

Comprueba que el contenido restaurado se carga correctamente y se visualiza como esperas.

4

Documentar resultados

Registra cualquier incidencia encontrada y el tiempo que tardaste en completar la restauración.

Regla de oro: Practicar la restauración hoy te ahorra pánico y tiempo perdido cuando surja una emergencia real.

Errores comunes y cómo evitarlos

No guardar códigos 2FA

Problema: Perder acceso al móvil significa perder acceso a WordPress.

Solución: Guardar códigos de recuperación en gestor de contraseñas seguro o imprimirlos y archivarlos.

Actualizar sin copia previa

Problema: Una actualización puede romper el sitio sin posibilidad de vuelta atrás rápida.

Solución: Automatizar backup completo antes de cualquier actualización importante.

Acumular plugins inactivos

Problema: Los plugins desactivados siguen siendo vulnerables y ocupan espacio.

Solución: Borrar completamente plugins y temas que no uses. Menos superficie de ataque.

Una sola copia en el servidor

Problema: Si falla el hosting, pierdes tanto el sitio como el backup.

Solución: Configurar envío automático off-site a S3, Google Drive o similar.

Nunca probar la restauración

Problema: Descubrir que el backup no funciona cuando ya es demasiado tarde.

Solución: Test en staging cada 1-3 meses para verificar integridad.

Registro de control de cambios

Mantener un registro simple te ayudará a rastrear las acciones realizadas y identificar cuándo fue la última vez que verificaste cada elemento de seguridad.

Fecha	Acción realizada	Responsable	Resultado	Ubicación backup
__/__/____	2FA activado admin	_____	OK / Pendiente	Gestor contraseñas
__/__/____	Updates core/plugins	_____	OK / Incidencia	Backup pre-update
__/__/____	Backup completo	_____	OK / Error	S3/Drive/Otros
__/__/____	Test restauración	_____	OK / Incidencia	Staging

Consejo: Mantén este registro en Notion, Google Docs o tu herramienta de documentación preferida, con enlaces a las evidencias relevantes.

Resumen y próximos pasos

Lo que has conseguido

Al completar esta checklist, has implementado las tres capas fundamentales de protección para tu WordPress:

🔐 2FA Implementado

Autenticación de doble factor activa para roles críticos, con códigos de recuperación guardados de forma segura.

🔄 Updates Automatizados

Rutina de actualizaciones seguras con backup previo y verificación posterior del funcionamiento.

💾 Backups 3-2-1

Sistema robusto de copias de seguridad automatizadas con almacenamiento off-site y pruebas de restauración.

Rutina de mantenimiento

- **Semanal:** Verificar actualizaciones pendientes
- **Mensual:** Revisar logs de backup y acceso
- **Trimestral:** Test de restauración en staging
- **Anual:** Auditoría completa de seguridad

¡Enhorabuena! Has dado pasos importantes para proteger tu sitio WordPress. La seguridad es un proceso continuo, no un destino.

Créditos y recursos adicionales

Esta checklist ha sido desarrollada por **Fabini (@ilfabini)** como recurso gratuito para la comunidad WordPress. Puedes compartirla libremente con atribución.

Condiciones de uso

- ✅ Uso personal gratuito
- ✅ Compartible con atribución
- ❌ No modificar para venta comercial
- ⚖️ No sustituye asesoría profesional de ciberseguridad

Síguenos para más recursos

🌐 Descarga más guías en **[tu-dominio]/recursos**

📱 Si te ha servido, compártelo y etiqueta **@ilfabini**

💬 Dudas y sugerencias siempre bienvenidas

Versión: 2025 v1.0

Licencia: Creative Commons con atribución

Soporte: Comunidad WordPress